

Volume 12 Issue 10

October 2021



ISSN 2156-5570(Online)

ISSN 2158-107X(Print)

# Editorial Preface

## *From the Desk of Managing Editor...*

It may be difficult to imagine that almost half a century ago we used computers far less sophisticated than current home desktop computers to put a man on the moon. In that 50 year span, the field of computer science has exploded.

Computer science has opened new avenues for thought and experimentation. What began as a way to simplify the calculation process has given birth to technology once only imagined by the human mind. The ability to communicate and share ideas even though collaborators are half a world away and exploration of not just the stars above but the internal workings of the human genome are some of the ways that this field has moved at an exponential pace.

At the International Journal of Advanced Computer Science and Applications it is our mission to provide an outlet for quality research. We want to promote universal access and opportunities for the international scientific community to share and disseminate scientific and technical information.

We believe in spreading knowledge of computer science and its applications to all classes of audiences. That is why we deliver up-to-date, authoritative coverage and offer open access of all our articles. Our archives have served as a place to provoke philosophical, theoretical, and empirical ideas from some of the finest minds in the field.

We utilize the talents and experience of editor and reviewers working at Universities and Institutions from around the world. We would like to express our gratitude to all authors, whose research results have been published in our journal, as well as our referees for their in-depth evaluations. Our high standards are maintained through a double blind review process.

We hope that this edition of IJACSA inspires and entices you to submit your own contributions in upcoming issues. Thank you for sharing wisdom.

**Thank you for Sharing Wisdom!**

**Kohei Arai**  
**Editor-in-Chief**  
**IJACSA**  
**Volume 12 Issue 10 October 2021**  
**ISSN 2156-5570 (Online)**  
**ISSN 2158-107X (Print)**

# Editorial Board

## Editor-in-Chief

**Dr. Kohei Arai - Saga University**

*Domains of Research: Technology Trends, Computer Vision, Decision Making, Information Retrieval, Networking, Simulation*

---

## Associate Editors

**Alaa Sheta**

**Southern Connecticut State University**

*Domain of Research: Artificial Neural Networks, Computer Vision, Image Processing, Neural Networks, Neuro-Fuzzy Systems*

**Domenico Ciuonzo**

**University of Naples, Federico II, Italy**

*Domain of Research: Artificial Intelligence, Communication, Security, Big Data, Cloud Computing, Computer Networks, Internet of Things*

**Doroła Kaminska**

**Lodz University of Technology**

*Domain of Research: Artificial Intelligence, Virtual Reality*

**Elena Scutelnicu**

**"Dunarea de Jos" University of Galati**

*Domain of Research: e-Learning, e-Learning Tools, Simulation*

**In Soo Lee**

**Kyungpook National University**

*Domain of Research: Intelligent Systems, Artificial Neural Networks, Computational Intelligence, Neural Networks, Perception and Learning*

**Krassen Stefanov**

**Professor at Sofia University St. Kliment Ohridski**

*Domain of Research: e-Learning, Agents and Multi-agent Systems, Artificial Intelligence, e-Learning Tools, Educational Systems Design*

**Renato De Leone**

**Università di Camerino**

*Domain of Research: Mathematical Programming, Large-Scale Parallel Optimization, Transportation problems, Classification problems, Linear and Integer Programming*

**Xiao-Zhi Gao**

**University of Eastern Finland**

*Domain of Research: Artificial Intelligence, Genetic Algorithms*

# CONTENTS

Paper 1: An Effective Design of Model for Information Security Requirement Assessment

*Authors: Shailaja Salagrama*

PAGE 1 – 5

Paper 2: UAV Aided Data Collection for Wildlife Monitoring using Cache-enabled Mobile Ad-hoc Wireless Sensor Nodes

*Authors: Umair B. Chaudhry, Chris I. Phillips*

PAGE 6 – 17

Paper 3: Collaborative Recommendation based on Implication Field

*Authors: Hoang Tan Nguyen, Lan Phuong Phan, Hung Huu Huynh, Hiep Xuan Huynh*

PAGE 18 – 28

Paper 4: Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats

*Authors: Asma A. Alhashmi, Abdulbasit Darem, Jemal H. Abawajy*

PAGE 29 – 35

Paper 5: Visual Selective Attention System to Intervene User Attention in Sharing COVID-19 Misinformation

*Authors: Zaid Amin, Nazlena Mohamad Ali, Alan F. Smeaton*

PAGE 36 – 41

Paper 6: Head Position and Pose Model and Method for Head Pose Angle Estimation based on Convolution Neural Network

*Authors: Kohei Arai, Akifumi Yamashita, Hiroshi Okumura*

PAGE 42 – 49

Paper 7: Introduction to NFTs: The Future of Digital Collectibles

*Authors: Muddasar Ali, Sikha Bagui*

PAGE 50 – 56

Paper 8: Hybrid e-Government Framework based on Datawarehousing and MAS for Data Interoperability

*Authors: Barakat Oumkalfoum, El beqqali Omar, Ouksel Aris, Chakir Loqman*

PAGE 57 – 64

Paper 9: Analyzing User Involvement Practice: A Case Study

*Authors: Asaad Alzayed, Abdulwahed Khalfan*

PAGE 65 – 72

Paper 10: Predictive Scaling for Elastic Compute Resources on Public Cloud Utilizing Deep Learning based Long Short-term Memory

*Authors: Bharanidharan. G, S. Jayalakshmi*

PAGE 73 – 81

Paper 11: Highly Efficient Parts of Speech Tagging in Low Resource Languages with Improved Hidden Markov Model and Deep Learning

*Authors: Diganta Baishya, Rupam Baruah*

PAGE 82 – 94

Paper 12: Critical Success Factors Associated to Tourism e-Commerce: Study of Peruvian Tourism Operators

*Authors: Sussy Bayona-Oré, Romy Estrada*

**PAGE 95 – 104**

Paper 13: A Survey on Computer Vision Architectures for Large Scale Image Classification using Deep Learning

*Authors: D. Dakshayani Himabindu, S. Praveen Kumar*

**PAGE 105 – 120**

Paper 14: University Course Timetabling Model in Joint Courses Program to Minimize the Number of Unserved Requests

*Authors: Purba Daru Kusuma, Abduh Sayid Albana*

**PAGE 121 – 127**

Paper 15: Symbolic Representation-based Melody Extraction using Multiclass Classification for Traditional Javanese Compositions

*Authors: Arry Maulana Syarif, Azhari Azhari, Suprpto Suprpto, Khafiizh Hastuti*

**PAGE 128 – 137**

Paper 16: LightGBM-based Ransomware Detection using API Call Sequences

*Authors: Duc Thang Nguyen, Soojin Lee*

**PAGE 138 – 146**

Paper 17: Integrated Document-based Electronic Health Records Persistence Framework

*Authors: Aya Gamal, Sherif Barakat, Amira Rezk*

**PAGE 147 – 155**

Paper 18: Cyber Threat Intelligence in Risk Management

*Authors: Amira M. Aljuhami, Doaa M. Bamasoud*

**PAGE 156 – 164**

Paper 19: Expert's Usability Evaluation of the Pelvic Floor Muscle Training mHealth App for Pregnant Women

*Authors: Aida Jaffar, Sherina Mohd Sidik, Novia Admodisastro, Evi Indriasari Mansor, Lau Chia Fong*

**PAGE 165 – 173**

Paper 20: Aligning Software System Level with Business Process Level through Model-Driven Architecture

*Authors: Maryam Habba, Samia Benabdellah Chaouni, Mounia Fredj*

**PAGE 174 – 183**

Paper 21: A Review of Modern DNA-based Steganography Approaches

*Authors: Omar Haitham Alhabeeb, Fariza Fauzi, Rossilawati Sulaiman*

**PAGE 184 – 196**

Paper 22: Adaptive Logarithmic-Power Algorithm for Preserving the Brightness in Contrast Distorted Images

*Authors: Navleen S Rekhi, Jagroop S Sidhu*

**PAGE 197 – 205**

Paper 23: A Meta-analytic Review of Intelligent Intrusion Detection Techniques in Cloud Computing Environment

*Authors: Meghana G Raj, Santosh Kumar Pani*

**PAGE 206 – 217**

**Paper 24: Machine Learning Mini Batch K-means and Business Intelligence Utilization for Credit Card Customer Segmentation**

*Authors: Firman Pradana Rachman, Handri Santoso, Arko Djajadi*

**PAGE 218 – 227**

**Paper 25: Intrusion Detection System for Energy Efficient Cluster based Vehicular Adhoc Networks**

*Authors: M V B Murali Krishna M, C. Anbu Ananth, N. Krishna Raj*

**PAGE 228 – 235**

**Paper 26: Chest Diseases Prediction from X-ray Images using CNN Models: A Study**

*Authors: Latheesh Mangeri, Gnana Prakasi O S, Neeraj Puppala, Kanmani P*

**PAGE 236 – 243**

**Paper 27: Detection of Acute Myeloid Leukemia based on White Blood Cell Morphological Imaging using Naïve Bayesian Algorithm**

*Authors: Esti Suryani, Wiharto, Adi Prasetya Putra, Wisnu Widiarto*

**PAGE 244 – 251**

**Paper 28: Automatic Essay Scoring: A Review on the Feature Analysis Techniques**

*Authors: Ridha Hussein Chassab, Lailatul Qadri Zakaria, Sabrina Tiun*

**PAGE 252 – 264**

**Paper 29: Forensic Analysis on False Data Injection Attack on IoT Environment**

*Authors: Saiful Amin Sharul Nizam, Zul-Azri Ibrahim, Fiza Abdul Rahim, Hafizuddin Shahril Fadzil, Haris Iskandar Mohd Abdullah, Muhammad Zulhusni Mustaffa*

**PAGE 265 – 271**

**Paper 30: Design of Decentralized Application for Telemedicine Image Record System with Smart Contract on Ethereum**

*Authors: Darrell Yonathan, Diyanatul Husna, Fransiskus Astha Ekadiyanto, I Ketut Eddy Purnama, Afif Nurul Hidayati, Mauridhi Hery Purnomo, Supeno Mardi Susiki Nugroho, Reza Fuad Rachmadi, Ingrid Nurtanio, Anak Agung Putri Ratna*

**PAGE 272 – 281**

**Paper 31: Multi-lane LBP-Gabor Capsule Network with K-means Routing for Medical Image Analysis**

*Authors: Patrick Kwabena Mensah, Anokye Acheampong Amponsah, Kwame Baffour Agyemang, Gabriel Kofi Armah, Mighty Abra Ayidzoe, Faiza Umar Bawah, Adebayor Felix Adekoya, Benjamin Asubam Weyori, Mark Amo-Boateng*

**PAGE 282 – 294**

**Paper 32: Healthcare Misinformation Detection and Fact-Checking: A Novel Approach**

*Authors: Yashoda Barve, Jafinderkumar R. Saini*

**PAGE 295 – 303**

**Paper 33: Evaluating Deep and Statistical Machine Learning Models in the Classification of Breast Cancer from Digital Mammograms**

*Authors: Amel A. Alhussan, Nagwan M. Abdel Samee, Vidan F. Ghoneim, Yasser M. Kadah*

**PAGE 304 – 313**

**Paper 34: Arabic Document Classification by Deep Learning**

*Authors: Taghreed Alghamdi, Samia Snoussi, Lobna Hsairi*

**PAGE 314 – 321**

**Paper 35: Comparative Analysis of Data Mining Algorithms for Cancer Gene Expression Data**

*Authors: Preeti Thareja, Rajender Singh Chhillar*

**PAGE 322 – 328**

**Paper 36: Proactive Virtual Machine Scheduling to Optimize the Energy Consumption of Computational Cloud**

*Authors: Shailesh Saxena, Mohammad Zubair Khan, Ravendra Singh, Abdulfattah Noorwali*

**PAGE 329 – 338**

**Paper 37: Expert Review on Mobile Augmented Reality Applications for Language Learning**

*Authors: Nur Asyiah Suwadi, Nazatul Aini Abd Majid, Meng Chun Lam, Nor Hashimah Jalaluddin, Junaini Kasdan, Aznur Aisyah Abdullah, Afifuddin Husairi Hussain, Azlan Ahmad, Daing Zairi Ma'arof*

**PAGE 339 – 347**

**Paper 38: Arabic Semantic Similarity Approach for Farmers' Complaints**

*Authors: Rehab Ahmed Farouk, Mohammed H. Khafagy, Mostafa Ali, Kamran Munir, Rasha M.Badry*

**PAGE 348 – 358**

**Paper 39: An NB-ANN based Fusion Approach for Disease Genes Prediction and LFKH-ANFIS Classifier for Eye Diseases Identification**

*Authors: Samar Jyoti Saikia, S. R. Nirmala*

**PAGE 359 – 367**

**Paper 40: Load Balanced and Energy Aware Cloud Resource Scheduling Design for Executing Data-intensive Application in SDVC**

*Authors: Shalini. S, Annapurna P Patil*

**PAGE 368 – 374**

**Paper 41: Design and Implementation of Collaborative Management System for Effective Learning**

*Authors: Tochukwu A. Ikwunne, Wilfred Adigwe, Christopher C. Nnamene, Noah Oghenefego Ogwara, Henry A. Okemiri, Chinedu E. Emenike*

**PAGE 375 – 382**

**Paper 42: Selection of Learning Apps to Promote Critical Thinking in Programming Students using Fuzzy TOPSIS**

*Authors: Kesarie Singh, Nalindren Naicker, Mogiveny Rajkoomar*

**PAGE 383 – 392**

**Paper 43: Complex Plane based Realistic Sound Generation for Free Movement in Virtual Reality**

*Authors: Kwangki Kim*

**PAGE 393 – 400**

**Paper 44: Reverse Vending Machine Item Verification Module using Classification and Detection Model of CNN**

*Authors: Razali Tomari, Nur Syahirah Razali, Nurul Farhana Santosa, Aeslina Abdul Kadir, Mohd Fahrul Hassan*

**PAGE 401 – 407**

**Paper 45: How to Analyze Air Quality During the COVID-19 Pandemic? An Answer using Grey Systems**

*Authors: Alexi Delgado, Denilson Pongo, Katherine Felipa, Kiara Saavedra, Lorena Torres, Lourdes Serpa, Ch. Carbajal*

**PAGE 408 – 414**

**Paper 46: Indonesia Sign Language Recognition using Convolutional Neural Network**

*Authors: Suci Dwijayanti, Hermawati, Sahirah Inas Taqiyyah, Hera Hikmarika, Bhakti Yudho Suprpto*

**PAGE 415 – 422**

**Paper 47: Increasing Randomization of Ciphertext in DNA Cryptography**

*Authors: Maria Imdad, Sofia Najwa Ramli, Hairulnizam Mahdin*

**PAGE 423 – 429**

**Paper 48: Multistage Sentiment Classification Model using Malaysia Political Ontology**

*Authors: Nur Farhana Ismail, Nur Atiqah Sia Abdullah, Zainura Idrus*

**PAGE 430 – 436**

**Paper 49: Factors Impacting Users' Compliance with Information Security Policies: An Empirical Study**

*Authors: Latifa Alzahrani*

**PAGE 437 – 447**

**Paper 50: The Application of Image Processing in Liver Cancer Detection**

*Authors: Meenu Sharma, Rafat Parveen*

**PAGE 448 – 457**

**Paper 51: Automating Time Series Forecasting on Crime Data using RNN-LSTM**

*Authors: J Vimala Devi, K S Kavitha*

**PAGE 458 – 463**

**Paper 52: Level Transducer Circuit Implemented by Ultrasonic Sensor and Controlled with Arduino Nano for its Application in a Water Tank of a Fire System**

*Authors: Omar Chamorro-Atalaya, Dora Arce-Santillan, Guillermo Morales-Romero, Adrián Quispe-Andía, Nicéforo Trinidad-Loli, Elizabeth Auqui-Ramos, César León-Velarde, Edith Gutiérrez-Zubieta*

**PAGE 464 – 471**

**Paper 53: Improvement of Deep Learning-based Human Detection using Dynamic Thresholding for Intelligent Surveillance System**

*Authors: Wahyono, Moh. Edi Wibowo, Ahmad Ashari, Muhammad Pajar Kharisma Putra*

**PAGE 472 – 477**

**Paper 54: Forecast Breast Cancer Cells from Microscopic Biopsy Images using Big Transfer (BiT): A Deep Learning Approach**

*Authors: Md. Ashiqul Islam, Dhonita Tripura, Mithun Dutta, Md. Nymur Rahman Shuvo, Wasik Ahmmed Fahim, Puza Rani Sarkar, Tania Khatun*

**PAGE 478 – 486**

**Paper 55: Mobile Application with Augmented Reality to Improve Learning in Science and Technology**

*Authors: Miriam Gamboa-Ramos, Ricardo Gómez-Noa, Orlando Iparraguirre-Villanueva, Michael Cabanillas-Carbonell, José Luis Herrera Salazar*

**PAGE 487 – 492**

**Paper 56: Learning Pick to Place Objects using Self-supervised Learning with Minimal Training Resources**

*Authors: Marwan Qaid Mohammed, Lee Chung Kwek, Shing Chyi Chua*

**PAGE 493 – 499**

**Paper 57: Time Line Correlative Spectral Processing for Stratification of Blood Pressure using Adaptive Signal Conditioning**

*Authors: Santosh Shinde, Pothuraju RajaRajeswari*

**PAGE 500 – 507**

**Paper 58: SMAD: Text Classification of Arabic Social Media Dataset for News Sources**

*Authors: Amira M. Gaber, Mohamed Nour El-din, Hanan Moussa*

**PAGE 508 – 516**

**Paper 59: P Systems Implementation: A Model of Computing for Biological Mitochondrial Rules using Object Oriented Programming**

*Authors: Mohammed M. Nasef, Bishoy El-Aarag, Amal Hashim, Passent M. El Kafrawy*

**PAGE 517 – 531**

**Paper 60: Skin Lesions Classification and Segmentation: A Review**

*Authors: Marzuraikah Mohd Stofa, Mohd Asyraf Zulkifley, Muhammad Ammirul Atiqi Mohd Zainuri*

**PAGE 532 – 541**

**Paper 61: The Development of Borneo Wildlife Game Platform**

*Authors: Ramadiani Ramadiani, Erdinal Respatti, Gubta Mahendra Putra, Muhammad Labib Jundillah, Tamrin Rahman, Muhammad Dahlan Balfas, Arda Yunianta, Hasan Jamal Alyamani*

**PAGE 542 – 552**

**Paper 62: Design of a Novel Architecture for Cost-Effective Cloud-based Content Delivery Network**

*Authors: Suman Jayakumar, Prakash S, C. B Akki*

**PAGE 553 – 564**

**Paper 63: Intelligent Locking System using Deep Learning for Autonomous Vehicle in Internet of Things**

*Authors: S. Zaleha. H, Nora Ithnin, Nur Haliza Abdul Wahab, Noorhazirah Sunar*

**PAGE 565 – 578**

**Paper 64: A Case Study on Social Media Analytics for Malaysia Budget**

*Authors: Ahmad Taufiq Mohamad, Nur Atiqah Sia Abdullah*

**PAGE 579 – 585**

**Paper 65: A Pattern Language for Class Responsibility Assignment for Business Applications**

*Authors: Soojin Park*

**PAGE 586 – 601**

**Paper 66: Implementing Flipped Classroom Strategy in Learning Programming**

*Authors: Rosnizam Eusoff, Syahanim Mohd Salleh, Abdullah Mohd Zin*

**PAGE 602 – 607**

**Paper 67: High Density Impulse Noise Removal from Color Images by K-means Clustering based Detection and Least Manhattan Distance-oriented Removal Approach**

*Authors: Aritra Bandyopadhyay, Kaustuv Deb, Aтанu Das, Rajib Bag*

**PAGE 608 – 614**

**Paper 68: MultiStage Authentication to Enhance Security of Virtual Machines in Cloud Environment**

*Authors: Anitha HM, P Jayarekha*

**PAGE 615 – 623**

**Paper 69: Computer Vision based Polyethylene Terephthalate (PET) Sorting for Waste Recycling**

*Authors: Ouiem Bchir, Shahad Alghannam, Norah Alsadhan, Raghad Alsumairy, Reema Albelahid, Monairh Almotlaq*

**PAGE 624 – 633**

**Paper 70: A New Approach for Training Cobots from Small Amount of Data in Industry 5.0**

*Authors: Khalid Jabrane, Mohammed Bousmah*

**PAGE 634 – 646**

**Paper 71: Evaluation of using Parametric and Non-parametric Machine Learning Algorithms for Covid-19 Forecasting**

*Authors: Ghada E. Atteia, Hanan A. Mengash, Nagwan Abdel Samee*

**PAGE 647 – 657**

**Paper 72: Comparison of Machine Learning Algorithms for Sentiment Classification on Fake News Detection**

*Authors: Yuzi Mahmud, Noor Sakinah Shaeali, Sofianita Mutalib*

**PAGE 658 – 665**

**Paper 73: Performance Analysis of IoT-based Healthcare Heterogeneous Delay-sensitive Multi-Server Priority Queuing System**

*Authors: Barbara Kabwiga Asingwire, Alexander Ngenzi, Louis Sibomana, Charles Kabiri*

**PAGE 666 – 673**

**Paper 74: A Survey on Sentiment Analysis Approaches in e-Commerce**

*Authors: Thilageswari a/p Sinnasamy, Nilam Nur Amir Sjaif*

**PAGE 674 – 679**

**Paper 75: Assessment Framework for Defining the Maturity of Information Technology within Enterprise Risk Management (ERM)**

*Authors: Rokhman Fauzi, Muharman Lubis*

**PAGE 680 – 689**

**Paper 76: Using Eye Tracking Approach in Analyzing Social Network Site Area of Interest for Consumers' Decision Making in Social Commerce**

*Authors: Suaini Binti Sura, Nona M. Nistah, Sungwon Lee, Daimler Benz Alebaba*

**PAGE 690 – 697**

**Paper 77: Chatbot Design for a Healthy Life to Celiac Patients: A Study According to a New Behavior Change Model**

*Authors: Eythar Alghamdi, Reem Alnanih*

**PAGE 698 – 707**

**Paper 78: Design of Optimal Control of DFIG-based Wind Turbine System through Linear Quadratic Regulator**

*Authors: Ines Zgarni, Lilia ElAmraoui*

**PAGE 708 – 716**

**Paper 79: Mask RCNN with RESNET50 for Dental Filling Detection**

*Authors: S Aparna, Kireet Muppavaram, Chaitanya C V Ramayanam, K Satya Sai Ramani*

**PAGE 717 – 724**

**Paper 80: Performance Analysis of Qualitative Evaluation Model for Software Reuse with AspectJ using AHP**

*Authors: Ravi Kumar, Dalip*

**PAGE 725 – 733**

**Paper 81: Analysis of the Asynchronous Motor Controlled by Frequency Inverter Applied to Fatigue Test System**

*Authors: Nel Yuri Huaita Ccallo, Omar Chamorro-Atalaya*

**PAGE 734 – 742**

**Paper 82: Heuristic Algorithm for Automatic Extraction Relational Data from Spreadsheet Hierarchical Tables**

*Authors: Arwa Awad, Rania Elgohary, Ibrahim Moawad, Mohamed Roushdy*

**PAGE 743 – 748**

**Paper 83: Effective Controlling Scheme to Mitigate Flood Attack in Delay Tolerant Network**

*Authors: Hanane ZEKKORI, Saïd AGOUJIL, Youssef QARAAI*

**PAGE 749 – 758**

**Paper 84: Efficient DNN Ensemble for Pneumonia Detection in Chest X-ray Images**

*Authors: V S Suryaa, Arockia Xavier Annie R, Aiswarya M S*

**PAGE 759 – 767**

**Paper 85: Delivery of User Intentionality between Computer and Wearable for Proximity-based Bilateral Authentication**

*Authors: Jaeseong Jo, Eun-Kyu Lee, Junghee Jo*

**PAGE 768 – 777**

**Paper 86: Digital Preoperative Planning for High Tibial Osteotomy using 2D Medical Imaging**

*Authors: Norazimah Awang, Faudzi Ahmad, Rosnita A. Rahaman, Riza Sulaiman, Azrulhizam Shapi'i, Abdul Halim Abdul Rashid*

**PAGE 778 – 783**

**Paper 87: Using Transfer Learning for Nutrient Deficiency Prediction and Classification in Tomato Plant**

*Authors: Vrunda Kusanur, Veena S Chakravarthi*

**PAGE 784 – 790**

**Paper 88: A New Protection Scheme for Biometric Templates based on Random Projection and CDMA Principle**

*Authors: Ayoub Lahmidi, Khalid Minaoui, Chouaib Moujahdi, Mohammed Rziza*

**PAGE 791 – 796**

**Paper 89: Verifiable Homomorphic Encrypted Computations for Cloud Computing**

*Authors: Ruba Awadallah, Azman Samsudin, Mishal Almazrooie*

**PAGE 797 – 808**

**Paper 90: Multi-logic Rulesets based Junction-point Movement Controller Framework for Traffic Streamlining in Smart Cities**

*Authors: Sreelatha R, Roopalakshmi R*

**PAGE 809 – 816**

**Paper 91: Employing Video-based Motion Data with Emotion Expression for Retail Product Recognition**

*Authors: Ahmad B. Alkhodre, Abdullah M. Alshanjiti*

**PAGE 817 – 825**

**Paper 92: Hybrid Model of Quantum Transfer Learning to Classify Face Images with a COVID-19 Mask**

*Authors: Christian Soto-Paredes, Jose Sulla-Torres*

**PAGE 826 – 836**

**Paper 93: Code Optimizations for Parallelization of Programs using Data Dependence Identifier**

*Authors: Kavya Alluru, Jeganathan L*

**PAGE 837 – 846**

**Paper 94: A Novel Deep Learning-based Online Proctoring System using Face Recognition, Eye Blinking, and Object Detection Techniques**

*Authors: Istiak Ahmad, Fahad AlQurashi, Ehab Abozinadah, Rashid Mehmood*

**PAGE 847 – 854**

**Paper 95: Faculty e-Learning Adoption During the COVID-19 Pandemic: A Case Study of Shaqra University**

*Authors: Asma Hassan Alshehri, Saad Ali Alahmari*

**PAGE 855 – 862**

**Paper 96: Joint Deep Clustering: Classification and Review**

*Authors: Arwa Alturki, Ouiem Bchir, Mohamed Maher Ben Ismail*

**PAGE 863 – 874**

# An Effective Design of Model for Information Security Requirement Assessment

Shailaja Salagrama

Scholar, Doctor of Philosophy, Computer Information System, University of the Cumberland's, Williamsburg, Kentucky, USA

**Abstract**—Information security is a major domain of analysis for enhancing the security of sensitive detained business organizations. These days, attackers are advancing themselves by applying highly advanced technological solutions such as artificially intelligent malicious codes, advanced phishing methods and many others to acquire sensitive and critical data from businesses. This paper presents a novel model framework to analyze the requirements of information security for a more robust information system and its assets in organizations. The framework of this model is designed in such a fashion that both new and legacy organizations can adopt it to define the requirement of security that will ensure confidentiality, integrity and availability of information systems and their components - including sensitive domain business and private data that is critical to the organization. There are two different model frameworks which are proposed here. The first one provides specifications of the security requirements and the second provides for the audit of the access logs to capture any unethical practices and violations by internal users. The proposed model for security requirements provides the roadmap to analyze and build proper security requirements to secure business sensitive data. Stepwise processes which are needed to analyze and define security requirements are the key factors of this security model, as they help in clear definitions of security frameworks and infrastructure for an organization. The Audit Model provides the framework for defining information auditing requirements, thus enabling the capture of unethical and unauthorized access to the information system components of the organization.

**Keywords**—Information security; network security; web security; confidentiality; integrity; availability; communication technology; information system; internet security; security framework introduction

## I. INTRODUCTION

Recent developments and advancements in information technology have shifted various systems onto the online platform. This new paradigm of processes and activities on the information and communication technology platform enables stakeholders to execute the required applications over the Internet so that the required services can be secured digitally without necessitating any physical movement to the service provider. Therefore, information security becomes one of the potent concerns of service providers and users. Protection of vital information such as business-related sensitive data, users' personal data, users' transaction data etc. is vital. In recent times, cybercriminals have become highly sophisticated with new-generation hacking methods and tools, making security and protection of vital information a significant challenge to business entities and users. Information security provides safeguards to systems which are typically used to process,

store, and communicate data. There are various sources of information, and these include the operating environment, management, databases, network infrastructure and the Internet. Securing all these artifacts associated with the information technology and systems is highly challenging - both directly and indirectly as they are heterogeneous in nature and in their functions. While some studies show that cryptography can provide the security to information and its related agents which are used to process, store, and transmit data, it may not be so. This is because the existing cryptographic algorithms may fail to secure the vital information once the decryption key is discovered [1]. Further, by using message analysis, the attackers can analyze the key and therefore decipher the messages that are encrypted. The numerous attacks on various cryptographic systems and their results have demonstrated that these algorithms have been breached by the attackers.

Information security has both technical and non-technical perspectives to it. Purely technical security measures are inadequate for securing information. Therefore, non-technical measures, such as social security measures should also be in place to enhance the overall security effectiveness, so that the information and information system assets can be completely secured. It is simple to design a social tool that can effectively launch a social engineering attack and secure vital information such as access identities and passwords from victims. This indicates that a purely technical security framework is not adequate for securing vital information [2][3].

Today, what we need is an adaptive security framework for securing information systems and assets. Adaptive security is considered to fall under active security measures that could secure the loopholes and vulnerabilities of the information systems and assets. The level of information security required is heavily dependent on the functional profile of the organization and the equipment and hardware used in the processing of sensitive information. Risk analysis and Vulnerability analysis are the primary processes through which security requirements are analyzed. This helps to identify, manage, and create countermeasures for securing critical information, information system assets and the components vulnerable to security threats. Adequate protection of data is very critical if the information system must generate trust among the stakeholders. A security breach may cause huge financial, trust and image losses [4]. This research article proposes the use of an Analytical Framework for Security Effectiveness that can be applied to critical business data associated with information systems.

## II. EFFECTIVE SECURITY FRAMEWORK

The analysis of various risks and vulnerabilities is performed on the information system to model the gaps in the security and privacy of sensitive and critical data. Any effective security framework should have the three basic components proposed in the Fig. 1.

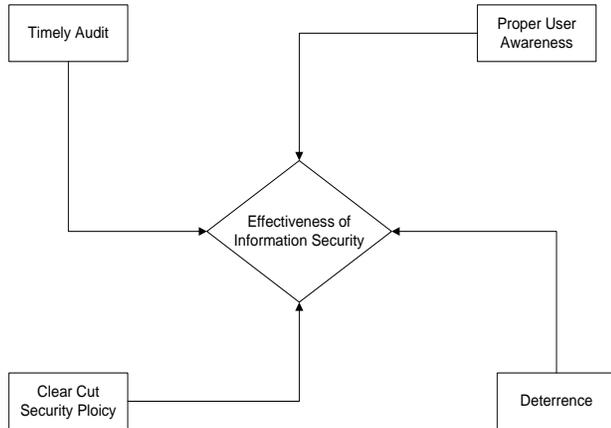


Fig. 1. Effectiveness of Information Security for any Firm, making the Information Security Effective.

To secure the vital information from misuse must be the main consideration. As shown in Fig. 1, four different aspects are mandatory for effective information security, where each one is related to the other to provide security to information [5][6].

To an individual information system firm or organization, the security policy must be very clear in concept and deployment [7]. A clear-cut security policy excludes not only the third party in practice but also direct deployment with respect to the information system assets. Deterrence always prompts the regulatory and legal aspects for the internal users not to go beyond the defined scope or violate the system to disclose sensitive information. This must be in place within the users of firm to assure robust security to the information system assets and critical information. User awareness to different categories of threats associated with social engineering attacks is mandatory and a regular process must be in place to make users aware of the latest trends and procedures of such types of attacks. Audit ensures establishing the violation parameters and depth along with the identity, so that a regular audit must be executed by using the right tools and technology to determine the violators and if necessary, to take legal actions. These four base frameworks provide effective information security to an information system.

## III. INTERNET AND SECURITY

Almost all online web application requires Internet services to be made available to the users. Internet is open to all as it is a public network in nature. Due to this fact the risks to confidentiality, integrity and availability of information are very high, with hackers constantly trying to acquire the sensitive information to gain potential benefits by disclosing and abusing the same.

## A. Security Analysis Framework

Security analysis is one of the most important processes to scope out the security requirements. Four parameters are considered to analyze the security for Internet based systems. The analysis parameters are detailed under Table I.

TABLE I. SECURITY ANALYSIS FRAMEWORK

Sl. No.	Analysis Factors & Security Breaches		
	Security Domain	Dependency Factor	Security Breaches
1	Physical Security	Medium	Theft, Loss of Data, Natural and Man-made Disasters
2	Data Security	High	Eavesdropping, Hacking, Impersonating, Malicious Activities
3	Network Security	High	Denial of Service Attack, Replay Attack, MAC Spoofing, Router Poisoning
4	Web Applications	High	Cross Site Scripting, Hijacking, Database Hacking, SQL Injection, Session High Jacking

These four security domains are mutually associated with the Internet world and analysis of security is performed with respect to the dependency factor the corresponding security breaches. The profiles of the information systems firms and organizations which deal with the business processes on Internet-based applications are detailed in Table II.

TABLE II. SECURITY DOMAIN

Sr. No	Web Applications and Security Risk Factor Level		
	Organization Type	Dependency on Web Application	Security and Risk Factor
1	Non-IT Domain	Nil	Nil
2	Mixed IT Domain	Moderate	Medium
3	Complete IT Domain	High	High
4	Third Party IT Support Domain	High	High
5	IT Cloud Support Domain	High	High

Firms are selected on the basis of the five different domains mentioned in Table I. The analysis parameters such as ‘not required’, ‘moderate’ and ‘high’ are defined with the security and risk factors. An equation is created to assess the risks and vulnerabilities to different domains of firms as defined below.

$R_i$ = Risk Factor Variable where $i = 1, 2, 3, 4$ $V_i$ = Vulnerability Variable where $I = 1, 2, 3, 4, \dots, n$ . $S_i$ = Severity Variable where $I = 1, 2, 3$ . $R_i \leftrightarrow V_i$ where value of $R = \text{Value } V$
---

$$\text{If } \sum_{i=1}^4 R \times \sum_{i=1}^n S \times \sum_{i=1}^3 V \geq 100 \quad (1)$$

- Analysis : All Four Domains of Security
- Include All Security Risks and Breaches
- Develop the Security Model for Each Risk and Breach
- Define Security Policy by Developed Security Model

$$\text{if } \sum_{i=1}^4 R \times \sum_{i=1}^n S \times \sum_{i=1}^3 V = 50 \text{ and } < 100 \quad (2)$$

- Analysis : Analyze only three domains of Security
- Include All Security Risks and Breaches
- Develop the Security Model for Each Risk and Breach
- Define Security Policy by Developed Security Model

If  $\sum_{i=1}^4 R \times \sum_{i=1}^n S \times \sum_{i=1}^3 = 25 \text{ and } < 50$  (3)

- Analysis : Analyze only two domains of Security
- Include All Security Risks and Breaches
- Develop the Security Model for Each Risk and Breach
- Define Security Policy by Developed Security Model

If  $\sum_{i=1}^4 R \times \sum_{i=1}^n S \times \sum_{i=1}^3 = 1 \text{ and } < 25$  (4)

- Analysis : Analyze only one domains of Security
- Include All Security Risks and Breaches
- Develop the Security Model for Each Risk and Breach
- Define Security Policy by Developed Security Model

**B. Analysis Functional Flow**

Analysis is the first critical process to advance the security to the information system and its Internet based applications to protect it from adversaries and security breaches. Functional Flow of Analysis is presented in Fig. 2.

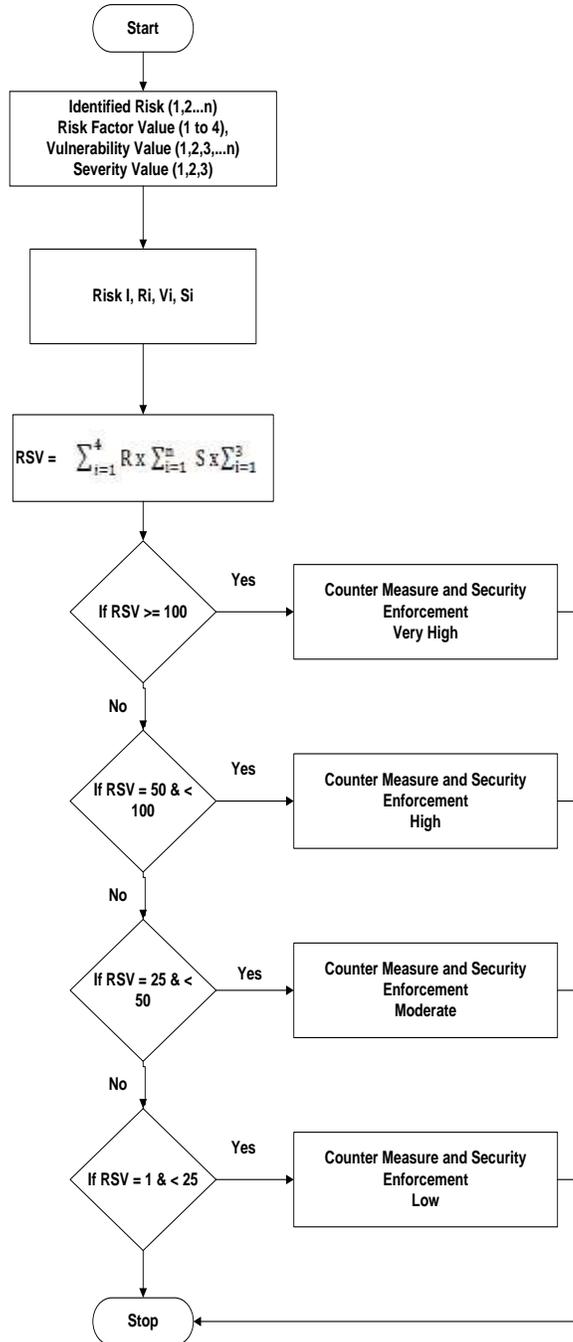


Fig. 2. Functional Flow Definition and Security Counter Measure.

#### IV. COUNTER MEASURE AND SECURITY ENFORCEMENT

Counter Measures are steps taken to secure the information system and data by preventing them from unauthorized access and disclosure, maintaining the integrity and providing the availability [8][9]. In accordance with Fig. 2 the requirement of countermeasures to secure the information system and its assets - specifically the Internet based applications and their data from security breaches - is identified by the following Table III.

In Table III, the defined equation-based countermeasure requirement specification is assessed as per the corresponding security domain. In Table IV, the security domains and counter measure tools and techniques are presented to enforce the security control.

According to Table IV, for security domain countermeasure tools and techniques that secure the information system and its assets, security from the network side can also be considered [10]. Advanced tools and technologies can also be employed to enhance the security of sensitive and vital data.

TABLE III. COUNTER MEASURE DETAILS FOR SECURITY BREACHES

Sl.No.	Security Standard and Counter Measure		
	Security Standard	Equation Map	Security Domain Counter Measure
1	Very High	1	Physical Security
			Data Security
			Network Security
			Web Application Security
2	High	2	Data Security
			Network Security
			Web Application Security
3	Moderate	3	Network Security
			Web Application Security
4	Low	4	Web Application Security

TABLE IV. SECURITY DOMAIN COUNTER MEASURE TOOLS AND TECHNIQUES

Security Domains	Tools/Technology and Techniques	
	Tools/Technologies	Techniques
Physical Security	Biometric Access, CCTV, Device Lock	Continuous Surveillance, Proper Locking Door and System Cabinets
Data Security	Storage Encryption, Storage Lock, Data Encryption	Sensitive Data backup, Backup Data Encryption, Strong Key for Encryption
Network Security	VPN, SSL, SSH, Firewall, DMZ	Proper Device Hardening, Proper Firewall Configuration
Web Application Security	Parameterized API, Input Validation, Secured Authentication, Prevent Directory Browsing, Hash and Salt Password, Role based Authentication and authorization, SSL, Proper Session Management	Validate the input of users to allow access, apply strong and robust authentication and authorization on role-based identity, use secured socket layer for all sensitive web pages, and do time out for inactive session.

#### V. SECURITY AUDIT FRAMEWORK

A parameterized security audit is important to assess all events that are being recorded with database logs and user account logs [11] [12] [13]. The parameters are defined with respect to priority. The audit parameters are derived by the given Pseudocode.

Input Security Parameter  $i = 1$  to  $n$

Priority =  $p$

Scope =  $s$

Interval =  $g$

Audit Process =  $a$

If  $p = \text{high}$  then  $\text{scope} = i \times 5$ ,  $g = 7$  and  $a = \text{Manual}$

If  $p = \text{medium}$  then  $\text{scope} = i \times 3$ ,  $g = 30$ ,  $a = \text{automated}$

If  $p = \text{low}$  then  $\text{scope} = i \times 1$ ,  $g = 90$ , and  $a = \text{Automated}$

The priority parameters with formulated Pseudocode are derived and the tentative benchmark to audit the logs related to the information system and its assets. They are presented in Table V.

TABLE V. DEFINED PARAMETRIZED SECURITY AUDIT

Role Name	Audit Parameters			
	Priority	Scope	Interval	Automated/Manual
Administrator	High	Identify all violations within the defined role	Weekly	Manual
Internal User	High	Identify all violations	Monthly	Manual
External User	Medium	Identify all accessed areas	Monthly	Automated
Others	Low	Identify as per role	Tri-Monthly	Automated

#### VI. CONCLUSION

Proposing a framework of information security is an extremely complex process. In this research, we have attempted to propose a model framework that would help analyze the security framework for a given information system and its assets; thus, enabling recommendations related to information security tools and technologies that would help in securing critical and vital data. The model framework includes two different models that provide the specifications of security such as information security requirements, tools, and technologies to apply security and security audit to capture any deviation from ethical practices by the users through access logs. The proposed models are effective in specifying the requirements and selecting the security technologies, tools and techniques that can be deployed and also for enhancing the features of security to critical system and sensitive data. The mathematical procedures ascertain the verification and assurance of the correct parameters being adopted, while analyzing the requirements of security with different security domains to secure the system and its critical assets.

#### VII. FUTURE SCOPE

The proposed Effective Design Model for Security Requirement Analysis and auditing information systems of

organizations provides an effective framework for specifying and defining the information security framework. The scope of this research can be furthered with the proposed research work to enhance the given model by adding the hazards analysis and recommendations by integrating the disaster recovery option and its various techniques. The assurance of business continuity with respect to disaster recovery requirements including all natural and other disasters related with information system can be studied along with the framework to ease the requirements-scoping and to enhance the overall security to business organizations.

#### REFERENCES

- [1] S. Kowalski, Lectures in Security management at the department of computer Sciences and Systems, University of Stockholm, 2011.
- [2] R. E. Turner, C. Edgely, & G. Olmstead, Informational control in conversations: Honesty is not always the best policy. *Kansas Journal of Sociology*, 11 (1975), pp. 69-89.
- [3] OASIS, Assertions and Protocols for the OASIS Security assertion Markup Language, 1(1).
- [4] NIST (2008). Performance measurement guide for information security. National Institute of Standards and Technology special publication 800-55.
- [5] ISO/IEC 9796-3 (2006). Information technology -- Security techniques - Digital signature schemes giving message recovery. International Organization of Standards and International Electrical Commission.
- [6] Common Criteria. (2009). Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model Retrieved June 2009, from: [www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf](http://www.commoncriteriaportal.org/files/ccfiles/CEMV3.1R3.pdf).
- [7] SOA. (2009). Service-Oriented Architecture. Retrieved September 2010, from: [http://www.soa.com/products/standards\\_support/](http://www.soa.com/products/standards_support/).
- [8] Zuccato, A. (2007). Holistic security management framework applied in electronic commerce. *Computers & Security*, 26(3), 256-265.
- [9] Anderson, R. (2001). Why Information Security is Hard, An Economic Perspective. Proceedings of the 17th Annual Computer Security Applications conference, IEEE computer society. Washington DC, USA.
- [10] N. Bar-Josef, The Structure of Cybercrime Organization- hackers has Supply Chains Too! Security Week, [www.securityweek.com](http://www.securityweek.com), 2010.
- [11] D. Dasgupta, J. Gomez, F. Gonzales, M. Kaniganti, K. Yallapu, and R. Yarramsetti, —MMDS: Multilevel Monitoring and Detection System II, Intelligent Security Systems Research Laboratory, Division of Computer Science, University of Memphis, USA.
- [12] Von Solms, S.H. (2010). The 5 waves of information security – From Kristian Beckman to the Present, Security Privacy, Silver living in the Cloud, Proceedings of the 25th IFIP TC 11 International Information Security Conference, SEC 2010, Held as Part of WCC 2010, Brisbane, Australia.
- [13] Mwakalinga, J., & Kowalski, S. (2011c). Architecture for adaptive information security systems as applied to social networks. The IEEE International conference on computer communications and networks, July 31 - August 4, 2011, Maui, Hawaii, USA.

# UAV Aided Data Collection for Wildlife Monitoring using Cache-enabled Mobile Ad-hoc Wireless Sensor Nodes

Umair B. Chaudhry, Chris I. Phillips

School of Electronic Engineering and Computer Science  
Queen Mary University of London (QMUL), London, United Kingdom

**Abstract**—Unmanned aerial vehicle (UAV) assisted data collection is not a new concept and has been used in various mobile ad hoc networks. In this paper, we propose a caching assisted scheme alternative to routing in MANETs for the purpose of wildlife monitoring. Rather than deploying a routing protocol, data is collected and transported to and from a base station using a UAV. Although some literature exists on such an approach, we propose the use of intermediate caching between the mobile nodes and compare it to a baseline scenario where no caching is used. The paper puts forward our communication design where we have simulated the movement of multiple mobile sensor nodes in a field that move according to the Levy walk model imitating wildlife animal foraging and a UAV that makes regular trips across the field to collect data from them. The unmanned aerial vehicle can collect data not only from the current node it is communicating with but also data of other nodes that this node came into contact with. Simulations show that exchanging cached data is highly advantages as the drone can indirectly communicate with many more mobile nodes.

**Keywords**—UAV; caching; sensors; MANETs; WSN; waypoint

## I. INTRODUCTION

The use of wireless sensor networks (WSNs) and mobile ad-hoc networks (MANETs) in various areas such as environmental monitoring, military, vehicular networks and animal tracking has been widely adopted [1]–[6]. Applications of such networks vary based on the targeted area. Humidity and seismic sensors, collision avoidance and parking sensors, pulse and temperature sensors are all examples of this. In WSNs, nodes are deployed with the intention of sensing and relaying information to a particular destination for evaluation purposes. In MANETs, nodes are mobile forming temporary networks throughout their runtime. Nodes in these networks are typically small and possess limited resources. They have restricted processing power and run on small batteries hence energy conservation is a serious concern for them. Data is routed from the source to the destination using routing protocols. The convergence and retransmission mechanisms of these protocols impose an additional overhead causing an additional energy drain. Many efforts have been put into making these protocols as efficient as possible [7]–[9]; however, there is always a trade-off. Conversely, we propose the use of an unmanned aerial vehicle (UAV) to periodically to collect data from caching assisted nodes, hence avoiding routing altogether.

In this paper, we focus on wildlife tracking and monitoring. Traditionally, this is achieved by strapping heavy tracking equipment to animals [10], [11]. Even with current technological trends, wildlife monitoring remains a challenging setting. Typical VHF transmitters are of very restricted range [12] and have a limited battery life and the ones that are longer in range are satellite oriented and hence require even more power, consequently providing a lower lifetime. Table I shows some of the existing devices available. Approaches such as [13], [14], [15], [16], [17] are either too expensive, require dedicated manpower, or the resource constraints of the devices can cause them to fail prematurely. Our aim is to make tracking and monitoring easier and less costly in terms of finance and operation.

Several tracking systems have already been proposed and some are even operational. ATLAS, in [16], employs 9 base stations and extensive computing to determine the location of flying animals. ARTS [14] uses VHF tags and hefty hardware and can only work on animals with small home ranges. [13], in addition to being composed of energy draining 3G modules, is highly dependent on manpower. [18] uses a three tier architecture and the authors claim energy conservation to be one of the biggest challenges of the model in addition to constraints such as the lack of physical intervention with the nodes after deployment and intermittent network connectivity. [15] uses dual chip collars and requires pre-processing at the nodes before transmission. Conversely, [19] requires image processing on static sensor nodes although the authors acknowledge that the accuracy of the system drops with time.

TABLE I. TRADITION DEVICES AND THEIR LIMITATIONS

Devices	<u>NANO</u>	<u>MICRO</u>	<u>SMALL</u>	<u>MEDIUM</u>
<b>Weight Range</b>	5g-20g	6g-50g	20g-100g	130g-250g
<b>Example Suitable Animals</b>	Birds, bats, and other tiny mammals	Lizards, tortoises, turtles, frogs, very small mammals	Animals that weight at least 500 grams	Foxes, Tasmanian Devils
<b>Data Recovery Method</b>	UHF Wireless	UHF Wireless	UHF Wireless	<u>Satellite</u>
<b>Drone Data Downloading</b>	Standard	Standard	Standard	N/A
<b>Base Station Battery Life</b>	2 days	5 days	2 days	N/A

This paper highlights a routing-less approach for data collection from mobile sensor nodes for wildlife monitoring using an unmanned aerial vehicle. In our application scenario, we assume the home range to be a large field or area where the animals roam. Our sensor nodes, according to our use-case scenario, will be wildlife and several of these will be dispersed across the home range. The nodes are considered to be mobile with some degree of purpose in their movement but at the same time having some randomness in their behaviour. An unmanned aerial vehicle will make periodic trips across the field. The nodes are equipped with sensing equipment, the type of which is not the focus of our research. The nodes upon encountering the UAV transfer their data to it. In this paper, we test this approach in two scenarios. One is without communication between the nodes and the other with caching enabled among the nodes allowing them to store data from the nodes they come into contact with. Our simulator uses the Levy walk movement model for the nodes.

## II. RELATED WORK

Retrieval of data from static and mobile sensor nodes deployed in a large field through an aerial vehicle is a fairly new concept. Lately, several researchers [24]–[36], have explored the use of a UAV to acquire data from sensor and ad-hoc nodes mainly due to the fact that a lot of energy draining forwarding and processing tasks are taken away from the resource sensitive nodes.

The authors in [20] describe their method of how a UAV can be used for wildlife monitoring and tracking. In their approach, the field is divided into virtual grids and each grid has a cluster of static sensors deployed. Each cluster has a cluster head which acts as a point of contact for the UAV to collect data. The network model is not a generic one and is highly dependent on data sets obtained from tracking equipment for specific animals. In their case, they used the movement data of zebras from ZEBRANET and the UAV visits the cluster heads of the most active grids for data collection. Another approach [21] has been to mount a cellular network base station on a UAV in an attempt to try to pick up cell phone data from users.

Another approach has been to mount a cellular network base station on a UAV in an attempt to try to pick up cell phone data from users [22]. While in communication with the nodes, the UAV allocates the whole bandwidth to the node with the least data in its buffer and moves towards it during the transfer. The drone moves with a moving node along the same trajectory and the base station may be in communication with more than one node at a time with different parameters. This requires it to adopt a consistent back and forth movement based on the attributes of the node(s) it is in communication with. Ignoring the back and forth movement, the synchronisation mechanism between the drone and a node may be considered suitable for cellular networks as the communication between the base station and the nodes may be extensive. However, the same cannot be said for mobile sensor nodes, especially when considering their limited resources.

Ariel assisted data collection using a UAV from limited capacity sensor nodes has also been considered in [25] using a Markov chain to model the movement of the UAV in addition

to modelling the irregularities in the movement due to several implicit and explicit factors. The authors in [26] also favour the same concept of acquiring data from sensor nodes deployed in a field using a UAV. They add to the approach by proposing a model that allows the sensor nodes to cooperate with each other to achieve simultaneous transfer of data to the UAV to reduce latency. In addition, their work highlights how they can reduce packet losses occurring in the backward direction while the UAV is receiving data and moving forward using an efficient forwarding scheme. However, one can argue that cooperation between the nodes is of limited use as multiple nodes can transmit to the UAV simultaneously using different channels.

Considering the low data transfer rates due to the brief contact duration of a UAV with a sensor node in UAV aided data collection, the authors in [27] propose a modified Media Access Control (MAC) protocol which uses beacon broadcast at the UAV together with Carrier Sense Multiple Access/Collision Avoidance (CSMA/CA) at the ground nodes. The nodes have to contend with each other to speak to the UAV in addition to remaining in the listening mode to receive the beacon which is a big drawback considering the limited battery life of the nodes.

Other researchers have focused on the most optimal traversal path of the UAV in reference to an age element associated with the data picked up from the sensor nodes [28]. They define the age of information as the time data is sensed by the node to the time it is delivered to the sink by the UAV hence the flight path and duration of the UAV plays an important role. Theoretically, they show that the optimal route for the UAV corresponds to a Hamiltonian path and hence they propose a trajectory planning scheme accordingly. Nevertheless, their approach promotes the use of static nodes and dynamic programming which is computational complex.

The feasibility of using a UAV for data collection from ground sensors has been tested in [29] against several parameters including weather, flight height, latency, throughput, jitters and communication channels an authors have recommended a configuration based on their observations. However, it can be argued that the values are highly subjective.

The authors in [30] propose an automatic tracking system that offers autonomous wildlife monitoring. In their approach, they suggest to equip the wildlife with a system that is a combination of a Global Positioning System (GPS) module and a wireless Subscriber Identity Module (SIM). The GPS coordinates are sent to a central server which is also equipped with a SIM which forwards the information to a SIM-equipped control system from where the received information is fed to a drone in addition to the drone control commands. The drone, using this information and the control commands, navigates to the coordinate location. The information is fed to the drone only at the take-off point. Thus, once the drone reaches the target location, the target might not be there resulting in waste of time, energy and the trip. In addition, the devices used to accomplish this have a limited lifespan which is greatly affected by the presence of two highly energy draining modules on the animals.

An approach that involves a combination of Q-learning and Neural Networks is considered in [31] to offer an energy-efficient method for portable base station positioning using UAV. The authors use the concept of landing spots from [32] to move the UAV. Once a suitable position is achieved by the UAV in terms of connectivity, the UAV uses the landing spots to save energy by landing and providing coverage rather than continuing to hover.

In addition to the concept of using a UAV for data collection from wireless sensor network nodes, researchers have proposed BEE-DRONES [23] to achieve energy efficiency at the UAV level and at the network level. The UAV, as with pollinating bees, visits specific targeted ground sensors for data collection. Their work in addition to dealing with minimal path planning of the UAV targets the synchronization issues between the ground sensors and the drone and proposes a wakeup mechanism for the nodes in accordance to the expected visit time of the drone. An efficient path planning approach is also considered in [24], focusing on the limited flight time and energy constraint of the UAV for data gathering in WSNs. They also show how a cluster-head can be selected from a cluster of sensor nodes based on node energy and value of information. This cluster head is the contact point of the UAV for data collection. However, choosing a cluster-head is still an additional burden for the nodes, and data communication between the nodes and the cluster-head employs a traditional routing mechanism incurring protocol overhead.

The researchers in [33] promote the concept of using a UAV for data collection and offer an approach to make it feasible in terms of energy efficiency and security. They propose a centralized framework which allows the UAV to carry the remaining energy of the nodes to the sink which then decides which nodes are suitable candidates for the cluster-head and which nodes should be marked as compromised and hence disqualified from the cluster-head election. Centralizing the cluster-head selection can add an additional delay to the communication and can result in unwanted exchanges between the nodes and a cluster-head now labelled as a disqualified candidate. Also, the approach can cause severe fluctuation of the cluster-head assignment if the nodes are mobile.

Despite the preceding research studies, intermediate caching between the nodes has, to our knowledge, never been considered. We believe that intermediate caching between the nodes can be advantageous for several reasons. Firstly, it does not impose additional strain on a particular node (i.e. a cluster-head). Secondly, there are no limitations on the positioning of the nodes and, finally, the UAV has more flexibility in terms of points of contact.

The next section outlines our proposed system. This is followed in Section 4 with a simulation-based evaluation where we employ a Levy movement model for the mobile nodes together with four different variations of caching. Finally we conclude the paper in Section 5.

### III. SYSTEM MODEL

We have implemented a discrete time event simulator in Java. Rather than feeding movement traces into the simulator

[20], our simulator has the ability to cope with different movement models, allowing for flexibility. However, for the sake of this paper, we only employ the Levy walk movement model. Historically, it was widely believed and accepted that animal movement could be explained by a simple random walk model; however, recent evidence has shown that the movement of different animal species are more relatable to the levy walk model [34], [35].

A Levy walk is based on the Levy foraging hypothesis that states that animals employ a Levy walk since it leads to optimal search efficiency. A Levy Walk according to Gautestad “describes a movement process with physical realism in the context of observing animal paths at fixed intervals” [36]. It is defined as a movement model where the subject continues to move in one particular direction and upon finding a resource patch, adopts random movement in and around it [37]. Fig. 1 from [38] highlights how a trace of a Levy walk may look.

Statistically, a Levy walk is a Markov based stochastic process. Rather than focusing on the biological nature of models, arguments over the past years have been restricted to statistical measures although the physicality and the movement pattern should matter more [39]. Humphries states “the real utility of the Levy research field is not, therefore, to accurately model animal movement paths, but as an exploratory tool to aid the behavioural analysis of animal movement datasets” [40]. Fig. 2 shows a typical Levy movement pattern of a node generated by our simulator.

In addition to the movement model, our model provides the opportunity for selectable caching depending on the scenario. In the case of Phase 1, we omit Intra-Node caching to provide baseline performance. In Phase 2 intra-node caching is enabled.

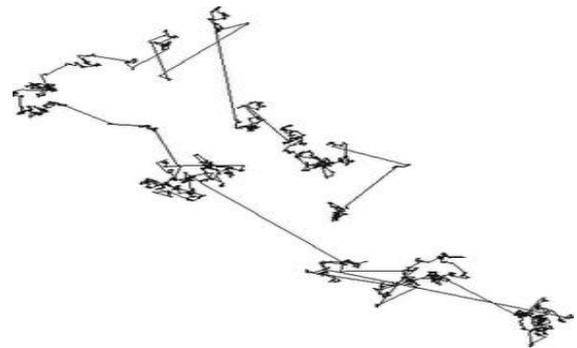


Fig. 1. Example Levy Walk [38].

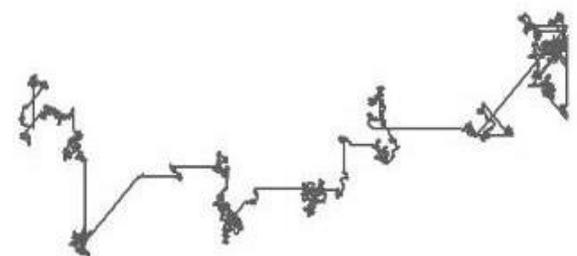


Fig. 2. Single Node Movement Trace for 12hrs at 11kph.

A. Phase 1: No Intra-Node Caching

In Phase 1, mobile nodes are dispersed in a field of size  $n \times n$ . The nodes do not have any ability to cache data received from other nodes. In fact, the nodes do not even communicate with each other. Each node gathers/senses data from the host animal while the animal moves around. A UAV is to be sent out periodically from a gateway/base station and the UAV follows a fixed path based on waypoints [41], [42] which have been selected in such a way that the UAV can cover the majority of the field during its trip. In other words, the trajectory of the UAV is fixed, and the UAV moves from waypoint to waypoint as shown in Fig. 3.

Our model considers two versions of this approach. In the first (termed ‘WP’), the UAV only captures the data cached at the designated waypoints and does not pick it up directly from the mobile nodes. These waypoints are equipped with caches and can cache data from the mobile nodes they have encountered. The UAV simply collects the data from the waypoint stations. This approach of capturing data from fixed waypoints imitates the existing approach of collecting data from static cluster heads in the field. In the second variation (termed ‘UAV’), rather than collecting data from the waypoints, if during the trip, the UAV encounters any node that has data to transmit, the node transmits that data directly to the UAV. The UAV can either, store that data and bring it back to the base station at the end of the trip or can use some wireless technology to transmit that data to the base directly. In our approach, the UAV does not wirelessly transmit the data but brings it back to the sink at the end of its trip.

B. Phase 2: Intra-Node Caching

In this phase, in addition to everything described in Phase 1, the nodes have an intra-node caching ability allowing them to cache data obtained during interactions with other mobile nodes they come into contact with. The caching mechanism can be better understood from Fig. 4.

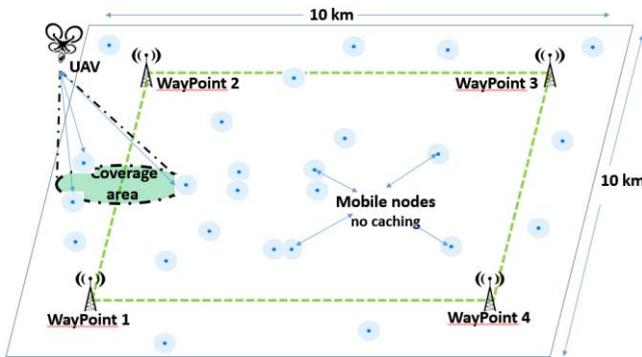


Fig. 3. Phase 1: No Intra-node Caching between Nodes.

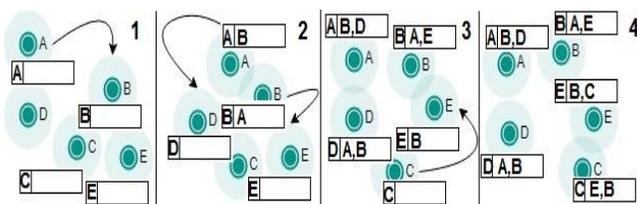


Fig. 4. Intra-node Caching Technique.

A node not only exchanges data with the node it comes in contact with directly but also exchanges data it has accumulated in its cache. Snapshot (2) of Fig. 4 shows that A and B exchange information upon coming in range of each other. Snapshot (3) shows that when D comes in contact with A, it not only caches A’s information but in addition, caches all the information that A has in its cache (information A gathered from B in its previous encounter with B). This means that even if a node has not encountered a certain node directly, it still has the ability to carry this “second-hand” data the node if it came into contact with it indirectly. Hence we refer to this as an ‘indirect caching technique’.

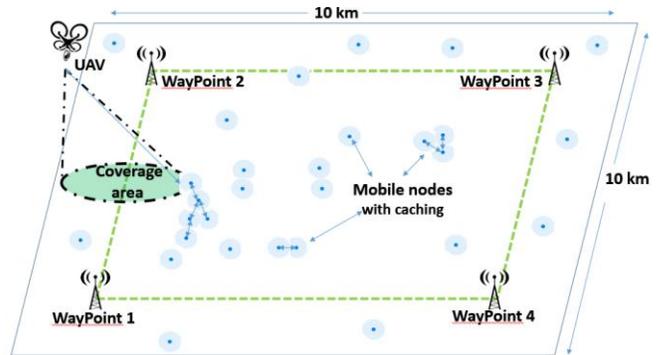


Fig. 5. Phase 2: Intra-node Caching between Nodes.

As shown in Fig. 5, the UAV follows the same path to complete its trip across the field which we term waypoint to waypoint communication. This phase also has two variants. The nodes have caching enabled in them in both versions which means if they come in contact with each other, they are allowed to exchange information and the receiving node can cache data that belongs to other nodes. In the first version (termed ‘WP+C’), the UAV only picks up data from the fixed route waypoints and not from the nodes directly. The fixed waypoints encountering a node not only take the node’s data but also accept all data that node has encountered from other nodes. In the second variant (termed ‘UAV+C’), if the UAV encounters a node that has data to send, the UAV collects that data directly. When the UAV encounters such a node, the node transfers to the UAV its own data in addition to the cached data of other nodes it has interacted with.

Data exchange between the nodes arises using a simple connectionless protocol shown as Algorithm 1. It assumes that nodes are transmitting regular beacons to announce their presence in the field in addition to scanning their coverage area to discover other nodes in their vicinity. This is the case with the UAV as well. If a node discovers another node in its vicinity (NeighborsFound = 1), it exchanges its data along with all messages of other nodes in its cache to the encountered node. For the UAV, it does not exchange its data with the encountered node; however, it does pick up the other node’s data in the same way. For intra-node communication, this is a two way process which means that both nodes in each other’s vicinity will exchange information. A node upon receiving a message (DataToReceive = 1) will first check its cache (NodeCache = null) to see if it already has that data. If this is true, the node will discard the oldest version of the data (remove old message) replacing it with the newer version (push

new message) by making use of timestamps (timestamps<sub>OldMsg</sub> & timestamps<sub>NewMsg</sub>). The vicinity of the node is termed the ‘range’ of the node in this paper and is defined by ‘i’, the radius around the node and its coverage area. The range of the node is one of the design parameters that we consider in subsequent experiments. Using this protocol, we eliminate the possibility of having duplicate data on nodes at any time.

**Algorithm 1:** Connection-Less Data Exchange Protocol

0 = False, 1 = True

**Node as a Sender**

```

while DataToSend == 1 do
    Scan for nearby nodes in coverage range;
    if NeighborsFound == 1 then
        transmit message/packet to all neighbors in range;
        DataToSend = 0;
    else
        break;
    end
end

```

**Node as a Receiver**

```

while DataToReceive == 1 do
    Receive incoming message from the sender;
    if NodeCache == null then
        push message to receiver’s NodeCache;
        DataToReceive = 0;
    else
        if message ∉ NodeCache then
            push message to receiver’s NodeCache;
        else
            if timestampNewMsg > timestampOldMsg then
                remove old message from receiver’s NodeCache;
                push new message to receiver’s NodeCache;
            else
                discard received message;
            end
        end
        DataToReceive = 0;
    end
end

```

The range of the UAV has been termed as the ‘coverage area’ of the UAV and is defined to be the projection imposed by the UAV’s antenna on the ground while flying at a constant height. The height is the altitude of the UAV whereas the coverage area is a circular area of radius ‘Radius’ as shown in Fig. 6.

The radius and coverage area of the UAV are defined by Equation 1 and 2, respectively. Throughout the evaluation, the range of the UAV is achieved by controlling the projection angle made by the UAV’s antenna with the ground.

$$\Phi = \frac{\text{Projection Angle}}{2} = \frac{\theta}{2}$$

$$\text{Radius} = \text{Altitude} \times \tan \Phi \tag{1}$$

$$\text{Coverage Area} = \pi \times (\text{Altitude} \times \tan(\Phi))^2 \tag{2}$$

Waypoints have been placed towards the edges of the field in such a way that optimum coverage is achieved by the UAV while on its flight between them. The coordinates for placing the waypoints have been set using equations 3, 4, 5 and 6.

$$WP1 = \left( \frac{\text{Radius}}{\sqrt{Nda}} \times i, \frac{\text{Radius}}{\sqrt{Nda}} \times i \right) \tag{3}$$

$$WP2 = \left( i - \frac{\text{Radius}}{\sqrt{Nda}} \times i, \frac{\text{Radius}}{\sqrt{Nda}} \times i \right) \tag{4}$$

$$WP3 = \left( i - \frac{\text{Radius}}{\sqrt{Nda}} \times i, i - \frac{\text{Radius}}{\sqrt{Nda}} \times i \right) \tag{5}$$

$$WP4 = \left( \frac{\text{Radius}}{\sqrt{Nda}} \times i, i - \frac{\text{Radius}}{\sqrt{Nda}} \times i \right) \tag{6}$$

Where ‘Radius’ is the coverage range of the UAV (m), ‘Nda’ is the node distribution area (m) and ‘i’ is equivalent to ‘n’ from the ‘n x n’ square matrix used in the code of the simulator for the node distribution area.

The flight pattern or the pattern of area coverage by the UAV can be understood from Fig. 7 which shows the series of areas covered by a UAV starting at time ‘n’ and increasing by ‘x’ (one second in our simulation) at each interval.

These concepts are realised in a simulation environment and then evaluated. Details of the experimental setup, the results and an assessment of their significance are provided for the different caching and non-caching variants in Section 4.

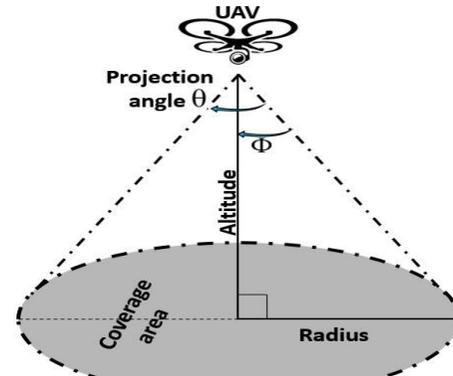


Fig. 6. Coverage Area of the UAV.

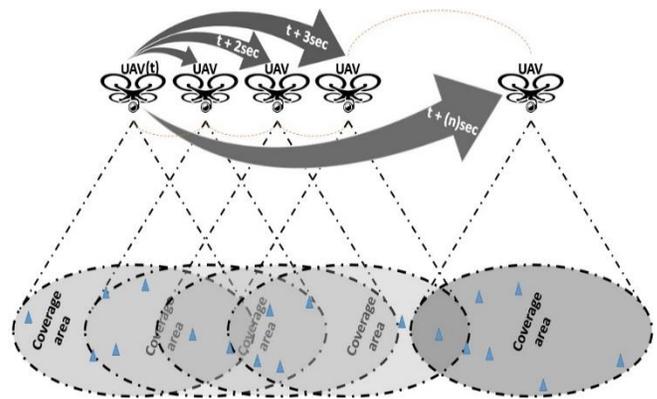


Fig. 7. Pattern of Area Coverage by the UAV.

#### IV. SIMULATION EVALUATION

To evaluate the benefit of caching, a bespoke JAVA run time event driven simulator was created. Several experiments were conducted testing comparing the various caching and non-caching variants presented in Section 3 under different conditions. The aim was to assess the efficacy of using intra-node caching on mobile wireless sensor nodes for animal monitoring.

Three different control parameters are considered, namely: node density, node coverage range and UAV coverage range. In each scenario 10 simulations have been run varying the initial node dispersion in the distribution area. The nodes are deployed with varying speeds but the speed of the UAV remains constant throughout all simulations. The speed of the UAV has been set according to some commercial copters available in the market whereas the speed of the nodes have been set assuming the animals roam under normal conditions without stress. The range of the nodes is dependent on the antenna they host and has been set according to [43] considering not just the basic motes currently available but advanced ones with a higher ranges [44]. We have tried to mimic large herbivores such as elephants which according to [45], [46] employ the Levy walk model, normally move with speeds in excess of 2mps, have a minimum home range of ten square kilometres [47], and can exist individually or in groups between 8-100 elephants in an area [48]. The mobility model is thus a stochastic Levy model where a node determines its next step according to a Markov based decision process, whereas the UAV follows a fixed linear flight path between multiple waypoints set within the distribution area. More details of the simulation parameters are provided in Tables II and III.

TABLE II. SIMULATION AND UAV CHARACTERISTICS

Simulation Parameters	
Simulations	10 per scenario
Node distribution area (Nda)	10km x 10km
Simulation duration	UAV's roundtrip ( $\approx 45$ mins)
UAV altitude	Constant (100m)
UAV speed	Constant ( $\approx 15$ m/s)
UAV coverage radius	Variable (80m - 720m)
UAV mobility	Linear (waypoint-waypoint)
Transfer time (UAV $\leftrightarrow$ node)	Instantaneous
Node Density(KM <sup>2</sup> )	1 - 7

TABLE III. NODE ATTRIBUTES

Node attributes	
Node type	Mobile
Node speed	Variable ( $\approx 2$ m/s - $\approx 5$ m/s)
Node coverage	Variable (80m - 720m)
Mobility	Levy model
Cache size	Unlimited
Energy	No Constraint

In each simulation, the UAV completes one flight starting and ending at the initial waypoint / take-off point. The field size, as pointed out previously is based on reported minimum home range of elephants however, other authors have also used such values [20] in similar scenarios. Node densities are considered using information presented in [49], [50] in addition to the values used for similar work in [51]. For the sake of simplicity, it is also assumed that the data transfer time between the nodes and the UAV is instantaneous. Specific UAV attributes can be seen in Table II which has been set considering current domestic and commercial UAV characteristics. It is assumed that the UAV is not resource-constrained compared to the sensor nodes, thus it can house an antenna potentially providing greater coverage than the sensing nodes. The node attributes can be seen in Table III. For the sake of this research, it is assumed that the nodes are not constrained by data storage or battery life; however, the coverage range has been selected based on motes available in the market and discussed in [52]. Movement speeds of nodes have been selected based on the stress free movement speed of the animals under consideration however they also match the parameters used for related work in [53].

Results are being presented using GNUPLOT version 5.2 patch 6.

Fig. 8 to Fig. 23 show the percentage of nodes encountered by the UAV and the Waypoints with and without the intermediate caching enabled between the nodes. The results are produced by varying certain perimeters to understand how it would affect the caching efficiency. All four variants of the two phases discussed in Section 3 are included.

In Fig. 8, the coverage of the UAV is set to 720m with a node density of 7 per square kilometres while varying the coverage radius of the nodes. Results show the 95% confidence intervals. Fig. 9 shows the percentage of nodes encountered by the UAV on its round trip when the coverage radius of the nodes is set to 720m, again with 7 nodes per square kilometres, while varying the coverage radius of the UAV. Fig. 10 illustrates that caching performance is consistent when the nodes are moving at lower speeds (equivalent to our animals in consideration). This means that for animals with movement speeds between  $\approx 1.9$ mps to  $\approx 5$ mps, the percentage of nodes captured by the UAV is more dependent on the parameters of the UAV and the nodes rather than the movement speeds of the sensors. Fig. 11 shows the percentage of nodes cached by the UAV on its round trip when the density of the deployed nodes in the distribution area is increased from 1 to 7 per square kilometre whilst keeping the UAV and node coverage range constant. Fig. 12, Fig. 13 and Fig. 14 is a repetition of the same scenario however; the UAV and node coverage ranges have been brought down to 560m. Fig. 15, Fig. 16 and Fig. 17 repeats this with the coverage ranges of the UAV and the nodes to be set to 400m. Fig. 18, Fig. 19 and Fig. 20 drops the coverage range further down to 240m followed by Fig. 21, Fig. 22 and Fig. 23 where the range has been set to 80m. All marking on the charts are with a 95% confidence interval.

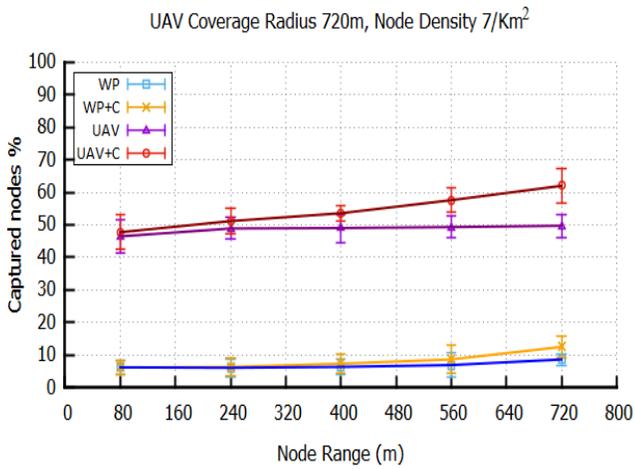


Fig. 8. Percentage of Encountered Nodes with Varying Node Coverage Range (inc. 95% CI).

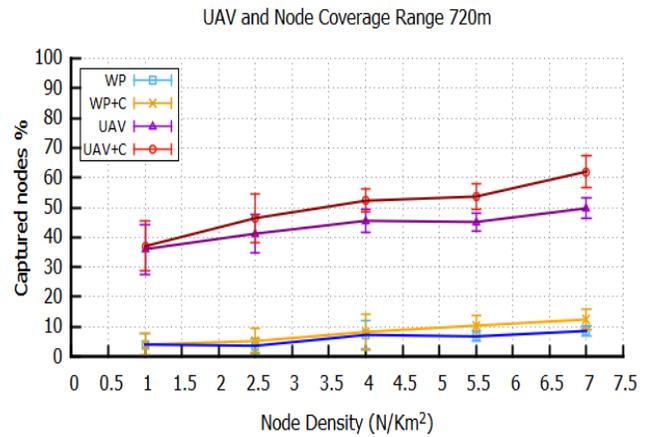


Fig. 11. Encountered Nodes % with Varying Deployed Node Density in Node Distribution Area (inc 95% CI) with Range  $\approx 0.7$ km.

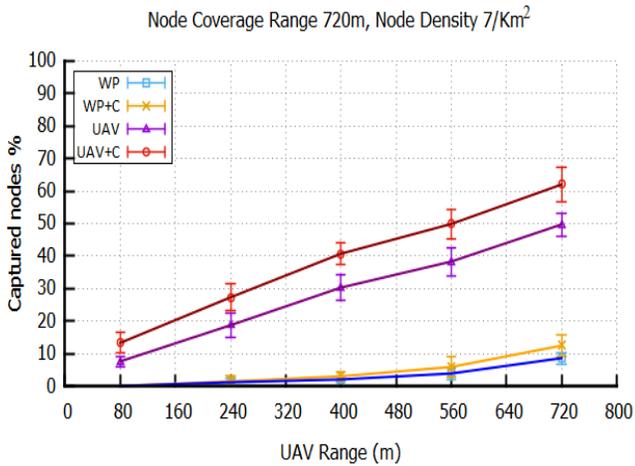


Fig. 9. Percentage of Encountered Nodes Varying UAV Coverage Range (inc. 95% CI).

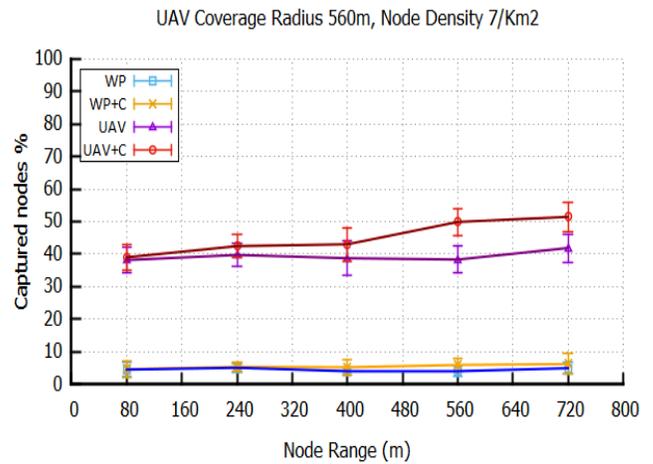


Fig. 12. Percentage of Encountered Nodes with Varying Node Coverage Range (inc. 95% CI).

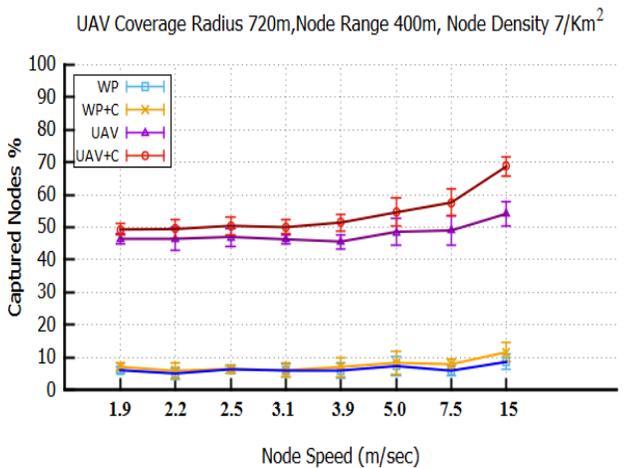


Fig. 10. Encountered Nodes % with Varying Deployed Node Speed in Node Distribution Area (inc 95% CI).

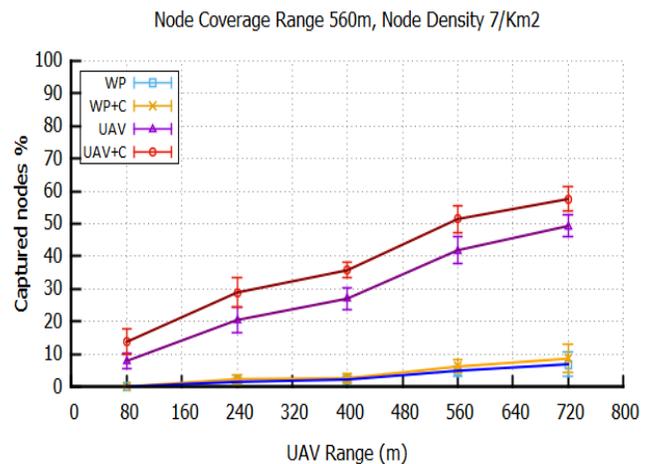


Fig. 13. Percentage of Encountered Nodes Varying UAV Coverage Range (inc. 95% CI).

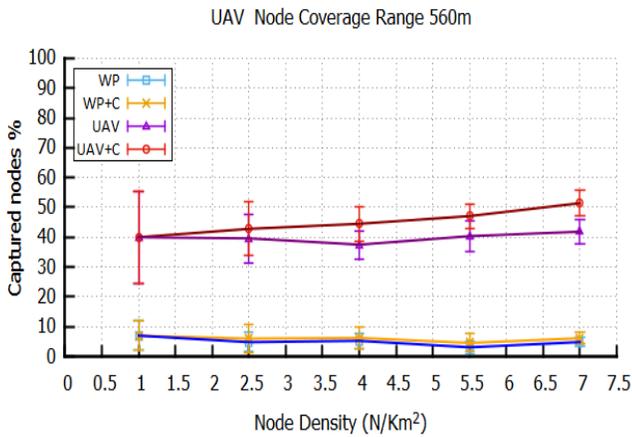


Fig. 14. Encountered Nodes % with Varying Deployed Node Density in Node Distribution Area (inc 95% CI) with Range  $\approx 0.5$ km.

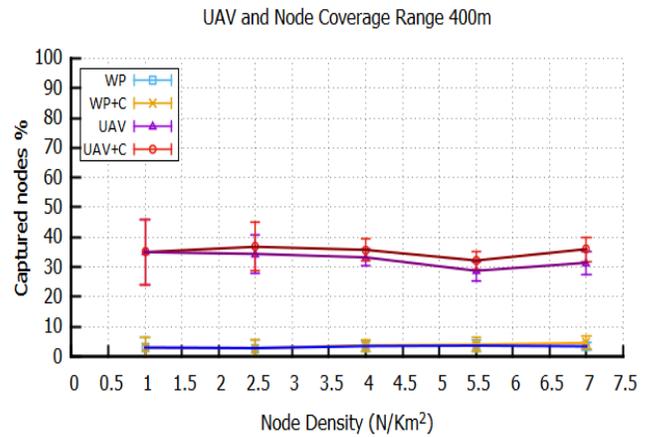


Fig. 17. Encountered Nodes % with Varying Deployed Node Density in Node Distribution Area (inc 95% CI) with Range  $\approx 0.4$ km.

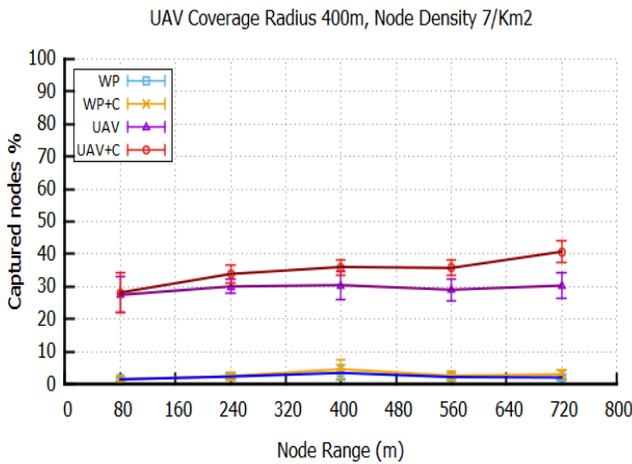


Fig. 15. Percentage of Encountered Nodes Varying Node Coverage Range (inc. 95% CI).

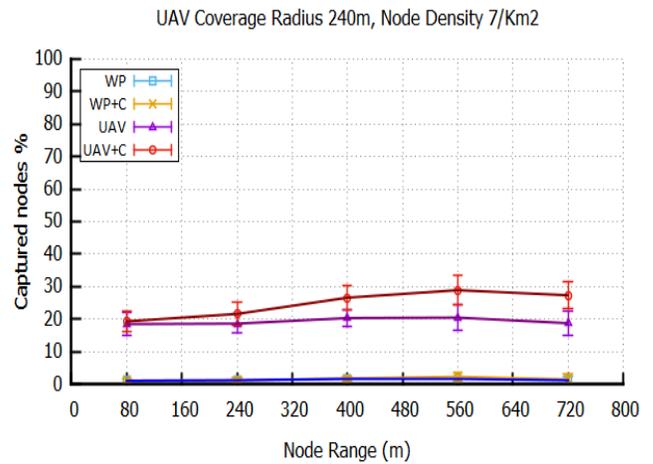


Fig. 18. Percentage of Encountered Nodes Varying node Coverage Range (inc. 95% CI).

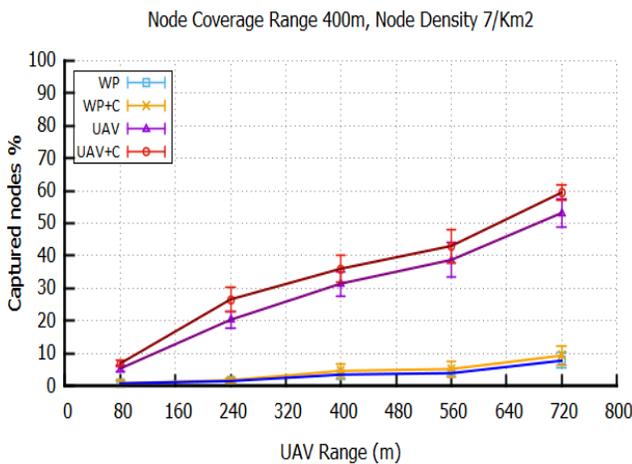


Fig. 16. Percentage of Encountered Nodes Varying UAV Coverage Range (inc. 95% CI).

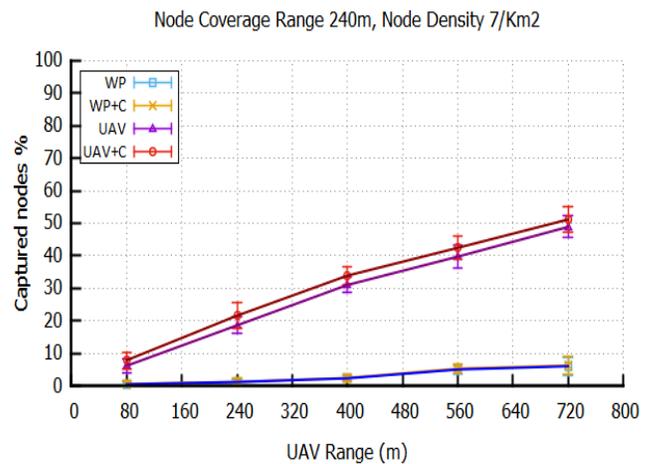


Fig. 19. Percentage of Encountered Nodes Varying UAV Coverage Range (inc. 95% CI).

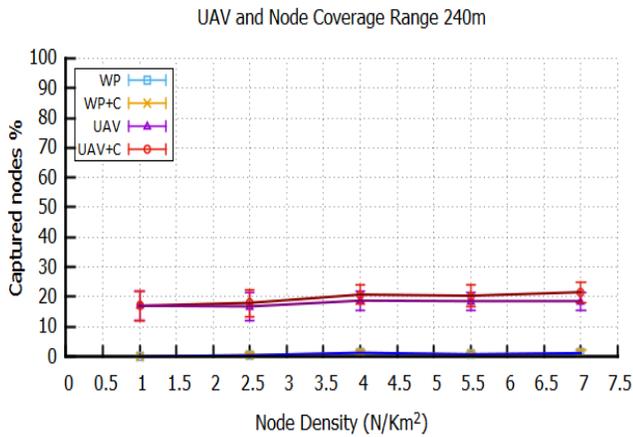


Fig. 20. Encountered Nodes % with Varying Deployed Node Density in Node Distribution Area (inc 95% CI) with Range  $\approx 0.25$ km.

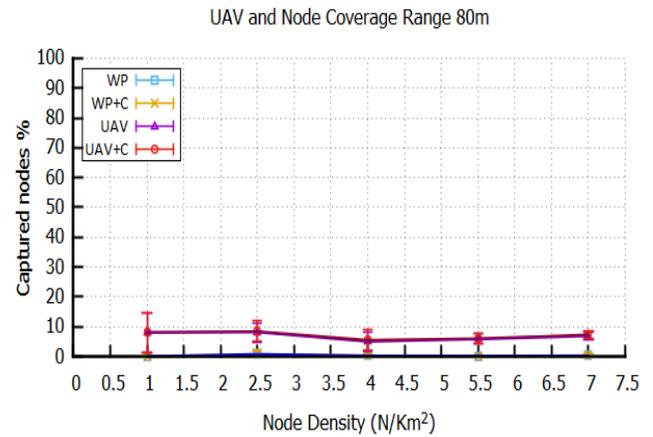


Fig. 23. Encountered Nodes % with Varying Deployed Node Density in Node Distribution Area (inc 95% CI) with Range  $\approx 0.1$ km.

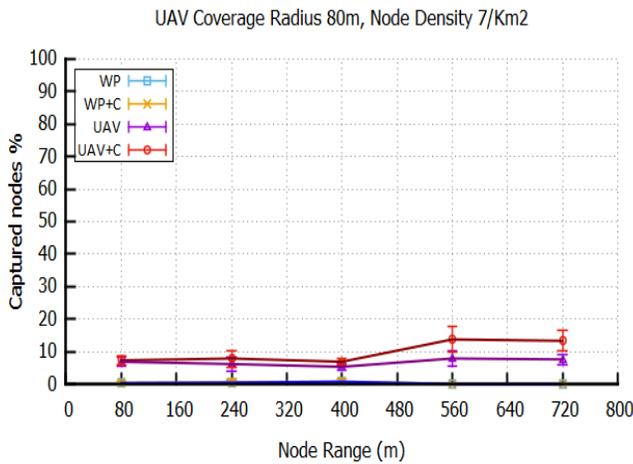


Fig. 21. Percentage of Encountered Nodes Varying Node Coverage Range (inc. 95% CI).

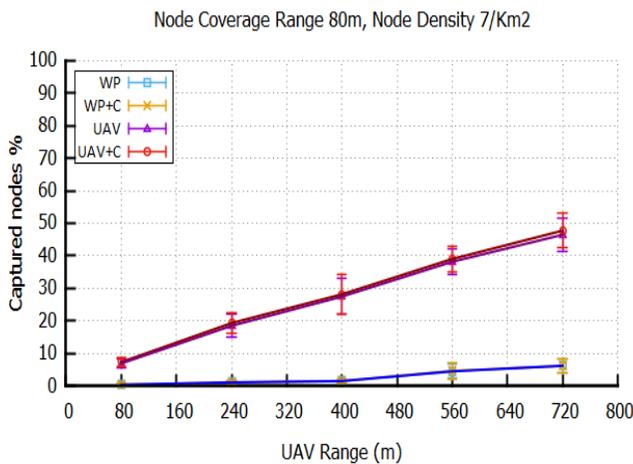


Fig. 22. Percentage of Encountered Nodes Varying UAV Coverage Range (inc. 95% CI).

Observing from the figures, we see that the percentage of encountered nodes is highly dependent on the coverage range of the nodes with higher efficiencies when the nodes coverage radius increases. Also, the ability of the UAV to directly interact with the mobile nodes provides considerable benefit. The figures show that when the range of the nodes remains constant throughout, the improvement in the number of nodes seen by the UAV does increase but not dramatically. The percentage of nodes seen by the UAV greatly improves when the nodes are allowed to move at high speeds. This is mainly because nodes have a higher probability of interacting with and caching other nodes when they are moving faster compared to when they are moving slower and ultimately, more nodes will be picked up by the UAV. The figures also seem to suggest that for the animals in our consideration (elephants) and other similar animals, their real time movement state/speed will not have a big impact on the results considering their top speeds are not that significant and lie within the values we have used. The figures also show that for a very low deployed node count, unless the node and UAV perimeters are considered, the benefit of caching at node level is negligible and the system behaves the same with and without intra-node caching. The improvement in the percentage of nodes seen by the UAV tends to increase with the growing node density. We note again that the percentage of encountered nodes is highly dependent on the coverage range of the nodes with higher efficiencies when the nodes coverage radius increases. It shows that even when the UAV range is low, the advantages of using intermediate caching over no caching at all is quite significant. It shows that in a densely populated areas, the advantages of using intermediate caching outweigh the scenario where no caching is used. At low densities, intermediate caching and no caching yield the same results. At low node ranges, there is no advantage of embedding caching mechanisms into the deployed nodes however, for nodes with higher coverage range, a significant improvement can be seen over the previous case of no intermediate caching. The figures also seem to suggest that the advantages of intermediate caching over no intermediate caching rely more on a higher node coverage range compared to a higher UAV coverage range. At low range nodes, regardless of what the density of the environment is,

intermediate caching yields almost no benefit. We can see that with a higher number of nodes deployed in the distribution area, the advantage of using intra-node caching is much more beneficial.

Fig. 24 and Fig. 25 demonstrated the benefits of using intermediate caching. The trend lines clearly show that in both scenarios (when the data is being collected by the UAV directly from the nodes and when it is being collected only from waypoints by the UAV), there is an improvement over the total number of nodes captured by the UAV during its trip where, a significant advantage is shown when the UAV is allowed to capture data by directly interacting with the nodes.

Our evaluation clearly shows the benefit of using intra-node caching in a routing-less wireless mobile ad-hoc sensor network environment and a UAV is used as a relay agent to move data between the sensor nodes and the sink. Fig. 26 below shows the average number of nodes captured by the UAV at different node densities in the distribution area. The next section outlines our conclusions and future work.

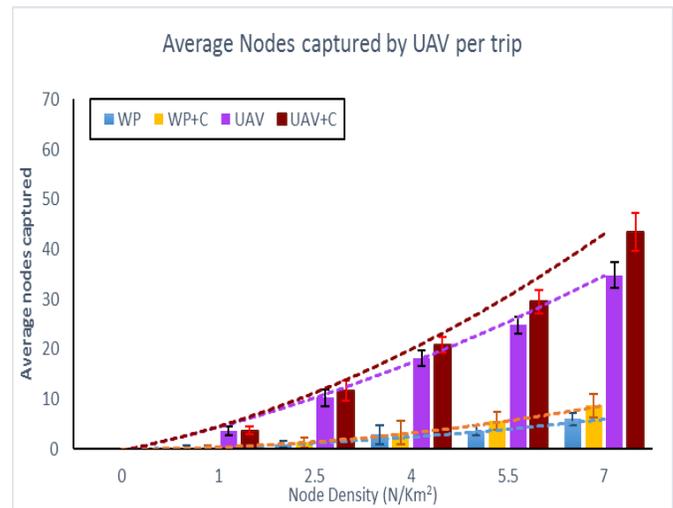


Fig. 26. Average Number of Nodes Encountered by the UAV While Increasing the Deployed Node Density (inc 95% CI).

### V. CONCLUSIONS AND FUTURE WORK

It is clear from the results that the use of caching in a mobile ad-hoc sensor network where a UAV is used to relay information from the nodes to the sink and vice versa rather than a routing protocol yields significant benefits compared to the scenario where no caching is used. We can see from the results presented in Section 4 that even for a short duration (45mins), we were able to achieve around 12% improvement on the encountered node percentage when the UAV interacts with the nodes directly and around 4% improvement when the UAV only collects data from the waypoints. Another thing to notice here is that the UAV was allowed only one trip across the field in our experimentations however, we predict that we can further see a significant increase in the nodes seen percentage provided that the UAV makes more than one trips to collect data from the sensor nodes. In addition, the trip timings may also play a reasonable role in the percentage of nodes encountered by the UAV as we did notice in some cases that the number of nodes cached at the sensor nodes and the waypoints were higher than the nodes encountered by the UAV. The reason behind this was that the nodes and waypoints had encountered additional nodes after the UAV's visit to them hence the UAV was unable to get that information from them. In our experimentations, we chose the simplest locations for the waypoints, being around the edges of the field however, introducing no-go zones in the area and most visited zones can also have an impact on the results. Also, repositioning the waypoints to other locations based on the geography of the area where the model is to be deployed can also have an impact on the nodes encountered by the UAV on its trip. With the addition of different obstacles in the distribution area, the positioning of the waypoints can greatly affect the performance of the approach. Another interesting area to consider is selective caching with a finite cache size as opposed to our infinite caching model. Also, effects on the percentage of nodes seen by the UAV when the animals are moving rapidly are shown in Section 4; however, when the UAV moves at varying speed or the relationship between the speed of the nodes and the perimeters of the UAV can be further investigated and can yield different results as well.

Caching Improvement Trend At the UAV

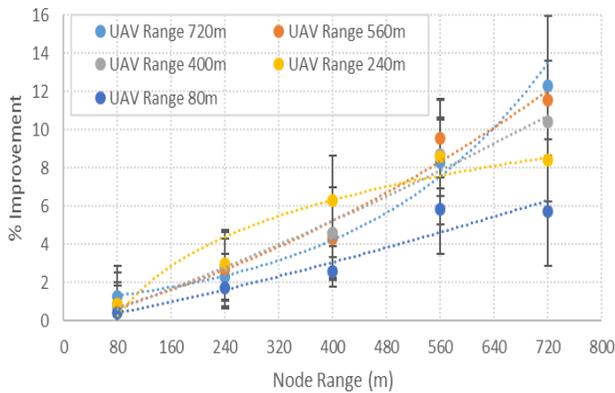


Fig. 24. Caching Improvement Trend for Nodes Captured by UAV with Intermediate Caching (inc. 95% CI).

Caching Improvement Trend At the WAYPOINT

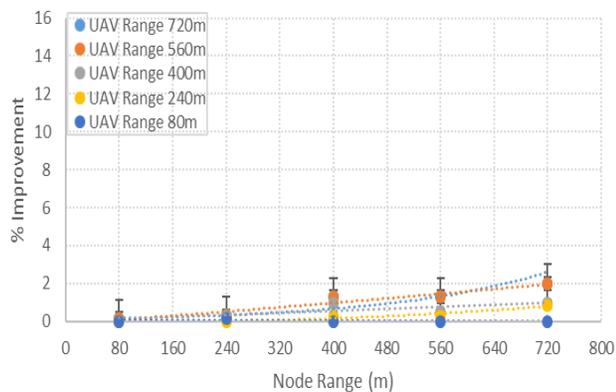


Fig. 25. Caching Improvement Trend for Nodes Captured by WAYPOINTS with Intermediate Caching (inc. 95% CI).

In addition to what has been discussed, there are several other parameters that we would like to check including different movement models and the use of multiple UAVs. We believe that our work opens up a very broad area of extensive research that can greatly benefit not only the field of tracking and preservation of wildlife but also, if implemented with custom parameters under different settings, can greatly assist in other areas as well including vehicular ad-hoc networks and disaster area networks as well.

#### REFERENCES

- [1] S. Jeong, J. Ko, and J. Kim, "The effectiveness of a wireless sensor network system for landslide monitoring," *IEEE Access*, vol. 8, pp. 8073–8086, 2020.
- [2] H. R. Galappaththi and G. T. Weerasuriya, "Implemented for Environmental Sensing," 2018 3rd Int. Conf. Inf. Technol. Res., pp. 1–6, 2018.
- [3] R. Vera-Amaro, M. E. R. Angeles, and A. Luviano-Juarez, "Design and Analysis of Wireless Sensor Networks for Animal Tracking in Large Monitoring Polar Regions Using Phase-Type Distributions and Single Sensor Model," *IEEE Access*, vol. 7, pp. 45911–45929, 2019.
- [4] T. Bensiradj and S. Moussaoui, "Strategy efficient to extend the lifetime of wireless sensor networks in a framework of hybrid sensors and vehicular networks for road safety," *IET Wirel. Sens. Syst.*, vol. 9, no. 6, pp. 416–423, 2019.
- [5] R. Singh and G. M. Asutkar, "Survey on various wireless sensor network techniques for monitoring activities of wild animals," *ICIIECS 2015 - 2015 IEEE Int. Conf. Innov. Information, Embed. Commun. Syst.*, pp. 1–5, 2015.
- [6] T. O. Olasupo, "Wireless Communication Modeling for the Deployment of Tiny IoT Devices in Rocky and Mountainous Environments," *IEEE Sensors Lett.*, vol. 3, no. 7, pp. 1–4, 2019.
- [7] "A detailed survey on Bandwidth efficient cluster based routing schemes in wireless sensor networks," no. *Iccsit*, pp. 1250–1253, 2019.
- [8] J. D. Á. V., D. L. A. S., R. P. León, and P. Sergio, "Analysis of energetic efficiency in routing protocols and sustaining quality service applied to a wireless sensor network," pp. 27–32, 2019.
- [9] T. M. Behera, S. K. Mohapatra, U. C. Samal, M. S. Khan, M. Daneshmand, and A. H. Gandomi, "I-SEP: An Improved Routing Protocol for Heterogeneous WSN for IoT-Based Environmental Monitoring," *IEEE Internet Things J.*, vol. 7, no. 1, pp. 710–717, 2019.
- [10] P. Juang, H. Oki, Y. Wang, M. Martonosi, L. S. Peh, and D. Rubenstein, "Energy-efficient computing for wildlife tracking: Design tradeoffs and early experiences with ZebraNet," *Int. Conf. Archit. Support Program. Lang. Oper. Syst. - ASPLOS*, pp. 96–107, 2002.
- [11] N. Adam, C. Tapparello, M. N. Wijesundara, and W. Heinzelman, "JumboNet Elephant Tracking Using Delay-Tolerant Routing with Multiple Sinks," 2018 Int. Conf. Comput. Netw. Commun., pp. 689–695, 2018.
- [12] R. Kays et al., "Tracking animal location and activity with an automated radio telemetry system in a tropical rainforest," *Comput. J.*, vol. 54, no. 12, pp. 1931–1948, Nov. 2011.
- [13] V. Dyo et al., "Wildsensing: Design and deployment of a sustainable sensor network for wildlife monitoring," *ACM Trans. Sens. Networks*, vol. 8, no. 4, 2012.
- [14] R. Kays et al., "Tracking animal location and activity with an automated radio telemetry system in a tropical rainforest," *Comput. J.*, vol. 54, no. 12, pp. 1931–1948, 2011.
- [15] E. D. Ayele, N. Meratnia, and P. J. M. Havinga, "Towards a new opportunistic iot network architecture for wildlife monitoring system," 2018 9th IFIP Int. Conf. New Technol. Mobil. Secur. NTMS 2018 - Proc., vol. 2018-Janua, pp. 1–5, 2018.
- [16] S. Toledo, O. Kishon, Y. Orchan, A. Shohat, and R. Nathan, "Lessons and Experiences from the Design, Implementation, and Deployment of a Wildlife Tracking System," in *Proceedings - 2016 IEEE International Conference on Software Science, Technology and Engineering, SwSTE 2016, 2016*, pp. 51–60.
- [17] S. Blake, I. Douglas-Hamilton, and W. B. Karesh, "GPS telemetry of forest elephants in Central Africa: Results of a preliminary study," *Afr. J. Ecol.*, vol. 39, no. 2, pp. 178–186, 2001.
- [18] P. Sommer, B. Kusy, P. Valencia, R. Dungavell, and R. Jurdak, "Delay-Tolerant Networking for Long-Term Animal Tracking," *IEEE Internet Comput.*, vol. 22, no. 1, pp. 62–72, 2018.
- [19] J. Xu, G. Solmaz, R. Rahmatizadeh, L. Boloni, and D. Turgut, "Providing Distribution Estimation for Animal Tracking with Unmanned Aerial Vehicles," 2018 IEEE Glob. Commun. Conf. GLOBECOM 2018 - Proc., 2018.
- [20] J. Xu, G. Solmaz, R. Rahmatizadeh, D. Turgut, and L. Boloni, "Animal monitoring with unmanned aerial vehicle-Aided wireless sensor networks," *Proc. - Conf. Local Comput. Networks, LCN*, vol. 26-29-Octo, pp. 125–132, 2015.
- [21] A. Fotouhi, M. Ding, and M. Hassan, "Dynamic base station repositioning to improve performance of drone small cells," 2016 IEEE Globecom Work. GC Wkshps 2016 - Proc., 2016.
- [22] A. Fotouhi, M. Ding, and M. Hassan, "Dynamic base station repositioning to improve performance of drone small cells," 2016 IEEE Globecom Work. GC Wkshps 2016 - Proc., no. 0, pp. 1–13, 2016.
- [23] A. Trotta et al., "BEE-DRONES: Energy-efficient Data Collection on Wake-Up Radio-based Wireless Sensor Networks," *INFOCOM 2019 - IEEE Conf. Comput. Commun. Work. INFOCOM WKSHPs 2019*, pp. 547–553, 2019.
- [24] J. Chen et al., "Efficient Data Collection in Large-Scale UAV-aided Wireless Sensor Networks," 2019 11th Int. Conf. Wirel. Commun. Signal Process. WCSP 2019, 2019.
- [25] A. Arvanitaki and N. Pappas, "Modeling of a UAV-based data collection system," *IEEE Int. Work. Comput. Aided Model. Des. Commun. Links Networks, CAMAD*, vol. 2017-June, 2017.
- [26] S. Say, H. Inata, M. E. Ernawan, Z. Pan, J. Liu, and S. Shimamoto, "Partnership and data forwarding model for data acquisition in UAV-aided sensor networks," 2017 14th IEEE Annu. Consum. Commun. Netw. Conf. CCNC 2017, pp. 933–938, 2017.
- [27] X. Ma, R. Kacimi, and R. Dhaou, "Adaptive hybrid MAC protocols for UAV-assisted mobile sensor networks," *CCNC 2018 - 2018 15th IEEE Annu. Consum. Commun. Netw. Conf.*, vol. 2018-Janua, pp. 1–4, 2018.
- [28] J. Liu, X. Wang, B. Bai, and H. Dai, "Age-optimal trajectory planning for UAV-assisted data collection," *INFOCOM 2018 - IEEE Conf. Comput. Commun. Work.*, pp. 553–558, 2018.
- [29] A. F. Khalifeh, M. AlQudah, R. Tanash, and K. A. Darabkh, "A Simulation Study for UAV- Aided Wireless Sensor Network Utilizing ZigBee Protocol," *Int. Conf. Wirel. Mob. Comput. Netw. Commun.*, vol. 2018-October, no. 1, pp. 181–184, 2018.
- [30] S. Tansuriyavong, H. Kojia, M. Kyan, and T. Anezaki, "The Development of Wildlife Tracking System Using Mobile Phone Communication Network and Drone," 2018 Int. Conf. Intell. Informatics Biomed. Sci. ICIIBMS 2018, vol. 3, pp. 351–354, 2018.
- [31] H. Bayerlein, R. Gangula, and D. Gesbert, "Learning to Rest: A Q-Learning Approach to Flying Base Station Trajectory Design with Landing Spots," *Conf. Rec. - Asilomar Conf. Signals, Syst. Comput.*, vol. 2018-October, pp. 724–728, 2019.
- [32] R. Gangula, D. Gesbert, D. F. Külzer, and J. M. Franceschi, "A landing spot approach for enhancing the performance of UAV-Aided wireless networks," 2018 IEEE Int. Conf. Commun. Work. ICC Work. 2018 - Proc., pp. 1–6, 2018.
- [33] G. Wang, S. Lee, B. Lee, J. Young, and A. Electronics, "Secure and Efficient Cluster Head Election in a UAV-aided Wireless Sensor Network," pp. 42–49, 2019.
- [34] A. M. Reynolds, "Current status and future directions of Levy walk research," *Biol. Open*, vol. 7, no. 1, pp. 1–6, 2018.
- [35] M. E. Wosniack, M. C. Santos, E. P. Raposo, G. M. Viswanathan, and M. G. E. da Luz, "The evolutionary origins of Lévy walk foraging," vol. 13, no. 10, 2017.
- [36] A. O. Gautesstad, "Brownian motion or Lévy walk? Stepping towards an extended statistical mechanics for animal locomotion," *J. R. Soc. Interface*, vol. 9, no. 74, pp. 2332–2340, 2012.

- [37] "Tikalon Blog by Dev Gualtieri." [Online]. Available: [http://tikalon.com/blog/blog.php?article=2011/Levy\\_flight](http://tikalon.com/blog/blog.php?article=2011/Levy_flight). [Accessed: 20-Apr-2020].
- [38] Emanuel Deutschmann, "The Spatial Structure of Transnational Human Activity - Emanuel Deutschmann." [Online]. Available: <https://www.emanueldeutschmann.net/home/new-working-paper-available-online>. [Accessed: 19-Feb-2020].
- [39] D. Boyer, "What future for Lévy walks in animal movement research? Comment on 'Liberating Lévy walk research from the shackles of optimal foraging', by A.M. Reynolds.," *Phys. Life Rev.*, vol. 14, pp. 87–89, 2015.
- [40] N. E. Humphries, "Why Lévy Foraging does not need to be 'unshackled' from Optimal Foraging Theory. Comment on 'Liberating Lévy walk research from the shackles of optimal foraging' by A.M. Reynolds," *Phys. Life Rev.*, vol. 14, pp. 102–104, 2015.
- [41] N. Kumbhare, A. Rao, C. Gniady, W. Fink, and J. Rozenblit, "Waypoint-to-waypoint energy-efficient path planning for multi-copters," *IEEE Aerosp. Conf. Proc.*, pp. 1–11, 2017.
- [42] M. T. S. Ibrahim, S. V. Ragavan, and S. G. Ponnambalam, "Way point based deliberative path planner for navigation," *IEEE/ASME Int. Conf. Adv. Intell. Mechatronics, AIM*, pp. 881–886, 2009.
- [43] K. Akash and P. Edreena, "Survey on nodes used in wireless sensor networks," *Int. J. Pharm. Technol.*, vol. 8, no. 4, pp. 21272–21278, 2016.
- [44] S. Light, "XBee S1," pp. 1–3, 2016.
- [45] X. Dai, G. Shannon, R. Slotow, B. Page, and K. J. Duffy, "Short-Duration Daytime Movements of a Cow Herd of African Elephants," *J. Mammal.*, vol. 88, no. 1, pp. 151–157, 2007.
- [46] K. M. Njoki, "Elephant Foraging Behaviour: Application of Levy Flights in Geo-information Science and Remote Sensing," 2009.
- [47] N. Shadrack, M. O. Moses, M. Joseph, M. Shadrack, N. Steve, and I. James, "Home range sizes and space use of African elephants (*Loxodonta africana*) in the Southern Kenya and Northern Tanzania borderland landscape," *Int. J. Biodivers. Conserv.*, vol. 9, no. 1, pp. 9–26, 2017.
- [48] "Basic Facts About Elephants - Global Sanctuary For Elephants." [Online]. Available: <https://globalelephants.org/the-basics/>. [Accessed: 18-Aug-2020].
- [49] K. Kangwana, *Studying Elephants*. 1996.
- [50] S. R. Loarie, R. J. V. Aarde, and S. L. Pimm, "Fences and artificial water affect African savannah elephant movement patterns," *Biol. Conserv.*, vol. 142, no. 12, pp. 3086–3098, 2009.
- [51] M. Dong, K. Ota, M. Lin, Z. Tang, S. Du, and H. Zhu, "UAV-assisted data gathering in wireless sensor networks," *J. Supercomput.*, vol. 70, no. 3, pp. 1142–1155, 2014.
- [52] R. P. Narayanan, T. V. Sarath, and V. V. Vineeth, "Survey on Motes Used in Wireless Sensor Networks: Performance & Parametric Analysis," *Wirel. Sens. Netw.*, vol. 08, no. 04, pp. 51–60, 2016.
- [53] M. B. Kim, "Doctorat De L ' Université De Toulouse Titre :," no. May, pp. 1–190, 2019.

# Collaborative Recommendation based on Implication Field

Hoang Tan Nguyen<sup>1</sup>  
Department of Information  
and Communications of  
Dong Thap province  
Dong Thap, Vietnam

Lan Phuong Phan<sup>2</sup>  
College of Information &  
Communications Technology  
Can Tho University  
Can Tho, Vietnam

Hung Huu Huynh<sup>3</sup>  
University of  
Science and Technology  
University of Da Nang,  
Da Nang, Vietnam

Hiep Xuan Huynh<sup>4\*</sup>  
College of Information &  
Communications Technology  
Can Tho University  
Can Tho, Vietnam

**Abstract**—Recently, recommender systems has grown rapidly in both quantity and quality and has attracted many studies aimed at improving their quality. Especially, collaborative filtering techniques based on rule mining model combined with statistical implication analysis (SIA) technique also achieved some interesting results. This has shown the potential of SIA to improve the performance of recommender systems. However, it is still not rich and there are several problems to be solved for better results such as the problem of non-binary data processing, dealing with bottleneck case of data partitioning method according to the number of transactions on the very sparse transaction sets during training and testing the model, and not paying attention to exploiting the trend of variation of statistical implication. In order to contribute to solving these problems, the paper focuses on proposing a new data partitioning method, and developing the recommendation model based on equipotential planes mining generated by variation of implication intensity or implication index in the implication field on both binary and non-binary data to improve the recommendations further. Experimental results have shown the success of this new approach through its quality comparison with collaborative filtering recommendation models as well as existing SIA-based ones.

**Keywords**—Implication intensity; implication rules; implication field; equipotential surface

## I. INTRODUCTION

As a result of the available online information and the rapid increase of e-business and e-commercial services, it is difficult for users to make a proper decision without supporting of recommendation engines. And therefore, recommender systems [1], [2], [3], especially those based on collaborative filtering, are more and more popular and become an indispensable part of e-commercial services and others and one of which [2], [5], [15], [16], [17] is recommender system based on association rules mining (ARM).

Although ARM is considered as a popular and effective tool in “market-basket analysis” tasks and developing e-commerce, in recommender systems, the contribution of this technique is limited due to many reasons. Therefore, there have been many studies to improve this technique for recommender systems such as using fuzzy logic [16], [17], binarization real data [7], [8], and some others to refine and improve the rules evaluation measures, etc. While these also obtained certain results [5], [15], [16], [17], it’s so hard to keep up with collaborative filtering others. In recent years, several

recommendation models using statistical implicative analysis (SIA) [12], [13], [14] approach to improve the quality and effectiveness of recommender systems [7], [9], [10], [18], [19], [20], [21] by discover the interesting rules using measures like implication intensity, entropy implication intensity, Cohesion, and so on as similarity measures. Almost of which has not paid attention to mining the trend of variation of statistical implication, except for the works [18], [19], [20], [21] that have been published recently.

This paper focuses on three proposals (1) building a recommendation model based on implication field that can deal with both binary and non-binary dataset, (2) proposal data partition method based on rated items on each transaction instead of number of transactions on dataset, and (3) for a more comprehensive assessment of the quality of the proposed models, Item rating-based accuracy metrics are also used in addition to classification-based and prediction-based accuracy metrics to assess the quality of the recommendation listing. Experiment’s results shown that proposed model has performed better than both collaboration filtering ones and existing SIA-based ones, not only on binary data but also on non-binary one.

The paper is organized in five parts. The first one introduces the context and issues to be solved by the present systems as well as proposing our approach. The second part presents a summary of SIA theory and relevant contents about the recommender system. The next one presents proposed solution and its model to improve further the efficiency of recommender systems based on SIA. The fourth part is the experiment and evaluation of the proposed model, which focuses on comparing its performance with previous SIA models and traditional collaborative filtering-based models. Finally, the paper is finished by the conclusion.

## II. LITERATURE REVIEW

### A. Statistical Implicative Analysis

Statistical implicative analysis (SIA) theory [13], [14], proposed by Régis Gras, studies the implication relationship of data variables. It can be presented as follows.

Let  $E = \{e_1, e_2, \dots, e_n\}$  be a population of  $n$  transactions described by a finite set  $I = \{i_1, i_2, \dots, i_m\}$  of  $m$  variables (attributes, criteria, etc.). Let  $e_k \in E, i_v \in I$  where  $1 \leq k \leq n$  and  $1 \leq v \leq m$ . Denote by  $\Omega(e_k)$  the set of items taken

\*Corresponding authors.

from a transaction  $e_k$ , and  $\Omega(e_k) \subseteq I$ . Let  $a$  and  $b$  be subsets of  $I$ . Denote  $A = \{e_k \in E | \forall j \in a, j \in \Omega(e_k)\}$  and  $B = \{e_k \in E | \forall l \in b, l \in \Omega(e_k)\}$ , and  $\bar{A}, \bar{B}$  are respectively complementary set  $A, B$  in  $E$ .

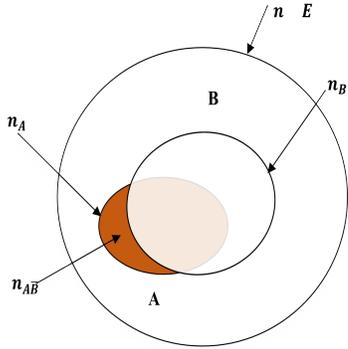


Fig. 1. Illustration of an implication rule  $a \rightarrow b$  in SIA by Venn diagram.

An implication relationship (association rule/implication rule) is a pattern of the form  $a \rightarrow b$ , where  $a$  and  $b$  are disjoint itemsets ( $a \subset I, b \subset I$ , and  $a \cap b = \emptyset$ ). In fact, it is relatively common to observe a couple of transactions which contain  $a$  and not  $b$  instead of having the general trend to have  $b$  when  $a$  is present. Therefore, in addition to  $n = \text{card}(E)$  of  $E$ , it is necessary to taken into account the number  $n_A = \text{card}(A)$  of  $A$ ,  $n_B = \text{card}(B)$  of  $B$ , and  $n_{A\bar{B}} = \text{card}(A \cap \bar{B})$  of counter-examples  $A \cap \bar{B}$  to statistically accept to retain or not the rule  $a \rightarrow b$ .

The implication relationship between  $a$  and  $b$  is presented in an implication rule  $a \rightarrow b$  could be modeled in the SIA as Fig. 1.

To further illustrate about an implication rule, let's see an example movie transaction data as presented in Table I(a). We can consider it as set  $E = \{e_k, |k = 1..9\}$ , and let  $I = \{Movie_1, Movie_2, Movie_3\}$  an itemset. The set of items  $\Omega(e_1) = \{Movie_1\}$ ,  $\Omega(e_2) = \{Movie_1, Movie_2\}$ , etc. The movies data in Table I can be represented in a binary format as shown in Table II, where each row corresponds to a transaction and each column corresponds to an movie. A movie can be treated as a binary variable whose value is 1 if the movie is present in a transaction and 0 otherwise. Now, let's consider an implication rule  $a \rightarrow b$ , where  $a = \{Movie_1, Movie_2\}, b = \{Movie_3\}$  then set  $A = \{e_2, e_4, e_5, e_6, e_8, e_9\}$ , and set  $B = \{e_4, e_5, e_6, e_9\}$ . Thus,  $n = 9, n_A = 6, n_B = 4$ , and  $n_{A\bar{B}} = 2$ , so that rule  $a \rightarrow b$  can be represented by  $(n, n_A, n_B, n_{A\bar{B}})$  is  $(9, 6, 4, 2)$ .

More detail, we compare the observed number of counter-examples to a probabilistic model. Let us assume that we randomly draw two subsets  $X$  and  $Y$  in  $E$  which respectively contain  $n_A$  and  $n_B$  transactions. The complementary sets  $\bar{Y}$  of  $Y$  and  $\bar{B}$  of  $B$  in  $E$  have the same cardinality  $n_B$ . In this case,  $N_{X\bar{Y}} = \text{card}(X \cap \bar{Y})$  is a random variable and  $n_{A\bar{B}}$  an observed value. The implication rule  $a \rightarrow b$  is admissible for a given threshold  $1 - \sigma$  if  $\sigma$  is greater than the probability that the number of counter-examples in the observations is greater than the number of expected counterexamples in a random drawing

TABLE I. AN EXAMPLE OF MOVIE TRANSACTION DATA

$E$	Items/ $\Omega(e_k)$
$e_1$	<i>Movie</i> <sub>2</sub>
$e_2$	<i>Movie</i> <sub>1</sub> , <i>Movie</i> <sub>2</sub>
$e_3$	<i>Movie</i> <sub>1</sub>
$e_4$	<i>Movie</i> <sub>1</sub> , <i>Movie</i> <sub>2</sub> , <i>Movie</i> <sub>3</sub>
$e_5$	<i>Movie</i> <sub>1</sub> , <i>Movie</i> <sub>2</sub> , <i>Movie</i> <sub>3</sub>
$e_6$	<i>Movie</i> <sub>1</sub> , <i>Movie</i> <sub>2</sub> , <i>Movie</i> <sub>3</sub>
$e_7$	<i>Movie</i> <sub>2</sub>
$e_8$	<i>Movie</i> <sub>1</sub> , <i>Movie</i> <sub>2</sub>
$e_9$	<i>Movie</i> <sub>1</sub> , <i>Movie</i> <sub>2</sub> , <i>Movie</i> <sub>3</sub>

TABLE II. A BINARY REPRESENTATION OF DATA IN TABLE I

$E$	<i>Movie</i> <sub>1</sub>	<i>Movie</i> <sub>2</sub>	<i>Movie</i> <sub>3</sub>
$e_1$	0	1	0
$e_2$	1	1	0
$e_3$	1	0	0
$e_4$	1	1	1
$e_5$	1	1	1
$e_6$	1	1	1
$e_7$	0	1	0
$e_8$	1	1	0
$e_9$	1	1	1

[14], i.e. if  $Pr(N_{X\bar{Y}} \leq n_{A\bar{B}}) \leq \sigma$ .

The distribution of random variable  $N_{X\bar{Y}}$  depends on the drawing pattern of  $X$  and  $Y$ . For a certain process of drawing, the random variable  $N_{X\bar{Y}}$  follows a Poissonian distribution [14]  $P(\lambda)$  with  $\lambda = \frac{n_A n_B}{n}$ . For cases where the approximation is justified (e.g.  $\lambda \geq 4$ ), the standardized random variable  $\tilde{N}_{X\bar{Y}} = \frac{\text{card}(X \cap \bar{Y}) - \lambda}{\sqrt{\lambda}}$  is approximately  $N(0, 1)$ -distributed. The observed value of  $\tilde{N}_{X\bar{Y}}$  is  $\tilde{n}_{A\bar{B}} = (\frac{n_{A\bar{B}} - \lambda}{\sqrt{\lambda}})$ .

The implication intensity expresses the unlikelihood of counter-examples  $n_{A\bar{B}}$  in  $E$ . The rule is admitted for a given threshold  $1 - \sigma$  if  $\varphi(a, b) \geq 1 - \sigma$ .

The implication intensity measure  $\varphi(a, b)$  [13], [14] of rule  $a \rightarrow b$  is defined by equation (1)

$$\varphi(a, b) = \begin{cases} 1 - Pr(\tilde{N}_{X\bar{Y}} \leq \tilde{n}_{A\bar{B}}), & \text{if } n_B < n \\ 0, & \text{otherwise,} \end{cases} \quad (1)$$

$$= \begin{cases} 1 - \sum_{s=0}^{n_{A\bar{B}}} \frac{\lambda^s}{s!} e^{-\lambda}, & \text{if } n_B < n \\ 0, & \text{otherwise,} \end{cases}$$

For cases where the approximation is justified, the standardized random variable  $\tilde{N}_{X\bar{Y}} = \frac{\text{card}(X \cap \bar{Y}) - \lambda}{\sqrt{\lambda}}$  is approximately  $N(0, 1)$ -distributed, and  $\varphi(a, b)$  is determined as equation (2)

$$\varphi(a, b) = \begin{cases} \frac{1}{\sqrt{2\pi}} \int_{q(a, \bar{b})}^{\infty} e^{-\frac{t^2}{2}} dt, & \text{if } n_B < n \\ 0, & \text{otherwise,} \end{cases} \quad (2)$$

where  $q(a, \bar{b})$  is the implication index [14], also known as the Gras implication index, and is determined as follows.

For binary variables [13], [14], the implication index  $q(a, \bar{b})$  is defined by equation (3)

$$q(a, \bar{b}) = \frac{n_{A\bar{B}} - \frac{n_A n_B}{n}}{\sqrt{\frac{n_A n_B}{n}}} \quad (3)$$

For modal variables [13]  $a, b \in [0, 1]$ , the implication index  $q_p(a, \bar{b})$  is defined by equation (4)

$$q_p(a, \bar{b}) = \frac{\sum_{t \in E} a(t)\bar{b}(t) - \frac{n_A n_{\bar{B}}}{n}}{\sqrt{\frac{(n^2 s_A^2 + n_A^2)(n^2 s_B^2 + n_B^2)}{n^3}}} \quad (4)$$

where  $a(t)$  is the values of element  $t^{th}$  of the  $a$  and  $\bar{b}(t) = 1 - b(t)$  is complement of element  $b(t)$  of  $b$  respectively; and  $s_A, s_B$  is their standard deviations.

For the frequency variables and the non-negative number variables, in order to use equation (4) they must be normalized [14] in advance by equation (5)

$$\tilde{a}(w) = a(w) / \max_{w \in E} a(w). \quad (5)$$

When  $a(t)$  and  $\bar{b}(t)$  are binary variables then  $q_p(a, \bar{b}) = q(a, \bar{b})$ .

The implication rule  $a \rightarrow b$  is admissible at the level  $\alpha$  if and only if  $\varphi(a, b) \geq 1 - \alpha$  [14].

Formula (2) definition of the implication intensity reminds its users, that it is of implication intensity interest only on condition that it is greater than 0.50, that means its  $q(a, \bar{b})$  should be negative. It is, therefore, more significant for an implication index that is strongly negative for patterns  $a \rightarrow b$ .

### B. Implication Field

Let's consider the implication index  $q(a, \bar{b})$  in the four-dimensional space, in which a point  $M$  whose coordinates are the parameters associated with  $(n, n_A, n_B, n_{A\bar{B}})$ . Then  $q(a, \bar{b})$  is a scalar field by applying the mapping from space  $R^4$  to space  $R$ . The vector  $grad\ q(a, \bar{b})$  containing the partial derivatives of  $q(a, \bar{b})$  by the variables  $(n, n_A, n_B, n_{A\bar{B}})$  is a special gradient field also known as implication field because it meets the Schwartz criterion for the mixed partial derivatives [12] of  $q(a, \bar{b})$  for all pairs of variables  $(n, n_A, n_B, n_{A\bar{B}})$ . That means for any pair  $(n_B, n_{A\bar{B}})$  then the partial derivatives by  $n_B$  of partial derivatives of  $q(a, \bar{b})$  by  $n_{A\bar{B}}$  equal to the partial derivatives by  $n_{A\bar{B}}$  of partial derivatives of  $q(a, \bar{b})$  by  $n_B$  as equation (6)

$$\frac{\partial}{\partial n_B} \left( \frac{\partial q(a, \bar{b})}{\partial n_{A\bar{B}}} \right) = \frac{\partial}{\partial n_{A\bar{B}}} \left( \frac{\partial q(a, \bar{b})}{\partial n_B} \right) = \frac{1}{2} \left( \frac{n_A}{n} \right)^{-\frac{1}{2}} \left( \frac{n_B}{n} \right)^{-\frac{3}{2}} \quad (6)$$

and similarly for remaining pairs.

In terms of structure, the implication field is the four-dimensional space, consisting of ordered ordinate surfaces corresponding to the successive and ordered values of  $q(a, \bar{b})$  with respect to the variation of the cardinalities  $(n, n_A, n_B, n_{A\bar{B}})$  [12], [14]. Now, the implication index is considered as a function of four parameters  $(n, n_A, n_B, n_{A\bar{B}})$ , a line or surface of equipotential in implication field is curve in  $E$ . A space along which or in which, point a variable  $M$  maintains the same value of potential of  $q(a, \bar{b})$ . The surface of equipotential is orderly. The curve equation of this surface [12], [14], [18],

[19], [20], [21] is shown in equation (7)

$$q(a, \bar{b}) - \frac{n_{A\bar{B}} - \frac{n_A n_{\bar{B}}}{n}}{\sqrt{\frac{n_A n_B}{n}}} = 0. \quad (7)$$

Consequently, on such a curve, the scalar product between gradient of  $q(a, \bar{b})$  and partial derivatives of  $M$ ,  $grad\ q(a, \bar{b}).dM$ , is zero [12]. This is interpreted as indicating the orthogonality of the gradient with the tangent or the hyperplane tangent to the curve, that is to say the line or the equipotential surface.

By illustrating, the potential  $S$  depends only on two variables, for example  $n_A, n_B$ . Fig. 2 below shows the orthogonal direction of the gradient for different equipotential surfaces where the potential  $S$  does not change on each surface, but it changes from the surface  $S = 7$  to  $S = 10$ . Thus,

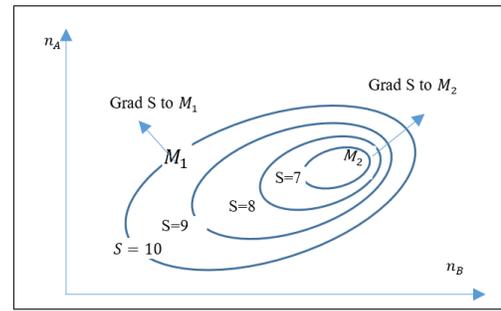


Fig. 2. Illustration on Cartesian Coordinates for an Implication Field.

implication field can be considered a space in which a set of equipotential surfaces corresponding to successive values of  $q(a, \bar{b})$  relative to the cardinals  $(n, n_A, n_B, n_{A\bar{B}})$  which one would vary. The various gradient fields, true “lines of force”, which are associated with them are orthogonal to the surfaces defined by the corresponding values of  $q(a, \bar{b})$  [12]. Behind this notion we can imagine a transport of information of variable intensity in a causal universe.

### C. Implicative Recommendation

SIA's original purpose is to analyze data for educational, psychological, and ontological applications [13], [14], etc. In recent years, however, attributable to recognize potential ability of SIA in recommender system techniques, there were several studies in recommender systems to improve their efficiency and have obtained remarkable results.

A typical proposal [7], [8], which has shown the potential of SIA to improve the performance of rule-based collaborative filtering recommender systems, however it also has a several disadvantages need to be addressed as (1) only processing on binary data, which leads to a problem to solve is the combinatorial explosion due to the binarization of non-binary data, (2) for models based on rules mining of these works, SIA is proposed in the post-processing stage of rules mining task, so they have not contributions considerably to limit the outcome rules' combinatorial explosion in large datasets. Another study using SIA to recommender systems [9], [10], which paid the attention to solve the problem on non-binary data and making some new contributions based on the recommendations

model with additional SIA metrics such as entropic version of implication intensity, cohesion, contribution, etc. This work is another proof show potential ability of SIA applying on recommender systems.

Most recently, SIA has also been proposed to recommender system models in the works [18], [19], [20], [21]. Accordingly, Nguyen *et al.* has contributed to overcome the shortcomings of previous studies following a new approach on SIA like reducing model's performance time, increasing predictions' accuracy, controlling generated rules set, compared to both traditional collaborative filtering model and former SIA model, by developing a recommender system based on implication rules mining (IRM) using implication variation measures.

In practice, research applying SIA to the development of recommender system models recently have made a positive contribution in this area, it can be seen as a potential research trend. However, in order to further improve the effectiveness of the recommendation models, there are still a few issues that need to be addressed as follows: (1) it is necessary to further mine the unique and outstanding features of the implication field such as equipotential planes, (2) the data sets for the recommendation models are mostly sparse, therefore, using cross k-folds evaluation for recommendation models by partitioning the data set by transactions is not optimal yet, because this will lead to limit number of known items (given items) in test sets, this can significantly affect to model's training quality, (3) using measures of accuracy of the predictions and classifications to evaluate the recommendation models is not enough yet, because in recommender systems, the position of items in the recommendation list is also important, therefore, it is necessary to use additional measures of items' position ranking in recommendation list.

### III. RECOMMENDATION MODEL

#### A. Model

The implication field and its particularly features, as shown in Section II-B, have opened a great potential for the implementation of recommendation models. In this paper, the implication field-based recommender system has been proposed to include the following components as shown in Fig. 3. This model has been experimentally proven on both binary and non-binary datasets to be more efficient than the traditional collaborative filtering models exploiting the association rules on both binary and quantitative data. The main components of the model include the following.

The implication field algorithms include two newly proposed algorithms. The first is responsible for generating the implication field consisting of a set of equipotential surfaces as discussed in Section II-B, This algorithm uses one of the implication variation measures. These measure are presented in Table III. They include four for implication index variation (first four rows) and four for implication intensity variation (four rows later) by  $n, n_A, n_B$ , and  $n_{A\bar{B}}$ . These SIA measures are determined as sum of the implication index (or implication intensity) and the partial derivative of the implication index (or implication intensity) by the variables  $n, n_A, n_B$ , and  $n_{A\bar{B}}$ , and SIA knowledge to generate the implication field, that is composed of a set of equipotential surfaces, from dataset. The second mines frequent implication patterns on

equipotential surfaces to provide recommendations to users. It makes personal recommendation by frequent implication pattern mining on equipotential surfaces in given threshold implication index (or implication intensity) for predicting and a recommendation the items or the top  $k$  items list to users. These algorithms will be shown in Section III-B.

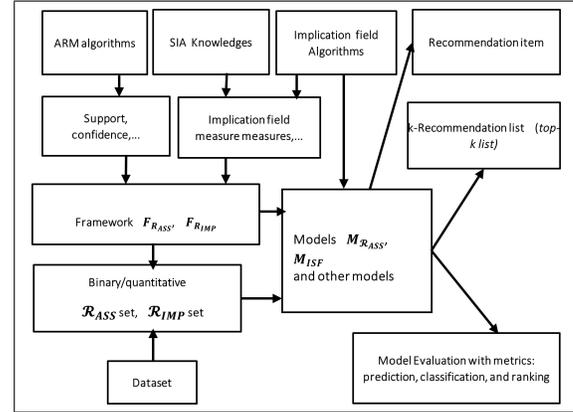


Fig. 3. The Overall Structure of Recommendation Model based on Implication Field.

In Fig. 3, The models  $M_{R_{ASS}}$ , (Model for Association), and  $M_{ISF}$ , (Model for Implication Statistical Field), are recommendation model based on ARM, and IRM respectively in implication field. These models include a set of association rules  $R_{ASS}$  or implication rules  $R_{IMP}$  and framework for association rules mining  $F_{R_{ASS}}$ , or implication rules  $F_{R_{IMP}}$  correspondingly [20], [21]. They are shown in equations (8) and (9)

$$M_{R_{ASS}} = \{X \mid R_{ASS}, F_{R_{ASS}}\}, \quad (8)$$

$$M_{ISF} = \{X \mid R_{IMP}, F_{R_{IMP}}\}, \quad (9)$$

where  $R_{ASS}$  and  $R_{IMP}$  are respective association rules set and implication rules set. Each of which is expressed by 4-tuples  $(n, n_A, n_B, n_{A\bar{B}})$  meeting the constraints as are defined as equation (10) and (11), respectively, where  $s$  (support),  $s_{min}$  (minimum support threshold),  $c$  (confidence),  $c_{min}$  (minimum confidence threshold),  $imp$  (a given SIA measures), and  $imp_{min}$  (minimum threshold of a given SIA measure) are support, confidence, and one of SIA measures (see Table III), and their respective minimum thresholds.

$$R_{ASS} = \left\{ (n, n_A, n_B, n_{A\bar{B}}) \left| \begin{array}{l} n_A \leq n, n_B \leq n, \\ \min(0, n_A + n_B - n) \\ \leq (n_A - n_{A\bar{B}}) \leq \\ \max(n_A, n_B), \\ s_{min} \leq s, c_{min} \leq c \end{array} \right. \right\}, \quad (10)$$

$$R_{IMP} = \left\{ (n, n_A, n_B, n_{A\bar{B}}) \left| \begin{array}{l} 0 \leq n_A \leq n_B \leq n, \\ 0 \leq n_{A\bar{B}} \leq n_A, \\ s_{min} \leq s, c_{min} \leq c, \\ imp_{min} \leq imp \end{array} \right. \right\}. \quad (11)$$

TABLE III. FAMILY OF VARIATION IMPLICATION MEASURES OF IMPLICATION RULES MINING FRAMEWORK

No	SIA Measures	Formulas
1	$q_n(a, b)$	$q(a, \bar{b}) + \frac{1}{2\sqrt{n}}(n_{A\bar{B}} + \frac{n_A n_B}{n})$
2	$q_{n_A}(a, \bar{b})$	$q(a, \bar{b}) - \frac{1}{2} \frac{n_{A\bar{B}}}{\sqrt{\frac{n_B}{n}}} (\frac{n_A}{n})^{\frac{3}{2}} - \frac{1}{2} \sqrt{\frac{n_B}{n_A}}$
3	$q_{n_B}(a, \bar{b})$	$q(a, \bar{b}) + \frac{1}{2} n_{A\bar{B}} (\frac{n_A}{n})^{-\frac{1}{2}} (n - n_B)^{-\frac{3}{2}} + \frac{1}{2} (\frac{n_A}{n})^{-\frac{1}{2}} (n - n_B)^{-\frac{1}{2}}$
4	$q_{n_{A\bar{B}}}(a, \bar{b})$	$q(a, \bar{b}) + \frac{1}{\sqrt{\frac{n_A(n - n_B)}{n}}}$
5	$\varphi_n(a, b)$	$\varphi(a, b) + \frac{1}{\sqrt{2\pi}} \int_{q(a, \bar{b})}^{q_n(a, \bar{b})} e^{-\frac{t^2}{2}} dt$
6	$\varphi_{n_A}(a, b)$	$\varphi(a, b) + \frac{1}{\sqrt{2\pi}} \int_{q(a, \bar{b})}^{q_{n_A}(a, \bar{b})} e^{-\frac{t^2}{2}} dt$
7	$\varphi_{n_B}(a, b)$	$\varphi(a, b) + \frac{1}{\sqrt{2\pi}} \int_{q(a, \bar{b})}^{q_{n_B}(a, \bar{b})} e^{-\frac{t^2}{2}} dt$
8	$\varphi_{n_{A\bar{B}}}(a, b)$	$\varphi(a, b) + \frac{1}{\sqrt{2\pi}} \int_{q(a, \bar{b})}^{q_{n_{A\bar{B}}}(a, \bar{b})} e^{-\frac{t^2}{2}} dt$

$F_{RASS}$  is framework of ARM [20], [21], including famous ARM algorithm, *a priori*, was proposed by [11], and measures support ( $s$ ), confidence ( $c$ ) meeting the constraints  $s \geq s_{min}$ , and  $c \geq c_{min}$  as are defined as equation (12) and  $F_{RIMP}$  is frameworks of IRM [20], [21], including IRM algorithms (see details in Section III-B following), and measures support, confidence, and ASI measures as defined in Table III meeting the constraints as are defined as equation (13)

$$F_{RASS} = \left\{ \left( \begin{array}{l} ARM\ algs, \\ supp\ s, conf\ c \end{array} \right) \left| \begin{array}{l} n_A \leq n, n_B \leq n, \\ \min(0, n_A + n_B - n) \\ \leq (n_A - n_{A\bar{B}}) \\ \leq \max(n_A, n_B), \\ s_{min} \leq s, c_{min} \leq c \end{array} \right. \right\} \quad (12)$$

$$F_{RIMP} = \left\{ \left( \begin{array}{l} IRM\ algs, \\ supp\ s, conf\ c, \\ SIA\ measure\ imp \end{array} \right) \left| \begin{array}{l} 0 \leq n_A \leq n_B \leq n, \\ 0 \leq n_{A\bar{B}} \leq n_A, \\ \min \leq s, c_{min} \leq c, \\ imp_{min} \leq imp \end{array} \right. \right\} \quad (13)$$

The evaluation models are designed for testing and evaluating recommendation models and they will be presented details in section III-C following, and then they are used in experiments of sections IV-D and IV-E.

### B. Algorithms

To generate the list of recommendations, the implication field-based recommendation system model focuses on the IRM algorithm including two phases. The first is to generate the implication field from the dataset, in this phase the IFGEN algorithm will be used to generate produce a set of equipotential planes for potential implication values, based on the variation of one of the four variables ( $n, n_A, n_B, n_{A\bar{B}}$ ). The second uses MAKEIFREC algorithm to mine implication patterns of

equipotential planes to generate a list of recommended items for the user.

### Algorithm IFGEN (Implication fields Generator)

**Input:** a dataset; the thresholds of confidence, support and an implication field measure; type of data (binary/quantitative).

**Output:** Implication rule set.

**Step 1:** Constructing implication field measure, defined as in the Table III.

**Step 2:** Generating the implication rules set from the dataset using a data mining algorithm (such as Apriori, Eclat, etc.) and the thresholds of support, confidence and implication field measure that is defined in step 1. Note that: if data is in binary form,  $q(a, \bar{b})$  is computed by equation (2); if the data is in quantitative form,  $q(a, \bar{b})$  is computed by equation (4) and (3).

**Step 3:** Presenting each implication rules by four values  $n, n_A, n_B$ , and  $n_{A\bar{B}}$  as well as its values according to the measures such as support, confidence, implication index, implication intensity, and implication field measures as shown in Table III.

With the algorithm IFGEN, the generated implication rules will be more accurate because of the high examples (from support /confidence measures) and low counterexamples (from the statistical implication measure). This will be confirmed in the Section IV.

**Algorithm MAKEIFREC** (making implication field recommendation).

**Input:** a dataset; the thresholds of confidence, support, and an implication field measure; type of data (binary/quantitative).

**Output:** predicting item or the list of top k items to be recommended to users.

**Step 1:** calling the IFGEN algorithm for generating the set of equipotential surfaces in implication rules.

**Step 2:** mining frequent implication patterns in equipotential surfaces for predicting and returning the recommendation result (1 item or k items) to users.

### C. Evaluation

Normally, to evaluate a machine learning model, evaluating procedures divide the dataset into a training set and test set based on transactions. In recommender systems, however, that can get a weaknesses for sparse datasets which have some transactions with very few users' rating, this leads to the maximal number of items to keep (*given*) on known set is limited considerable because it cannot be greater than the number of rated items on any transaction in dataset, see example in Fig. 4, because there are only two rating in transaction  $u_6$ , we cannot set  $given \geq 2$ . This could lead to limit learning ability considerably and therefore quality of recommendation model will be not good. Moreover, some of the proposed models only focus on processing the binary data and try to binarize the non-binary datasets [7], [8], [9]. This could be the main cause to the accuracy of recommendation models to be affected.

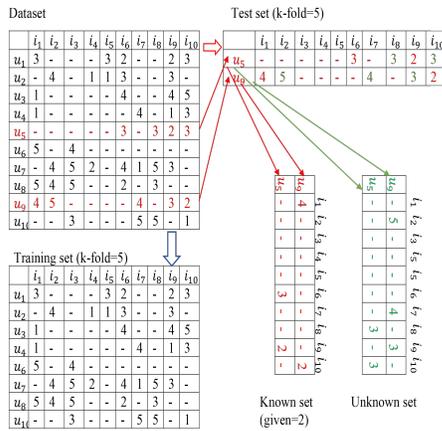


Fig. 4. An Example about Typical Partition Data Method.

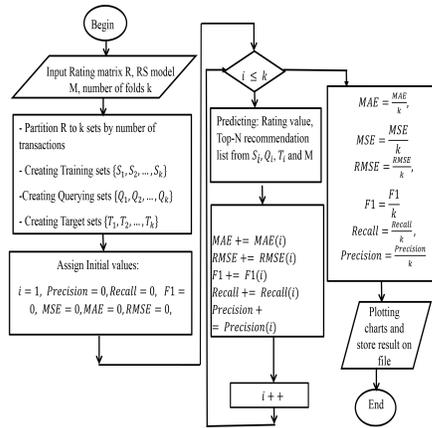


Fig. 5. Flowchart of Algorithm for Evaluation Recommendation Model.

In addition, see flowchart of evaluation model algorithm in Fig. 5, the recommended evaluation measures used in [9], [10] focus on only two main groups, the first is the accuracy of the ratings such as  $MAE$ ,  $MSE$  and  $RMSE$  [4], [6] to determine the accuracy of the prediction ratings are missing and the second group is predictive predictions such as  $precision$ ,  $recall$ , and  $F1 - score$  [4], [6], which focus on introducing items that are useful to the user and helping them make the right decision. These metrics, however, have a major downside: they are concerned with the entire dataset rather than top-N recommendation lists. Therefore, it is not easy to assess accurately the recommender systems when comparing the list of items recommended to the list of relevant items, because the metrics do not focus on the identification of rank and position of an item in the list.

In practice, good recommender systems are not only interested on how many relevant results they give, they also want to give users with a good order. They need to be able to put relevant items remarkably high up the list of recommendations. Most probably, the users will not scroll through hundreds of items to find favorite item they like. Take now famous

searching engines like Google \*, Bings † as an example, it is evident that they prioritize relevant query results in some sort of descending order. Therefore, it is necessary to need metrics of ranking awareness properly to select recommender systems that can solve major aims: (1) Where position of item that recommender system suggests is in list of recommendation result, (2) how good recommender system could solve in modeling users' relative preference.

To overcome this shortcoming of the recommender system model, two suggestions are given for improving the evaluation quality of the recommender system.

The first, in terms of dataset partitioning method for evaluating, the dataset that has  $n$  transactions and  $m$  items can be partitioned into two sets of training and testing based on number of items ranked per transaction instead based on numbers of transaction on dataset.

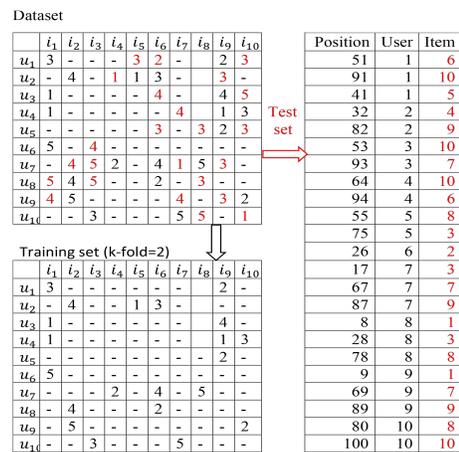


Fig. 6. An Example of Proposed Data Partition Method.

Accordingly, for each transaction, items will be randomly partitioned into  $k$  folds:  $n \times (k - 1)/k$  items for training set and  $n/k$  items for testing set. In Fig. 6, dataset's items are partitioned in 2 folds randomly (for simplicity in illustration), in which items for test set are presented in red, (remained items in black for training set). In this way the training and testing sets are formed from all transactions, which means that all transactions are involved in both the training and testing set, and the number of items per sets are  $(k - 1) \times n/k$  and  $n/k$  percent of items' dataset correspondingly. A problem in test set's presentation is that it will be very sparse compared to the dataset. In order to save memory and time for manipulation, a good suggestion that using one-dimension array namely positions for storing position of all items in test set where  $0 < position[k] < n \times m$ . Accordingly, the row  $i$  and column  $j$  of an item are defined respectively as follows the quotient +1 and the remainder in  $\frac{position}{n}$ , if  $quotient = m$  then  $(i, j) = (n, m)$ . For instance, in Fig. 6 position[1]= 51 means that transaction of user  $u_1$  rated item  $i_6$  (since the remainder of  $51/10$  is 1, and the quotient of  $51/10$  plus 1 is 6). It is apparent that items in the training and testing set are

\* <https://www.google.com/>

† <https://www.bing.com/>

extracted from all transactions of the dataset, which makes better model testing and training. Moreover, this approach also fixes the shortcoming of k-fold partitioning based on transaction because the number of items retained to build a training model that is no longer limited to the minimum number of items per transaction in dataset.

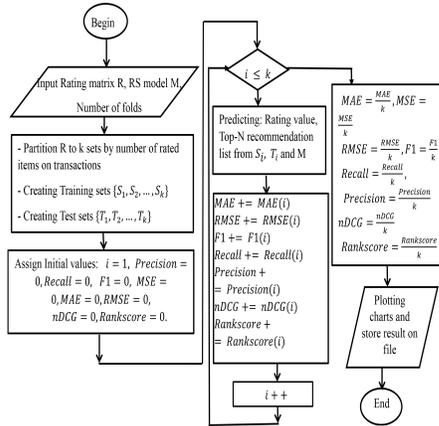


Fig. 7. Proposed Algorithm Flowchart to Improve Recommendation Model.

In addition, due to the way of partitioning the dataset by items on each transaction, it is not necessary to create the unknown and know set from the test set as in transaction-based dataset partitioning way.

The second, in relation to using of evaluating measures, besides predicting-based and classifying-based precision evaluating metrics, the ranking-based ones are also suggested to evaluate more comprehensively the recommendation list's quality. Although there are many metrics of this type like *MRR*, *MAP*, *nDCG* and *Rankscore* [4], [6], only *nDCG* and *Rankscore* are suggested because they can be used to deal with both binary and none-binary dataset.

Finally, these proposals are presented in the algorithm as shown in Fig. 7. This is a revision of algorithm in Fig. 5 based on two major changes, that is using a new method for dataset partition based on number of ranked items per transaction and adding measures *nDCG* and *Rankscore* measures. These are the major changes for improving the efficiency and quality of the recommended system as discussed in the following experiments.

#### IV. EXPERIMENT

##### A. Datasets

Using collaborative filtering based-on implication field recommendation model described above, we conduct experiments on both the binary dataset (MSWeb)<sup>‡</sup> and the quantitative dataset (MovieLens)<sup>§</sup>. The MSWeb dataset is created by sampling and processing the www.microsoft.com logs of 38.000 anonymous, randomly selected users in one-week timeframe. For each user, the dataset lists all the areas of the web site

(Vroots) that user visited in a one-week timeframe in February 1998. This dataset contains 32710 valid users and 285 Vroots. The MovieLens dataset collected by GroupLens consists of 100.000 ratings made by 943 users for 1.682 films. The ratings range from 1 to 5 corresponding to from the lowest to the highest.

To serve the experiment to be more accurate, the datasets are preprocessed by:

**Normalization of data:** Users who rank high (or low) for all their films/Vroots depending on the individual can lead to bias. Eliminate this effect by normalizing the data so that the average rating of each user is the same scale.

**Selecting relevant data:** Ignoring data can lead to bias and to speed up computation, by not interested in the films/Vroots has had only a few times, because the ratings of these films/Vroots may be subject to bias due to lack of data, and users rated only a few films because their ratings may be biased.

Using k-fold cross validation method (with k=5 for this paper): to avoid overfitting problems as well as to get better accuracy as for each model evaluation. The dataset (MovieLens or MSWeb) is split into equal sized k-fold to build training set (using k-1 fold) and test set (using remaind fold) by the number of ratings on transaction instead of by number of transactions on dataset to overcome the limitations as analyzed in Section III-B.

##### B. Tool

The experiments were performed on implication field RS tools developed in the R language<sup>¶</sup>. This tool is developed for making, performing, and evaluating models of recommender system based on implication field as described in Section III-A. In addition, it can build and run other collaborative filtering-based recommender systems for mutual comparison and evaluation. The SIA measure is used for  $F_{RIMP}$  is  $\varphi_{n_{AB}}(a, b)$ .

##### C. Analyze Equipotential Surfaces in Implication Field

1) *Experiment Description:* To analyze the implication field as a set of equipotential planes, In this experiment, the Implication field-based recommender system model was performed on the MovieLens non-binary dataset that was described in Section IV-A, on the  $F_{imp}$  (minsup = 0.1, minconf = 0.3,  $\min\varphi_{n_{AB}}(a, b) = 0.5$ ).

2) *Results and Discussions:* Results are presented in Fig. 8 and 9, they are presented in the form of 3D scatter and 3D graph, representing equipotential surfaces with a warm color (red) that is common in the implied intensity range of 0.8 to 1.0, and the remaining scattered is the equipotential surfaces have the implication intensity decreasing by the gradual cold color (blue).

In Fig. 10, contour form, accordingly, the implication field with equipotential surfaces has a variable value spectrum of implication intensity concentrated in the range 0.8 to 1 represented by the gray spectrum and the remainder is

<sup>‡</sup><https://grouplens.org/datasets/movielens/100k/>

<sup>§</sup><https://kdd.ics.uci.edu/databases/msweb/msweb.html>.

<sup>¶</sup><https://www.r-project.org/about.html>

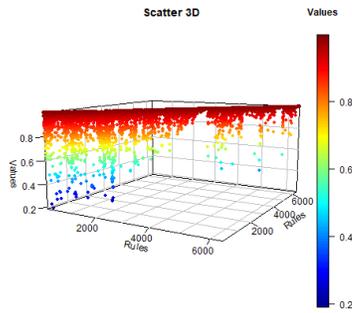


Fig. 8. Implication Field and Its Equipotential in Scatter 3D.

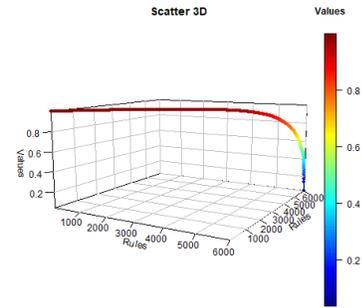


Fig. 11. The Implication Variation in the Implication Field.

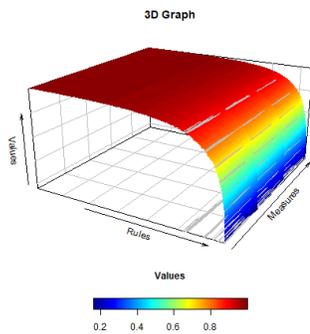


Fig. 9. Implication Field and Its Equipotential in Graph 3D.

represented by the gradual transition color spectrum green. Fig. 11, the implication intensity variation on the equipotential surfaces presented in 3-dimensional form, it is easy to see that the implication samples with high implication intensity are concentrated on warm colored equipotential surfaces and rapidly decrease. in the low intensity region is represented by blue. The common recommendations will be filtered on high intensity equipotential surfaces, whereas those for specific, rare items will be provided in low implication equipotential surfaces.

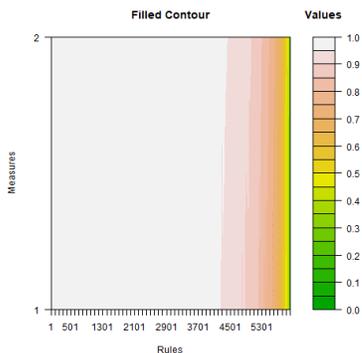


Fig. 10. Implication Field and Its Equipotential in Contour.

#### D. Scenario 1. Comparing with Traditional Recommendation Models

1) *Experiment Description:* In this experimental scenario, the recommender system model based on the implication statistical field (ISFRS), is compared with the traditional collaborative filtering recommendation models based on user for both Cosine (UBCF\_cRS) and Pearson measures (UBCF\_psRS), and collaborative filtering recommendation models based on item for both Cosine (IBCF\_cRS) and Adjusted Cosine measures (IBCF\_acRS), The data set used in this experiment is the Movielens non-binary data set described in Section IV-A. For the collaborative filtering models to have good results, a problem needs to face is how to choose the number of neighbors best, we try to experiment on many neighbor k parameters for these models including k=2, 5, 10, and 15, and finding that k = 15 is better than other values. Moreover, dataset partitioning for training and testing is conducted based on number of items in transactions instead of numbers of transaction. Recommendation models were experimented on two groups' measure: classification and ranking.

2) *Results and Discussions:* The first, models were experimented on classification measures, on ROC curve, precision/recall, F1, The results are shown in Fig. 12 to 14. As a result, the ISFRS model is the best, next is the collaborative filtering model based on user using both Pearson and cosine measures, and finally weakest model is item-based collaborative filtering model (in case of both Pearson and adjusted cosine measures).

The second, models were experimented on ranking measures, on  $nDCG$  and  $Rankscore$ . The results, have presented in Fig. 15 and 16, also show the preeminence of the ISFRS model over the collaborative filtering model, which is the same as the case of the group of classification measures that is discussed above.

These result in this experiment shows the contribution of both the proposed ISF RS model and the proposed data partitioning method to evaluation in improving the model's classification and ranking capability and training quality compared to the recommended models based on traditional collaborative filtering.

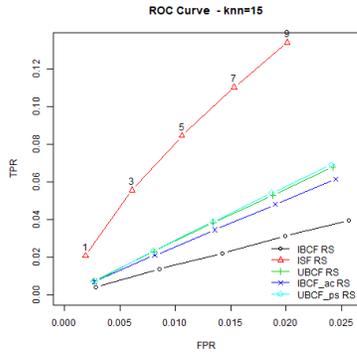


Fig. 12. ROC Curve of ISF Model and CF others, k=15.

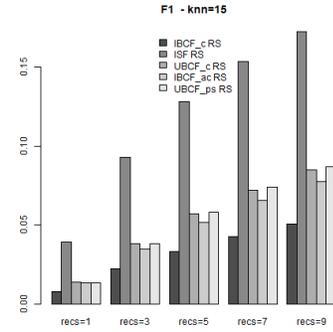


Fig. 14. F1 of ISF Model and CF others, k=15.

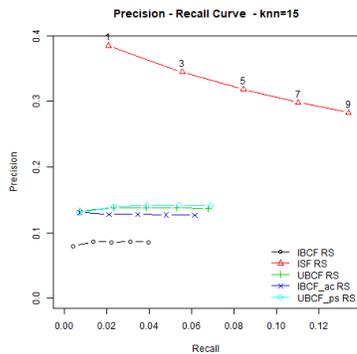


Fig. 13. Precision/ Recall of ISF Model and CF others, k=15.

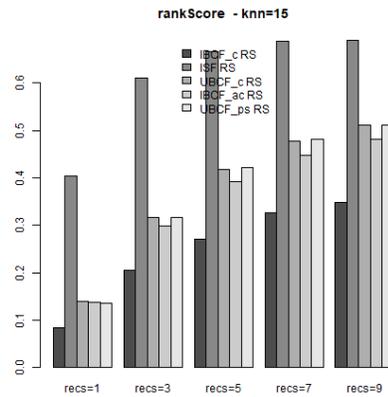


Fig. 15. RankScore of ISF Model and CF others, k=15.

### E. Scenario 2. Comparing with Implicative Recommendation Models

1) *Experiment Description:* In this experimental scenario, the MSWeb binary data set is used to compare the implication statistical field recommender system (ISFRS) model with two other SIA models that was reviewed in Section II-B including works in [7], [8] (Implication index and intensity - IIRS) and [9], [10] (Phi-Cohesion- Gamma- PCGRS) on two types of measure. Reason that MSWeb is chosen to use in this experiment instead of Movielens as in previous one is attributable to models in [7], [8] was designed and performed on binary dataset only as mentioned in Section II-C. In addition, to get more precision results, dataset partitioning for training and testing sets is conducted based on number of rated items in transactions instead of numbers of transaction.

2) *Results and Discussions:* The first is classification measures including precision/ recall, ROC, F1, experimental results show the preeminence of IFS RS recommendation model compared to PCG RSmodel and IIRS model, in which the weakest is the model IIRS on all 3 evaluation measures, as shown in Fig. 17 (for Recall/Precision), Fig. 18 (for ROC curve), Fig. 19 (for F1).

The second is ranking measures, the experimental results, were shown in Fig. 20 (for RankScore) and Fig. 21 (for nDCG), are quite similar to the results on the group of classification measures. This means that the ISFRS model has the best

results ranking items according to the nDCG and RankScore indicators, followed by the PCGRS model and the worst is the IIRS model.

This indicates that recommender system based on the implication statistical field has ability better on both classification and ranking compared to previous recommendation model based on SIA applying. The experiment proofed that proposed ISFRS resolved three problems of recommender systems based on applying SIA previously as mentioned in Section II-B. Therefore, it is apparent that it is a new and promising trend in applying statistical implication analysis theory to the recommender systems domain.

### V. CONCLUSION

In order to ensure relevance and novelty for recommender systems, its proposal has to be personalized enough to meet the user's personal preferences and deep enough to make a pleasant surprise for the user. In this regard, the paper has proposed a novel recommendation model based on the implication field to significantly improve the quality of the recommender system compared to the traditional collaborative filtering-based recommender systems. The second contribution of the paper is to propose a new data set partitioning method to build training and test sets to build and train the recommendation model,

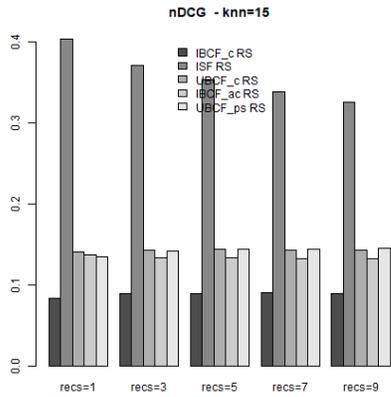


Fig. 16. nDCG of ISF Model and CF others, k=15.

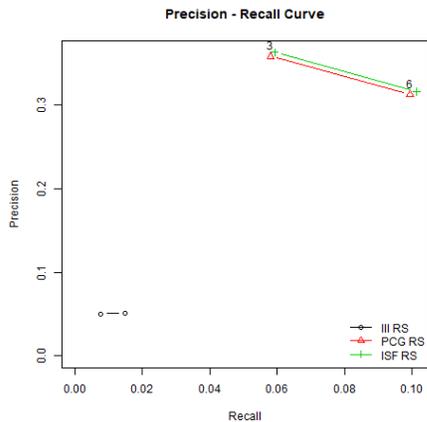


Fig. 17. Precision/Recall of ISF Models and others in SIA.

based on the rating ratio per transaction instead of based on the number of transactions, which overcomes the limitation of sparse datasets in recommender systems, making them more likely to recommend accurately. Another contribution to this paper is to propose metrics that provide a more in-depth assessment of the quality of recommendations. In addition to the metrics for precision of classification like precision, recall, and F1, metrics for rank score were also added that evaluate the relevance of recommendations like nDCG and Rankscore and using them to compare among different models. This helps evaluate outputs' quality of recommendation models more comprehensively as shown in the experimental results. Finally, this paper also aggregates and compare the effectiveness of the works existing SIA-based recommendation systems, experiment's results showing that the application of the implication variation tendency in the implication field is the most satisfactory result in all these recommender systems.

From these results, it is clear that the exploitation of the relationships between variables (objects/ individuals/ attributes/ items) in the form implication rules in the implication field has achieved positive results for recommender systems. Therefore,

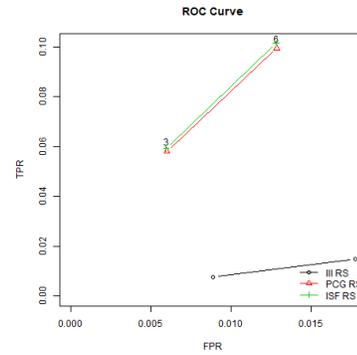


Fig. 18. ROC Curve of ISF Models and others in SIA.

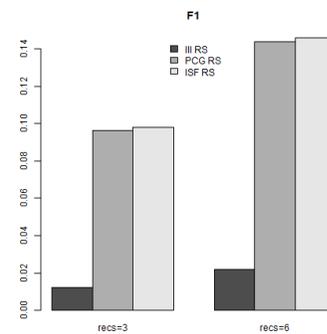


Fig. 19. F1 of ISF Models and others in SIA.

the study to extend further these relationships in the form between rules or/and between rules and variables in the implication field and exploitation them to further improve the effectiveness of the recommendation system is a promising one in the future.

## REFERENCES

- [1] Adomavicius Gediminas, Tuzhilin Alexander, Toward the Next Generation of Recommender Systems: A Survey of the State-of-the-Art and Possible Extensions, *IEEE Transactions on Knowledge and Data Engineering*, Vol.17 No.6, pp.734-749, 2005.
- [2] Ahmed Mohammed K. Alsalama, "A Hybrid Recommendation System Based On Association Rules", *International Science Index, Computer and Information Engineering Vol:9, No:1*, pp.55-62, 2015.
- [3] Francesco Ricci, Lior Rokach and Bracha Shapira, *Introduction to Recommender Systems Handbook*, Springer-Verlag and Business Media LLC, pp.1-35, 2011.
- [4] Guy Shani, Asela Gunawardana, "Evaluating Recommendation Systems", *Recommender System Handbook*, Springer, pp.257-297, 2010.
- [5] Gavin Shaw, Yue Xu and Shlomo Geva, "Using Association Rules to Solve the Cold-Start Problem in Recommender Systems", *Advances in Knowledge Discovery and Data Mining*, pp.340-347, 2010.
- [6] Herlocker J.L et al. "Evaluating collaborative filtering recommender systems". *ACM Transactions Information System*, vol. 22, no. 1, pp.5-53, 2004.
- [7] Nghia Quoc Phan, Phuong Hoai Dang, Hiep Xuan Huynh, "Collaborative recommendations based on statistical implication rules", *Journal of Computer Science and Cybernetics*, Vol. 33, No. 3, pp.247-262, 2017.

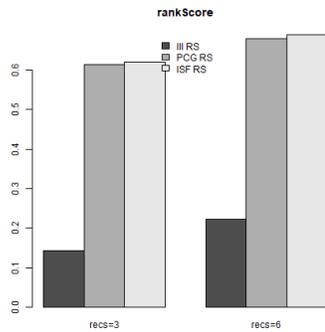


Fig. 20. Rankscore of ISF Model and others in SIA.

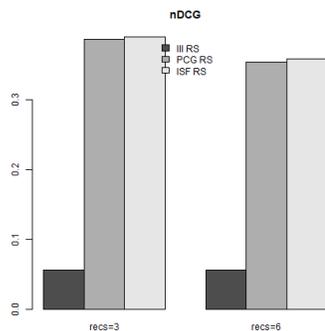


Fig. 21. nDCG of ISF Models and others in SIA.

[8] Nghia Quoc Phan, Ky Minh Nguyen, Hoang Tan Nguyen, Hiep Xuan Huynh, "The recommendation system is based on association rules and statistical implication measures". *Proceedings of The 8th National Conference on Fundamental and Applied IT Research – (FAIR'15)*; Natural Science and Technology Publishing House, pp.297-308, 2015.

[9] Lan Phuong Phan, Hung,Huu Huynh, Hiep , Xuan Huynh, "Recommendation using Rule based Implicative Rating Measure", *International*

*Journal of Advanced Computer Science and Applications (IJACSA)*, pp.176-181, 2018.

[10] Lan Phuong Phan, Hung Huu Huynh, Hiep Xuan Huynh, "Recommender systems based-on implication intensity and contribution measure", *Proceedings of the X National Conference on Fundamental and Applied IT Research (FAIR18)*; Natural Science and Technology Publishing House, pp.256-274, 2017.

[11] Rakesh Agrawal, Ramakrishnan Srikant, "Fast algorithms for mining association rules", *Proceedings of the 20th International Conference on Very Large Data Bases*, p.487-499, 1994.

[12] Régis Gras, Pascale Kuntz and Nicolas Greffard, "Notion of implicative field in implicative statistical analysis", *The 8th International Meeting on Statistical Implicative Analysis*, Tunisia, pp.1-21, 2015. (in French)

[13] Régis Gras, Raphael Couturier, "Specificities of Implicative Statistical Analysis (A.S.I.) compared to other quality measures of association rules", *Quaderni di Ricerca in Didattica - GRIM (ISSN on-line 1592-4424)*, pp.19-57, 2010. (in French)

[14] Régis Gras, Einoshin Suzuki Fabrice Guillet, Filippo Spagnolo (Eds.), *Statistical Implication Analysis - Theory and Application*, Springer Verlag, 2008.

[15] Timur Osadchiy, Ivan Poliakov, Patrick Olivier, Maisie Rowland, Emma Foster,"Recommender system based on pairwise association rules", *Expert Systems with Applications 115*, pp.535–542. 2018.

[16] Tzung-Pei Hong, Chun-Hao Chen, Yeong-Chyi Lee, and Yu-Lung Wu., "Trade-off between computation time and number of rules for fuzzy mining from quantitative data", *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, pp.587-604,2001.

[17] Tzung-Pei Hong, Chun-Hao Chen, Yeong-Chyi Lee, and Yu-Lung Wu, "Genetic-Fuzzy Data Mining with Divide-and-Conquer Strategy", *IEEE Transactions on Evolutionary Computation*, pp.252-265, 2008.

[18] Hoang Tan Nguyen, Hung Huu Huynh, and Hiep Xuan Huynh, "Collaborative filtering recommendation with threshold value of the equipotential surface in implication field", *Second ACM International Conference on Machine Learning and Soft Computing*, pp.39-44,2018.

[19] Hoang Tan Nguyen, Hung Huu Huynh, and Hiep Xuan Huynh, "Collaborative Filtering Recommendation in the Implication Field", *International Journal of Machine Learning and Computing, Volume 8 Number 3*, pp.214-222, 2018.

[20] Hoang Tan Nguyen, Lan Phuong Phan, Hung Huu Huynh, Hiep Xuan Huynh, "Recommendation with quantitative implication rules", *EAI Endorsed Transactions on Context-aware Systems and Applications, Volume 6 , Issue 16*, pp.1-8, 2019.

[21] Hoang Tan Nguyen, Lan Phuong Phan, Hung Huu Huynh, Hiep Xuan Huynh , "Improved collaborative filtering recommendations using quantitative implication rules mining in implication field", *ICMLSC 2019: Proceedings of Third ACM International Conference on Machine Learning and Soft Computing*, pp.110–116, 2019.

# Taxonomy of Cybersecurity Awareness Delivery Methods: A Countermeasure for Phishing Threats

Asma A. Alhashmi<sup>1</sup>, Abdulbasit Darem<sup>2</sup>, Jemal H. Abawajy<sup>3</sup>

Department of Computer Science, Northern Border University, Arar 91431, Saudi Arabia<sup>1,2</sup>  
Cybersecurity Research and Innovation Centre, Deakin University, Burwood, VIC 3217, Australia<sup>3</sup>

**Abstract**—Phishing is a serious threat to the Internet users and has become a vehicle for cybercriminals to perpetrate large-scale crimes worldwide. A wide range of technical and educational measures have been developed and used to address phishing threats. However, the technical anti-phishing measures have been widely studied in the current literature whereas comprehensive analysis of the non-technical anti-phishing techniques has generally been ignored. To close this gap, we develop a new taxonomy of the most common cybersecurity training delivery methods and compare them along various factors. The work reported in this paper is useful for various stakeholders. For organizations conducting or considering phishing training, it helps them understand the various awareness training and phishing campaigns capabilities and design an appropriate program with a meaningful return. For researchers, it offers a clearer understanding of the main challenges, the existing solution space, and the potential scope of future research to be addressed.

**Keywords**—Phishing attack; human factors in cybersecurity; cybersecurity threats; cybersecurity awareness; anti-phishing awareness delivery methods

## I. INTRODUCTION

Internet technology coupled with advances in mobile devices such as smartphones have enabled regular every-day people to learn, work, purchase, entertain, connect, and network from anywhere and at any time. With the increasing reliance on the Internet, so is the threat of being falling a victim to cybersecurity attacks. Cybercrime is the fastest growing crime worldwide and continue to increase in sophistication and costs to the global economy with an estimated \$6 trillion by 2021 [4]. Phishing is the most prominent attack vector used by cyber criminals today and phishing prevalence is at all-time high [5]. Phishing impacts online users and organisations of all size and sectors including banks and public services. The financial costs to victims due to phishing attacks worldwide are staggering and currently estimated to surpass a trillion dollars [38]. In the U.S. alone, the financial costs to businesses between 2013 and 2019 are estimated to be more than \$10 billion [17]. With phishing attacks accounting close to 90% of the estimated cybercrime costs [10], there is a substantial economic benefit for putting in place appropriate anti-phishing measures to fight phishing threats. As a result, a serious effort to combat phishing threats has been pursued both in academia and industry.

Various technical measures have been proposed in the literature to address phishing threats. These automated anti-phishing measures include email filtering [1,7], machine

learning based techniques to identify phishing emails and websites [20], and browser security indicators that warn end-users potential dangers from malicious email messages and fake websites [23]. Although automated anti-phishing solutions are powerful defence, phishing attacks remain a significant threat to individuals and businesses currently accounting for more than 80% of reported security incidents [24]. Moreover, it takes 32 days on average for technical countermeasures to detect and mitigate phishing attacks [42]. In addition, cybercriminals continue to become more creative and changing tactics to get around the anti-phishing measures in place and sending much more plausible-looking phishing messages [39]. Therefore, despite considerable advances in anti-phishing technical solutions, the automated anti-phishing measures are still inadequate to combat phishing threats [33].

Cybercriminals are increasingly shifting from exploiting software and hardware vulnerabilities to depending on human weaknesses to perpetrate an attack on individuals and businesses. For phishing threats to be realised, the cyber attackers must first institute a trust with the potential victims. This means automated solutions alone do not provide complete safeguard against phishing attacks. Since phishing attacks primarily exploit human vulnerability, human intelligence based anti-phishing approach is the best defence to narrow the gap left by technical measures. Therefore, intervention programs that improve human awareness and security behaviour have been developed to augment the technical solutions. These intervention programs implement different delivery methods to build vital security awareness skills and changes both awareness and behaviour of the end users.

This paper provides a new taxonomy of the most common cybersecurity training delivery methods developed to train the workforce to protect themselves from phishing threats. Second, we will survey and critically analyse a variety of phishing awareness delivery methods based on the taxonomy we developed with emphases on those that focus on what delivery methods are effective in increasing the ability of the people to detect and mitigate phishing threats. This provides useful information that will enable organisations to explore various alternatives when conducting workforce security awareness training. Third, existing literature does not provide bases for future researchers to build on in the cybersecurity awareness training sphere [14]. There are state-of-the-art reviews on various aspects of the technical solutions for phishing attack [1,3,6,8,12,19,27-28,36,43]. However, there is no work to the best of our knowledge that has conducted a review of the

Grant no. SAT-2018-3-9-F-7926 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.).

literature about cybersecurity awareness training methods. Therefore, this study is useful for future researchers interested in developing human intelligence based anti-phishing countermeasures to combat phishing threats.

This paper is structured as follows: Section 2 presents phishing awareness techniques and the taxonomy of the delivery methods. Comparison of the delivery methods along various factors is also presented. Section 4 presents some open problems for future research. Section 5 discusses the conclusions.

## II. ANTI-PHISHING CYBERSECURITY INTERVENTION PROGRAMS

Cybercriminals are increasingly targeting employees across all sectors to infiltrate corporate networks to steal confidential client data and corporate secrets. Phishing attempts that normally evaded detection by the technical measures put in place are often recognized and reported by employees [11]. Therefore, fortifying end users to defend themselves against phishing threats through cybersecurity intervention program such as phishing awareness training is necessary to thwart phishing attacks.

### A. Cybersecurity Awareness Training

For organisations to ensure that their employees contribute to the enterprise cybersecurity program, employees should be provided with regular cybersecurity training so that they are able to make appropriate choices to prevent or mitigate the risks posed by phishing attacks. The primary aim of the anti-phishing intervention program is to improve cybersecurity awareness and behaviour at workplace by reducing end-user susceptibility to phishing threats.

Therefore, we define cybersecurity awareness training as

‘a proactive measure deployed to combat cybersecurity threats using various delivery methods to raise end-user’s awareness and foster secure behaviour with overall aims of empowering users to recognise and report malicious activities in a timely manner and use best cybersecurity practices in daily routine.’

Anti-phishing cybersecurity intervention program empowers end users and employees to recognize and neutralize phishing cyberattacks. In order for the enterprise cybersecurity intervention program to yield positive awareness and behaviour, employees should be given cybersecurity training intervention on the threats posed by phishing attacks, how to identify phishing attempts such as malicious websites, and how to take the appropriate decisions to prevent or mitigate phishing attacks [16]. Such anti-phishing intervention program will pay dividends to the organisation by protecting businesses from adverse disastrous consequences, which includes data breaches, business continuity issues (e.g., due to ransomware attacks), reputational damages, financial losses and much more. This is confirmed by a recent large-scale study that included various parts of the world (i.e., the UK, France, Germany, Spain, the US, Australia, and Japan) found that about 78% of firms involved in the study indicated that their cybersecurity awareness training resulted in measurable declines in phishing attack vulnerability [35].

There is a general consensus within the existing literature that cybersecurity intervention program can minimize human factors related cybersecurity issues including phishing threats [2,3,8,9,13,15,26,41]. For example, the study by Sheng et al. [41] showed that cybersecurity intervention programs are effective and decreased by 40% the people who enter confidential and sensitive information on fake webpages. Therefore, cybersecurity awareness and training of employees become extremely crucial in keeping enterprises and organizations better protected from phishing attacks. There are a wide range of cybersecurity awareness training intervention programs that train, educate, and persuade end users against phishing attacks. The intervention programs to instil vital security awareness skills and subsequently bring changes in employee cyber behaviours are implemented using different delivery methods. Therefore, for the cybersecurity intervention program to be effective and successful in reducing human factor related security issues, appropriate delivery methods for cybersecurity awareness training intervention programs should be used. In the next section, we propose a new taxonomy of the delivery methods.

### B. Taxonomy of Delivery Methods

Cybersecurity awareness program to raise awareness and educate users on phishing attacks is conducted using one or more delivery methods. There are various types of cybersecurity training and awareness delivery methods. In this section, we discuss the most prominent delivery methods.

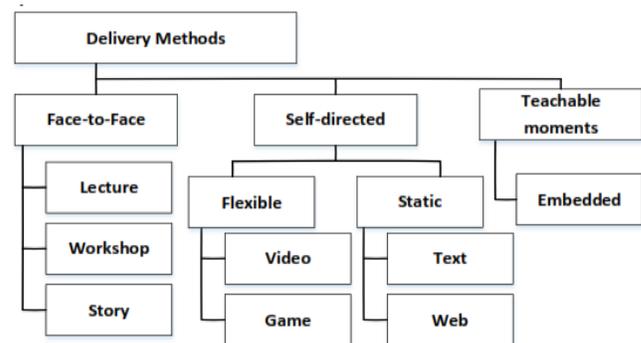


Fig. 1. Taxonomy of Cybersecurity Training Delivery Methods.

Fig. 1 shows the proposed taxonomy of cybersecurity awareness training delivery methods. Basically, we classify the delivery methods into three main classes namely, face-to-face class, self-directed class, and embedded class. The self-directed class of the delivery method is further sub-divided as flexible and static categories. In the following subsections, we describe each in detail.

1) *Face-to-face delivery methods:* The face-to-face cybersecurity intervention program delivery method involves physical learning environment with or without direct involvement of cybersecurity expert as a facilitator. Examples of such delivery methods are a lecture-based, a workshop-based and a story-based delivery method.

a) *Lecture-based delivery method:* Lecture-based cybersecurity intervention program delivery method is one of the most prevalent delivery methods [22,26,42]. The training

primarily consists of formal presentations (i.e., lectures) by an instructor in a classroom setting for a group of participants. The instructor may use power point slides as well as other resources such as audio-visual aids. The lecture is delivered by a security expert (instructor) and requires physical attendance of both the learners and the instructor in the classroom.

Although the knowledge transfer is one way (i.e., from the expert to the learners), it encourages direct interaction between learners and the instructor. Through incorporating group learning activities, it can also enable interaction as well as collaboration among the trainees allowing the learners to learn from each other. It also has the flexibility of providing tailored session to the specific industry or a particular department within a workplace. The learners can ask for further clarifications on concepts that are not clear in the class, and any question and doubt can be addressed immediately during the session.

Lecture-based delivery method is relatively costly as it includes expenses related to hiring the instructor, preparation of the content and the employee time away from their regular jobs. A major challenge of the lecture-based method is ensuring the engagement of the participants and avoiding boredom. This challenge can be easily addressed by initiating short breaks when attendees become distracted or bored and include activities that require the participants apply the concepts covered to their role or quizzes throughout the session.

*b) Workshop-based delivery method:* Workshop-based cybersecurity intervention program emphasises dialogue and plenary reflection with the ideal size of about 15 participants over several plenary discussions [13]. The participants are divided into small groups of individuals. Each group is allotted a timeframe to discuss on a given cybersecurity-related scenario among themselves to create a reflection. This is followed by a plenary discussion where each group presents its possible answer to their scenario and then the other groups were asked to provide their comments on the response provided by the group. Each plenary session is closed by a brief concluding remark of the instructor on the scenario followed by questions or remarks from the workshop participants.

Workshop-based training is similar to the lecture-based training in that it involves an expert and attendees gathered in a workshop venue such as classroom. Unlike the lecture-based program where the expert drives the training, the role and involvement of the expert is restricted mainly to define the workshop topics, develop learning materials needed for the session, manage time, occasionally answering specific questions directed to the expert during the workshop, and ensuring that the workshop discussion remain within the scope of the defined topic. The workshop participants drive the training through dialogue, participation, and collective reflection in small groups [13]. The workshop attendees steer most of the discussions among themselves by actively exchanging their thoughts with each other and the instructor in plenary reflections.

*c) Story-based delivery method:* Story-based cyber security awareness uses narrative stories about real-life

cybersecurity events to train employees about security as a relatable experience [30,39]. A personal story narrative may contain information about the approach used by the phisher to deceive the storyteller, the consequences of being phished and what steps to take not to make similar mistakes. Basically, the story-based training explores the intuition that people tend to learn about cyber security by hearing positive and/or negative real stories as well as security warnings from experts/peers.

For example, people who have personally experienced security attacks such as identity theft learn a hard way about security threats and how to better protect themselves against attacks. Wash and Cooper [39] used social stories about prior experience of phishing attacks to train employees in an organisation and tested to see if the employees can recognise and avoid falling victim to phishing attacks. They found that stories are more effective when the learners think that the stories originate from people with similar characteristics.

*2) Self-directed delivery methods:* The cybersecurity awareness training delivery methods within the self-directed category includes the delivery methods that cater to virtual learning environment and learners' self-regulation. It can be divided into two subcategories; one is Flexible category and the other is static category. Examples of self-directed delivery methods include web-based training, text-based, video-based, and game-based approaches.

*a) Video-based delivery:* In the video-based awareness delivery method, a 2-to-5-minute micro-learning style videos used are used for self-directed learning about phishing and how to defend against it. It is a self-paced learning where the learner can pause the video at any time and re-watch it later. The content normally contains real scenarios and examples in the form of clips, animation, and cartoons related to phishing attacks. For example, the phishing awareness video developed by Volkamer et al. [32] includes authentic-looking messages laced with tricks to seduce potential victims to click on a malicious link embedded in the message. The content also includes misconceptions about phishing normally found in the literature and warning messages such as the likely impacts of clicking on a malicious link.

The video used in Tschakert and Ngamsuriyaroj [26] is approximately 2 to 3 minutes and offers a basic overview of phishing, a brief description of the tactics used by phishers to deceive potential victims, the potential impacts, and the possible clues that can be used to recognise dishonest emails and URLs. The videos offer visual learning, which may shorten the time employees require to commit to the training. However, it could be expensive to develop and may be difficult to make the learners engaged in the content [32].

*b) Game-based delivery:* Educational game-based cybersecurity training provides a learning environment coupled with entrainment where employees (as players) learn phishing methods and how to detect them through playing the game. Learning takes place in a virtual environment involving teaching agent (virtual) and the learner (physical). Normally, story-based method in which the story is shown to the learners in a comic format is used. Game flows are structured on

progressive levels normally from basic to advanced levels such that players are required to successfully complete the content at a specific level before they are allowed to proceed further to a higher level. Each level is normally designed with several sequential activities/questions and the players may be forced to complete/answer each activity/question in the sequences program in the game before moving to the next activities/questions. Also, some games have built-in timer to restrict the player to complete a given activity/question within certain period. The side effect of a restriction on game play time is that it can make self-paced learning impossible.

The design's philosophy of exiting game-based cybersecurity delivery methods is summarized in [25]. Game-based training have emerged as a powerful security awareness and training delivery methods resulting in several systems such as Phishy [29], What Hack [44], and NoPhish [18]. Generally, this game-based training software that teaches end-users how to detect phishing URLs using cues, distinguish between fake and genuine sites using cues, and how to decide if a given site is legitimate or not using search engines. Asanka et al. [33] describe a mobile game-based delivery method that teaches people how to identify URL-related phishing threats such that the people who are trained with the game will be able to differentiate malicious websites from genuine ones. Game-based model are highly interactive and engaging medium. Also, it offers visual learning and has inherent option of self-paced, pausing the game and resuming it at any suitable time. A well-designed game-based training delivery method can potentially offer quick learning and proficiency of cybersecurity fundamentals [16].

*c) Text-based delivery:* Text-based training consists of an educational reading material that takes about 15–20 minutes. The reading material is prepared by an expert and distributed to the potential learners to master the content. Generally, the content covers topics such as "look for https", "type in URLs don't click on them", "phishing is your problem; don't rely on others to protect you", and "misspellings can signal fake emails". The content may also include examples and the description of the best security practices. In the basic form of text-based training, the learner is normally provided with a hardcopy of the material used in lecture-based training or text derived from corporate guidelines/warnings usually available on the organisation's website. However, a softcopy text in a form such as PDF require an electronic device with appropriate software (PDF reader). A tool called NoPhish [18] provides text-based delivery capability and commonly used in training [26,42].

Similar to web-based training method, text-based model has inherent option of self-paced, pausing and resuming at any suitable time and studying the material in any order. Although the reading material is expected to take 15–20 minutes of reading time, the trainees can spend as much time as they needed to go through it. Unfortunately, the text-based training is static and not interactive. Also, it does not have the option to provide feedback to the learners. Tschakert et al. [26] and Stockhardt et al. [42] used text-based delivery method for training learners on how to detect phishing emails and fake websites. The lessons cover topics on introduction to phishing,

examples of phishing emails and websites as well as the possible impacts of a successful phishing attack, markers of dishonest emails and URL addresses.

*d) Web-based training:* Web-based delivery methods can be based on anti-phishing contents on websites (basic form) or advanced for, which we refer to as a computer-based training (CBT). In its basic form, web-based training method are freely available online resources that contain facts and advice about phishing threat, various ways to identify it, and what to do to avoid falling prey to phishing scams. Examples of the basic anti-phishing web-based training material include the Anti-Phishing Working Group website (APWG) [5] and Cornell's PhishLine [6] web pages on phishing. CBT version is normally commercially available and is advanced web-based training methods. It is generally interactive, developed on the principles of instructional design and have six basic elements that enable the learner to control his/her learning namely, capability to 'skip, supplement, sequence, pace, practice (for users to assess their understanding of phishing) and guidance identified' [37]. For example, Abraham et al. [40] discusses a web-based training method with topics covering counterfeit webpages and malicious links organized as hyperlinks.

The web-based delivery method enables the learner to schedule the most convenient time to access the content of the awareness training modules, stop at any time and come back to it at a later point of time. The content can be organised in such a way that the trainees could select the topics to learn in any sequence. Normally, web-based method includes quizzes and tests that measure the performance of the trainees and provides direct feedback on the performance of the end users. Similarly, web-based training method allows for interactivity that optimizes the learning experience.

The consistency of the content and the simplicity of use are the virtues of web-based training method. Also, web-based training method is often deemed a cost-effective way of raising employee cybersecurity awareness. Web-based training method does not provide facility for further explanation, may encourage finishing the learning modules with nominal time or diligence, and it may be monotonous and unchallenging [21]. Some of these shortcomings can be addressed by incorporating resources such as visuals and animations into the content. Each learner completes the training modules online individually using desktop computers or hand-held devices (e.g., tablets, iPad, and smartphones).

*3) Teachable moment delivery methods:* This class of awareness delivery methods follows the test-train concept such that only people who fail the test will be trained using other delivery methods such as story-based or text-based methods. An example of this class is the embedded method discussed below.

*a) Embedded delivery method:* The idea of embedded phishing training is to send simulated phishing emails to users, usually without letting them know about it, to test their ability to identify phishing attempt. A user who falls for the simulated phishing attack receives a remedial training about phishing and how to recognize phishing emails immediately (known as

“teachable moments”) following the click on the link. For example, an email with embedded link to an external website is sent to the employees and urged them to click on the link where they would input their login credentials. If an employee acts upon the request and clicks the link in the email, then a remedial training is provided to the employee typically a webpage where training materials are hosted. Following the remedial training, another simulated phishing emails can be used to check if the ability to detect phishing threats have improved or not.

Essentially, embedded training provides continual real time training experience to the employees by embedding the

training into the day-to-day tasks the employees perform [39]. There are many tools such as PhishGuru [34] that provides an embedded training to end-users based on simulated phishing email. It is believed that embedded training can help the learners to retain the learnt knowledge for an extended period as compared to the other methods [34]. However, it can also increase the frequency of the click rate on phishing link by the end users [31].

In Table I, we show a comparative analysis of the delivery methods presented in the previous sections.

TABLE I. COMPARATIVE ANALYSIS OF THE DELIVERY METHODS

	Classroom		Pace		Feedback			Learning			Instructor		Communication			Tracking			Time
	Physical	Virtual	Lecturer	Self	None	Real	Direct	Active	collaborate	Personal	Active	Passive	One-one	One-many	Many-many	Participate	completed	reporting	Minutes
Lecture		×		×	×			×		×		×	×		×			×	30 to 45
Workshop		×		×	×			×		×		×	×					×	30 to 45
Story	×		×	×	×		×		×		×	×		×	×	×	×	×	15 to 20
Text	×		×			×	×		×		×			×	×			×	15 to 20
Web	×		×		×		×		×		×			×	×				15 to 20
Video	×		×			×	×		×		×			×	×				2 to 5
Game	×		×		×		×		×		×			×	×				30
Embedded	×		×	×	×		×		×		×			×	×	×	×	×	15 to 20

### III. OPEN PROBLEMS

There has been ample research in countering phishing threats with emphases on human factor dimension with encouraging results. However, phishing threat prevalence continues and expected to remain significant problem in cybersecurity. In this section, we highlight some of the gaps that need to be closed in the current state-of-the-art phishing studies.

There are still many open problems that need to be researched. First, existing research shows that the approaches proposed so far can reduce significantly click rates down to rates closer to 20% [34,39]. However, this still exposes a substantial number of users susceptible to phishing threats. Therefore, there is still room to improve existing approaches or develop novel approaches to counter phishing attacks. Also, there is very little work in terms of retaining the acquired knowledge. This requires longitudinal study of various delivery methods.

Another area that needs to be explored is the performance of various delivery methods in a multinational environment. This requires investigating how cultural traits manifest themselves in making users susceptible to phishing attacks. There is a gap in clearly identifying what factors are responsible for exactly triggers and when a person is at most vulnerable to phishing attacks. Today, users tend to have multiple emails (e.g., work emails and outside emails such as

Gmail). Some employees forward all their emails to an outside account. How this practice exacerbates the phishing attack needs to be addressed.

The attackers use a variety of persuasive techniques and channels (e.g., email, USB, social networks) to bait users into clicking on malicious links embedded in the emails or obtaining personal information. This raises several research questions. First, how effective the different persuasive techniques are in terms of enticing end users to fall prey for the phishing attacks. This research is necessary for developing an effective anti-phishing solution informed by an in-depth knowledge on the subject of persuasion techniques used by the cybercriminals. Second, how does persuasive techniques and different channels interact with user demographics to facilitate of demographically different people susceptible to phishing attack. Third, one can also consider the effect of the phishing emails content over channels and different persuasive techniques.

Several large-scale users studied in the field is really needed to validate the efficacy of the various delivery methods. Furthermore, game-based cybersecurity training for enterprise-wide users received relatively less attention in the research community. Similarly, studies with respect to the various evasive techniques employed by the cybercriminals and their degree of difficult for the end users to detect phishing threats is another research gap that need to be addressed. The challenges in how to measure the retention rate and motivate behaviour

change needs to be researched. The verdict on whether or not cybersecurity awareness training changes the behaviour of the end users has not resolved yet; finally, how to evidence the need for investment in cybersecurity awareness training.

#### IV. CONCLUSION

Phishing attacks are becoming prevalent and affecting individuals and businesses in all sectors regardless of their sizes causing losses of sensitive data and financial costs. Since phishing are only effective if they are acted upon by the end users, in addition to ensuring that technical countermeasures such as email filters are configured to prevent phishing messages from getting into employee's inbox, equipping employees with the skills necessary to protect themselves and their organization against phishing threats is a key part of a robust cybersecurity program. This paper provides a review of cybersecurity training program delivery methods used by organizations aimed at improving personnel information security awareness and behaviour in the context of phishing training. The paper also presents a description and taxonomy of the most common cybersecurity training delivery methods. Although the exiting research shows that well-crafted end-user cybersecurity awareness and training program can be very effective in minimizing susceptibility to phishing attacks, there are still room for improvement. Moreover, phishing threat remains prevalent and will continue to be a significant problem, thus more research is needed to minimize its impact.

#### ACKNOWLEDGMENT

The authors gratefully acknowledge the approval and the support of this research study by grant no. SAT-2018-3-9-F-7926 from the Deanship of Scientific Research at Northern Border University, Arar, K.S.A.

#### REFERENCES

- [1] A. Almomani, B. B. Gupta, S. Atawneh, A. Meulenberg, and E. Almomani, "A survey of phishing email filtering techniques," *IEEE Commun. Surv. Tutor.*, vol. 15, no. 4, pp. 2070–2090, 2013.
- [2] A. Carella, M. Kotsoev, and T. M. Truta, "Impact of security awareness training on phishing click-through rates," in *2017 IEEE International Conference on Big Data (Big Data)*, 2017.
- [3] A. Gendre, "Facebook Phishing Is Exploding: Why the Social Media Giant is the Latest Phishers' Favorite." [Online]. Available: <https://www.vadesecure.com/en/facebook-> [Accessed: 25-May-2021].
- [4] A. Gendre, "The art of deception in social media phishing," *Vadesecure.com*. [Online]. Available: <https://www.vadesecure.com/en/the-art-of-deception-in-social-media-phishing/>. [Accessed: 25-May-2021].
- [5] APWG, *Phishing Activity Trends Report 1st Quarter 2020*. Anti-Phishing Working Group, 2020.
- [6] B. B. Gupta, A. Tewari, A. K. Jain, and D. P. Agrawal, "Fighting against phishing attacks: state of the art and future challenges," *Neural Comput. Appl.*, vol. 28, no. 12, pp. 3629–3654, 2017.
- [7] R. Islam and J. Abawajy, "A multi-tier phishing detection and filtering approach," *J. Netw. Comput. Appl.*, vol. 36, no. 1, pp. 324–335, 2013.
- [8] Barracuda Networks, Inc, "Click Thinking Content," *Phishline.com*. [Online]. Available: <https://www.phishline.com/complimentary-content>. [Accessed: 25-May-2021].
- [9] C. I. Canfield, B. Fischhoff, and A. Davis, "Quantifying phishing susceptibility for detection and behavior decisions," *Hum. Factors*, vol. 58, no. 8, pp. 1158–1172, 2016.
- [10] C. Konradt, A. Schilling, and B. Werners, "Phishing: An economic analysis of cybercrime perpetrators," *Comput. Secur.*, vol. 58, pp. 39–46, 2016.
- [11] D. D. Caputo, S. L. Pfleeger, J. D. Freeman, and M. E. Johnson, "Going spear phishing: Exploring embedded training and awareness," *IEEE Secur. Priv.*, vol. 12, no. 1, pp. 28–38, 2014.
- [12] D. Goel and A. K. Jain, "Mobile phishing attacks and defence mechanisms: State of art and open research challenges," *Comput. Secur.*, vol. 73, pp. 519–544, 2018.
- [13] E. Albrechtsen and J. Hovden, "Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study," *Comput. Secur.*, vol. 29, no. 4, pp. 432–445, 2010.
- [14] E. Amankwa, M. Loock, and E. Kritzingner, "A conceptual analysis of information security education, information security training and information security awareness definitions," in *The 9th International Conference for Internet Technology and Secured Transactions (ICITST-2014)*, 2014.
- [15] E. Rader and R. Wash, "Identifying patterns in informal sources of security information," *J. cybersecur.*, p. tyv008, 2015.
- [16] E. Trickel, F. Disperati, E. Gustafson, F. Kalantari, M. Mabey, N. Tiwari, Y. Safaei, A. Doupe, G. Vigna, Shell we play a game? CTF-as-a-service for security education, 2017 USENIX Workshop on Advances in Security Education (ASE 17), USENIX Association, Vancouver, BC (2017).
- [17] FBI, "Internet Crime Complaint Center (IC3)," *ic3.gov*, 2019. [Online]. Available: <https://www.ic3.gov/media/2019/190910.aspx>. [Accessed: 25-May-2021].
- [18] G. Canova et al., "Learn to spot phishing URLs with the android NoPhish app," in *Information Security Education Across the Curriculum*, Cham: Springer International Publishing, 2015, pp. 87–100.
- [19] I. Qabajeh, F. Thabtah, and F. Chiclana, "A recent review of conventional vs. automated cybersecurity anti-phishing techniques," *Comput. Sci. Rev.*, vol. 29, pp. 44–55, 2018.
- [20] I. R. A. Hamid and J. H. Abawajy, "An approach for profiling phishing activities," *Comput. Secur.*, vol. 45, pp. 27–41, 2014.
- [21] J. Abawajy and T.-H. Kim, "Performance analysis of cyber security awareness delivery methods," in *Communications in Computer and Information Science*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 142–148.
- [22] J. Abawajy, "User preference of cyber security awareness delivery methods," *Behav. Inf. Technol.*, vol. 33, no. 3, pp. 237–248, 2014.
- [23] J. Abawajy, A. Richard, and Z. A. Aghbari, "Securing websites against homograph attacks," in *Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering*, Cham: Springer International Publishing, 2018, pp. 47–59.
- [24] J. Fruhlinger, "Top cybersecurity facts, figures and statistics," *Csoonline.com*, 09-Mar-2020. [Online]. Available: <https://www.csoonline.com/article/3153707/top-cybersecurity-facts-figures-and-> [Accessed: 25-May-2021].
- [25] J.-N. Tioh, M. Mina, and D. W. Jacobson, "Cyber security training a survey of serious games in cyber security," in *2017 IEEE Frontiers in Education Conference (FIE)*, 2017.
- [26] K. F. Tschakert and S. Ngamsuriyaroj, "Effectiveness of and user preferences for security awareness training methodologies," *Heliyon*, vol. 5, no. 6, p. e02010, 2019.
- [27] K. L. Chiew, K. S. C. Yong, and C. L. Tan, "A survey of phishing attacks: Their types, vectors and technical approaches," *Expert Syst. Appl.*, vol. 106, pp. 1–20, 2018.
- [28] K. RaniSahu and J. Dubey, "A survey on phishing attacks," *Int. J. Comput. Appl.*, vol. 88, no. 10, pp. 42–45, 2014.
- [29] M. Baslyman and S. Chiasson, "'Smells Phishy?': An educational game about online phishing scams," in *2016 APWG Symposium on Electronic Crime Research (eCrime)*, 2016.
- [30] M. Fernando and N. A. Arachchilage, "Perth Why Johnny can't rely on anti-phishing educational interventions? Why Johnny can't rely on anti-phishing educational interventions to protect himself against contemporary phishing attacks?", *Australasian Conference on Information Systems*, 2019.
- [31] M. M. Al-Daeef, N. Basir, and M. M. Saudi, "Security awareness training: A review," in *Lecture Notes in Engineering and Computer*

- Science: Proceedings of The World Congress on Engineering 2017. International Association of Engineers (IAENG), Newswood Limited, 446–451, 2017.
- [32] M. Volkamer et al., “Developing and evaluating a five-minute phishing awareness video,” in *Trust, Privacy and Security in Digital Business*, Cham: Springer International Publishing, 2018, pp. 119–134.
- [33] N. A. G. Arachchilage, S. Love, and K. Beznosov, “Phishing threat avoidance behaviour: An empirical investigation,” *Comput. Human Behav.*, vol. 60, pp. 185–197, 2016.
- [34] P. Kumaraguru, S. Sheng, A. Acquisti, L. F. Cranor, and J. Hong, “Teaching Johnny not to fall for phish,” *ACM Trans. Internet Technol.*, vol. 10, no. 2, pp. 1–31, 2010.
- [35] Proofpoint, “Threat Report: 2020 State of the Phish Report.” [Online]. Available: <https://www.proofpoint.com/us/resources/threat-reports/state-of-phish>. [Accessed: 25-May-2021].
- [36] R. M. Mohammad, F. Thabtah, and L. McCluskey, “Tutorial and critical analysis of phishing websites methods,” *Comput. Sci. Rev.*, vol. 17, pp. 1–24, 2015.
- [37] R. N. Landers and C. M. Reddock, “A meta-analytic investigation of objective learner control in web-based instruction,” *J. Bus. Psychol.*, vol. 32, no. 4, pp. 455–478, 2017.
- [38] R. Valecha, A. Gonzalez, J. Mock, E. J. Golob, and H. Raghav Rao, “Investigating phishing susceptibility—an analysis of neural measures,” in *Information Systems and Neuroscience*, Cham: Springer International Publishing, 2020, pp. 111–119.
- [39] R. Wash and M. M. Cooper, “Who provides phishing training?: Facts, stories, and people like me,” in *Proceedings of the 2018 CHI Conference on Human Factors in Computing Systems - CHI '18*, 2018.
- [40] S. Abraham and I. Chengalur-Smith, “Evaluating the effectiveness of learner-controlled information security training,” *Comput. Secur.*, vol. 87, no. 101586, p. 101586, 2019.
- [41] S. Sheng, M. Holbrook, P. Kumaraguru, L. F. Cranor, and J. Downs, “Who falls for phish?: A demographic analysis of phishing susceptibility and effectiveness of interventions,” in *Proceedings of the 28th international conference on Human factors in computing systems - CHI '10*, 2010.
- [42] S. Stockhardt et al., “Teaching Phishing-Security: Which Way is Best?,” in *ICT Systems Security and Privacy Protection*, Cham: Springer International Publishing, 2016, pp. 135–149.
- [43] V. Suganya, “A review on phishing attacks and various anti phishing techniques,” *Int. J. Comput. Appl.*, vol. 139, no. 1, pp. 20–23, 2016.
- [44] Z. A. Wen, Z. Lin, R. Chen, and E. Andersen, “What.Hack: Engaging anti-phishing training through a role-playing phishing simulation game,” in *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems - CHI '19*, 2019.

# Visual Selective Attention System to Intervene User Attention in Sharing COVID-19 Misinformation

Zaid Amin<sup>1</sup>, Nazlena Mohamad Ali<sup>2\*</sup>, Alan F. Smeaton<sup>3</sup>

Institute of IR4.0 (IIR4.0), Universiti Kebangsaan Malaysia, Malaysia<sup>1,2</sup>

Faculty of Informatics Engineering, Universitas Bina Darma, Palembang, Indonesia<sup>1</sup>

INSIGHT: Centre for Data Analytics, Dublin City University, Dublin 9, Ireland<sup>3</sup>

**Abstract**—Information sharing on social media must be accompanied by attentive behavior so that in a distorted digital environment, users are not rushed and distracted in deciding to share information. The spread of misinformation, especially those related to the COVID-19, can divide and create negative effects of falsehood in society. Individuals can also cause feelings of fear, health anxiety, and confusion in the treatment COVID-19. Although much research has focused on understanding human judgment from a psychological underline, few have addressed the essential issue in the screening phase of what technology can interfere amidst users' attention in sharing information. This research aims to intervene in the user's attention with a visual selective attention approach. This study uses a quantitative method through studies 1 and 2 with pre-and post-intervention experiments. In study 1, we intervened in user decisions and attention by stimulating ten information and misinformation using the Visual Selective Attention System (VSAS) tool. In Study 2, we identified associations of user tendencies in evaluating information using the Implicit Association Test (IAT). The significant results showed that the user's attention and decision behavior improved after using the VSAS. The IAT results show a change in the association of user exposure, where after the intervention using VSAS, users tend not to share misinformation about COVID-19. The results are expected to be the basis for developing social media applications to combat the negative impact of the infodemic COVID-19 misinformation.

**Keywords**—Visual selective attention; COVID-19 misinformation; user attention; information sharing; implicit association test

## I. INTRODUCTION

The disruption of major changes in the digital environment makes social media applications an "omnipresence" in human life. This change also affects the overload of information on the internet. According to Statista [1], there are currently 4.2 billion active users of social media applications, and this number will remain to grow. As a result of this diverse digital environment, users relatively get distracted, primarily when they receive and share information on social media [2]. The behavioral factor of human attention has long been a key factor in science and research that focuses on Human-Computer Interaction (HCI). The study conducted by [3] states that the attention factor's role is essential when users share information on social media. In line with that, recent studies conducted by Gabielkov et al. [4] stated that about 59% of users in Twitter share information without even reading the content first (in

other words, in a hurry and without attentive behavior to share the information they have just received).

Several technological innovations have been developed, one developed by Facebook, which relies on an algorithm to detect false information. However, the approach that relies on robot-based applications needs to be re-examined by carrying out additional "hybrid" integration, specifically considering the psychological factors of human decisions. This is in line with research by [5], where they found that the spread of false information was carried out by humans more than bot-based applications. This shows that the spread of false information on social media requires a lot of collaborative studies and research that can understand human decision factors.

The spread of misinformation, especially regarding COVID-19, can have a multidimensional negative impact on society. These negative impacts include false information about treatment, belief in certain drugs and medical treatments, economic incentive motives for pharmaceutical companies, and polarization of mental exposure [6] and [7]. Furthermore, the destructive impact of spreading COVID-19 misinformation can affect the mitigation process's pace in handling democracy and economic recovery in a country, for example, in expediting the implementation of COVID-19 vaccination to the public.

Several studies from [8] - [10] state that this "visual selective attention" technique can influence user decisions when facing a task. Therefore, in this study, we build a tool with a visual selective attention technique to intervene the user's attention when deciding to share information on social media. In the context of this study, users deal with ten information they receive using the Visual Selective Attention System (VSAS). In each pre-and post-intervention task, the VSAS will stimulate the user with an interface using "spotlight" and "zoom-lens" design techniques [11], where these techniques are a sub-theory of visual selective attention, which has been known to play an important role in decision-making.

In this study, we aim to 1) intervene in user attention using VSAS when they will share misinformation about COVID-19, 2) measure the effectiveness of VSAS in intervening users, 3) measure user association and evaluation when they will share misinformation about COVID-19 using Implicit Association Test (IAT). This paper is divided into six sections. Section 1 contains the introduction. Section 2 contains relevant and related studies. Section 3 contains the methods used in study 1

\*Corresponding Author.

and study 2. Section 4 contains the results of analysis and experiments. Section 5 contains discussions and research limitations, and section 6 contains conclusions.

## II. BACKGROUND WORK

### A. User Attention Factor

The study in [2] shows that one of the key factors underlying why users share misinformation on social media is that users' attention is distracted, and when users do not think critically about the information they receive, they are likely to share the information.

The attention factor is one of the fundamental psychological factors in humans when interacting with their environment. The attention factor is a set of cognitive processes that make a person able to process a set of information in limited conditions either because the capacities of environment or the cognitive state s/he has [12]. From another perspective, the attention factor is related to a person's level of awareness and focus when receiving and confirming information [13].

A study by [14] found that the role of the attention factor is vital in explaining the phenomenon of how users behave in online media. This attention behavior relates to when a user reads tweets, surfs any websites, and accesses e-mails. The study by [15] states that social media designers need to maximize users' level of attention and awareness when accessing the information on social media. For example, design properties that can stimulate user visibility when using social media applications can be shape or pattern components with contrasting color strengths.

### B. The influence of Selective Attention on user Decisions

An example of a concrete concept of selective attention technique is when we get a pop-up message from sending an email. The design of the pop-up message with a "quick display" design can distract us and influence our decision to open the incoming email. This visual selective attention technique was also described by [9] when designing different interfaces in the form of multi-display patterns and locations. This technique can increase the user's attention when searching for information. As for the health and medical aspects, Lopes and Ramos [16] found that selective attention, integrated into the health application interface, showed significant results, particularly increasing user attention in understanding health literacy.

### C. The influence of Social Influences and Epistemic Belief in Sharing Information

According to Chen et al. [17], when sharing information on social media, users are very easily influenced by the social influence factor. For example, if users receive information from related or emotionally close people, they are more likely to trust and re-share the information. This is in line with the study conducted by [18], who found that the effect of self-actualization only appeared when the user focused on close friends (focused on bonding social relationships). Based on this, we then included the narrative stimuli of social influence in pre- and post-intervention sessions using VSAS.

Another psychological factor that can trigger the possibility of sharing information without attention is the epistemic belief factor. A study conducted by Chua and Banerjee [19] stated that epistemic belief factors could influence user decisions to share health rumors online. Users with confidence and experience with certain drugs or medical treatments tend to be easily influenced when processing false health information and are more likely to share it again.

The theoretical basis and the role of the epistemic belief factor align with the Implicit Association Test (IAT) measurement method, where the IAT measures the level of the user's association tendency or exposure to a concept in a person. In this paper context, the user is expected to evaluate the ten-information provided in pre-and post-intervention using VSAS.

## III. METHODS

### A. VSAS Tool

In the VSAS experiment, we conducted pre-and post-intervention sessions for two weeks. Thirty-eight participants joined in this experimental session. Participants (n=38) consisted of 11 females and 27 males with an average age of 20 (SD = 1.11), and all were students. Participants were compensated \$5 for their time. Each experiment section took 1.5 to 2 hours. In the first week, we used VSAS without any design intervention. In the second week, the intervention was carried out using visual selective attention by adding a label design to the ten-information provided to participants. This label design was generated based on credible fact-checking sources. The same ten items of information in weeks 1 and 2 were given to participants, while the content of the information relates to the political, sensational, and sensitive context [20].

We built and designed this VSAS using JAVA programming through the Android Studio 4.1.1 application. The storage media for each response from our participants uses the services of the Firebase Real-Time Database. This VSAS instrument concept is built and designed for mobile-based applications. The layout of the VSAS instrument wireframe design can be seen in Figures 1 and 2.



Fig. 1. Wireframe Design using Spotlight Technique.

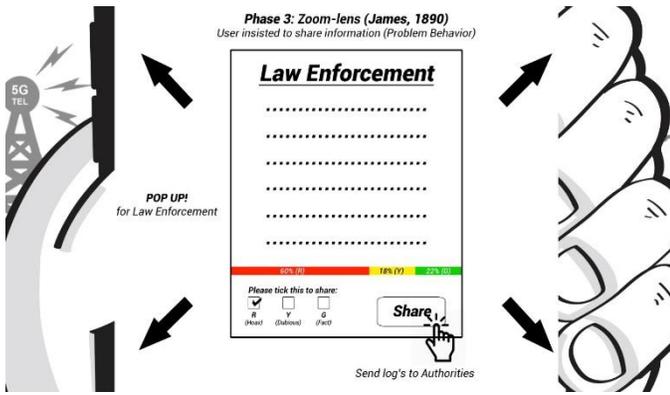


Fig. 2. Wireframe Design using Zoom-Lens Technique.

### B. Procedures

In the first week's session (pre-intervention), each participant registered in advance to communicate with the administrator. After 38 participants were registered and had an account in VSAS, they sent their respective profile and demographic data. Then, administrators sent participants through individual chats of ten information contexts, of which five items were misinformation, and the other five were fact information. Each participant was asked to respond to the chat from the administrator by replying using a Likert-based scale between 1 - 5. Participants will be asked and narrated at each delivery of context information, representing the social influence factor like "if you got this information from your family, would you share it again." To answer these questions, participants replied with the Likert scale between 1 - 5, where "1" indicates strongly disagrees with sharing information, "2" disagrees with sharing information, "3" is neutral, "4" agrees to share information, and "5" for strongly agrees to share information.

After participants responded to ten information contexts in the pre-intervention session, we stored the respondent's data in the Firebase Real-Time Database for tabulation and analysis. After the experiment using VSAS is carried out, the participants will start the Implicit Association Test (IAT) session through the Pavlovla website. The IAT content is related to how participants evaluate "Misinformation vs. Fact Information or Positive vs. Negative Words." In this IAT session (see Figure 3), participants will quickly determine the information according to their respective perceptions. The process of associating factual information and misinformation is combined with the participant's ability to determine "Positive vs. Negative Words."

In the second week session (post-intervention), participants will be sent the same ten contexts of information as in session 1. The difference is that the concept of visual selective attention through spotlight and zoom-lens design techniques has been applied. The attention of participants will be intervening by focusing on the design of the spotlight color bar properties, where red color stimuli indicate the label "hoax," yellow is "dubious," and green is "fact" (see Figure 4).

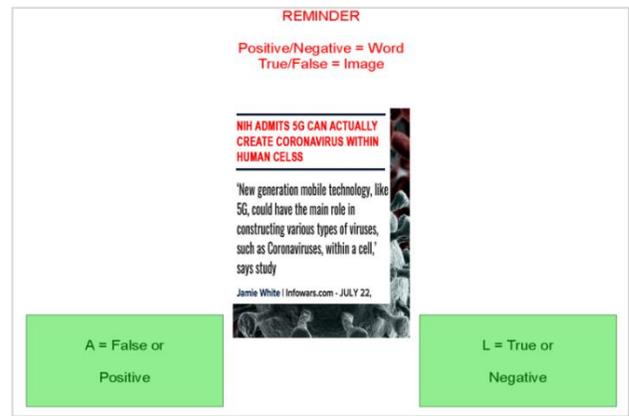


Fig. 3. Example of IAT Test Selection.

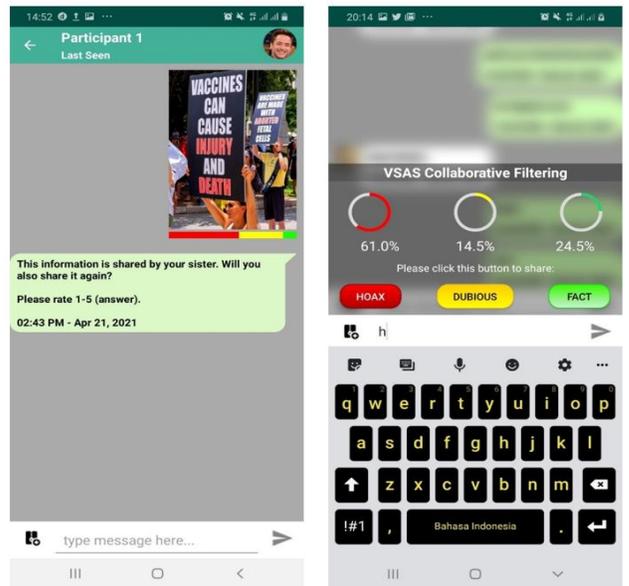


Fig. 4. Intervention Process on VSAS.

The labeling method for each of the ten information contexts is carried out based on fact-checking sources. In this intervention session, participants will also be asked to be involved in providing collaborative corrections. Next, at the last intervention stage, participants will be intervened with pop-up warning notifications in the form of law enforcement. This pop-up law enforcement increases each participant's attention with the "zoom-lens" animation technique. After the post-intervention was completed, participants would start the IAT with the same as the first-week session.

### IV. RESULTS

We summarized using descriptive statistical analysis to briefly examine the pre-and post-intervention results (see Figure 5). After conducting the second-week session (post-intervention), only 23 participants completed the entire VSAS and IAT experimental process, and 15 participants experienced errors. Therefore, we could not analyze the data responses.

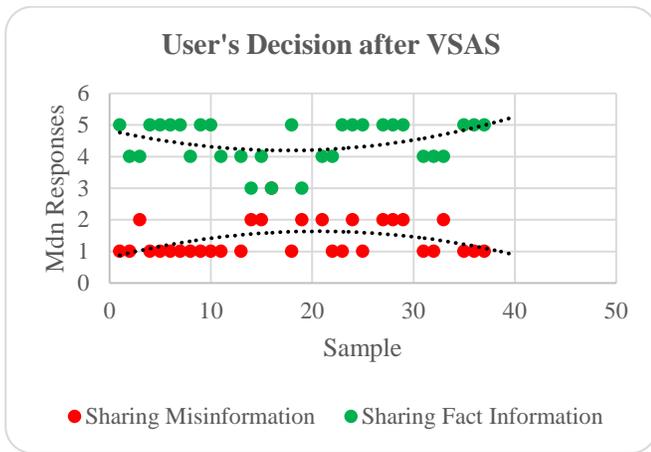


Fig. 5. User Response during Post-Intervention.

The significant results in 23 participants in post-intervention showed a behavior change, whereas 15 participants increased their attention and chose to confidently respond with an answer of "1" for each context of the misinformation sent. The results in Figure 6 describe the successions of the VSAS experiments, which is 65.2% of participants strongly disagreed with sharing the misinformation provided.

This result asserts that VSAS has succeeded in intervening in users' attention when they decide to share information. A total of 7 participants, or 30.4%, chose answer "2" where they did not agree to reshare the misinformation they received. A total of 22 participants significantly chose answers in the Likert range of 1-2, especially about the context of misinformation on implementing COVID-19 vaccination. In the descriptive analysis of the post-intervention results using VSAS, we can conclude that most of the participants' decision tendencies are  $Mdn=1$ ,  $IQR=1$ . The results of  $IQR=1$  indicate that the distribution of the participants' median responses at post-intervention also shows a linear result, which has less variability about its median.

Finally, to ensure the success of changing responses and evaluating participants on the IAT, we analyzed the IAT calculations using a D-score. This D-score (see Table 1) is similar to the Cohen's d effect measurement, ranging from -2.00 to 2.00. In detail, the frequency distribution of the D-score category shows as 17 participants in the "Neutral/No Preference" D-Score category, 4 participants in the "Slight negative" D-Score category, and 1 participant in the "Slight positive" D-Score category. Based on these results (see Figure 7), we can state that the use of VSAS can validly improve participant evaluation in the context of measuring the concept of "Misinformation vs. Fact Information or Positive vs. Negative Words."

In the last IAT analysis step, we calculated the correlation between the IAT Score and the MdnScore (Median Score). We then also calculated the percentage weights for each question's score, calculated the variance and the ranking (see Figure 7). The correlation between IAT Score and MdnScore (Median) in sharing misinformation showed a significant moderate positive correlation of  $p = +0.3344$ .

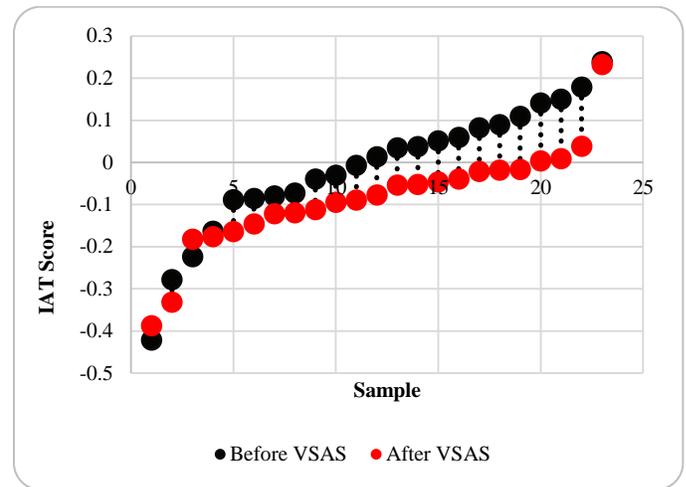


Fig. 6. User Evaluation during Post-Intervention.

TABLE I. DISTRIBUTION OF IMPLICIT SCORES AFTER VSAS

D-score	Category	n	Percent
-2 to -0.65	Strong negative	0	0.0
-0.65 to -0.36	Moderate negative	1	2.6
-0.35 to -0.15	Slight negative	4	10.5
-0.15 to 0.15	Neutral/ No Preference	17	44.7
0.15 to 0.36	Slight positive	1	2.6
0.36 to 0.65	Moderate positive	0	0.0
0.65 to 2	Strong positive	0	0.0
	Missing	15	39.5
<b>Total</b>		<b>38</b>	<b>100.0</b>

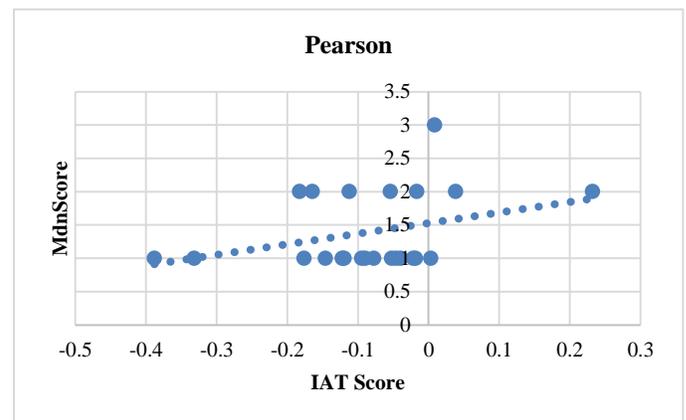


Fig. 7. The Correlation between IAT Score and Median in Sharing Misinformation.

## V. DISCUSSION AND LIMITATIONS

The previous two studies have determined relevant attention-based design, including Implicit Association Test principles, later implemented on the Visual Selective Attention System (VSAS) while evaluating information about COVID-19. These findings are useful to inform researchers/designers on design requirements that should consider in developing an attention-based design that significantly influences user

decision on sharing COVID-19 misinformation. This study has also stated that visual techniques have a more optimal role in influencing user behavior and decisions on a task. For this reason, we recommend that this visual technique could be the preference when building a technology related to user behavior in sharing information on social media. Several techniques or designs in building attention-based interfaces need further exploration and adaptation. The stimulant technique using sound or video media and the multiscreen technique might be preferred in future research. This study only carried out VSAS interactions in the distribution of 10 (ten) information contexts and social influence narratives within the scope of "individual chats." In future research, we suggest that the process of sending ten contexts of information and social influence narratives can be carried out within the scope of a "group chat." The point is to determine how different user responses are between in/out-group with the same interests or beliefs. In designing and building VSAS applications, we have limitations in obtaining secondary data in the form of datasets from social media platforms. In future studies, this dataset can be used as a reference and comparison to understand the diffusion process and information dissemination patterns in social media. Knowing this real-world situation will enhance an entire perspective in developing VSAS applications.

## VI. CONCLUSION AND FUTURE WORK

Based on the results of this study, we conclude that VSAS can increase attentive behavior when deciding to share misinformation about COVID-19. The future development of VSAS requires a more extensive study of understanding other psychological factors that influence user attention when deciding to share information. The results of this study can be the basis for developing social media applications that can be used in a wider domain, not only in the context of the COVID-19 issue, but also in the context of other domains such as security issues, handling disaster mitigation, and others, especially in communication management in handling crisis.

In future research, it is necessary to have categories of participants with different and diverse demographic backgrounds. This aims to enrich the experimental results and develop the features in VSAS, especially in selecting intervention techniques to be carried out. Research collaboration is needed to understand the essence of other key psychological concepts related to attentional behavioral factors in sharing information on social media. Meanwhile, to measure in detail, future research needs to consider how to measure the "attention span" aspect and its relationship with a person's critical thinking ability. This is important so that further research can know the intervention's effectiveness precisely and then will be able to answer the challenge of how quickly the intervention process can be carried out in the context of user interaction when sharing information. The research results reported in this study ultimately clearly show that the VSAS system has succeeded in changing user behavior in deciding whether to share information, in line with the IAT results, which show significant changes in user tendencies while evaluating information about COVID-19.

## ACKNOWLEDGMENT

This work was supported by the Universiti Kebangsaan Malaysia research grant under Grant GPK-4IR-2020-019.

## REFERENCES

- [1] Johnson, J. (2020, May 18). Topic: Social media. Retrieved April 26, 2021, from <https://www.statista.com/statistics/617136/digital-population-worldwide/>. Accessed 6 Feb 2021.
- [2] Pennycook, G., Epstein, Z., Mosleh, M., Arechar, A.A., Eckles, D. and Rand, D.G., 2021. Shifting attention to accuracy can reduce misinformation online. *Nature*, 592(7855), pp.590-595.
- [3] Z. Amin, N. M. Ali and A. F. Smeaton, "Attention-Based Design and User Decisions on Information Sharing: A Thematic Literature Review," in *IEEE Access*, vol. 9, pp. 83285-83297, 2021, doi: 10.1109/ACCESS.2021.3087740.
- [4] Gabielkov, M., Ramachandran, A., Chaintreau, A., & Legout, A. (2016, June). Social clicks: What and who gets read on Twitter? In *Proceedings of the 2016 ACM SIGMETRICS international conference on measurement and modeling of computer science* (pp. 179-192).
- [5] S. Vosoughi, D. Roy, and S. Aral, "The spread of true and false news online," *Science*, vol. 359, no. 6380, pp. 1146-1151, Mar. 2018.
- [6] Amin, Z., Ali, N.M. and Smeaton, A.F., 2021, July. Attention-Based Design and Selective Exposure Amid COVID-19 Misinformation Sharing. In *International Conference on Human-Computer Interaction* (pp. 501-510). Springer, Cham.
- [7] Erku, D. A., Belachew, S. A., Abbra, S., Sinnollareddy, M., Thomas, J., Steadman, K. J., & Tesfaye, W. H. (2021). When fear and misinformation go viral: Pharmacists' role in deterring medication misinformation during the 'infodemic' surrounding COVID-19. *Research in Social and Administrative Pharmacy*, 17(1), pp. 1954-1963.
- [8] P. Baudisch, D. DeCarlo, A. T. Duchowski, and W. S. Geisler, "Focusing on the essential: Considering attention in display design," *Commun. ACM*, vol. 46, no. 3, pp. 6066, Mar. 2003.
- [9] K. Chen and J. Chen, "Selective attention performance contributed by cognitive styles and user interface designs," *J. Chin. Inst. Ind. Eng.*, vol. 19, no. 3, pp. 7585, Jan. 2002.
- [10] L. Zizlsperger, T. Sauvigny, and T. Haarmeier, "Selective attention increases choice certainty in human decision making," *PLoS ONE*, vol. 7, no. 7, Jul. 2012, Art. no. e41136.
- [11] M. I. Posner, C. R. Snyder, and B. J. Davidson, "Attention and the detection of signals," *J. Exp. Psychol., Gen.*, vol. 109, no. 2, p. 160, 1980.
- [12] Jacko, J. A. (Ed.). (2012). *Human computer interaction handbook: Fundamentals, evolving technologies, and emerging applications*. CRC Press.
- [13] McAvinue, L. P., Habekost, T., Johnson, K. A., Kyllingsbæk, S., Vangkilde, S., Bundesen, C., & Robertson, I. H. (2012). Sustained attention, attentional selectivity, and attentional capacity across the lifespan. *Attention, Perception, & Psychophysics*, 74(8), (pp. 1570-1582).
- [14] Weng, L., Flammini, A., Vespignani, A., & Menczer, F. (2012). Competition among memes in a world with limited attention. *Scientific Reports*, 2, (p. 335).
- [15] N. O. Hodas and K. Lerman, "How Visibility and Divided Attention Constrain Social Contagion," 2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Conference on Social Computing, Amsterdam, 2012, pp. 249-257, doi: 10.1109/SocialCom-PASSAT.2012.129.
- [16] C. T. Lopes and E. Ramos, "Studying how health literacy influences attention during online information seeking," in *Proc. Conf. Hum. Inf. Interact. Retr.*, Mar. 2020, pp. 283-291.
- [17] J. Chen, C. Wang, Q. Shi, Y. Feng, and C. Chen, "Social recommendation based on users' attention and preference," *Neurocomputing*, vol. 341, pp. 1-9, May 2019.

- [18] P.-W. Fu, C.-C. Wu, and Y.-J. Cho, "What makes users share content on facebook? Compatibility among psychological incentive, social capital focus, and content type," *Comput. Hum. Behav.*, vol. 67, pp. 2332, Feb. 2017.
- [19] A. Y. K. Chua and S. Banerjee, "To share or not to share: The role of epistemic belief in online health rumors," *Int. J. Med. Informat.*, vol. 108, pp. 36-41, Dec. 2017.
- [20] B. Osatuyi, "Information sharing on social media sites," *Comput. Hum. Behav.*, vol. 29, no. 6, pp. 26222631, Nov. 2013.

AUTHOR'S PROFILE



ZAID AMIN is currently pursuing the Ph.D. degree with the Institute of IR4.0, Universiti Kebangsaan Malaysia. He is currently a Lecturer with the Faculty of Computer Science, Universitas Bina Darma, Indonesia. He is very enthusiastic about human-computer interaction. His research interests include interaction design, UI/UX, persuasive technology, and social computing



NAZLENA MOHAMAD ALI received the Ph.D. degree in human-computer interaction from Dublin City University, Ireland, in 2009. She is currently an Associate Professor and a Senior Research Fellow with the Institute of IR4.0, Universiti Kebangsaan Malaysia. Her research interests include interaction design, UI/UX, persuasive technology, digital games, and user engagement.



ALAN F. SMEATON (Fellow, IEEE) is currently a Professor of computing and the Former Director of the Insight-Centre for Data Analytics, Dublin City University. His research interests include human memory, why we forget some things and not others, and how we can use technology like search systems, to compensate for when we do forget. He was the winner of the Royal Irish Academy Gold Medal for Engineering Sciences, in 2015. He is the Chair of ACM SIGMM and an IEEE Fellow.

# Head Position and Pose Model and Method for Head Pose Angle Estimation based on Convolution Neural Network

Kohei Arai, Akifumi Yamashita, Hiroshi Okumura

Faculty of Science and Engineering, Saga University, Saga City, Japan

**Abstract**—Head position and pose model is created. Also, a method for head poses angle estimation based on Convolution Neural Network (CNN) is proposed. 3D head position model is created from these locations and obtain 3D coordinate of head position. The method proposed here uses CNN. As for the head pose detection, OpenCV and Dlib of the open-source software tools are used with Python program. The images used were RGB images, RGB images + thermography, grayscale images, and RGB images assuming images obtained by near infrared rays, with only the red channel elements extracted. As a result, the RGB image model was the most accurate, but considering the criteria set, the RGB image model was used for morning and daytime detection, and the near-infrared image was used for nighttime and rainy weather scenes. It turned out that it is better to use the model obtained by the training in. The experimental results show almost perfect head pose detection performance when the head pose angle ranges from 0 to 180 degrees with 45 degrees steps.

**Keywords**—CNN; head pose; OpenCV; Dlib; open-source software; python

## I. INTRODUCTION

Head movement detection has received significant attention in recent research. One of the specific purposes for head movement detection and tracking is to allow the user to interact with a computer or new devices like mobile phone. The increased popularity of the wide range of applications of which head movement detection is a part, such as assistive technology, virtual reality, and augmented reality, have increased the size of research aiming to provide robust and effective techniques of real-time head movement detection and tracking [1].

Most of the head pose estimation method is based on computer vision approach, like [2], [3]. Liu et al. [2] introduced a video-based technique for estimating the head pose and used it in an image processing application for a real-world problem; and attention recognition for drivers. Murphy-Chutorian and Trivedi presented a static head pose estimation algorithm and a visual 3-D tracking algorithm based on image processing and pattern recognition<sup>1</sup>. Kupetz et al. [3] implemented a head movement tracking system using an IR camera and IR LEDs.

Another approach for head movement detection is by using sensors such as gyroscopes and accelerometers. King et al. [4] implemented a hands-free head movement classification system which uses pattern recognition techniques with

mathematical solutions for enhancement. A dual axis accelerometer mounted inside a hat was used to collect head movement data. A similar method was presented by Nguyen et al. [5]. The method detects the movement of a user's head by analyzing data collected from a dual-axis accelerometer and pattern recognition techniques. But still no application based on the proposed method was suggested. Other sensor-based approaches are like [6], [7]. However, it needs more theoretical proofs and more experiments and accuracy analysis.

A combination of different techniques can be used in head tracking systems. Satoh et al. [8] proposed a head tracking method that uses a gyroscope mounted on a head mounted device (HMD) and a fixed bird's-eye view camera responsible for observing the HMD from a third person viewpoint.

In our previous research work, we propose head movement detection and tracking as a controller for 3D object scene view [9] and the combination of user's head and body movement as a controller for virtual reality labyrinth game [10]. One of the problems of the previous method for head pose angle estimation is week accuracy.

In this paper, 3D head position model is created from these locations and obtain 3D coordinate of head position. Then, the method proposed here uses Convolutional Neural Network (CNN) in order to improve head pose angle estimation accuracy. As for the head pose detection, OpenCV and Dlib<sup>2</sup> of the open-source software tools are used with Python program. The experimental results show almost perfect head pose detection performance when the head pose angle ranges from 0 to 180 degrees with 45 degrees steps.

The following section describes related research works followed by the proposed method. Then experiments are described followed by conclusion with some discussions and remarks.

## II. RELATED RESEARCH WORK

Computer input just by sight, human eyes only require head pose detection and head pose angle estimation.

Communication aid and computer input system with human eyes only is proposed [11]. Meanwhile, computer input by human eyes only and its applications are presented [12]. On the other hand, electric wheelchair control with gaze detection and

<sup>1</sup> <http://dx.doi.org/10.1109/TITS.2010.2044241>

<sup>2</sup> <http://dlib.net/>

eye blinking is proposed [13] together with electric wheelchair control with gaze detection and eye blinking [14].

Computer input with human eyes only using two Purkinje images which works in a real time basis without calibration is proposed [15]. Meanwhile, a prototype of electric wheelchair control by eye only for paralyzed use is created [16].

Robot arm utilized having meal support system based on computer input by human eyes only is also proposed and developed [17]. Also, a prototype of electric wheelchair controlled by eyes only for paralyzed users is created [18].

Autonomous control of eye based electric wheelchair with obstacle avoidance and shortest path finding based on Dijkstra algorithm, is attempted [19]. Meantime, eye-based human-computer interaction allowing phoning, reading e-book/e-comic/e-learning is created [20] together with eye based electric wheelchair control system-I(eye) can control EWC (Electric Wheelchair) [21].

Evaluation of users' impact for using the proposed eye based HCI: Human-Computer Interaction with moving and fixed keyboard by using EEG signals is conducted [22] together with electric wheelchair controlled by human eyes only with obstacle avoidance [23]. Also, evaluation of users' impact for using the proposed eye based HCI with moving and fixed keyboard by using EEG (Electroencephalography) signals is proposed with experimental validations [24].

Electric wheelchair controlled by human eyes only with obstacle avoidance is proposed and created [25] together with eye based HCI, a new keyboard for improving accuracy and minimizing fatigue effect [26].

Moving keyboard for eye based HCI is proposed [27]. Also, eye-based domestic robot allowing patient to be self-services and communications remotely is proposed and created [28].

Method for psychological status estimation by gaze location monitoring using eye based HCI is created and proposed [29]. Meanwhile, method for psychological status monitoring with line-of-sight vector changes (Human eyes movements) detected with wearing glass is proposed [30].

Wearable computing system with input output devices based on eye based HCI allowing location-based web services is proposed and realized [31]. Meanwhile, speed and vibration performance as well as obstacle avoidance performance of electric wheelchair controlled by human eyes only is evaluated [32] together with speed and vibration performance as well as obstacle avoidance performance of electric wheelchair controlled by human eyes only [33].

Service robot with communication aid together with routing controlled by human eyes is created [34]. On the other hand, information collection service system by human eyes for disabled persons is proposed [35]. Meanwhile, relations between psychological status and eye movements are investigated [36].

Method for 3D image representation with reducing the number of frames based on characteristics of human eyes is proposed [37]. Also, error analysis of line-of-sight estimation

using Purkinje images for Eye-Based Human Computer Interaction: EBHCI is proposed [38].

Mobile phone operations using human eyes only and its applications are created [39]. Meanwhile, method for thermal pain level prediction with eye motion using Support Vector Machine: SVM is proposed [40]. On the other hand, pedestrian safety with eye contact between autonomous car and pedestrian is proposed [41].

### III. 3D HEAD POSITION AND POSE MODEL

#### A. 3D Head Pose Model

In 3D head pose model is used to convert 2D face features into 3D head pose. The face features such as eyes, eyebrows, nose, and mouth are used. Head are modeled into 3 planar: XY, XZ, and YZ planar. Head pose is shown as rotation degree value ( $\theta$ ) of each planar. By using this model, 3D head pose is expected can be able to calculate only using 2D image. Head pose result is shown as  $\theta(x, y, z)$ .

Fig. 1 show head pose model on each planar. On Fig. 1(a), it shows head pose model on XY planar which look at face on front side. Central axis is assumed on bellow of mouth. When head is rotate, face features position will move follow their rotation against central axis. The new position of face features determines as  $R_i < \theta_i$ , where R is face feature radial and  $\theta$  is rotation angle. On Fig. 1(b), it shows head pose model on XY planar which look at lateral view.

Assume one of face feature has location  $P(x, y)$ , radial R, initial angle  $\theta_0$ , and central axis O (0, 0). If  $P(x, y)$  rotate against central axis, new point  $P_1(x_1, y_1)$  will be obtained. Both values can obtain rotation angle value. Rotation angle is calculated using equation (1).

$$\theta_{xy} = \tan^{-1} \left[ \frac{x'}{y'} \right] - \tan^{-1} \left[ \frac{x}{y} \right] \quad (1)$$

The same way, we also can calculate it for YZ and XZ planar using rotation radial of head. By assume rotation radial value, rotation angle for each planar will be known.

$$\theta_{yz} = \sin^{-1} \left[ \frac{y'}{R} \right] - \sin^{-1} \left[ \frac{y}{R} \right] \quad (2)$$

$$\theta_{xz} = \sin^{-1} \left[ \frac{x'}{R} \right] - \sin^{-1} \left[ \frac{x}{R} \right] \quad (3)$$

In a real condition, all information is shown on pixel coordinate. Therefore central axis will has  $O(x, y)$  coordinate and face feature will have  $P_i(x, y)$ . We can directly convert from pixel coordinate into rotation angle based on equation (2).

$$\theta_{xy} = \tan^{-1} \left[ \frac{O_x - P_x'}{O_y - P_y'} \right] - \tan^{-1} \left[ \frac{O_x - P_x}{O_y - P_y} \right] \quad (4)$$

$$\theta_{yz} = \sin^{-1} \left[ \frac{O_y - P_y'}{R} \right] - \sin^{-1} \left[ \frac{O_y - P_y}{R} \right] \quad (5)$$

$$\theta_{xz} = \sin^{-1} \left[ \frac{P_x' - O_x'}{R} \right] - \sin^{-1} \left[ \frac{P_x - O_x}{R} \right] \quad (6)$$

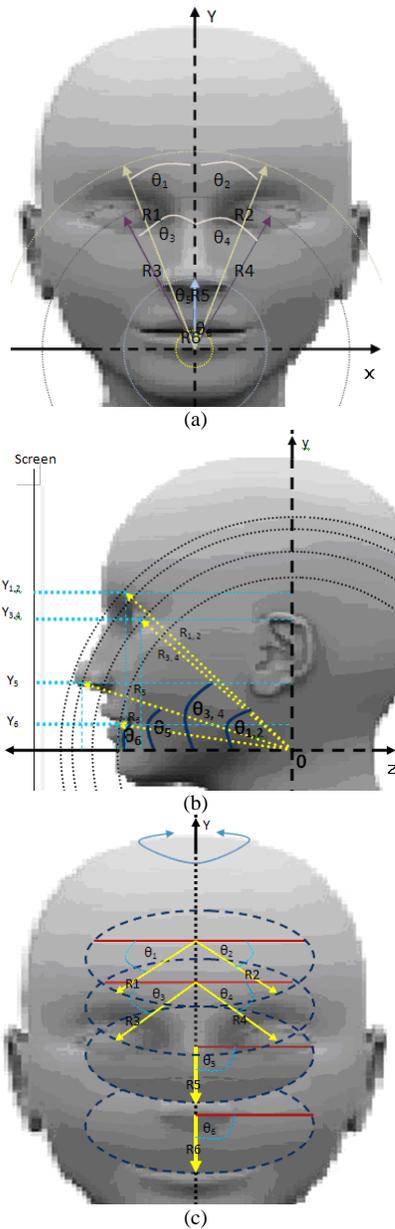


Fig. 1. 3D Head Model, (a) is Model on XY Planar, (b) is Model on YZ Planar, and (c) is Model on XZ Planar.

#### IV. PROPOSED METHOD

##### A. Head Pose Detection Overview

This section proposes a method for estimating the head posture of a pedestrian. Normally, on a road without a pedestrian crossing, when a pedestrian and a car driven by a person are close to each other, they exchange their intentions through nonverbal communication to ensure safe and secure traffic. However, in the case of an autonomous vehicle in which a person does not intervene in the operation, communication cannot be performed, and the following behavior cannot be assumed. As a result, it is easy to imagine that many people will be worried about autonomous vehicles running on the road and will feel uneasy when crossing the road.

OpenCV is an open-source computer vision and machine learning software library. It has C / C++, Python, Java, and MATLAB interfaces, and supports Windows, Linux, Android, and Mac OS. The library has over 2500 computer vision and machine learning algorithms. These are face detection and recognition, object identification, classification of human behavior in video, camera movement tracking, moving object tracking, 3D model extraction of objects, 3D point group generation from stereo cameras, image composition, scenes. It can be used to generate an entire high-resolution image, search for similar images from an image database, remove red eyes from images using a flash, and track eye movements. OpenCV is widely used by businesses, research groups and government agencies.

Dlib is an open-source software library written in C++. It is used in a wide range of fields such as robotics, embedded devices, mobile phones, and large-scale high-performance computing environments. In recent years, components for processing in a wide range of fields such as GUI (Graphical User Interface), machine learning, image processing, data mining, mathematical optimization, and Bayesian networks have been developed.

##### B. Representation of 3D Objects

A three-dimensional object with respect to a camera can be represented by the following two actions,

- 1) Translation: Moving the camera from one 3D position (X, Y, Z) to a new 3D position (X', Y', Z'). There are 3 degrees of freedom in movement, and it can move in the "X, Y, Z" directions.
- 2) Rotation: The camera can be rotated around the "X, Y, Z" axes. Rotation can be expressed by Euler angles (roll, pitch, yaw). In other words, it is possible to estimate the posture in three dimensions by finding three translations and rotations.

Fig. 2 shows an example of 3D representation of the face. Also, Fig. 3 shows the coordinate system conversion among the camera, the image (camera) and the world coordinate systems.

The coordinates of facial features shown in three dimensions are expressed in world coordinates. Three coordinate systems are used to estimate the attitude. If the attitude can be obtained, it will be possible to convert the 3D point in world coordinates to the 3D point in camera coordinates. The 3D points of the camera coordinates can be projected onto the image plane using camera-specific parameters such as focal length and lens distortion.



Fig. 2. 3D Mapping of the Face.

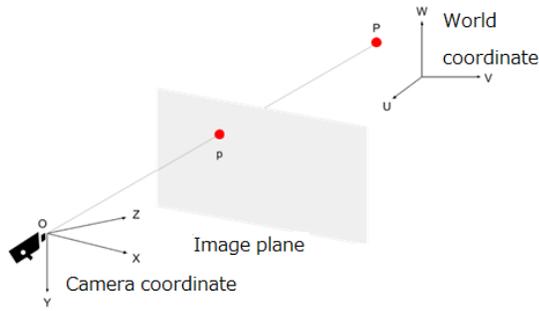


Fig. 3. Coordinate System Conversion.

Let the coordinate system fixed to the camera be  $(X, Y, Z)$ , the coordinate system fixed to the human head be  $(U, V, W)$ ,  $R$  be the rotation matrix, and  $t$  be the translation vector. The point  $P$  seen from the coordinate system fixed to the camera is expressed as follows.

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = R \begin{bmatrix} U \\ V \\ W \end{bmatrix} + t \quad (7)$$

Expressing this as an in-order transformation matrix, Eq. (8) is obtained.

$$\begin{bmatrix} X \\ Y \\ Z \end{bmatrix} = [R|t] \begin{bmatrix} U \\ V \\ W \\ 1 \end{bmatrix} \quad (8)$$

If the camera-specific parameters are known and the scale factor is  $s$ , then Eq. (9) is obtained.

$$\begin{bmatrix} x \\ y \\ 1 \end{bmatrix} = s \begin{bmatrix} f_x & 0 & c_x \\ 0 & f_y & c_y \\ 0 & 0 & 1 \end{bmatrix} \begin{bmatrix} X \\ Y \\ Z \end{bmatrix} \quad (9)$$

The relationship between  $(x, y)$  and  $(X, Y, Z)$  can be expressed. Using this relationship, if  $R$  and  $t$  can be derived so that the error between the point  $p'$  that will be projected on the two-dimensional plane and the point  $p$  that is actually projected can be minimized, the attitude estimation will be performed.

### C. Head Pose Detection based on CNN

In the head posture estimation based on deep learning in image recognition, the angle of the face is divided into 45 degrees in the left-right direction as shown in Fig. 4, and the face faces at 90 degrees, 45 degrees, 0 degrees, -45 degrees, and -90 degrees. Also, Fig. 5 shows the definition of the head pose angle (the geometric relation between the car and the pedestrian).

Preliminary experiments have shown that it is difficult to discriminate even the finest angles of the face. For example, even if two images with only one degree difference in face angle are given, it is difficult to distinguish them because there is no difference in features between the two images. Moreover, in this study, it is only necessary to be able to grasp a rough angle, so we could not find the need to discriminate even a fine angle. Therefore, classification is performed in 5 classes of 90 degrees, 45 degrees, 0 degrees, -45 degrees, and -90 degrees.



Fig. 4. Examples of Head Pose with the different Pose Angles.



Fig. 5. Definition of the Head Pose Angle (the Geometric Relation between the Car and the Pedestrian).

The angle is based on the line of sight between the car and the pedestrian. The model used is a convolutional neural network (CNN). CNN is a forward propagation network that includes a convolution layer and a pooling layer. A learning method often used for image recognition and natural language processing.

### D. Face Detection with Dlib

A trained model distributed by Dlib is used to detect facial feature points. As shown in Fig. 6, 68 feature points could be detected, and 6 of them (nose tip, chin, left end of left eye, right end of right eye, left corner of mouth, right corner of mouth) were used for head posture estimation.

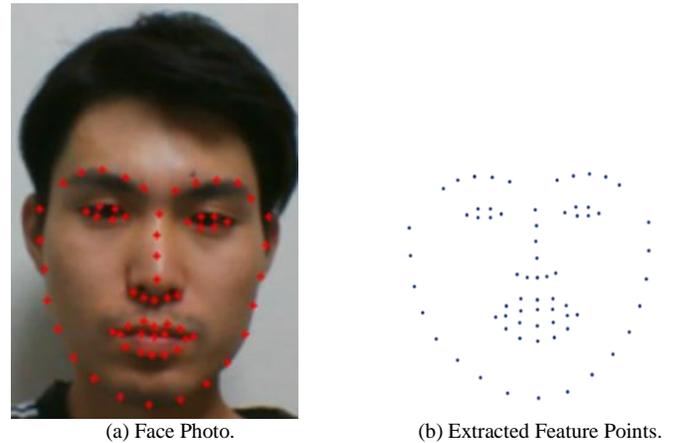


Fig. 6. Face Detection with Dlib.

## V. EXPERIMENTS

### A. Head Pose Detection

The camera used in the experiment was an HD (High Definition) webcam (manufactured by Sony Corporation) equipped with an "Exmor R for PC" CMOS (Complementary Metal Oxide Semiconductor) sensor, and the frame rate was 15 [fps]. The PC specifications for running this program are OS: Windows10 (64bit), CPU: Intel Core i5-5275U, and memory: 8.00GB.

The state of estimation is as shown in the figure below. Fig. 7 shows the coordinate system fixed to the head, which uses the rotation of the three axes to represent the angle. In addition, the estimation result expresses a three-dimensional view of the face with a green cube so that it is easy to understand visually, and as the estimation result, the angle of the face can be calculated accurately to a fine value. It was a good result.

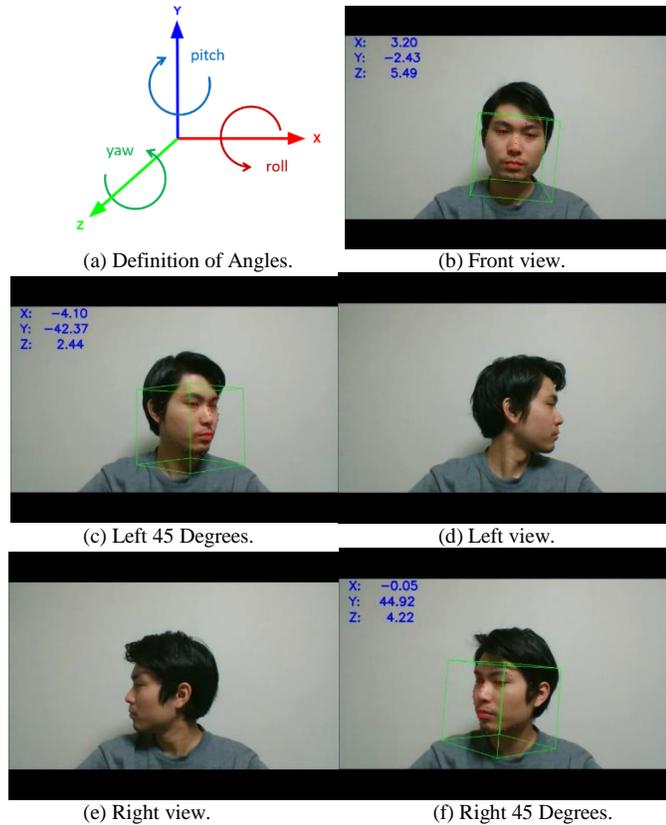


Fig. 7. Results from Head Pose Angle Detection.

### B. Head Pose Angle Detection

The verification experiment of head posture estimation and its result are described. The image used was Head Pose Image Database [23]. In the experiment, the data used was divided

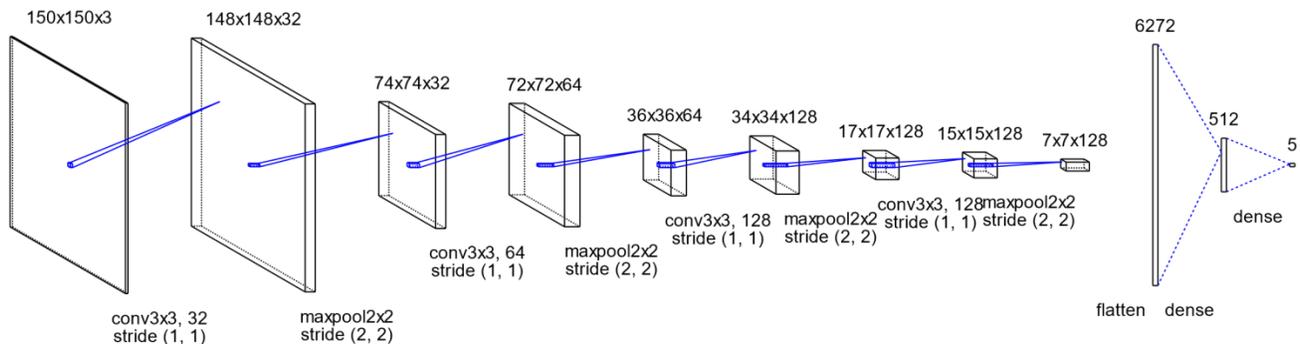


Fig. 9. CNN used.

into four patterns (RGB, RGB + thermography, grayscale image, RGB image assuming an image obtained by near infrared rays, and only the red channel element was extracted), and the accuracy was compared. Classify into five classes of 90 degrees, 45 degrees, 0 degrees, -45 degrees, and -90 degrees, respectively. The evaluation criteria for the classification results are set as shown in Fig. 8.

In the Fig. 8, marks are shown as follows:

⊙: Angle estimation was successful. The only thing left is how to respond (deceleration, warning).

○: Angle estimation failed, but within the permissible range. Correspondence is the same as ⊙ and there is no problem.

△: Angle estimation failed. There is a car approaching the pedestrian's field of view, but it may not be recognized, so safety first (not visible) is taken into consideration. Therefore, there is no problem in the end.

□: Angle estimation failed. However, as with △, safety first is taken as a result, so there is no problem in the end.

×: Angle estimation failed. Even though there are no approaching cars in the field of view of pedestrians, there is a possibility of taking dangerous measures.

Designated Angle	90°	⊙	○	△	□	□
	45°	○	⊙	△	□	□
	0°	△	△	⊙	□	□
	-45°	×	×	□	⊙	○
	-90°	×	×	□	○	⊙
	Estimated Angle	90°	45°	0°	-45°	-90°

Fig. 8. Evaluation Criteria.

In this study, we do not consider the actual response method that the automobile side will take after the estimation. The structure of the convolutional neural network was generated using an open-source Python implementation known as ConvNet Drawer<sup>3</sup>. Fig. 9 shows the CNN structure used.

C. Head Pose Detection Performance

There are three cameras, visible, NIR (Near Infrared) and thermal cameras for acquisition of face images. The purpose of this study is to detect head pose in all weather condition and in day and night-time condition. Therefore, the aforementioned three cameras are considered. As for the number of images of training data for learning process of CNN and the number of images for performance evaluation, Table I shows the numbers for each designated head pose angle for visible, NIR and thermal cameras while, Table II shows these numbers for visible and thermal cameras. In the later case, both of visible and thermal camera data are used together for training and performance evaluation.

The results using RGB images are shown in Fig. 10(a). The number of data used was 480, and the ratio of training data to verification data was 4:1. The facial images used for each class are data for 15 people. Most of the classified results were successful angle estimation for RGB images. Although there are parts where estimation fails in three places, we were able to create a model with high accuracy and no problems because it corresponds to the evaluation standard ○.

The number of data used was 480 RGB images and 160 thermography. The ratio of RGB images of each class to thermography is 3:1.

TABLE I. THE NUMBER OF IMAGES OF TRAINING DATA FOR LEARNING PROCESS OF CNN AND THE NUMBER OF IMAGES FOR PERFORMANCE EVALUATION FOR VISIBLE, NIR AND THERMAL CAMERAS

Head pose angle	No. of training data	No. of test data	Total
90°	72	18	90
45°	72	18	90
0°	90	30	120
-45°	72	18	90
-90°	72	18	90
Total	378	102	480

TABLE II. THE NUMBER OF IMAGES OF TRAINING DATA FOR LEARNING PROCESS OF CNN AND THE NUMBER OF IMAGES FOR PERFORMANCE EVALUATION FOR BOTH VISIBLE AND THERMAL CAMERAS

Head pose angle	No. of training data	No. of test data	Total
90°	96	24	120
45°	96	24	120
0°	120	30	160
-45°	96	24	120
-90°	96	24	120
Total	512	128	640

In the classification results, erroneous estimation was found in the parts corresponding to △ and □. Although there is no erroneous estimation at the point x, it can be said that the accuracy is lower than the result of only RGB images, which are all within the permissible range. In addition, although it was within the permissible range, there were many false estimates at 90 degrees and 45 degrees as shown in Fig. 10(b).

The data used is a grayscale version of all 480 images used in the experiment using only RGB images.

The results were predicted to some extent, but they were the worst compared to the experimental results of the other three patterns as shown in Fig. 10(c).

This is thought to be due to the fact that grayscale images have less information than RGB images.

As the amount of information is reduced, it becomes difficult to capture the features. The results of using only the image obtained by extracting only the red channel elements from the RGB image assuming the image obtained by near infrared rays are described.

The data used is only the red channel elements extracted from all 480 images used in the experiment using only RGB images. Originally, the image actually taken by the near-infrared camera should be used, but since there is no equipment, the simulation was performed in this way. By extracting only, the elements of the red channel from the RGB image, information on short wavelengths can be dropped, so we decided to regard the image used this time as an image obtained by shooting with a near-infrared camera.

Most of the classification results were successful angle estimation. Although there was an erroneous estimation outside the permissible range at only one location, the accuracy was second only to the result using only RGB images as shown in Fig. 10(d).

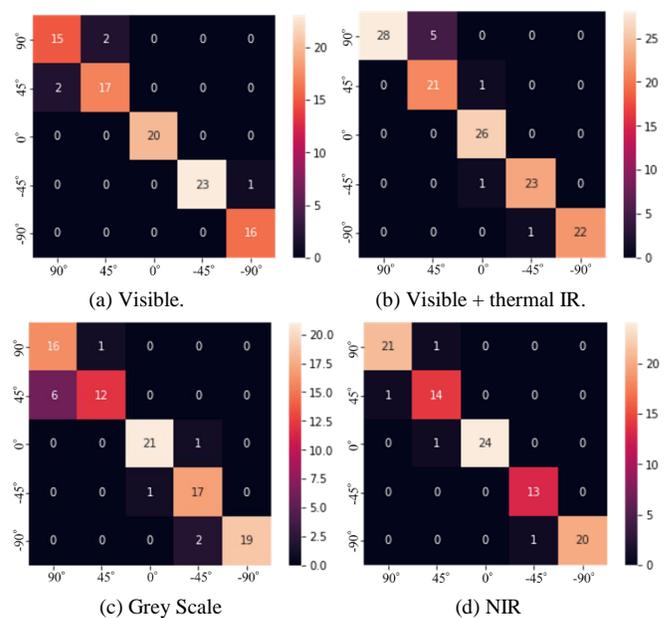


Fig. 10. Results from the Head Pose Detection Performance.

<sup>3</sup> <https://github.com/yu4u/convnet-drawer>,

In the head posture estimation using the feature points, even if the machine used has low specifications, the program can be processed with almost no delay, and the angle can be calculated with high accuracy. However, it did not work when the feature points were turned in a hidden direction, resulting in a disappointing result. If the angle can be calculated using the feature points on only one side of the face, it may be possible to handle it even when facing sideways.

In head posture estimation using deep learning, we conducted experiments with four patterns and classified angles. The order of accuracy was 1) RGB image, 2) Near infrared ray (red channel), 3) RGB image and thermography, and 4) Gray scale. From this result, it is considered better to use a normal camera for estimation in bright hours such as morning and noon. At night or in poor visibility, it is better to irradiate the front of the vehicle with near-infrared rays to make estimation, although the accuracy will be slightly lower. In addition, since automobiles usually illuminate headlights at night, we think that it may be possible to clearly capture pedestrians in combination with near infrared rays.

## VI. CONCLUSION

In this study, we proposed a method for estimating the head posture of a pedestrian and conducted a verification experiment in order for the autonomous vehicle to make contact with the pedestrian. Although the facial feature points could be detected in detail by the method using facial feature points, the necessary feature points could not be extracted when facing sideways, so angle classification was performed using a convolutional neural network.

The images used were RGB images, RGB images + thermography, grayscale images, and RGB images assuming images obtained by near infrared rays, with only the red channel elements extracted.

As a result, the RGB image model was the most accurate, but considering the criteria set, the RGB image model was used for morning and daytime detection, and the near-infrared image was used for nighttime and rainy weather scenes. It turned out that it is better to use the model obtained by the training in.

## VII. FUTURE RESEARCH WORKS

As a future task, we would like to create a mechanism to feed back the cognitive status to pedestrians. In addition, we would like to verify whether this system can behave in the same way as a human-driven vehicle and a pedestrian when this system is installed in an actual autonomous driving vehicle.

## ACKNOWLEDGMENT

The author would like to thank Professor Dr. Osamu Fukuda for their valuable discussions.

## REFERENCES

- [1] A. Al-Rahayfeh and M. Faezipour, "Eye Tracking and Head Movement Detection: A State-of-Art Survey," *IEEE Journal of Translational Engineering in Health and Medicine*, vol. 1, pp. 11- 22, 2013. <http://dx.doi.org/10.1109/JTEHM.2013.2289879>, 2013.
- [2] K. Liu, Y. P. Luo, G. Tei, and S. Y. Yang, "Attention recognition of drivers based on E. Murphy-Chutorian and M. M. Trivedi, "Head pose estimation and augmented reality tracking: An integrated system and evaluation for monitoring driver awareness" *IEEE Trans. Intell. Transp. Syst.*, vol. 11, no. 2, pp. 300-311, Jun. 2010.
- [3] D. J. Kupetz, S. A. Wentzell, and B. F. BuSha, "Head motion controlled power wheelchair" in *Proc. IEEE 36th Annu. Northeast Bioeng. Conf.*, Mar. 2010, pp. 1-2, 2010.
- [4] L. M. King, H. T. Nguyen, and P. B. Taylor, "Hands-free headmovement gesture recognition using artificial neural networks and the magnified gradient function," in *Proc. 27th Annu. Conf. Eng. Med. Biol.*, 2005, pp. 2063-2066. <http://dx.doi.org/10.1109/ieems.2005.1616864>, 2005.
- [5] S. T. Nguyen, H. T. Nguyen, P. B. Taylor, and J. Middleton, "Improved head direction command classification using an optimised Bayesian neural network" in *Proc. 28th Annu. Int. Conf. EMBS*, 2006, pp. 5679-5682, 2006.
- [6] S. Manogna, S. Vaishnavi, and B. Geethanjali, "Head movement based assist system for physically challenged" in *Proc. 4<sup>th</sup> ICBBE*, 2010, pp. 1-4, 2010.
- [7] S. Kim, M. Park, S. Anumas, and J. Yoo, "Head mouse system based on gyro- and opto-sensors" in *Proc. 3rd Int. Conf. BMEI*, vol. 4, 2010, pp. 1503-1506, 2010.
- [8] K. Satoh, S. Uchiyama, and H. Yamamoto, "A head tracking method using bird's-eye view camera and gyroscope" in *Proc. 3<sup>rd</sup> IEEE/ACM ISMAR*, Nov. 2004, pp. 202-211, 2004.
- [9] Kohei Arai, H. Tolle, A. Serita, "Mobile Devices Based 3D Image Display Depending on User's Actions and Movements. *International Journal of Advanced Research in Artificial Intelligence (IJARAI)*, 2013, vol 2, no. 6. pp.71-78, 2013.
- [10] H. Tolle, A. Pinandito, EM. Adams J., K. Arai, "Virtual reality game controlled with user's head and body movement detection using smartphone sensors". *ARPN Journal of Engineering and Applied Sciences*. Nov. 2015, vol 10, no 20, pp 9776-9782, 2015.
- [11] Kohei Arai and Kenro Yajima, *Communication Aid and Computer Input System with Human Eyes Only*, Electronics and Communications in Japan, Volume 93, Number 12, 2010, pages 1-9, John Wiley and Sons, Inc., 2010.
- [12] Kohei Arai, *Computer Input by Human Eyes Only and Its Applications, Intelligent Systems in Science and Information*, 2014, Studies in Computer Intelligence, 591, 1-22, Springer Publishing Co. Ltd., 2015.
- [13] Djoko Purwanto, Ronny Mardiyanto, Kohei Arai, Electric wheel chair control with gaze detection and eye blinking, *Proceedings of the International Symposium on Artificial Life and Robotics*, GS9-4, 2009.
- [14] Djoko Purwanto, Ronny Mardiyanto and Kohei Arai, Electric wheel chair control with gaze detection and eye blinking, *Artificial Life and Robotics*, AROB Journal, 14, 694,397-400, 2009.
- [15] Kohei Arai and Makoto Yamaura, Computer input with human eyes only using two Purkinje images which works in a real time basis without calibration, *International Journal of Human Computer Interaction*, 1,3, 71-82,2010.
- [16] Kohei Arai, Ronny Mardiyanto, A prototype of electric wheelchair control by eye only for paralyzed user, *Journal of Robotics and Mechatronics*, 23, 1, 66-75, 2010.
- [17] Kohei Arai, Kenro Yajima, Robot arm utilized having meal support system based on computer input by human eyes only, *International Journal of Human-Computer Interaction*, 2, 1, 120-128, 2011.
- [18] Kohei Arai and Ronny Mardiyanto, A prototype of electric wheel chair controlled by eyes only for paralyzed users, *Journal of Robotics and Mechatronics*, 23, 1, 66-75, 2011.
- [19] Kohei Arai, Ronny Mardiyanto, Autonomous control of eye based electric wheel chair with obstacle avoidance and shortest path finding based on Dijkstra algorithm, *International Journal of Advanced Computer Science and Applications*, 2, 12, 19-25, 2011.
- [20] Kohei Arai, Ronny Mardiyanto, Eye-based human-computer interaction allowing phoning, reading e-book/e-comic/e-learning, Internet browsing and TV information extraction, *International Journal of Advanced Computer Science and Applications*, 2, 12, 26-32, 2011.
- [21] Kohei Arai, Ronny Mardiyanto, Eye based electric wheel chair control system-I(eye) can control EWC-, *International Journal of Advanced Computer Science and Applications*, 2, 12, 98-105, 2011.

- [22] Kohei Arai, Ronny Mardiyanto, Evaluation of users' impact for using the proposed eye based HCI with moving and fixed keyboard by using eeg signals, *International Journal of Research and Reviews on Computer Science*, 2, 6, 1228-1234, 2011.
- [23] Kohei Arai, Ronny Mardiyanto, Electric wheel chair controlled by human eyes only with obstacle avoidance, *International Journal of Research and Reviews on Computer Science*, 2, 6, 1235-1242, 2011.
- [24] Kohei Arai, R.Mardiyanto, Evaluation of users' impact for using the proposed eye based HCI with moving and fixed keyboard by using eeg signals, *International Journal of Research and review on Computer Science*, 2, 6, 1228-1234, 2012.
- [25] Kohei Arai, R.Mardiyanto, Electric wheel chair controlled by human eyes only with obstacle avoidance, *International Journal of Research and review on Computer Science*, 2, 6, 1235-1242, 2012.
- [26] R.Mardiyanto, Kohei Arai, Eye-based Human Computer Interaction (HCI) A new keyboard for improving accuracy and minimizing fatigue effect, *Scientific Journal Kursor*, (ISSN 0216-0544), 6, 3, 1-4, 2012.
- [27] Kohei Arai, R.Mardiyanto, Moving keyboard for eye-based Human Computer Interaction: HCI, *Journal of Image and Electronics Society of Japan*, 41, 4, 398-405, 2012.
- [28] Kohei Arai, Ronny Mardiyanto, Eye-based domestic robot allowing patient to be self-services and communications remotely, *International Journal of Advanced Research in Artificial Intelligence*, 2, 2, 29-33, 2013.
- [29] Kohei Arai, Ronny Mardiyanto, Method for psychological status estimation by gaze location monitoring using eye-based Human-Computer Interaction, *International Journal of Advanced Computer Science and Applications*, 4, 3, 199-206, 2013.
- [30] Kohei Arai, Kiyoshi Hasegawa, Method for psychological status monitoring with line of sight vector changes (Human eyes movements) detected with wearing glass, *International Journal of Advanced Research in Artificial Intelligence*, 2, 6, 65-70, 2013.
- [31] Kohei Arai, Wearable computing system with input output devices based on eye-based Human Computer Interaction: HCI allowing location based web services, *International Journal of Advanced Research in Artificial Intelligence*, 2, 8, 34-39, 2013.
- [32] Kohei Arai Ronny Mardiyanto, Speed and vibration performance as well as obstacle avoidance performance of electric wheel chair controlled by human eyes only, *International Journal of Advanced Research in Artificial Intelligence*, 3, 1, 8-15, 2014.
- [33] Kohei Arai Ronny Mardiyanto, Speed and vibration performance as well as obstacle avoidance performance of electric wheel chair controlled by human eyes only, *International Journal of Advanced Research in Artificial Intelligence*, 3, 1, 8-15, 2014.
- [34] Kohei Arai, Service robot with communication aid together with routing controlled by human eyes, *Journal of Image Laboratory*, 25, 6, 24-29, 2014.
- [35] Kohei Arai, Information collection service system by human eyes for disable persons, *Journal of Image Laboratory*, 25, 11, 1-7, 2014.
- [36] Kohei Arai, Relations between psychological status and eye movements, *International Journal of Advanced Research on Artificial Intelligence*, 4, 6, 16-22, 2015.
- [37] Kohei Arai, Method for 3D Image Representation with Reducing the Number of Frames Based on Characteristics of Human Eyes, *International Journal of Advanced Research on Artificial Intelligence*, 5, 8, 7-12, 2016.
- [38] Kohei Arai, Error Analysis of Line of Sight Estimation Using Purkinje Images for Eye-Based Human Computer Interaction: EBHCI, *International Journal of Advanced Research on Artificial Intelligence*, 5, 10, 14-23, 2016.
- [39] Kohei Arai, Mobile Phone Operations using Human Eyes Only and Its Applications, *International Journal of Advanced Computer Science and Applications IJACSA*, 9, 3, 2018.
- [40] Kohei Arai, Method for Thermal Pain Level Prediction with Eye Motion using SVM, *International Journal of Advanced Computer Science and Applications IJACSA*, 9, 4, 170-175, 2018.
- [41] Kohei Arai, Akihiro Yamashita, Hiroshi Okumura, Pedestrian safety with eye contact between autonomous car and pedestrian, *International Journal of Advanced Computer Science and Applications IJACSA*, 10, 5, 161-165, 2019.

#### AUTHOR'S PROFILE

**Kohei Arai**, He received BS, MS and PhD degrees in 1972, 1974 and 1982, respectively. He was with The Institute for Industrial Science and Technology of the University of Tokyo from April 1974 to December 1978 also was with National Space Development Agency of Japan from January, 1979 to March, 1990. During from 1985 to 1987, he was with Canada Centre for Remote Sensing as a Post Doctoral Fellow of National Science and Engineering Research Council of Canada. He moved to Saga University as a Professor in Department of Information Science on April 1990. He was a councilor for the Aeronautics and Space related to the Technology Committee of the Ministry of Science and Technology during from 1998 to 2000. He was a councilor of Saga University for 2002 and 2003. He also was an executive councilor for the Remote Sensing Society of Japan for 2003 to 2005. He is a Science Council of Japan Special Member since 2012. He is an Adjunct Professor of University of Arizona, USA since 1998. He also is Vice Chairman of the Science Commission "A" of ICSU/COSPAR since 2008 then he is now award committee member of ICSU/COSPAR. He wrote 55 books and published 620 journal papers as well as 450 conference papers. He received 66 of awards including ICSU/COSPAR Vikram Sarabhai Medal in 2016, and Science award of Ministry of Mister of Education of Japan in 2015. He is now Editor-in-Chief of IJACSA and IJISA. <http://teagis.ip.is.saga-u.ac.jp/index.html>.

# Introduction to NFTs: The Future of Digital Collectibles

Muddasar Ali, Sikha Bagui  
Department of Computer Science  
University of West Florida, Pensacola, FL 32514

**Abstract**—This paper commences by introducing the essentials of blockchain technology and then goes into how Ethereum blockchain revolutionized blockchain. Smart contracts are presented in the context of showing how they play an important role in implementing rules regarding the Ethereum blockchain, allowing the user to regulate digital assets. The standards used in the Ethereum blockchain to build Non-Fungible Tokens (NFTs) are discussed. The paper concludes by presenting the benefits of NFTs as well as the use of Ethereum blockchain for future applications.

**Keywords**—Blockchain technologies; smart contracts; cryptocurrencies; ethereum; non-fungible tokens (NFTs)

## I. INTRODUCTION: WHAT IS BLOCKCHAIN TECHNOLOGY?

Blockchain technology, considered to be one of the most secure technologies to keep data safe, is constructed on blocks of data. Blockchain technology is fast, public, cheap, easy to use, transparent and programmable technology that allows for the transfer of information and/or financial assets instantaneously from one part of the world to another. It is a protocol that governs the rules and regulations for value exchange. Blockchain technology can contain any type of information and the link between each block and the next is called a chain because the blocks are connected in a way that cannot be altered [1]. Blockchain also enables users to safely transfer values globally. The safety comes from the fact that once the information is recorded in the blockchain, it becomes infeasible to alter it. This feature is called immutability [2]. This is especially important for storing bank records or transactions. The safety of this technology is based on the characteristics of the chains between the blocks. A new block is added to the chain by calculating the hash of the previous block and using that as part of the data for the next block [3].

To understand how the blockchain technology works, one needs to first understand what is stored in a single block. Each block contains three types of information, the data, its hash, and a pointer to the hash of the previous block. And each application of blockchain technology can have its own type of data that is completely different from all other applications. For example, bitcoin stores information about the transactions of bitcoins, such as the sender, the receiver, and the amount of bitcoin that is transferred. The hash of the block is a unique identifier for the block. Each block's hash will be different based on the data that is stored in it, so if the data gets changed the hash also changes. The addition of the previous block's hash is the main reason behind the success of blockchain technology and this is also why the alteration of data stored in

the blockchain becomes infeasible. And this is what makes it reliable to store any kind of information that needs to be kept safe. If one wants to alter the blockchain by changing the information stored in a block, this will also lead to a change in the hash of the block, which will consequently not match with the hash that is in its next block, causing a chain reaction. So, any alteration in a single block will invalidate the whole blockchain [3].

Even though blockchain technology is not totally new, its implementations are still in their early stages, and it is for this reason that many people struggle to understand the real use of blockchain technology. For some time, its implementation seemed limited to cryptocurrencies but there is much more to where this technology can be applied and in today's world. We constantly see new applications based on blockchain technology and we will get more familiar with them as they become part of our daily lives.

Blockchain technology has the potential to upgrade any system that requires a third-party regulatory authority that serves to define the authenticity of any changes that will take place in the system. More specifically, the technology can replace the authority decentralizing the authenticity process to every member that is present in the organization. One of the most widely known applications of blockchain technology is proposed by the Bitcoin whitepaper published in 2008 [4]. This work introduced the concept of cryptocurrencies or electronic cash that would be transferred without going through a financial institution. A digital ledger was introduced that would be distributed to every node present in the blockchain to keep track of all the transactions that were taking place in an organization. The development of bitcoin has radically changed the concept of money and currency [4]. Bitcoin is the first-ever form of a digital asset or money that not only has no backing or intrinsic value but also no centralized issuer or controller. It is decentralized. While its introduction is proof of the potential of blockchain technology, the fact that it is used as a distributed tool has attracted even more attention and has inspired more applications of blockchain technology. Colored coins [5] also use blockchain digital assets to represent custom currencies and financial instruments; Smart Property represents the ownership of an underlying physical device, NameCoin [6]. NameCoin also represents non-fungible assets such as domain names. Complex applications rely on digital currency or assets as being directly controlled by pre-programmed code with functionalities, enabling the implementation of Smart Contracts [7]. Hence a turning point in blockchain technology took place with the introduction of Ethereum in 2014 [8]. This is where

the nodes were not only keeping track of the transactions, but they could also program and execute software, hence taking the name of smart contracts. Being able to write specific instructions atop Ethereum's digital protocol makes it more resourceful for many more applications.

With this introduction to blockchain technologies, next this paper goes into how Ethereum blockchain revolutionized blockchain. Smart contracts are presented in the context of showing how they play an important role in implementing rules regarding the Ethereum blockchain, allowing the user to regulate digital assets. The standards used in the Ethereum blockchain to build Non-Fungible Tokens (NFTs) are discussed. The paper concludes by presenting the benefits of NFTs as well as the use of Ethereum blockchain for future applications.

## II. ETHEREUM BLOCKCHAIN

Transactions in bitcoin are based on who is moving money to whom and how much. But it is also important to know how much money is present in the network. For this, there must be a database storing how much money can be spent and how much money can be moved. There must also be a centralized environment with centralized authority that has access to this database where the amounts are registered. But what if we want a decentralized environment, which is the basic spirit behind blockchain technologies and more specifically, is the most important factor that made bitcoin blockchain famous [bitcoin-cash]. Nakamoto's solution [4] is the most basic and practical solution in this open permission-less context. To extend the concept of decentralization and make it accessible to any type of application, the Ethereum blockchain provides simple features. Ethereum, by its founder and inventor Vitalik Buterin [8], is described to be based on a concept of crypto-economics. Ethereum is a combination of major concepts of cryptography and economics. Concepts like hashing and digital signatures used in cryptographic algorithms, and the economic incentives that keep systems like bitcoins going, are used to create decentralized networks with memory [8]. This means that not only the network but also the database will be decentralized. This was considered a breakthrough in blockchain technology as it helped to break new ground in the areas of application of the technology [9]. This was a broader view of how blockchain could be applied, greatly improving the concept of peer-to-peer digital currency transactions. Many different applications were introduced. The first one was NameCoin [6] which was based on bitcoin technology and provided a peer-to-peer decentralized DNS service.

Using this new concept, many different applications can be decentralized. Many other digital assets can be created. But a problem arises when we want to apply this concept for each digital asset and create a different system for every type of service to be developed on the blockchain. This will end up in there being too many services running separately and keeping track of all of them would become tedious; hence the idea behind creating Ethereum. Ethereum is a single general purpose blockchain that can have different types of applications running on it [8]. This blockchain will not have specific rules for transactions for each type of application but will have general rules and access to a general-purpose

programming language. Hence Ethereum gives the freedom to build and run applications on the blockchain. Though Ethereum offers this flexibility where a broad range of applications can be built, the main categories of applications still remain related to currencies, mainly due to the fact that the main aspects of a blockchain are decentralization and shared memory, making it suitable for cryptocurrencies.

An Ethereum blockchain state is composed of accounts, which actually are objects. These accounts have a 20-byte address. The blockchain state transitions when there are direct transfers of value and information between accounts or objects. An Ethereum account has four parts:

- The nonce. A nonce is a counter set to make sure each transaction can only be processed once.
- The current balance of the ether account.
- The contract code of the account.
- The storage of the account, which is empty by default.

Ether is used to pay, and is the key crypto-fuel or cryptocurrency of Ethereum. It is used to pay transactional or operational fees. In general, there are two account types: externally owned accounts and contract accounts. Externally owned accounts, which have no code, are controlled by private keys, and contract accounts play by the rules of their contract code. Messages (or instructions) can be sent from externally owned accounts by creating transactions and signing them. Contract accounts, however, are used to send messages or instructions and/or create contracts every time the contract account receives a message. Also, when messages or instructions are received in contract accounts, internal storage can be read from and written to.

## III. SMART CONTRACTS

The concept of Smart Contracts was introduced [7] in the 1990s. This is another category of applications that will suit blockchain technology. To understand the concept behind smart contracts we can make an analogy to a vending machine. A vending machine is a device implemented in hardware that implements conditions of an agreement. In this case, a simple condition for this agreement would be that a user puts an amount of money in the vending machine and a related item comes out. If the user does not insert adequate money, the item will not come out. The vending machine is encoded with a set of rules that also keeps the items secured. The security is proportional to the value of the items that the vending machine holds. The vending machine is a very simple example of a contract with a bearer. In this case, anybody with coins in the right currency can participate in an exchange with the vendor, the vending machine. And, the lockbox and other security mechanisms (including programmed security mechanisms) protect the stored coins and contents from attackers.

This concept is applied to digital assets, but with broader rules and more complicated types of contracts. Smart contracts provide stronger and more secure verification for access to the property. Another example is digital security systems for automobiles. The protocol defines the conditions to give authority of the property based on who is the rightful owner at

a certain time. Considering cryptographic keys as means to access a car, we can determine conditions that will make the owner change, and therefore change the conditions in which the car can be used. A smart lien protocol can be created, described as follows: if the owner fails to make the scheduled payments, the smart contract invokes the lien protocol. This would give back authority of the car keys to the bank. A further step would probably remove the lien in the event the loan gets paid off [7]. A graphical representation of this example can be seen in Fig. 1.

To keep digital assets secure, a computer program that has direct control of them is put into service. This means that there is not a person that will control the asset but a computer that follows a digital contract that provides specific rules to handle it, and it cannot be controlled by any user. The decisions will be made directly by the computer program. Once again, the smart contract should include conditions that are strong enough to keep the asset secure, in proportion to the importance of the digital asset. This specific environment can be implemented on the Ethereum blockchain. Once an amount of ether is sent to a

computer program as a digital asset, and this follows a smart contract, it can then handle the money as specified in the contract. So, if the contract specifies that a certain amount of money will go to an address, the money will move as per the conditions of the contract and no human interaction will take place. The concept of smart contracts can be extended to any other application which is based on a self-executing financial contract such as insurance. Here a set of rules would be specified and when the condition is met an asset would be unlocked for the user.

Smart contracts have been used in the area of crowdfunding where the contract defines certain conditions before letting the money go to a certain project that people are supporting. For example, if a developer requires a certain amount of money to kickstart his/her project, the money will be managed by a computer program that will follow the rules given by the smart contract. In this case, no user can intervene in the process to move any asset, and everything is managed by the program. This transparency gives all the members that are participating in crowdfunding more trust in the process.

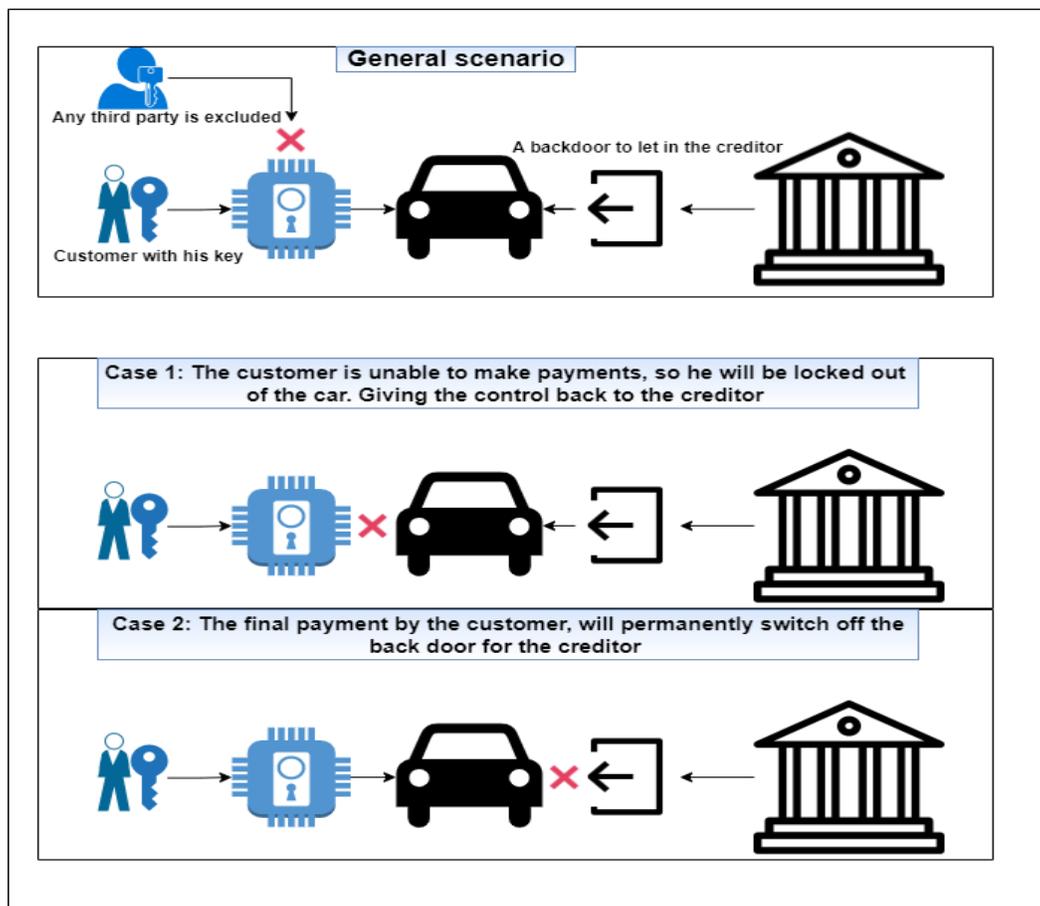


Fig. 1. Hypothetical Digital Security System for Automobiles that Relies on a Smart Contract.

#### IV. ETHEREUM STANDARDS

As presented above, smart contracts are basically pre-programmed or intelligent programs that get executed when certain conditions are met or certain events happen. Since the process is automated, they have no downtime. They also allow for the creation of decentralized applications [9].

The Ethereum Virtual Machine (EVM), which runs on an Ethereum network, simplifies the process of building blockchain applications. EVM allows developers of each application to build new blockchains from scratch. And, developers do not have to use any specific programming language. This allows Ethereum to technically build the first decentralized world computer on a public blockchain [9].

The native currency for Ethereum is Ether (ETH). The platform is mainly maintained through transactional or operational fees. One of the most useful advantages of Ethereum is its ability to create unique tokens, with various functionalities, and operate on the Ethereum blockchain. These tokens have multiple utility-like purposes.

Ethereum Request for Comments (ERC) are application level standards for Ethereum. ERCs include token standards, name registries, library/package formats, and other features. An ERC can be created by anyone, but it falls on the creator to clearly explain the standard. This will also help the creator gain support from within the community. There are common ERC standards for functions of each token type, allowing applications and smart contracts to interact with them in pre-determined or pre-planned ways. ERC-20, which allows for the simple creation, use, and exchange of Ethereum-based tokens, is the most common ERC standard used to date.

##### A. Explanation of Terms

Ethereum accounts, identified by 20-byte addresses, have externally owned user accounts and contract accounts. Users can create accounts, call or access accounts, or issue transactions (which are signed data packages) that transfer value to users of other accounts and contracts. All transactions are recorded on the Ethereum blockchain. A contract gets activated by a user transaction or by a message or instruction from another contract. Messages only exist in the execution environment of the Ethereum Virtual Machine (EVM), hence are not recorded on the Ethereum blockchain. This is because messages are consequences of an initial transaction. Their existence is limited to the execution environment of the Ethereum Virtual Machine (EVM) and this can be seen in the execution trace logs and potential state changes.

Abstract Binary Interface (ABI) [10]: Most Ethereum contracts follow the ABI standard. The ABI standard identifies functions by signatures. These signatures are made of the first four bytes of the Keccak-256 hash of the function name plus parameter types. The presence or absence of a function in a contract is checked by locating the corresponding 4-bytes hash in the deployed bytecode. This also allows the compliance of a contract with interface standards to be determined by its bytecode.

##### B. Functionalities Available for Token Contracts

There are presently several functionalities available for token contracts: (i) keeping track of token holdings; (ii) transferring ownership of token contracts. The transfer of ownership is shown in the logs. A safe transfer is where the information is known. Hence, after approval, tokens are taken or withdrawn from the known address, as opposed to being sent or transferred to an unknown address where they may be lost. So, in a safe transfer, both the sender and receiver would be known to the sender and receiver respectively; (iii) the creation of tokens and destruction of tokens. This is also called minting or burning of tokens; (iv) the distribution of tokens. This includes trading (e.g., via ICOs and airdrops) of tokens; (v) token contracts are also programmed to check for authentication and have various roles built into the system. Roles include roles that control the system, like pause or lock, and information provisions like view functions; and (vi) other functionalities including utilities.

##### C. Token Standards

There are several accepted token standards which are determined by the community that establishes standard interfaces for tokens. The programming language used is Solidity. This programming language is prevalent on Ethereum. The standards that have been accepted so far are:

- ERC-20 Token Standard [11]: This is the most widely used and most general token standard. This standard is programmed to provide very basic functionality like ability to transfer tokens. This standard also allows tokens to be approved and disapproved. This means that they can be spent by another on-chain third party. ERC-20 has six mandatory and three optional functionalities as well as two events to be implemented by a conforming API.
- ERC-721 Non-Fungible Token Standard [12]: In ERC-721, each token is distinct and non-fungible, hence this allows for the tracking of unique assets. Each asset has individual ownership and is atomically tracked. ERC-721 requires each token to have ten functions that are considered mandatory and three events.
- The ERC-777 Token Standard [13]: ERC-777 provides advanced functionalities for interaction with tokens while keeping compatibility with ERC-20. It's advanced functions include operations to send tokens on behalf of other addresses and ways or hooks for sending and receiving. This allows token holders more control over their tokens. ERC-777 requires each token to have 13 functions that can be considered mandatory and five events.
- ERC-1155 Multi Token Standard [14]: ERC-1155 is considered a multi-token standard since any combination of fungible and non-fungible tokens can be managed in a single contract with this token standard. Multiple token types can also be transferred at once. ERC-1155 requires each token to have six functions that can be considered mandatory functions and four events.

#### D. Proposed Security Token Standards

In addition to the accepted standards discussed in the last section, others token standards are being discussed. ERC-1462 is more general, while ERC-1450 and ERC-1644 are project oriented.

- ERC-1462 [15] Base Security Token. Though ERC-1462 this is similar to ERC-20, it is an extension to ERC-20. ERC-1462 provides compliance with securities regulations and legal enforceability. Though it is mainly used for general use cases, added functionality and limitations as pertaining to particular projects or markets can be enforced effectively. ERC-1426 also includes KYC (Know Your Customer) and AML (Anti Money Laundering) regulations and the ability to lock tokens for an account and restrict them from transfer due to a legal dispute. An added benefit is that this standard also allows for the attachment of documents to tokens. ERC-1426 requires it's compliant tokens to implement four mandatory checking functions while still implementing ERC-20 standards functions. It also gives the opportunity of two optional documentation functions.
- ERC-1450 LDGR Token [16]. ERC-1450, which also extends ERC20, is a security token for issuing and trading SEC-compliant securities. The ERC-1450 standard allows for the recording of ownership and transfer of securities sold in compliance with the Securities Act Regulations CF, D and A. ERC-1450 has mandatory functions of its own, and it requires some optional parts of ERC-20 to be mandatory. It also requires certain modifier and constructor arguments to be set up and implemented.
- ERC-1644 Controller Token Operation Standard [ERC-1644]. Sometimes the issuer (or an entity delegated to by the issuer) or owner, may have to have the ability to force transfer tokens. ERC-1644 allows a token to clearly declare whether or not a controller can unilaterally transfer tokens between addresses. The ERC-1644 standard requires compliant tokens to have three mandatory functions and two events.

#### E. ERC-20 Standard

The ERC-20 standard was the first to lay down the concept of dealing with tokens and their implementations. A token can virtually represent anything in Ethereum, from lottery tickets to an ounce of gold or financial assets like a share in a company. This concept has been used to re-invent the concept of crowdfunding, introducing the Initial Coin Offerings (ICOs) [17] that are equivalent to Initial Public Offerings (IPOs) but for companies looking to raise money to create a new coin, app, or service. ICOs are tokens that are bought by people that agree to invest in a company, whereas IPO investors buy stocks of a company. Having a powerful feature that can represent this variety of valuable elements comes along with the necessity of having a robust standard that is also capable of handling all the assets in a proper way. The ERC-20 standard allows for the implementation of a standard API for tokens within smart contracts. This standard provides basic functionality to transfer

tokens, as well as allows tokens to be approved so they can be spent by another on-chain third party. The implementation of this standard also provides a standard interface to allow any tokens on Ethereum to be re-used by other applications.

ERC-20 also introduces a standard for Fungible Tokens, which means that they have a property that makes each token exactly the same in type and value as another token [11]. The ERC-20 standard is one of the most important standards that led to the concept of NFTs.

If a Smart Contract implements the methods and events provided by the ERC-20 standard, it can be called an ERC20 Token Contract and once deployed it will be responsible to keep track of the created tokens on Ethereum.

#### F. ERC-721: The Standard for Non-fungible Tokens

The ERC-721 (Ethereum Request for Comments 721), proposed by [12], is a Non-Fungible Token Standard. ERC-721 has an API for tokens within Smart Contracts. This is a free open standard that allows for the building of non-Fungible or unique tokens on the Ethereum blockchain [12]. ERC-721 introduces an extension to the common interface for tokens by additional functions, which led to having unique tokens, thus non-fungible. These unique tokens took the name of NFTs [18]. The fundamental characteristic of NFTs is the uniqueness, which means they cannot be exchanged with like-for-like items, making it the most suitable way to identify something or someone that is not substitutable. This type of token can be used on platforms that offer collectibles, access keys, lottery tickets, numbered seats for concerts or sports matches, etc. Once one comes in possession of any of these unique items, he/she can use these NFTs to represent ownership. Uniqueness is guaranteed by NFTs because there is only one token that has some specific characteristic, and they are completely different from any other NFT that is present in the market. Furthermore, there is only one official owner at a time and the ownership is secured by the Ethereum blockchain, which guarantees that no one can modify the record of ownership or copy/paste a new NFT into existence.

Every NFT is essentially a decentralized application, and its properties can be summarized as follows [9].

- Verifiability: This means that the NFT's token metadata as well as ownership can be publicly verified.
- Transparent Execution: This means that all activities on NFTs including minting, selling, and purchasing are publicly available.
- Availability: This means that NFTs are always available to be sold and bought. The system for NFTs never goes down.
- Tamper-resistance: This means that trading records related to NFTs are persistently stored and cannot be changed or manipulated in any way after the transactions are confirmed.
- Usability: This means that each NFT has its most recent ownership information, and this information is clear and user friendly.

- Atomicity: The process of trading NFTs is atomic.
- Tradability: Every NFT can be traded and exchanged.

In other words, each token created or minted has a unique identifier that is not interchangeable with any other token and has only one owner which is easily verifiable. If the owner decides to sell an NFT, he/she can only use the Ethereum-based NFT market. In some cases, the original creator can also earn resale royalties. In some cases, an owner can also decide to hold the NFT forever without worrying about losing the asset because it is secured in the wallet on Ethereum. Every NFT has a creator that decides an element on which he/she wants to apply the standard to make it a digital asset. The creator can:

- Easily prove that he/she is the creator of that particular NFT.
- Determine the scarcity: The creator of an NFT can determine how many replications will exist. To make an asset unique, the creator may create an NFT where only one is minted as a special rare collectible.
- Earn royalties every time it's sold. Some creators can program royalties into it so each time the item is sold from one owner to another they earn a percentage as royalties.
- Sell it on any NFT market or peer-to-peer. The creator will not be locked to any platform and will not have the necessity of anyone to intermediate.

Non-fungible tokens are powerful due to the standards. The standards provide developers with the guarantee that the assets will behave in certain ways. Standards also describe how to interact with the basic functionality of the assets. Fungible tokens are regulated by the ERC-20 standard, whereas NFTs are regulated through an ERC-721 standard. ERC-721 was the

first standard for representing non-fungible digital assets. ERC-721 is an inheritable Solidity smart contract standard, meaning that developers can easily create new ERC-721 compliant contracts. The standard relates the unique identifiers (each of which represents a single asset) to addresses. Basically, the owner is mapped to the unique identifier. It also provides a regulated way to transfer these assets using the *transferFrom* method.

In the beginning potential use of these unique tokens was unclear, mainly because they were totally different from the concept of fungible tokens and their applications. But they soon became the most suitable way for digital artists to make their art worth [18]. Digital artists create immense amounts of content, which require a lot of time and dedication. But often they are not compensated enough for their work. The problem with creating any type of digital content is that it can be easily copied and replicated without giving the creator any compensation or credit. The market of digital art and digital collectibles grew from fifty-two million to four hundred and ninety million dollars within the past year [19].

An artist who creates digital content and wants to sell his/her product online will not be able to fully secure his/her art, since anyone can make a copy of it. But, if the same digital work is combined with the Ethereum blockchain standard ERC-721 and converted into a NFT, this will make the art unique; in this case, nobody can have ownership of the digital product other than the person written on the NFT. In this situation, even though the same product can be replicated on the internet, no one else can have the ownership until the NFT is bought from the creator. This solution gave a huge boost to the market of digital art and digital collectibles, which had a growth of more than four hundred million dollars within the past year. Table I lists the ten most valuable NFTs ever sold [19].

TABLE I. THE TABLE SHOWS THE TOP 10 MOST VALUABLE NFTS EVER SOLD (RETRIEVED ON 08/04/2021) [19]

Name	Artist	Description	Price sold \$
Metarift	Pak	Group of spherical objects moving	904,4013
Forever Rose	Kevin Abosch	Digital photograph of a rose	1 Million
CryptoPunk 4156	Algorithm-generated	Pixel art	1.5 Million
"Genesis" Estate	Axie Infinity virtual game	Estate bought within the Game	1.5 Million
CryptoPunk 6965	Algorithm-generated	Pixel art	1.6 Million
Twitter's first-ever tweet	Jack Dorsey	Twitter's first ever tweet	2.9 Million
Crossroads	Beeple	Digital video	6.6 Million
CryptoPunk 7804	Algorithm-generated	Pixel art	7.57 Million
CryptoPunk 3100	Algorithm-generated	Pixel art	7.58 Million
Everydays: the first 5000 days	Beeple	Piece made up of 5,000 images	69 Million

## V. CONCLUSION

Blockchain technologies have been around for some time now and have been used for various types of applications in the last few years. One of the most recent applications, NFTs, are revolutionizing the market of digital collectibles and digital assets. Since NFTs are a complicated technology to understand, these applications are accessible only to a restricted set of people. This paper presented a balance between the technical and theoretical aspects that make up this technology, making it suitable for beginners who have an interest in learning the background and implementation of NFTs. This paper is also suitable for those who have a basic comprehension of blockchain technologies and want to extend their knowledge in the field.

### REFERENCES

- [1] Richard Twesige. A simple explanation of Bitcoin and Block Chain technology. Jan. 2015. doi: 10.13140/2.1.1385.2486.
- [2] Dejan Vujičić, Dijana Jagodic, and Siniša Randić. "Blockchain technology, bitcoin, and Ethereum: A brief overview". In: (Mar. 2018), pp. 1–6. doi: 10.1109/INFOTEH.2018.8345547.
- [3] B.Singhal, G. Dhameja, and Panda. How Blockchain Works. Beginning Blockchain. 2018, pp. 31–148. doi: 10.1007/978-1-4842-3444-0\_2.
- [4] Satoshi Nakamoto. "Bitcoin: A Peer-to-Peer Electronic Cash System". In: Cryptography Mailing list at <https://metzdowd.com> (Mar. 2008).
- [5] Assia Yoni et al. "Colored Coins whitepaper". url: [https://docs.google.com/document/d/1AnkP\\_cVZTCMLLzw4DvsW6M8Q2JC0llzrTLuoWu2z1BE/edit#heading=h.wxrvzqj8997r](https://docs.google.com/document/d/1AnkP_cVZTCMLLzw4DvsW6M8Q2JC0llzrTLuoWu2z1BE/edit#heading=h.wxrvzqj8997r).
- [6] Satoshi Nakamoto. namecoin white paper. url: <https://www.namecoin.org>.
- [7] Szabo Nick. "The Idea of Smart Contracts". In: (). url: <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html>.
- [8] Dejan Vujičić, Dijana Jagodic, and Siniša Randić. "Blockchain technology, bitcoin, and Ethereum: A brief overview". In: (Mar. 2018), pp. 1–6. doi: 10.1109/INFOTEH.2018.8345547.
- [9] Buterin Vitalik. "Ethereum white paper". In: GitHub repository (2013).
- [10] Contract ABI Specification. 2019. url: <https://solidity.readthedocs.io/en/latest/abispec.html>.
- [11] Vogelsteller Fabian and Buterin Vitalik. "EIP-20: ERC-20 Token Standard". In: (Nov. 2015). url: <https://eips.ethereum.org/EIPS/eip-20>.
- [12] Entriken William et al. "EIP-721: ERC-721 NonFungible Token Standard". In: (Jan. 2018). url: <https://eips.ethereum.org/EIPS/eip-721>.
- [13] J. Dafflon, J. Baylina, and T. Shababi. "ERC-777 token standard". In: (2015). url: <https://eips.ethereum.org/EIPS/eip-777>.
- [14] W. Radomski et al. "ERC-1155 multi token standard". In: (2015). url: <https://eips.ethereum.org/EIPS/eip-1155>.
- [15] M. Kupriianov and J. Svirsky. "Base security token standard draft". In: (2019). url: <https://eips.ethereum.org/EIPS/eip-1462>.
- [16] H. Marks J. Shiple and D. Zhang. "Ldgrtoken standard draft". In: (2019). url: <https://eips.ethereum.org/EIPS/eip-1450>.
- [17] Frankenfield Jake. ICOs explanation. 2020. url: <https://www.investopedia.com/terms/i/initial-coin-offering-ico.asp>.
- [18] Qin Wang et al. Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges. 2021. arXiv: 2105.07447[cs.CR].
- [19] Luno Team. Top 10 most valuable NFTs ever sold. May 2021. url: <https://www.luno.com/blog/en/post/top-10-most-valuable-nfts-ever-sold>.

# Hybrid e-Government Framework based on Datawarehousing and MAS for Data Interoperability

Barakat Oumkaltoum<sup>1</sup>, El beqqali Omar<sup>2</sup>, Chakir Loqman<sup>4</sup>  
Dept. of Computer Science  
University Sidi Mohamed Ben Abdellah  
Fes, Morocco

Ouksel Aris<sup>3</sup>  
Dept. of Computer Science  
University of Illinois Chicago  
Chicago, USA

**Abstract**—The exponential growth in technological innovation is driven in large part by the digitization of multiple domains and assumes environments of increasing data volumes, arriving at high velocity and variety. e-Government is one such domain that exploits current ICT innovations to improve the delivery of public services to its citizens, businesses, and other stakeholders. This imposes to continuously maintain information on daily operations, activities, and assets as well as extensive profiles on citizens, institutions, and organizations. In addition, current centralized platform-based approaches suffer from the single-point-of-failure, which may result in data breaches and leakages, leading to the need for efficient robust mechanisms to ensure secure information sharing, data interoperability, and privacy. In this paper, we propose a business intelligence approach to design a data interoperability framework for e-governance based on data warehousing technology to improve transparency and data accessibility. We also present a hybrid data filtering mechanism, which relies both on the Extraction, Transformation, and Loading (ETL) process, and multi-agent technology to integrate data quality and data interoperability, and supports data transformation into human-readable format. Finally, the framework emphasizes the availability of materialized views to enable efficient execution of analytical queries directly on the large volumes of raw data in the data warehouse.

**Keywords**—e-Government; interoperability; multi-agent system; materialized views; datawarehouse; business intelligence

## I. INTRODUCTION

E-government refers to the development of new public services and service delivery models that use digital technologies and government and citizen information systems assets.

While the development of government electronic services may have met resistance in the past due to the complexity of governmental policies and/or the lack of flexibility and capability of available technologies. This is no longer the case, in recent years, digital government architectures[1] have received special attention from researchers, embodying contemporary technologies and methodologies that will not only improve digital government performance, but also accelerate the pace of innovation by supporting the development of secure, autonomous, and transparent digital systems for the delivery of services and the management of rapidly and continuously increasing data volumes and varieties.

E-government provides a significant motivation for moving forward in the twenty-first century with higher-quality, more cost-effective government services and a stronger citizen-government interaction. In Morocco, the e-government program is part of the “Maroc Numéric plan”[2] which was launched in 2013 as the program aims to improve government efficiency by increasing the quality-of-service delivery to customers and investors from all segments of society in an easy, quick, accurate, and efficient manner, to become a new type of government employee and government performance. Such a goal requires cross-administration coordination, which could be difficult to achieve at times.

Moroccan governments are on pace with their digital transformation. Some ministries were among the first to implement the transition, while others are still getting acquainted which is the case of the supreme council of justice, the presidency of the prosecution, and the ministry of justice, which are nevertheless among the most frequented, seem to be the least connected since this judicial system is one of the most important and complex in Morocco and is a key component of the e-government initiative, it is critical to solve one of the system's primary issues: separation of data management and data interoperability.

The interoperability affects an organization's performance and is a difficult problem for Moroccan judicial entities adopting big data systems. Because of the varied nature of the data they handle, the Heterogeneity in developing E-Gov, the quantity of Data, the Interaction between these Data, and the dynamicity of these Data. Finding trustworthy answers between data acquisition and data management is more challenging than ever, and strategic decision-making in the supreme Moroccan council of justice necessitates the utilization of numerous sources of information that involve all justice departments. Therefore, these challenges of interconnecting the government information system in general and justice information system particularly to public administrations require rapid access to essential data in an interoperable manner.

Adopting a business intelligence approach to design a data interoperability framework for e-governance based on warehousing technology seems to be the most suitable solution.

This paper is the continuation of our previous work (Big Data Interoperability for E-Governance[3]), the contribution of

our work is to propose a data interoperability framework for e-governance based on warehousing technology and also to present a secure hybrid data filtering mechanism based on business intelligence approach and multi-agent system, considering widely adopted international standards for the exchange of government data. We show the benefits of such an approach in the area of usability, security, cost-reduction, and supporting e-government projects. The remainder of this paper is structured as follows. The background section presents the basic concepts that are necessary to understand our research problem. The second section presents the proposed framework and the study methods, followed by the section that describes our case study. The fourth section discusses the security and privacy aspect of the framework and the final section concludes by briefly presenting some of the study's implications for research and practice and future works.

## II. BACKGROUND

In this section, we provide a brief overview of the related works and the basic concepts relevant to our proposed framework for the data interoperability of e-government system that are required to explain deeply this study in the article.

### A. Related Work

Researchers have recommended several approaches such as citizen-centric, one-stop portal, social networking, and integrated e-government as viable ways to improve e-government service delivery. These approaches increase e-government service by offering an efficient service interface via which users may access services. Concerning the e-governance model, the majority of designs incorporate G2G and G2C. G2B is used by just nine architectures out of fourteen. As a result, the most widely used e-governance models are G2G and G2C. The Table I present a summary of existing e-government architecture from (2017-2020).

According to some research, SOA-based architecture is more appropriate for e-government since it uses component-based applications that allow the composition of services from multiple service providers.

E-governments now-a-days require collaboration and integration of different public services entities to meet the varied requirements and desires of the end user[4]. Integration, coordination, and interaction inside and between various generated data in public sector organizations are among the requirements[5]. SOA approaches enable the reuse of services and thus the SOA layered model includes enterprise service bus (ESB) and service component architecture (ScA), which can increase interoperability in a diverse context[6].

Based on our early study[7] and the related work presented above, there is still limited work that provides a comprehensive architectural framework towards a real data interoperability for e-governance. Hence, this work proposes a hybrid and distributed e-government based on business intelligence and by using an easy and a simple architecture such as ETL mechanism and multi agent system to ensure interoperability among government services and private services. The proposed

framework helps to reduce redundancy data provided by many agencies. Inter-department service sharing and reuse can also be improved thus it enhances decision making.

### B. E-Government Interoperability

Because more administrations shift to internet operations and search for ways to improve their service provision and citizens' obligations, they are faced with bundling services, engaging with supply chains, opening up their data and developing innovative service options. Instead of only making use of their own internal data, machines are communicating to each other, and government entities now need to connect their systems to each other. Interoperability is one of the most important problems facing the government in terms of access to information from various information systems[8]. With the emergence of open data movements[9], Interoperability could become more important. When viewing interoperability as the ability of multiple systems and organizations to work together, there are different layers of abstraction. In addition to the structures and the level of organization, the following stages can be differentiated.

Organizational interoperability aims at ensuring that organizations cooperate in a harmonized manner[10]. Collaboration of networks and a single government will be accomplished in this way.

Interoperability of processes[11] refers to the ability of different business processes to collaborate, or "inter-operate. It aims at making separate managerial and policy-making systems work together. Cross-agency systems or supply chains may be generated in this manner.

Service interoperability[12] aims at developing new services or structures through the identification and composition of services and the exchange of these services. In this way, new services can be built from existing components.

Application interoperability refers to the capacity of an application to communicate with another application through the use of external services (e.g., middleware services). It seeks to combine programs with each other in such a manner that they function in collaboration, operating collectively as one.

Data interoperability[13] seeks to work together with multiple data structures in diverse query languages to exchange data from heterogeneous systems. It is concerned with the ability of systems and services that create, and consume data to have clear, shared expectations about the data's content, context, and meaning so data and information can be shared, merged and made accessible in this manner.

### C. Multi Agent System based ETL Approach

A Multi-agent System (MAS) is a group of actors that interact between each other. In addition, each agent (actor) is able to deliver specific services and has a well-defined objective[23]. Each agent is able to autonomously execute multiple tasks and dispatch the result to a receiving actor (human or software). A MAS must adhere to the programming requirements established by the Intelligent Physical Agents Foundation[24].

TABLE I. COMPARISON OF EXISTING E-GOVERNMENT ARCHITECTURE

Architecture Name	MODEL			Architectural Pattern						e-Gov performance		
	G2G	G2C	G2B	SOA	EA	Big data analytics	EDA	MAS	BI	security	privacy	scalability
Enterprise Integration of Employee Onboarding Process Using Zachman Framework[14]	×	×	×		×					×	×	
Collaboration vs. Choreography conformance in bpmn[15]	×	×										
Enterprise Architecture for e-government[16]	×	×	×		×					×	×	×
Census Web Service Architecture for e-Governance Applications[17]	×	×		×								×
A Layered Architecture for Open Data: Design, implementation and experiences [18]	×	×		×							×	×
A Model and Architecture for Building a Sustainable National Open Government Data (OGD) Portal[ 19]	×	×	×	×						×	×	×
Big Data Interoperability for E-Governance[3]	×					×				×	×	×
Toward A Business Intelligence Model for challenges of interoperability in egov system: Transparency, Scalability and Genericity[5]	×	×	×	×					×	×	×	×
Business Intelligence and EDA Based Architecture for Interoperability of E-Government Data Services[6]	×		×				×		×	×	×	×
A Feasible Community Cloud Architecture for Provisioning Infrastructure as a Service in the Government Sector [4]	×		×	×						×		×
Cloud based architecture for interoperability of Data e-government Services [7]	×	×	×			×				×	×	×
e-Government Architectural Planning Using Federal Enterprise Architecture Framework in Purwakarta Districts Government[20]	×		×	×						×		
Preserving Privacy of Integrated e-Government Information Architecture [21]	×	×		×							×	
Business Intelligence and SOA Based Architecture for E-government System Interoperability [22]	×	×	×	×					×	×	×	×

Therefore, the purpose of using and combining a MAS and ETL (Extracting, Transforming and Loading) approach is developing an interoperability and data management system that would be able to have properties such as:

- Reactivity, which is defined as the ability to respond to user requests as well as the complexities of the human organization that characterizes the system's environment.
- Proactivity in anticipating user expectations or preventing problems in relation to the organization's goals.
- Flexibility to allow the system to adapt (addition of new agents, new roles for agents, etc.) in response to information and human organization evolution (capitalization and management of new types of knowledge, addition of new people in the organization, etc.)

#### D. Overview of Data Warehousing Materialized View

A materialized view is a database entity containing the query results. For example, it may be a local copy of remotely located data, or it may be a subset of a table's rows and/or columns, or it may be a description that uses an aggregate function[25].

Basically, materialized views are used to improve the efficiency of queries when they provide query data. For a faster execution, they can be used for reporting instead of a table.

Generally, data flows on a monthly, weekly, or regular basis from one or more online transaction processing (OLTP) databases into a data warehouse. Data is usually handled in a staging file before being added to the data warehouse. Data warehouses typically vary in scale from hundreds of gigabytes to a few terabytes. Usually, in a few very large fact tables, the vast majority of the data is held.

The creation of summaries is one technique employed in data warehouses to enhance performance. Summaries are particular types of aggregate views that by pre-calculating

costly joins and aggregation operations prior to execution and storing the results in a database table, maximize query execution times. In this study we construct many summary tables, for instance, to include the number of judiciary cases by district and province or to determine for each district the cases and the rate of cases with a “judgment of innocence” by the courts under the judicial district of the Court of Appeal, in 2019

### III. BI DATA INTEROPERABILITY FRAMEWORK FOR E-GOVERNANCE

Data warehouses are gradually being accessed through so-called information portals, which provide a standardized Web interface for OLAP, query, report generation, navigation, and data mining. In addition, portals offer coordinated access to a wide range of structured and unstructured data, particularly new information channels and digital libraries, that is stored outside of data warehouses. End users are given a personalized view of all data based on their business files and access rights.

This adds new interoperability requirements for the collaboration of different government portals repositories with other government warehouse specific repositories.

The construction of the data warehouses consists of implementing a series of data marts, each of which provides a dimensional view of a single business process. These data marts can be built around a set of shared dimensions[26].

In this paper, we discuss the data interoperability in the e-government system based on data warehouses in more details. This discussion is based on a three-dimensional classification of the main types of metadata groups used by organizations as show in “Fig. 1”, these data warehouse metadata groups are divided into users, business processes, and data dimensions. The “Fig. 2” illustrates an explanation of the three dimensions mentioned in the first figure, as well as the various relationships between them.

The “users” dimension, is where we make a clear distinction between internal and external users. The internal users are primarily responsible for the system's development and maintenance (e.g., managers, analysts, and others...).

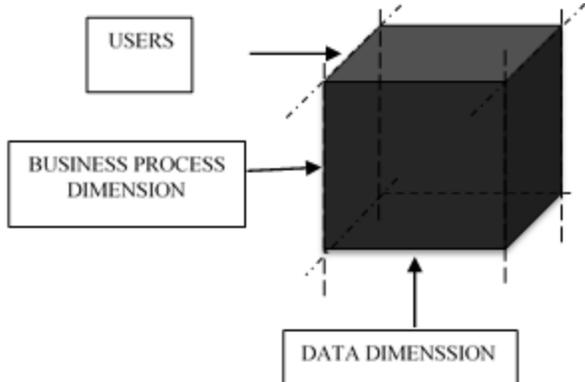


Fig. 1. Three-Dimensional Groups of Datawarehouse Metadata.

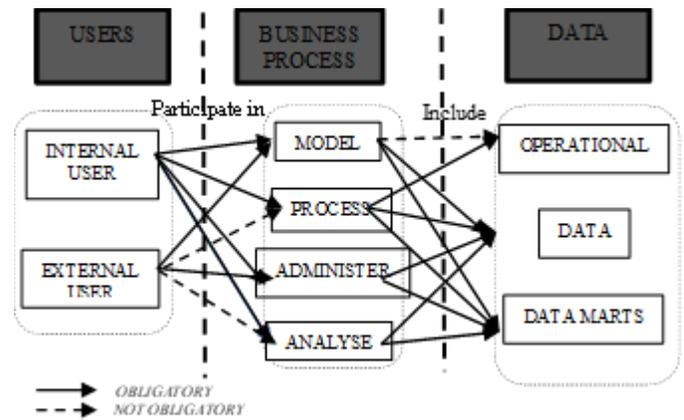


Fig. 2. Datawarehouse Metadata Classification Scheme.

The "business process" dimension is concerned with dynamic aspects and encompasses the metadata associated with the four major warehouse processes, namely model, processing, administration, and analysis. The model process is usually based on a modeling tool, which illustrates conceptual models, views, and other elements of the warehouse and data marts. It requires combining metadata obtained from different data sources. The processing process is strongly based on ETL tools [6]. The data warehouse and data marts must be provided with the data needed for analysis. It must execute data integration by transforming, cleansing, and mapping operational data into the data warehouse or data marts using rules and scripts. The administration process covers the management, maintenance, and tuning of the entire data warehouse environment except for the operational systems and finally, analysis processes are fully assisted by end-user specific data access tools for decision support, e.g., navigation, query and reporting, OLAP and data mining.

The “data” dimension organizes metadata into categories based on the information provided. We differentiate metadata associated with operational systems, data warehouses, and data marts based on warehouse architecture.

Our proposed Business Intelligence Data Interoperability Framework for e-governance (eGov-BDIF) is based on the business intelligence architecture. It addresses the challenges in terms of interoperability for data extraction, interoperability for reporting results and interoperability for data security and analysis. It develops advanced functionalities for better e-governance at different level as shown in “Fig. 3” (District, province, national). The aims of interoperability offering intuitive and straightforward public digital services to citizens and development of information sharing across different organizations and administration which represent a real complexity of cross-organizational collaboration. This is why the development of a common framework is very important for a data interoperability platform that could be scaled up and refined to elaborate robust solutions for different e-governance scenarios.

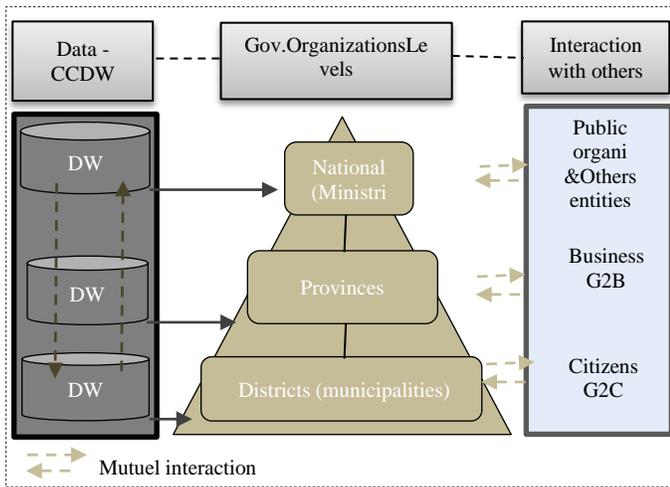


Fig. 3. Levels of Government Data Interoperability.

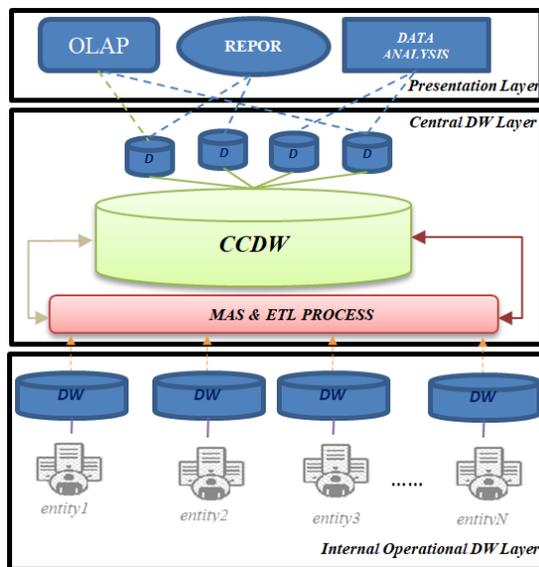


Fig. 4. Generic Architecture.

The eGov-BDIF is a comprehensive framework based on previous work[6] to address the government's need to maintain information about its daily operations, activities, assets and the details of its citizens, institutions and organizations secure for better e-governance in the collection, processing, storage, analysis and visualization of data stream .

Our framework illustrated in "Fig. 4" consists of an orchestration of various technological architectures that are represented as three complementary layers including presentation layer (or service access layer), Central Data warehousing & MAS layer and internal operational DW layer that consist of the diverse data mart or small DW of the different entities. The presentation layer comprises of e-government users and various devices for providing access, computing resource, and OLAP queries, reporting tools and data analysis.

The Central Data warehousing layer is meant to store different data sources such as PDFs, DOCs, contracts, and other files that are too huge to store or need to be deleted or

altered in the future. With different access-management protocols, each level (district, regional and national) of the agency builds its own data warehouse. High-priority data is not available for general access and must be secured from misuse or unwanted access.

Therefore, for access and performance reason, an important technique to speed up analytical queries is used "the materialized view" which consist of pre-computing and materializing aggregations. Since intelligent agents are used today in all aspects of life to solve difficult challenges by distributing work. In the ETL [26] Multi Agent layer, we aim to integrate different agents that operate together and each agent executes various tasks based on the assigned role in the ETL process to minimize the error's occurrence. In fact, the addition of agents at different level of ETL process (data extraction level, data transformation and data loading level) minimizes the risk of error, improves performance and reliability and minimize execution time. Agents will invoke notifications when a problem occurs. A warning is created for missing or insignificant data. Each agent is assigned a particular function by adopting the standards for semantics and data format. In our case, the ETL-based agent method is used to help make the extraction, transformation and loading process effective, efficient and secure. In our system agents are grouped into four classes within a multi-agent system.

- Monitoring\_Environment\_Agent group1
- Extracting\_Agent group2
- Transforming\_Agent group3
- Loading group4

#### IV. CASE STUDY DESCRIPTION

##### A. E-government Data Warehousing Architecture for E-Justice

The sharing of legal and judicial information[27] is one of the areas in which the e-government interoperability project can provide a level that cannot be matched by traditional mechanisms in obtaining this type of information, whether in terms of speed in reaching the required information, accuracy in arranging and classifying it, or being able to retrieve it When necessary, and also at the level of the vast amount of legal and judicial data that can be stored, downloaded, sent, searched and exploited [28].

The key entry point for the success of the e-government interoperability is the ease of access to justice by those seeking judicial services, including professionals, litigants and the general public, which comes through taking a set of measures, on top of which is the adoption of clear, smooth and accurately targeted electronic platforms, which are easy to distinguish between what was directed at specific groups and what was related to judicial, quasi-judicial or administrative services.

The aim of our eGov-BDIF in the case of the justice system is to help establishing legal and judicial security by providing an easy-to-use database of jurisprudence and various legislative texts. In addition, it enables the digital court to provide all the information related to a specific file to help make the right decision and thus, it enables the judicial process to speed up,

especially for similar files, with the possibility of making sure to single out files that know specific peculiarities.

The scenario of our eGov-BDIF applied in the Moroccan e-justice system defines three main entities:

- MJ (Ministry of Justice)
- PMP (Presidency of the Public Prosecutor's Office)
- CSPJ (Supreme Council of the Judicial Power)

These three entities interact with each other through the Process Legal Case (PLC) "l'affaire juridique".

In fact, the process of a legal case involves a set of sub-business processes (SBP).

$$PLC = \sum_i SBP_i$$

Our approach defines for each sub-business process a set of data-marts and Data warehouses namely (DW\_MJ, DW\_PMP, DW\_CSPJ) to build the common global DW related to the legal case process which in particular facilitate access to judicial services and better management of the judicial system and guarantee data interoperability between the three entities.

The common global DW "CGDW," is at the heart of our approach, it is made up of many physical data warehouses, such as DW\_MJ, DW\_PMP, DW\_CSP, and each warehouse can be physically located on various servers and geographically in different locations, but these separate data warehouses function as a collection of materialized views by queries. We may have different data sources partitioned by regions (SDR), districts, or provinces, such as SDR-Casa, SDR-Marrakech, SDR-Rabat, SDR-Fes, etc. There will be a separate ETL process for each data source, which will be orchestrated by a multi-agent system to extract the source data to the corresponding target data warehouse.

Moreover, the most used sub-requests or other logical views are materialized in order to enable the access of the end user to information placed in various databases whenever he needs and wherever he is and to speed up the processing of requests on a vast volume of data processed in our data warehouses, so that the cost of processing requests is reduced with an optimum maintenance cost. Therefore, the "Fig. 5" present an instantiation of our proposed generic architecture detailed previously in "Fig. 4".

Withal, the main results of the application of our approach in the justice system are summarized as follows:

- Modernizing the judicial administration
- Improving the quality of services provided to users
- Facilitating access to them

- Improving the effectiveness of judicial performance on the horizon of achieving the digital court
- Simplifying and standardizing the judicial procedures, thus contributing to shortening deadlines and speeding up the procedures for resolving cases
- Contribute to speeding up the implementation of judicial decisions
- A smart environment by digitalizing judicial procedures, it contributes to the success of the zero-paper strategy and promotes environmental standards
- A smart court makes technologies at the service of judicial security
- A judicial facility that protects the rights of litigants and places the beneficiaries at the core of his mission
- Affordable justice system
- Effective, transparent and open services.

## V. DISCUSSION

### A. Security and Privacy Aspect

The security, confidentiality and privacy of the large information base envisaged are vital to the sustainability and efficiency of the data warehouse. Research on data warehouse security has allowed us to identify two classes of approaches:

- The approaches dealing with the security of operations: this work allows us to answer the questions who has the right of access and what does he have the right to?
- Approaches dealing with prevention against inference problems: they allow answering the question How to forbid a user to infer protected data from accessible data?

Obviously, the two classes of approaches complement each other in the security services they offer.

Nonetheless, many security risk concerns emerge from the implementation of ICT in Moroccan courts and imply simple security safeguards such as authentication, non-repudiation, transparency, integrity of data and intrusion into privacy. In order to be enforced, the justice system will need to consider and handle legal and non-legal security risks in the most reliable and successful way in order to excel in the data warehouse implementation. To avoid erroneous assumptions and to discourage profiling and stigmatization of some classes of people, the data warehouse should be used with caution. The Judiciary will need to determine the consistency of the data, establish quality assurance design & create standards. This may involve identifying data consistency specifications, data processing procedures and validation of records, executing ETL logic tests and business rules.

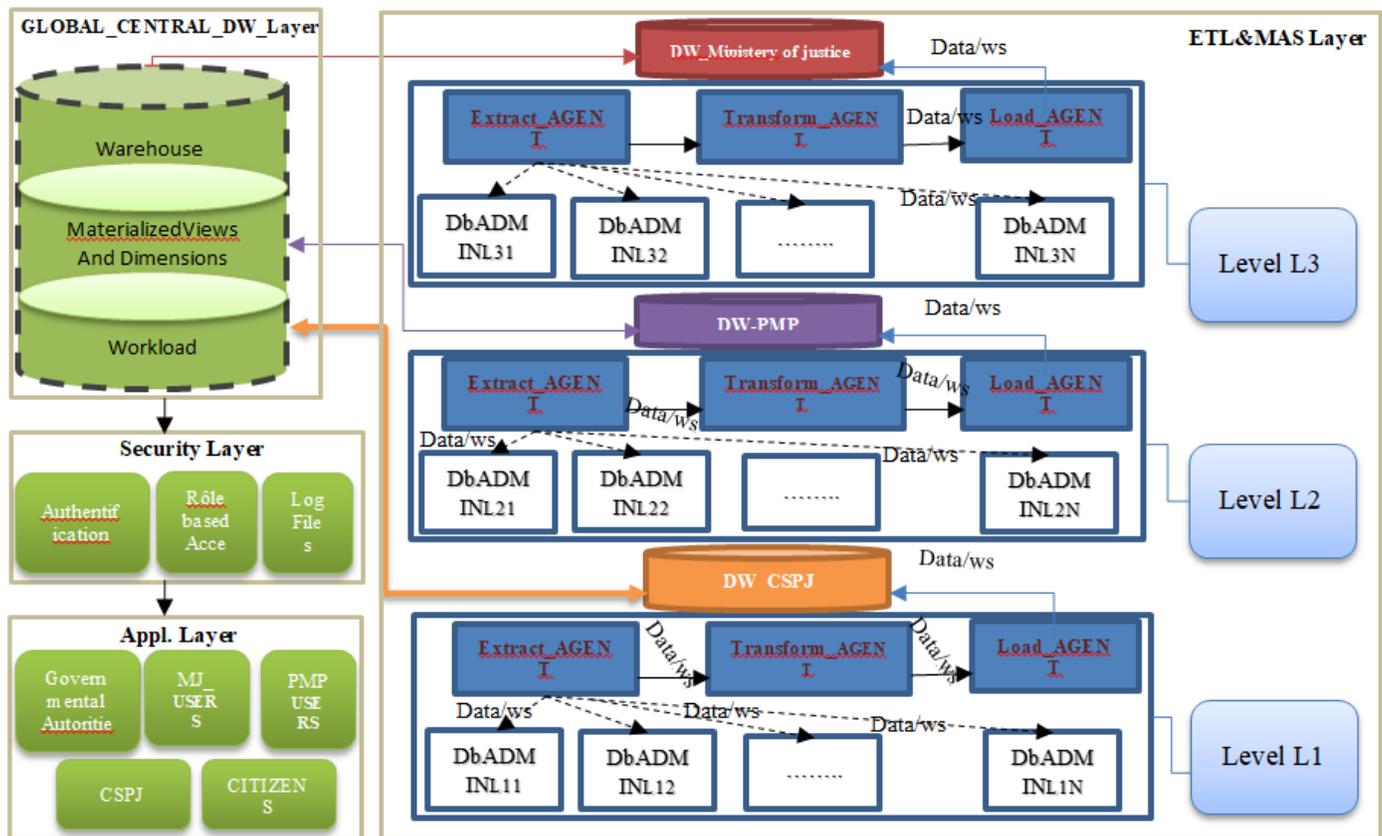


Fig. 5. E-justice Interoperability based on Datawarehousing Architecture and Multi Agent System.

## VI. CONCLUSION AND FUTURE WORK

Data warehousing is constantly being used for exploration and analysis to provide new information helping in decision-making. This work was intended to show how a hybrid approach of the ETL based on MAS and Data warehouses with Materialized views used to support the interoperability and the analysis of judicial data.

The present research is managed to simplify the data collection process by using the multi-agent ETL process to organize data loaded into the common global data warehouse. The data sources available in the Moroccan Judiciary system have been specifically outlined. The proposed Business Intelligence Data Interoperability Framework for e-governance has been developed. We also considered the query performance aspect by integrating and storing materialized views in the warehouses, which pre-aggregate the data, therefore avoiding access to the raw data and speeding up queries.

Finally, the implications of the project help the strategic choices of governments on the digital transformation within smart cities to support actors in co-creating organizational value, and societal well-being from business strategies and IT initiatives and foster the idea of environmentally sustainable e-government and create a more environmentally conscious public sector.

The perspective expounds on the study of possible improvement and validation of our eGov-BDIF framework. The main object if that will constitute our future research axe is

the development of advanced data warehousing systems by using a blockchain-based approach that constitute a crucial potential for improving the e-government business processes and data interoperability, providing transactional transparency and security in the value chain, and reducing operational cost.

## ACKNOWLEDGMENT

We would like to thank all the people who have supported this work, as well as special thanks to Pr. Aris Ouksel, Professor of Information and Decision Sciences, from the University of Illinois at Chicago, USA for the support and assistance all along the project and to Dr. Chakir Loqman professor in the department of computer science at the university Sidi Mohamed Ben Abdellah of fes, Morocco for providing us the valuable data and statistics used in this research.

## REFERENCES

- [1] B. A. Baheer, D. Lamas, and S. Sousa, "A Systematic Literature Review on Existing Digital Government Architectures: State-of-the-Art, Challenges, and Prospects," *Administrative Sciences*, vol. 10, no. 2, Art. no. 2, Jun. 2020, doi: 10.3390/admsci10020025.
- [2] A. Ennam, "The Emerging ICT Sphere in Morocco: Investigating the Feasibility and Usability of Massive Open Online Courses (MOOCs) -- Surveying the Case of Ibn Tofail University EFLers," *IISTE*, vol. 60, 2017.
- [3] E. B. M. Mahmoud, E. B. Omar, and A. M. Ouksel, "Big Data Interoperability for E-Governance," *Journal of Computer Science*, vol. 15, no. 10, pp. 1430-1438, Oct. 2019, doi: 10.3844/jcsp.2019.1430.1438.

- [4] K. Rodrigues de Castro, "A Feasible Community Cloud Architecture for Provisioning Infrastructure as a Service in the Government Sector," in Proceedings of the 20th Annual International Conference on Digital Government Research, Dubai United Arab Emirates, Jun. 2019, pp. 35–40. doi: 10.1145/3325112.3325229.
- [5] B. Oumkaltoum, E. B. Mohamed Mahmoud, and E. B. Omar, "Toward A Business Intelligence Model for challenges of interoperability in egov system: Transparency, Scalability and Genericity," in 2019 International Conference on Wireless Technologies, Embedded and Intelligent Systems (WITS), Fez, Morocco, Apr. 2019, pp. 1–6. doi: 10.1109/WITS.2019.8723756.
- [6] B. Oumkaltoum, E. I. Mohammed, E. B. M. Mahmoud, and E. B. Omar, "Business Intelligence and EDA Based Architecture for Interoperability of E-Government Data Services," in 2019 IEEE International Smart Cities Conference (ISC2), Casablanca, Morocco, Oct. 2019, pp. 402–407. doi: 10.1109/ISC246665.2019.9071769.
- [7] O. Barakat, M. M. El Benany, and O. El Beqqali, "Cloud based architecture for interoperability of Data e-government Services," in 2019 Third International Conference on Intelligent Computing in Data Sciences (ICDS), Marrakech, Morocco, Oct. 2019, pp. 1–6. doi: 10.1109/ICDS47004.2019.8942293.
- [8] E. C. D.-G. for Informatics, New European Interoperability Framework: Promoting Seamless Services and Data Flows for European Public Administrations. Publications Office, 2017.
- [9] H. Masoumi, B. Farahani, and F. S. Aliee, "An Ontology-based Open Data Interoperability Approach for Cross-Domain Government Data Services," in 2020 25th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Iran, Jan. 2020, pp. 1–8. doi: 10.1109/CSICC49403.2020.9050079.
- [10] H. B. Sta, "Organisational structure for the e-government coordination and interoperability framework: a case study of Tunisia," EG, vol. 14, no. 1, p. 51, 2018, doi: 10.1504/EG.2018.089540.
- [11] W. A. Khan, M. Hussain, K. Latif, M. Afzal, F. Ahmad, and S. Lee, "Process interoperability in healthcare systems with dynamic semantic web services," Computing, vol. 95, no. 9, pp. 837–862, Sep. 2013, doi: 10.1007/s00607-012-0239-3.
- [12] F. Dzikrullah and M. A. Rinjani, "A framework design to develop integrated data system for smart e-government based on big data technology," Bull.Socinf.The.App, vol. 1, no. 2, pp. 41–51, Dec. 2017, doi: 10.31763/businta.v1i2.26.
- [13] K. Cenci, P. Fillottrani, and J. Ardenghi, "Government Data Interoperability: a Case Study from Academia," in Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance - ICEGOV '17, New Delhi AA, India, 2017, pp. 625–628. doi: 10.1145/3047273.3047382.
- [14] W. Abbas, S. Ismail, H. Haron, W. Amalina, and W. A. Wan Hariri, "Enterprise Integration of Employee Onboarding Process Using Zachman Framework," International Journal of Engineering and Technology, vol. 7, pp. 46–51, Jan. 2018, doi: 10.14419/ijet.v7i4.31.23340.
- [15] Corradini, Flavio, Morichetta, Andrea, Polini, Andrea, Re, Barbara, and Tiezzi, Francesco, "Collaboration vs. choreography conformance in BPMN," Logical Methods in Computer Science; Volume 16, p. Issue 4; 18605974, Oct. 2020, doi: 10.23638/LMCS-16(4:7)2020.
- [16] R. Agarwal, V. Thakur, and R. Chauhan, "Enterprise Architecture for e-Government," in Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance, New Delhi AA India, Mar. 2017, pp. 47–55. doi: 10.1145/3047273.3047330.
- [17] A. Dutta, M. S. Devi, and M. Arora, "Census Web Service Architecture for e-Governance Applications," in Proceedings of the 10th International Conference on Theory and Practice of Electronic Governance, New Delhi AA India, Mar. 2017, pp. 1–4. doi: 10.1145/3047273.3047390.
- [18] G. Cordasco, D. Malandrino, D. Pirozzi, V. Scarano, and C. Spagnuolo, "A Layered Architecture for Open Data: design, implementation and experiences," in Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway Ireland, Apr. 2018, pp. 371–381. doi: 10.1145/3209415.3209466.
- [19] L. L. Idowu, I. I. Ali, and U. G. Abdullahi, "A Model and Architecture for Building a Sustainable National Open Government Data (OGD) Portal," in Proceedings of the 11th International Conference on Theory and Practice of Electronic Governance, Galway Ireland, Apr. 2018, pp. 352–362. doi: 10.1145/3209415.3209454.
- [20] M. Defriani and M. G. Resmi, "E-Government Architectural Planning Using Federal Enterprise Architecture Framework in Purwakarta Districts Government," in 2019 Fourth International Conference on Informatics and Computing (ICIC), Semarang, Indonesia, Oct. 2019, pp. 1–9. doi: 10.1109/ICIC47613.2019.8985819.
- [21] H. AlAbdali, M. AlBadawi, and M. Sarrab, "Preserving Privacy of Integrated E-Government Information: Architecture Approach," in 2019 2nd IEEE Middle East and North Africa Communications Conference (MENACOMM), Manama, Bahrain, Nov. 2019, pp. 1–5. doi: 10.1109/MENACOMM46666.2019.8988522.
- [22] O. Barakat and O. El beqqali, "Business Intelligence and SOA Based Architecture for E-government System Interoperability," in Proceedings of the 13th International Conference on Intelligent Systems: Theories and Applications, New York, NY, USA, Sep. 2020, pp. 1–5. doi: 10.1145/3419604.3419790.
- [23] Z. Elagougne, R. Maamri, and I. Boussebough, "A Multi-Agent Framework for Multi-Criteria Business Intelligence driven Smart Data in a Big Data Environment," p. 6.
- [24] V. Gancheva, "SOA Based Multi-Agent Approach for biological data searching and integration," International Journal of Biology and Biomedical Engineering, vol. 13, 2019.
- [25] A. Gosain and K. Sachdeva, "A Systematic Review on Materialized View Selection," in Proceedings of the 5th International Conference on Frontiers in Intelligent Computing: Theory and Applications, vol. 515, S. C. Satapathy, V. Bhateja, S. K. Udgata, and P. K. Pattnaik, Eds. Singapore: Springer Singapore, 2017, pp. 663–671. doi: 10.1007/978-981-10-3153-3\_66.
- [26] D. Dzemydienė, S. Maskeliūnas1, And V. Radzevičius1, "An Approach Of Ensuring Interoperability Of Multi-Dimensional Data Warehouses For Monitoring Of Water Resources," Journal Of Environmental Engineering And Landscape Management, 2021.
- [27] G. Lupo and J. Bailey, "Designing and Implementing e-Justice Systems: Some Lessons Learned from EU and Canadian Examples," Laws, vol. 3, no. 2, pp. 353–387, Jun. 2014, doi: 10.3390/laws3020353.
- [28] G. Lupo and M. Velicogna, "Making EU Justice Smart? Looking into the Implementation of New Technologies to Improve the Efficiency of Cross Border Justice Services Delivery," in Smart Technologies for Smart Governments, vol. 24, M. P. Rodríguez Bolívar, Ed. Cham: Springer International Publishing, 2018, pp. 95–121. doi: 10.1007/978-3-319-58577-2\_6.

# Analyzing User Involvement Practice: A Case Study

Dr Asaad Alzayed, Dr. Abdulwahed Khalfan

Computer Science Department, Public Authority for Applied Education and Training (PAAET), Kuwait

**Abstract**—Engaging users in software development is recognized as effective in furthering the likelihood of product efficacy and a successful project, together with user contentment. Furthermore, user involvement is potentially applicable to numerous organizational contexts that can incorporate a focused user-centered group. This research analyzes the findings of a case study carried out to assess the user involvement situation within a business specializing in innovative software for general consumers, service providers, and enterprises. This company has now formed a user experience group that is devoted to applying user-centered approaches for the overall development of the organizational structure. General feedback was confirmed as the most typical means of gaining user insight, with the level of user involvement in focused development falling short. Nevertheless, the study led to recognition that a firm plan for drawing users into development processes is necessary moving forward.

**Keywords**—User involvement practices; user involvement challenges; usability; user-center practice; user feedback; end users communication

## I. INTRODUCTION

Having users participate in software development is a vital hurdle to overcome but problematic to achieve. While developers are always inventing and releasing new, fancy features, they can easily overlook that their key focus needs to be on the quality of end-user experience [1]. Businesses are accustomed to incorporating new features that improve their products, but comprehending the processes their customers benefit from should in fact be their primary concern [2]. Indeed, while customers tend to be seen as the crucial factor for the cash flow their role creates, system users themselves need to also be viewed as vital, considering that the issues they face with securing smooth processes can have a profound knock-on effect on the subsequent engagement and cost-effectiveness [3]. The most difficult problem in the software development process is to understand users' needs and priorities; therefore, issues that need to be overcome and the applicability of updates are essential attributes for furthering the ultimate value a customer base will then receive. To help developers gain a better understanding of user requirements, getting those same users to be involved throughout the development process is seen as crucial for securing overall system functionality and user satisfaction [4]. User participation may also help to improve customer loyalty and sustain long connections with users [5-7]. In summary, figuring out how to answer the various user issues can result in a more profitable business, so should not be considered an inferior priority.

There are several approaches to involving users in the developmental contexts. However, going to the extent of challenging users to produce their own applications has

met with little success; indeed, it resulted in a lack of understanding between departments, although user productivity has been increased in such a manner [8]. Other approaches have also focused on having users take a planning and coordination approach to developers' workloads [9], together with occupying managerial positions in terms of adopting and implementing new IT innovations [10,11].

Getting users to closely engage with various levels of development can appear to be an inviting approach. In reality, however, it comes with many potential problems and pitfalls. Specific roles, for example, can become obscured, depending on how the user is linked with other departments [12]. Users can be both hostages and propagandists – both of which undermine the ultimate design goals. Hostage users tend to find their efforts blocked from within the design team of which they are supposed to be an important part. On the other hand, propagandists are redirected into developmental training as a result of failing to have a telling impact, but this only means their perspective is no longer relevant as users. Plus, users' involvement in developmental efforts offers no certainty that the actual system design will benefit from their presence, as developers may still overlook them [7,13]. Agile methodologies have been embraced to increase the potential of users' and customers' participation by putting them into the same area as developers, but it remains problematic to take developers' focus away from software functions, even when they are working closely with users [14].

To address these issues, the aim is to establish effective and reliable methods for incorporating users' perspectives and skills into development processes, which must be adapted to the unique company setting, as well as the departments and functions in question. So, taking marketing as an example, users will tend to be involved in research and assessment above all else, whereas product management will be more closely concerned with usability and performance [15].

This research explores the findings of an analysis of how user involvement practice is currently progressing in a business with a key focus on software solutions for various service suppliers and businesses, as well as consumers. Through assessing the means by which the varying activities of a company draw users into their everyday itineraries, together with analyzing how much information they already have on the users, we can aim for productive and in-depth observations on how effective user involvement methods have been. Ideally, we aim for the observations and insights made to serve as advice for professionals and organizations looking to make the most of user involvement moving forward.

The paper consists of five sections. Section 2 presents a literature review to analyze the concept of user involvement in greater depth, informed by available research. Section 3

covers the research methodology, interviewee backgrounds, and the organization under scrutiny. Section 4 then deals with the various case study outcomes, before Section 5 brings all this together with discussion and conclusions, backed up by research comparisons, and provides suggestions for ongoing research initiatives.

## II. LITERATURE REVIEW

### A. User Involvement

User involvement is a crucial aspect of developing any robust software. If developers continue to be unaware of the specific needs of their users, this will result in inaccurate assumptions and potentially disastrous consequences. This is backed by the literature, which shows that involving users early in the development process is effective and influential as the expense involved in making modifications grows throughout system development [16]. It has been found that user engagement and involvement have a beneficial influence on system success [5,17,18]. Bano and Zowghi [19] found that the relationship between user involvement and system success is not straightforward and is dependent on a variety of factors and conditions concerning the system development process, including the type and size of organizations and projects, the method of data collection and the phases of the system development life cycle during which data was collected, and user involvement or a participative approach to system development, such as agile, user-centered design (UCD), and participatory design (PD), are widely used. Previous research has indicated that involving users as early as possible in the development process it can be cost effective because it minimizes the expenses associated with the modification and redesigns made later in the software development process [16]. Particularly, research in Participatory Design has resulted in the development of a diverse variety of tools and approaches [20]. As defined in the standard ISO 9241-210:2010, [21], in order to fully comprehend end users' needs and requirements and to create a system that meets their job, end users should be participated across the whole development process. There are several issues, nevertheless, when you try to involve users to elicit their requirements and there are many developers also fail to exploit them to their full potential [16]. Many developers are also interested in finding out what the overall role of users should be if they have a say in software development. According to Abelein and Paech (2015) [5], the relevant context factors receive minimal attention. As a result, they requested further empirical study on numerous elements of user participation and involvement. Their research showed that the majority of user involvement and participation occurs during the validation and requirement elicitation phases, with only very few methods focusing on user participation and involvement during the software design and implementation processes, despite the fact that many important decisions are made during these processes. The function of users in design projects is not carefully decided in most companies. As a result, users are confused and believe they lack competence in engaging and running the system usually provided (Damodaran, 1996) [12].

User participation, according to Kujala (2003) [18] and Taha et al., (2013) [22], has a favorable influence on user

satisfaction and increases the likelihood of product success. Involving users in product design should benefit developers by reducing product risks, lowering product costs and market failure, and increasing business profit [23,24,25]. Several research have concluded that involving users early in the design process is beneficial. The rationale for this is because users may play an important role in product development by interacting with product developers, who then translate the input into product design specifications [24]. However, direct contact with users does not ensure the success of a new product if the product developers do not understand how to engage users in product development. Many approaches have been tried throughout the years to make the product development process more controllable and effective [22]. However, there are no precise approaches for increasing the success of a new product. Furthermore, most approaches that engage the user in the product development process have not been effectively described and clarified. Traditional approaches are more engineering-driven and mostly connected to the manufacturing phase of the design process, and they are not used correctly or employed at the incorrect point of the design process [26].

Rather than imposing techniques and tools, true user participation and involvement will always require an in-depth awareness of the organization's structure and a comprehensive grasp of local conditions to guide user representations and involvement. Users are sometimes involved as information providers to the project team. Users contribute to such projects but have little impact on important decisions, which is one reason of project and IT development failures to reflect properly for real human and organizational demands [12]. Damodaran (1996) [12], classified several forms of user involvement as 'informative' (users supply or obtain information), 'consultative' (users remark on a specified service or set of facilities), or 'participative' (users impact decisions connected to the whole system). There are several documented benefits to the implementation of user involvement in system design, such as accurate user requirements leading to higher quality systems, eliminating unwanted features, and promoting greater levels of acceptance of the system.

### B. The Level to which users are involved

According to Ives and Olson [27], the level of influence wielded over the final results is related to the extent of user involvement. The extent of user involvement, therefore, depends upon the efficacy of the system, with the following definitions applied to describe the level of contribution:

- No involvement: users are either not asked to get involved or are not keen to provide their expertise.
- Symbolic involvement: users are asked to contribute, but their perspective is not actually taken on board.
- Advisory involvement: direction is sought via various means of feedback.
- Involvement via weak participation: users do offer some expertise but have to sign off responsibility as each stage is complete.

- Involvement by action: a user is a very active part of the design team, perhaps as an on-site colleague or else as an official contact that information is fed through.
- Involvement by strong control: users take a hands-on approach as a result of funding the developments, but also in scenarios where an assessment of the user's overall performance is reliant upon robust and innovative system design.

The extent and form of user involvement can be viewed as the two levels upon which the various actions or decisions are understood. Perhaps the only kind of user participation in which it is found that the user has a real influence on results is a participatory role. With approaches that are informative and consultative, user direction is available, but there is no guarantee it will not be ignored or overlooked. A participatory form of role and the extent level of user involvement both strongly imply that the user is a member of the design team; however the form also allows the user to have a voice on developed systems, whilst the level implies that it may change.

As these comparisons show, it is entirely possible for user involvement levels to overlap, though this does not necessarily mean the outcomes will be negative. Such an overview will be applied to our findings to inform an empirical approach.

### III. METHODOLOGY

The authors conducted a qualitative research methodology consisting of a semi-structured interview with open-ended questions to collect the data for this research study. In addition, case study methods were adopted to direct our research practices. Yin [28] defined a case study as an applicable social science discipline, incorporating both organizational and managerial contexts. The use of a case study approach in this case is intended to be illustrative, since the aim is to connect the dynamics of current practice while avoiding any influence on the processes at the research analysis.

#### A. Research Analysis

Our research has been carried out by observing a software business company throughout 2020. More than 300 staff are employed by this company, whose core operations focus on software solutions sourced by general consumers, service providers, and also small and medium enterprises. Their structural approach includes having a designated user experience team, which is tasked with achieving robust user-centered practices and services for the complete company operations. However, prior to research taking place, this team had only been operational for three months. Part of the research goals, therefore, was to allow the user experience team to gain a firm overview of the situation concerning user involvement practice throughout the various departments, so they could respond by upgrading their activities to suit applicable challenges and goals.

#### B. Data Collection and Analysis

We performed 6 face-to-face semi-structured interviews with open-ended questions, each lasting approximately 30-60

minutes. All interview questions were asked in English, but the interviewees were given the right to answer the questions in English or Arabic. To reflect the diverse functional responsibilities, case study participants were selected from a variety of departments (details in Table I). The participants were then asked to reply and explain while commenting on their experiences by explaining the scenarios they faced in the context of user participation in their presently ongoing or recently completed projects. Upon completion of the interviews, a professional transcription service was applied to transcribe all interview recordings in order to extract the essential information from the recordings. Both authors were present at all interviews and made field notes as needed. The field notes and incomplete transcripts were then categorized and thematically evaluated. The data from the interviews was subjected to thematic analysis in the form of template analysis. Template analysis is ideal for comparing the views of various groups within a given setting [29]. Template analysis allows for the creation of conceptual themes that fit under bordered groupings, ultimately allowing for the identifying of master themes and their subordinate component themes.

TABLE I. ROLES AND FUNCTIONS OF CASE STUDY INFORMANTS

No.	Role	Function
1	Project Manager	Customer Involvement
2	Marketing Manager	Marketing
3	Product Manager	Product Manager
4	Technical Writer	Localization & Documentation
5	Software Architect	Research & Development
6	Software Engineering	Research & Development

### IV. RESEARCH RESULTS

The case study results are presented in this section. The user groups indicated by the participants show how the employees tasked with various organizational functions recognize the company's end users as the crucial stakeholders. The information gathered highlights the extent to which end users are understood, together with the means by which such insight has been obtained. We then move on to describe the internal communication networks in place, before indicating work practices that already draw users into system development. Lastly, we focus on the most important hurdles to overcome in order to enhance the user involvement performance.

#### A. Identified user Groups

To start with, participants were requested to provide various personal background info, together with their working priorities, and particular projects or products they had expertise in. Then questions moved on to the user groups who benefitted from their various projects and products – covered in Table II. In doing so, all participants identified home users and service providers as the two key user groups. Two interviewees identified both corporate and administrator groups, with the remaining groups all identified by one source only.

TABLE II. IDENTIFIED USER GROUPS

User Group	No.
Service provider	6
Home User	7
Administrator	3
Corporate Employee	2
Consumer	2
Corporate	2
Mobile User	2
Partner	1
Internal Customer	2
Wholesaler	3

This broad selection of different user groups is in some part due to the situation of the various departments – in some cases different employees – utilizing different terminology. For example, product management, which appeared to have closer end-user involvement than other departments, used both ‘consumer’ and ‘partner’ to indicate either home user or service provider. Other interviewees employed different definitions, using ‘partner’ to describe both service providers and corporate clients. Furthermore, studying Table II also makes it clear that, as well as using varying terminology, user groups themselves were also understood in different contexts. Some responses, for example, indicated a complete service provider as an end user, while others recognized that any company will have different levels operating within, with the customer involvement employee being one such example.

### B. User Data Types

User data is used in this study to refer to any information gathered directly from users, including their needs, challenges they must overcome, and the specific activities to which their responsibilities are applicable. The participants’ responses show how the various departments view and understand company operations, together with the reasons for why they have come to understand operations in such a way.

User response for product previously received and used, along with feedback from a trial test before to release of the product, were the most common sort of data source. The majority of employees were found to be sharing information well, although there were also signs of information being kept within specific teams. Support allows key user data feedback from products in use to be accessed, while customer involvement allows for tryout stage feedback to be readily available. See Table III for the complete lists of user data as expressed by the various departments.

Customer involvement feedback is available via tryout testing that is carried out by focused testers looking to identify specific problems with a product. While products are still in their pre-testing phase, small issues can be ironed out, while bigger problems that don’t offer a simple fix are scheduled for future product development and upgrades.

Aside from these two types of feedback, product management focuses on collecting vital insights through interaction with end users, which is regarded critical for

product concept and definition. Semi-structured interviews, which often include open-ended questions, are the most commonly utilized technique for gathering this information.

### C. User Data Distribution

Fig. 1 depicts the spread of user Data throughout the company. As the two primary data sources, support and customer participation, their combined feedback is delivered to the majority of other departments. Feedback from support is sent to all structural levels, while the tryout testing before releasing the product undertaken by customer participation is drawn upon to inform product management, research and development, localization and document. The information is particularly vital to product management, who draw feedback from all structural levels to inform their designs and also to pass on key details to other contributors. In terms of getting a product from concept to production, adhering to a common vision is the primary driver of user data.

The two key avenues of product management information are the information each employee has at their disposal and the customer, which is unlike other departments that sometimes rely on less-specific information. Plus, the overall product vision is not necessarily bought into by all the managers involved. However, if a team agrees on a product view, the information is preserved on an official site. When a product is at its conceptual stage, numerous incentives will be stimulated as research and development goals are realized. Crucially, if some of these goals are considered low-level at an early stage, then any correspondence on them will be restricted rather than risk compromising a grander vision. Typically, this vision will be summarized as part of a product vision document.

Key data are supplied by support to other departments in the shape of reports. Participants from localization and document confirmed that such reports could only be accessed via the support function, with the exception of some random examples. The majority of functions log the reports on specialized network drives, upon which they can be difficult to locate. Customer involvement shares tryout-stage feedback concerning product performance, typically as reports. The employees overseeing this task aim to gain a user’s role perspective so they can make clear judgments on what corporate partners require and how end users can benefit. Frequent meetings take place between customer involvement and research and development to assess the latest tryout test feedback.

TABLE III. USER DATA TYPES

Data	No.
Feedback from End User	8
Feature Request	2
Tryout Feedback	7
Usability Problems	2
Wholesaler Profile	1
Vision Document	2
Conceptual Requirement	1

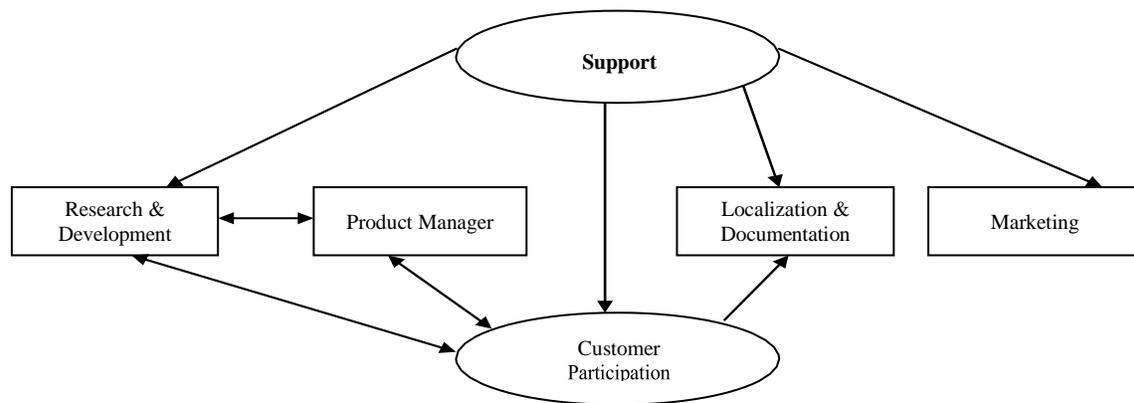


Fig. 1. User Data Communication Networks between various Company Departments.

Participants were requested to confirm their favored forms of communication. The majority preferred punchy and precise summaries or reports to set out the findings of the various tests and studies. These summaries and reports were not judged to be intriguing in themselves, but they turned out to be productive if they happened to relate clear and applicable information. The representative from product management confirmed a preference for communicating in an interactive manner, which could include events as well as more typical meetings and correspondence. As far as simple and fixed reports are concerned, the product manager expresses doubt they are always effective for communication unless some more sophisticated accompaniment is incorporated – such as being part of a presentation printout.

#### D. User Involvement Actions

According to the replies from the interviews, there are three actions that include some form of user involvement: focus groups, introspection and interviews. In doing so, all practices involved an informative or consultative form, rather than any firm participative role.

**Focus groups.** Intermittent market research had been carried out by the marketing manager via focus groups. This involved a group of consumers being asked to focus on the performance of a certain product or subject matter.

Conducting these groups offered crucial information on how the organization's key products are judged by those who actually utilize their capabilities. As a type of user involvement, this approach is clearly consultative in nature, as those involved have their attention focused on a particular product, concept, or service.

**Introspection.** Customer involvement participants confirmed that, in addition to tryout testing, employees have also looked to role play by envisioning themselves as the client, as a way of making judgments from a user's perspective. In some respects, users then become an indirect information source as part of this procedure. Consequently, this user involvement approach is clearly informative in nature.

**Interviews.** End users were sourced for interviews via product management in order to enhance a new product concept. This approach was judged to be an effective means for gaining firm and precise feedback via clear end user

insight. Because end users were acting as an information source, user involvement is clearly informative in nature.

#### E. Issues and Challenges

The interviewees identified several challenges and issues during the system implementation process:

- **Lack of User Data issues.** As the majority of participants confirmed, the largest obstacle they face in making the most of user involvement insights is making up for the lack of it. Indeed, some responses expressed real concern that usability as a concept is completely absent from procedures, with others confirming a desire to have robust user studies to draw upon. As previously stated, the user data available is largely made up of feedback, which alerts teams to existing issues but goes nowhere in terms of avoiding them during product development.

Sourcing user perspectives throughout early developmental periods or, preferably, as products are still in their conceptual stages, enables developers to focus on user value early on in the process, making it a part of the overall product life cycle. In contrast, when these concerns are only addressed in later stages of development, finding solutions can prove more problematic for going against the initial design, making fixes more expensive and possibly less effective. There are financial incentives as well, therefore, for end user involvement earlier in product development.

- **Customer value issues.** The customer involvement project manager confirmed that, at present, the organization's operations tend to be technology-led, with a commitment to addressing any issues identified rather than preventing them from occurring during design periods. This leaves us with a clear interpretation that user-centered design has yet to be fully embraced as a company priority, meaning that users' perspectives are not utilized to inform the early stages of product development.
- **User interface issues.** A big problem is how to judge end users' feedback when it is mixed. For example, if as many users complain about the user interface as those who compliment it. Drawing a conclusion on when to pay attention to criticism and when not is not

easy. At the present time, it is difficult to be confident that a feature or usability solution will increase product value for users, leaving a gray area with regard to which improvements should be given priority and whether they are necessary. Furthermore, this scenario is complicated by the range of alternatives that exist on who the most important clients are and what they are like, due to a lack of user profiles. Plus, as research and development are responsible for the majority of user interfaces, they have little to go on to assess whether an interface is offering quality performance.

- **Integration issues.** User insight, therefore, needs to be incorporated into the current process, which, according to the product manager, needs to be achieved without relying on a separate user involvement process. If approached in any other manner, there is a real danger that aligning current processes could be problematic and have knock-on negative effects. Additionally, it might be that current development processes do not integrate with a user involvement process, meaning it will create a clear risk.
- **Understanding main requirements issues.** Any major implementation process needs to be made conscious of the overall company requirements; therefore, a product management participant believed that the various employees involved in such an implementation need to have a grasp of the overall company needs, as well as low-level requirements. However, in practice, the focus should be away from low-level issues in terms of establishing the overall vision, as focusing on smaller issues too early in the restructuring risks occupying developers in an unproductive manner.
- **User Feedback issues.** As product development takes place, no outside feedback is currently available. This is another issue that needs to be addressed while pursuing new product visions. At the moment, tryout-stage consultation is in place but largely becomes available too late to make anything greater than small adjustments or upgrades. Gaining key information as products are in earlier developmental stages would pave the way for a more thorough approach to addressing usability issues that is cost-effective and less time-consuming over the long term. At the same time, however, better access to vital feedback alone will not answer all the problems if there are issues with current processes and workplace dynamics that remain unidentified. The localization and document technical writer indicated a number of departments from which no feedback is currently available; with no process underway to put avenues of communication in place either.
- **User importance issues.** The company lacks a clear means of gaining user perspectives, with the product manager raising many issues in this context. Indeed, his priority issue was that no structured approach exists at any level within the company to facilitate reaching an understanding of client needs. Even when diligent employees strive to produce their best results, they are

working without valuable insight that might enhance the efforts of even the most perceptive of developers. Plus, in the event that a developer does have extensive expertise on their user's requirements, there is no process in place for integrating this knowledge with the rest of the company's operations. Furthermore, current design practice is restricted to obtaining a list of key product features but without any greater conceptual design that would merge all user requirements and product objectives together.

- **User interaction issues.** The lack of correspondence between developers and their products' end users remains a real issue. For example, the research and development quality engineer and architect brought up a number of user involvement practice issues. In doing so, the most pressing was the absence of contact with end users in their own department, which means the communication channels are simply not open or else entirely reliant on indirect interactions. Indeed, responses can be described as passive in nature due to not being sourced with purpose or for a particular developmental context.
- **User data Access issues.** User perspectives are vague, muddled, and problematic to secure. One participant from customer involvement, for example, confirmed that the majority of feedback sourced tends to end up on a database or network drive, which might not be the most user friendly for research purposes and makes it difficult to find specific pieces of information. As a result, it is probably more accurate to describe such resources as data rather than as a live resource, as the information has by then been examined, given a category, and moved on from the attention of any employee. Furthermore, such databases and online resources are packed with various other reports and documents that employees will not immediately appreciate the context of just because they are readily available.
- **User experience issues.** Moving forward, user experience needs to be approached as integral to all company operations. Analyzing the responses of the marketing manager revealed similar issues to those raised by the technical writer, being conscious that user experience involves multiple components – not just the various software, handbooks, and packaging, but online support and Internet content too. An additional marketing issue raised was the trend of service-oriented business operations becoming more prevalent, which comes with the necessity of understanding a great deal about end users rather than relying on habit or firmly structured approaches. Another observation the marketing manager made is that client opinions and expectations are shifting as a result of software solutions becoming merged with operating systems. Consequently, the levels of market research and user feedback required are far greater than ever before, and the current marketing operations are simply not yet equipped to handle the challenge.

## V. DISCUSSION

This research has explored the results of an ongoing state analysis carried out within a software house focused on developing software solutions to suit the needs of service providers, enterprises, and general consumers. A case study approach was adopted to reach our conclusions, based largely on feedback drawn from semi-structured interviews. Furthermore, this study is conducted within the context of setting up a focused group of user experience to define user-centered working practices into which all businesses may buy into. The process has included offering clarity on which user groups utilize the organization's products, the form of user information currently available from within the company, and the methods employed for communicating that information. In addition, the research explores the practices undertaken to draw feedback from users, and at the same time looks to define the most significant obstacles the company faces, with the task of enhancing its user involvement potential.

The results show how various company functions approach this challenge differently – and view end users differently – while agreement was reached on home users and service providers being the vital players. User feedback sourced via tryout tests and support products already on the market made up the most significant portion of user data available. This means processing such information is problematic due to the large quantity involved. Overall, however, the most significant issues are the lack of applicable user data, the difficulties faced in applying what information there is to working practices, and a general absence of ongoing communication with end users. To begin answering these issues, setting up a smooth and convenient means of corresponding with end users' needs to be prioritized, with the user experience team being the obvious choice for leading the way in this breakthrough.

As mentioned in Section 2, Damodaran [12] drew upon three separate forms to define user involvement: informative, consultative, and participative. From our research, it has become clear that all the available user information is currently either informative or consultative in nature. There are no signs of any user participation at any stage of the design process. Similar results are found when analyzing the actual user involvement practices, which were also either informative or consultative. In summation, therefore, no specific form of user participation is currently undertaken within the company.

As covered in Section II, Ives and Olson [21] established six levels to indicate stages of user involvement. As far as this research is concerned, all user participation may be defined as falling between symbolic and advisory involvement. The involvement of customers and support function have to some extent been successful in drawing customer responses, however, this is ignored owing to the lack of resources to use the information. Although there have been significant marketing focus groups and interviews carried out by product management, which does show some efficacy in terms of drawing user experiences into the company's processes, it is also clear this information is not applied to the earliest design stages, so its impact is limited to response only.

Muller and Czerwinski [30] identified another distinct user-centered function that is linked with product organization methods. They explain how a central group enables a company's usability experts to correspond and continually upgrade developers' working methods and vision to suit more robust final products. This approach is crucial for making sure the most skilled developers, though they may be working in isolation, are able to benefit from in-depth insights into how their work is received by and benefits others. Our own research shows a similar scenario, with the user experience professionals responsible for the whole company's user-centered services, which needs to be achieved at the same time as adhering to their own standards. Nevertheless, to realize such an effective merging of departmental priorities, there are numerous hurdles to overcome that are holding back the usability experts from having a profound impact on earlier stages of development [31,32]. Currently, no clear information is obtainable regarding how well these efforts are progressing, as our focus has been on available user involvement channels as opposed to any that are in development.

The obstacles that need to be overcome in order for a successful user involvement upgrade mean a great deal of enhancement for the user experience team to carry out so that early development tasks and product visions can genuinely benefit from user feedback. One key example is that the team could begin by establishing a means of conveniently and effectively examining the available user and tryout-test feedback so that the most important issues can be highlighted and addressed. Moving forward, integrating an efficient way of obtaining and interpreting a variety of market research should be aspired to, and in a manner that makes the most of user input from the earliest design stages. At the moment, a reliance on feedback after product release shows an over-reliance on technology-oriented working standards, in which responding to issues and fixing them during later developmental stages is the only means via which upgrades are achieved. It would be much better, however, to incorporate user insight from the beginning of the developmental process, because incorporating such information later on is always restricted in terms of the overall benefits that can be achieved.

## VI. CONCLUSION

This research study makes it clear that the company is too technology-oriented within its current practices. A variety of organizational factors are at play in terms of obtaining user feedback, but there is no robust method of drawing such value into overall product development. Consequently, it is hard to argue that user feedback has any kind of profound impact on product design. Although it is doubtful that having users present at an early stage would be enough to deal with this issue, the majority of participants did call for enhanced user-centered practices and objectives.

The user experience team has a vital role to play if user insight is to be made the most of throughout all levels of product design. This research offers a depth of information in terms of how this can be achieved, the enhancements that need to be made, and the standards that need to be adhered to. The most important aspect to take on board moving forward is that

new methods need to be dedicated to gaining a greater comprehension of user requirements so this can be applied throughout the design stages, without undermining other standards in the process.

Looking ahead, further research should focus on the extent that the user experience team has been effective in terms of integrating themselves seamlessly with other processes and departments. Ideally, this paper will offer expertise to any practitioners keen to address similar user involvement issues, together with any who are at the stage of setting up a centralized user experience department. We also hope the conclusions drawn here are applicable for guiding future user involvement research in a number of contexts.

#### REFERENCES

- [1] K. C. Brata, D. Liang, "An Effective Approach to Develop Location-Based Augmented Reality Information Support," *International Journal of Electrical & Computer Engineering*, 2019, vol. 9, no. 4, pp. 2088-8708.
- [2] S. D. J. Barbosa, "Investigating the Integration of User Values With Design Rationale and Its Effects on HCI Design Artifacts," Doctoral dissertation, PUC-Rio, 2020.
- [3] S. Kujala, M. Kauppinen, L. Lehtola, T. Kojo, "The Role of User Involvement in Requirements Quality and Project Success," In 13th IEEE International Conference on Requirements Engineering (RE'05), pp. 75-84. IEEE, 2005.
- [4] M. Bano, D. Zowghi, F. da Rimini, "User Satisfaction and System Success: An Empirical Exploration of User Involvement in Software Development," *Empirical Software Engineering*, 2017, vol. 22, no.5, pp. 2339-2372.
- [5] U. Abelein, B. Paech, "Understanding the Influence of User Participation and Involvement on System Success – A Systematic Mapping Study," *Empirical Software Engineering*, 2015, vol. 20, no. 1, pp.28-81. doi: 10.1007/s10664-013-9278-4.
- [6] P. Mohagheghi, M. Jorgensen, "What Contributes to the Success of IT Projects? Success Factors, Challenges and Lessons Learned from an Empirical Study of Software Projects in the Norwegian Public Sector," *IEEE/ACM 39th International Conference on Software Engineering Companion (ICSE-C)*, 2017, pp. 371-3.
- [7] M. Bano, D. Zowghi, F. Rimini, "User Satisfaction and System Success: An Empirical Exploration of User Involvement in Software Development," *Empirical Software Engineering*, 2017, vol. 22, no.5, pp.2339–72. doi: 10.1007/s10664-016-9465-1.
- [8] K. Siakas, E. Georgiadou, D. Siakas, "The Future of the IT Department: Is There a Threat by End User Application?" *The Cyprus Journal of Sciences*, 2017, vol. 15, pp. 63-82.
- [9] T. Issa, P. Isaias, "User Participation in the System Development Process," *Sustainable Design*, 2015, pp. 37-57.
- [10] A. M. Baronas, R. Louis, "Restoring a Sense of Control During Implementation: How User Involvement Leads to System Acceptance," *Management Information Systems Quarterly*, 1988, vol. 12, no.1: pp. 111-123.
- [11] T. H. Kwon, R. W. Zmud, "Unifying the Fragmented Models of Information Systems Implementation," In Boland, R. J. & Hirschheim, R. A. (Eds.), *Critical Issues in Information Systems Research*, John Wiley, New York, 1987.
- [12] L. Damodaran, "User Involvement in the Systems Design Process – A Practical Guide for Users," *Behaviour & information technology*, 1996, vol. 15, no. 6, pp.363-377.
- [13] K. K. O. Tha, "Developing a Framework for User Participation in Information System Development Projects," Paper presented at the 25th Americas Conference on Information Systems. (2019).
- [14] J. Klemets, T. C. B. Storholmen, "Towards Super User-Centred Continuous Delivery: A Case Study," In *International Conference on Human-Centred Software Engineering*, 2020, pp. 152-165, Springer, Cham.
- [15] K. Redlarski, P. Weichbroth, "Hard Lessons Learned: Delivering Usability in IT Projects," In 2016 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 1379-1382, IEEE, 2016.
- [16] J. M. Noyes, A. F. Starr, & C. R. Frankish, "User Involvement in the Early Stages of the Development of an Aircraft Warning System," *Behaviour & Information Technology*, 15, 2, 67-75. 1996.
- [17] M. Bano, D. Zowghi, "A Systematic Review on the Relationship Between User Involvement and System Success," *Information and Software Technology*, 2015, vol. 58, pp. 148-169.
- [18] S. Kujala, "User Involvement: A Review of the Benefits and Challenges," *Behaviour & Information Technology*, 2003, vol. 22, no.1, pp. 1–16.
- [19] M. Bano, & D. Zowghi, "User Involvement in Software Development and System Success: A Systematic Literature Review,," In *Proceedings of the 17th International Conference on Evaluation and Assessment in Software Engineering* (pp. 125-130). New York: ACM, 2013.
- [20] J. Simonsen, & T. Robertson, (Eds.). "Routledge International Handbook of Participatory Design,," London: Routledge. 2013.
- [21] ISO 9241-210: 2010. Ergonomics of Human-System Interaction - Part 210: Human-Centered Design for Interactive Systems, 2010. <https://www.iso.org/standard/52075.html>.
- [22] Z. Taha, H. Alli & S. H. Abdul-Rashid, "The characteristics of a new product through user knowledge in the early stages of a design process,," *Journal of Advanced Materials Research*, vol. 739, pp. 678-683. 2013.
- [23] J. Janhager, "User consideration in early stages of Product Development: Theories and methods,," Stockholm: PhD Thesis, Royal Institute of Technology. 2005.
- [24] Z. Taha, H. Alli, & S. H. Abdul-Rashid, "User's requirement and preference in the success of a new product: A case study of automotive design,," *Journal of Applied Mechanics and Materials*, vol. 215, pp.484-488. 2012. Trans Tech Publications Ltd.
- [25] H. Alli, "User involvement method in the early stage of new product development process for successful product,," *Alam Cipta: International Journal of Sustainable Tropical Design Research and Practice*, 11(1), 23-28. 2018.
- [26] M. E. A. Webber, M. Weggeman, & J. E. van Aken, "Developing what customers really need: Involving customers in innovations,," *International Journal of Innovation and Technology Management*, vol. 9, no. 3, pp. 1-15. 2010.
- [27] B. Ives, M. Olson, "User Involvement and MIS Success: A Review of Research,," *Management Science*, vol. 30, no. 5, pp586–603. 1984.
- [28] R. Yin, *Case Study Research – Design and Methods*. Sage Publications, 2003.
- [29] N. King, C. Cassell, and G. Symon, "Using templates in the thematic analysis of text. Essential guide to qualitative methods in organizational research," 2004. Vol. 2, pp. 256-70.
- [30] M. Muller, M. Czerwinski, "Organizing Usability Work to Fit the Full Product Range,," *Communications of the ACM*, 1999, vol. 42, no. 5, pp. 87–90.
- [31] N. Anjum, M. Sarker, S. I. Ahmed, "Evaluation of Web Usability Requirement Model and Web Application Interface Components. Evaluation, 2018.
- [32] W. Wang, J. Cheng, J. L. Guo, "How Do Open Source Software Contributors Perceive and Address Usability? Valued Factors, Practices, and Challenges,," *IEEE Software*, 2020.

# Predictive Scaling for Elastic Compute Resources on Public Cloud Utilizing Deep Learning based Long Short-term Memory

Bharanidharan. G<sup>1</sup>

Phd. Research Scholar, Department of Computer Science  
VISTAS, Pallavaram, Chennai

Dr. S. Jayalakshmi<sup>2</sup>

Professor, Department of Computer Applications  
VISTAS, Pallavaram, Chennai

**Abstract**—The cloud resource usage has been increased exponentially because of adaptation of digitalization in government and corporate organization. This might increase the usage of cloud compute instances, resulting in massive consumption of energy from High performance Public Cloud Data Center servers. In cloud, there are some web applications which may experience diverse workloads at different timestamps that are essential for workload efficiency as well as feasibility of all extent. In cloud application, one of the major features is scalability in which most Cloud Service Providers (CSP) offer Infrastructure as a Service (IaaS) and have implemented auto-scaling on the Virtual Machine (VM) levels. Auto-scaling is a cloud computing feature which has the ability in scaling the resources based on demand and it assists in providing better results for other features like high availability, fault tolerance, energy efficiency, cost management, etc. In the existing approach, the reactive scaling with fixed or smart static threshold do not fulfill the requirement of application to run without hurdles during peak workloads, however this paper focuses on increasing the green tracing over cloud computing through proposed approach using predictive auto-scaling technique for reducing over-provisioning or under-provisioning of instances with history of traces. On the other hand, it offers right sized instances that fit the application to execute in satisfying the users through on-demand with elasticity. This can be done using Deep Learning based Time-Series LSTM Networks, wherein the virtual CPU core instances can be accurately scaled using cool visualization insights after the model has been trained. Moreover, the LSTM accuracy result of prediction is also compared with Gated Recurrent Unit (GRU) to bring business intelligence through analytics with reduced energy, cost and environmental sustainability.

**Keywords**—Predictive auto-scaling; business intelligence; virtual machines (VM's); deep learning models; analytics; elasticity; high performance public cloud data centre (HP-PCDC); right sizing

## I. INTRODUCTION

Cloud Computing (CC) is a paradigm aimed at retrieving a collection of computer assets such as servers, networks, storage that allow applications to expand resource on demand with agility through virtualization. Cloud computing is the developing model for delivering subscription oriented pay-as-you-go services to access compute resources for deploying applications. One such characteristic, namely, elasticity that enables customers to buy and release the correct quantity of

compute resources based on their demands so that more responsive web application developers are continually attracted to use cloud services. Cloud infrastructure and services have become the major aspect [1] [2]. The previously siloed or on-premise data Centre is obsolete immediately, since the client base tends to shift quickly based on business demands. The auto-scale technology from IaaS in cloud enables the dynamic adjustment of the number of VMs, to be added or removed based on the capacity of workloads or user traffic [3]. If a web shop in the cloud has more requests or with seasonal trends, extra VMs can be made available to handle load. Conversely in the case of reduction of traffic, VM instances may also be removed automatically. The application load balancer supports containerized applications powerfully. It operates like a gateway to receive TCP/HTTP applications received by end-users and disseminate it equally to many clusters with master and slave nodes managed by Kubernetes (K8's) minions to support modern containerized workloads. In this research, we utilize a framework intended for supporting classic and application load balancing, with predictive Auto-scaling approach which is used to forecast the traffic in advance and provision of resources with high-quality services and to minimize the expense of cloud utilization without violating Quality of Service (QoS) and Service Level Agreement (SLA).

Projection of cyclic workload is one of the most crucial and vital aspect in the perfect management of cloud infrastructure. Each request necessitates resources to finish its implementation and such resources are virtually made available through resource pool. The cutting edge CDC consists of different resources such as bandwidth, software, CPU, memory etc., in a virtualized form through Type-1 hypervisors from hardware layer whereas the users are assigned to finish their task performance on request. In accordance to preceding works, it is important to remember that resources are always larger than the real resources needed in order to finish the application [4]. The rationale for the supply of resources is that SLA violations are evaded and QoS satisfaction is attained. The resources are in most cases squandered during the allocation procedure. Although auto-scaling offers extremely excellent advantages, it is a difficult process to execute. Effective auto-scaling involves a new predictive strategy to predict the resources exactly using Machine Learning (ML) or Deep Learning (DL) to handle critical workloads. Auto-scaling shown in Fig. 1 comprises of three techniques, namely:

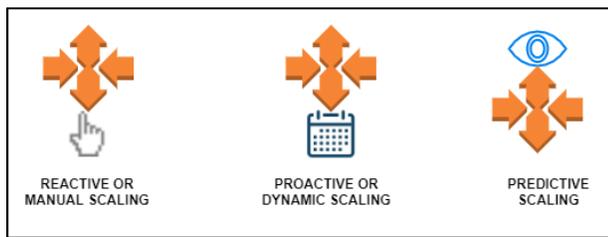


Fig. 1. Types of Scaling Techniques.

The strategy of reactive or manual auto-scaling where the resources has been wasted most of the times when workloads may get exceeded suddenly or decreased due to user specifies the threshold values and the required instances are automatically optimized as per the values hardcoded in the policy. The Proactive Scaling is Reactive with time scheduling to scale up or scale down the resources. In the case of predictive strategy, the cloud application workloads have been predicted through analyzing and visualizing those historical workload traces with minimum 24 hours of metrics history is needed to add or remove the instance capacity in before the first arrival of traffic. Thus, the predictive scaling is more efficient than reactive scaling and even familiar due to its spontaneous nature to allocate instances in advance to maintain optimum performance and the limitation in the predictive scaling is mixed instance policy in Auto-Scaling Groups cannot be supported, supports only CPU Metrics to forecast, and suits only for the applications which undergo periodic traffic spikes.

Precise predictions can be utilized to determine the right quantum of resources required to meet the needs. In order to accurately estimate the future workload, a precise and trustworthy prediction model is necessary. Normally in CDC, the job of the user comes in a pattern with irregular requirements on the resource. This is a big difficulty to anticipate the accurate workload [5]. Researchers have created many models for estimating workload and resource usage, focused mostly on forecasting the memory and CPU [6-8]. Several research projects have solely utilized statistical approaches to estimate load and for huge and diverse data, they cannot anticipate reliable outcomes. By means of machine learning models, numerous study efforts is done to forecast large and changing working loads in cloud. The results of these predictions are shown to be encouraging. Nevertheless, in regulated settings the statistical models can proactively anticipate time burdens. It is thus known that when using heterogeneous data, it will lead to greater predictability by integrating both statistical and machine teaching technologies. However, somewhat few research works were carried out in a field of resource forecasting at task stage [9]. The use of resources at task level helps to characterize activities that have a substantial influence on the capacity planning process, development of VM and assignment apportionment [10].

The CPU usage is one of the key metrics for the performance assessment of the cloud data center host and is utilized by researchers for server performance assessment [11]. CPUs are the utmost challenging resource in cloud data center servers and hence the main reason for not having a resource [12]. For cloud resource usage prediction and capacity

planning of CPU, several approaches have been employed namely, Auto-Regressive Moving Average (ARIMA), K-Nearest Neighbor (KNN), Feed-forward artificial Neural Network (FNN), Auto-Regression (AR), Recurrent artificial Neural Network (RNN), Extreme Learning Machine (ELM), Autoregressive Neural Network (AR-NN), and Multi-Layer Perceptron (MLP)[13], [14]. The use of CPU may be regarded as time function such that it could be pronounced as a time series issue. As a result, it becomes a regression problem that may be handled using neural networks or traditional time series.

The aim of the research is to avoid reactive nature of auto-scaling by introducing the predictive nature of auto-scaling solutions with AWS cloud platform which has the capacity to comply with the constantly changing load with QoS standards. The evaluated combinations of Maternal Data Centers in Dortmund and AWS Auto Scaling of Elastic Compute Nodes have been utilized for accessing the predictive auto scaling options. However, the trials are carried out using the LSTM deep learning concept with Explorative Data Analysis (EDA) to forecast the resource needed in advance by means of predictive scaling with visual analytics that has a capacity to auto-scale in and out to the Dev-Ops demand quickly. Hence, this technique is initially presented in the document has utilized to assess auto-scaling performance. Thus, the DCs are one of the biggest responsible for global warming and it our responsible to find some innovative ways for overcome this issues. The initiative of green cloud broker with LSTM based predictive auto-scaling has assisted to reduce CPU utilization, memory usage as well as energy consumption values to maintain in its directory.

The paper discusses the literature of elastic scaling of predictive method using time series forecasting method as well as auto-scaling of resource utilization using Machine Learning (ML) in Section 2. The Section 3 discusses the predictive auto-scaling of Dev-Ops user's resource allocation by EDA and LSTM technique for better and accurate prediction of unprecedented workload. Section 4 discusses experimental AWS platform and visualized real-world workloads to evaluate the predictive scaling approach. Section 5 has concludes that predictive auto-scaling by LSTM has improved the Dev-Ops users resource allocation for developing and running the applications with less compute and memory usage in a lesser time.

## II. LITERATURE REVIEW

The IaaS cloud uses predictive scaling technologies that guarantees cloud energy efficiency with reduced bill cost. Bi Jing et al. suggested a technique to forecast the amount of tasks at a successive interval in data center using ARIMA and hair wavelets, and findings showed that hybrid approaches lead to a greater predictive accuracy. The work does not address computer resources such as CPU, RAM, etc. which play a key role for the distribution of resources [15].

Janardhanan et al., in the Google cluster data utilized ARIMA and LSTM models to predict CPU workloads. The outcomes show that LSTM is 20 percent lower than the ARIMA model and has a higher consistency in its predictions [16]. The experiment on a single computer is implemented and

the use of CPU for this machine is projected. Furthermore, Cetinski et al. suggested an Advanced Model for Efficient Workload Prediction in the Cloud (AME-WPC) that utilizes both statistical and machine learning techniques to improve the job prediction precision over time. In aspects of lowering operational costs and handling resource, the proposed strategy is efficient. However, the prediction of certain cloud resources would help to automate and schedule the scale of resources [17].

In a novel method, M. U. Farooq et al. suggested RR. Initially, the most time of explosion is retrieved in RQ. The quantum time value is then derived by computing the 0.8 percent of this BT. If the number of processes in the queue is less than the quantum, they will be given the CPU, while the others will be queued. When all of the processes are completed, a quantum is given a new value equal to the highest BT, and the CPU is freed up for the remaining activities. This new technique worked wonderfully in terms of average waiting times, context switches, and turnaround times [18].

B. Dave et al. recommended a unique method to CPU scheduling the strategy's objective is to compute the best quantum time depending on the left over burst time in ready queue for the said work. Various tests have been carried out to determine the efficacy of this method. In evaluation to DQRRR, SARR, RR, MRR and IRRVQ algorithms, the findings show a reduction in the amount of context switches in queues or resources as well as outperformance [19]. A. Kaushik and D.Khokhar presented a novel approach to solve the RR algorithm's drawbacks. They developed a novel method for determining the optimum time quantum using the mean and median burst time of activities. Experience has proven the effectiveness of a new algorithm in terms of reducing waiting time and turnaround time [20].

Priyanka Singh, Palak Baaga, and Saurabh Gupta offer a detailed overview of the numerous methods that have been published earlier in their paper Assorted Load Balancing Algorithms in CC. Researchers looked at different algorithms and analyzed them based on numerous criteria to find a viable solution for load balancing in a CC environment. The algorithms' benefits and drawbacks are explored. The Minimum Connections Algorithm is one such algorithm. This approach takes the number of active connections that each server will have into consideration. Once a client tries to connect, the load balancer looks for the server with the fewest connections and allocates newer connections to that server. The Least Connections Algorithm is named from the fact that each server's connection is taken into account. It only prevents the server from becoming overburdened [21].

In their paper "Performance Evaluation of Round Robin (RR) Algorithm in Cloud Context," Neethu Myshri, R and Asha, M. L have highlight the RR algorithm's performance in a cloud-based atmosphere. For the goal of simulating and understanding the reaction of cloud computing and its deployment patterns, the use of a cloud analyst toolset has been chosen as a unique method. The proposed method is fairly similar to the Throttled algorithm. Load balancing is achieved in a way of delivering requests in a round-robin way to each server. RR is a typical load balancing scheduling technique for

distributing workload amongst servers. This method works well on clusters of servers that have the same specifications. It picks a node at random and distributes the job in a circular pattern [22]. Despite the fact that round robin is the simplest approach for distributing client requests over a set of servers, it suffers from non-uniformity in workload distribution owing to the servers' specs being similar. Furthermore, the Round Robin algorithm ignores priority, resource capabilities and job size. As a result, higher-priority and longer-duration operations have longer response times that can lead to server overloading.

Ming Yan et al. [23] presented a fusion elastic scaling strategy for Kubernetes (k8's) that combined reactive and proactive approaches. The proactive technique uses the Bi-LSTM model to learn the physical host and pod resource consumption history in order to anticipate future workload (Memory usage, CPU utilization). The Bi-LSTM prediction model is used with the online reinforcement learning with reactive model to achieve elastic scaling judgments. It has been shown in experiments that it can help the system achieve micro service SLAs in edge computing environments. The Bi-LSTM model has the least prediction error for the Root Mean Square Error (RMSE) metric when compared to ARIMA, LSTM, and RNN models. Despite this, no strategy for reducing oscillations has been offered.

Machine learning-based auto-scaling architecture is also suggested by Imdoukh et.al. The resource estimator tested the 1998 World Cup website dataset with the help of the LSTM model. They compared the results to those obtained using both the ANN and ARIMA models. The findings showed that while the proposed LSTM model has a little higher prediction error in one-step forecasting than the ARIMA model, it predicts 530 to 600 times faster [24].

Tang et al. proposed a Bi-LSTM-based container load prediction model that forecasts future load based on the container's historical CPU consumption. The recommended model has the lowest prediction error when compared to ARIMA and LSTM models. The authors, on the other hand, give no instructions on how to set up the parameters of the proposed model. Furthermore, the essay focuses only on future load projections and does not address auto-scaling concerns [25].

Mahmoud Imdoukh et al. proposed predictive auto-scaling for running container applications with docker containers for handling dynamic workload characteristics and for timely manner provisioning. The authors used the MAPE (Monitor, Analyzer, Planner and Executor) in auto-scaling architecture connected with Time-Series database. Further LSTM prediction model is used with multi step prediction and it as been compared with ARIMA where LSTM is 130 times faster to predict the real time usage of container auto-scaling. Further they discussed LSTM model performs better in terms of provisioning and elastic agility with auto-scaler metrics [26].

This session has discussed the literature instance of forecasting model of cloud computing resource allocation, provisioning and predictive scaling using Machine Learning ARMA, ARIMA, deep learning models like LSTM, Bi-LSTM that have played a major role in proactive scaling and to overcome the reactive scaling gaps. Similarly, the discussion

about load balancing schedule technique by dynamic Round Robin algorithm has utilized for better workload scheduler rather than classic load balancer. However, the support of this literature has addressed the issues of reactive auto-scaling and advantage of predictive auto-scaling by LSTM model. Therefore, this paper has motivated to fill the research gap using Predictive scaling on public cloud infrastructure by LSTM.

### III. RESEARCH METHODOLOGY

The cloud computing applications are involved with large variation in both development and operation areas that consist of an alternative existence during the solutions of suitable cloud infrastructure. The middleware solutions have involved by accomplishing Dev-Ops requirements with green cloud broker. However, this research has proposed a predictive scaling with green broker management method to maintain the elastic provisioning of VMs based on Public Cloud Service Provider (PCSP) to resolve Dev-Ops requirements without compromising QOS and SLA. Hence, deep learning technique has played a key role in predicting the required resource and allocates it to CSP with Dev-Ops knowledge that currently spread across various VMs or docker containers through virtualization or containerization in the form of elastic cluster management. The allocation of predictive VM resources using dynamic weighted Round Robin (RR) which is applied in scheduling the task based on the CPU time with weights for distribution over the Virtual Machines in a physical host. The RR technique efficiency act as the application load balancer that completely depends upon quantum or traffic. When the application traffic is high or quantum size is very large, then the RR technique may follow the first come first serve method with weights These application load balancers is called as new generation load balancer. It handles multiple applications on a unique physical host that contains VM's. The routing decisions are carried out in layer 7.

The proposed infrastructure of predictive scaling using LSTM technique is shown in Fig. 2. When the Dev-Ops users have cyclic workloads that have been sending through green cloud broker are sequenced as cloudlets by dynamic round robin technique applied in application elastic load balancer for regulating the incoming application traffics that has been distributed equally towards multiple target optimum instances for predictive scaling.

Then the predictive scaling engine utilizes the dataset along with timestamp to forecast the CPU resource utilization to provision the instances or nodes exactly from public Cloud data Centre which has virtualized resources to be provisioned with agility to the dev-Ops users as shown in Table I. The traces are gathered during a three-month period in the dispersed Materna Data Centers in Dortmund [27]. A month's worth of data is shown by each trace. The three dataset consists of the running 527 VMs in trace 1, 527 VM's in trace 2 and 547 VM's in trace 3 respectively of 69 cores and 6780 GB RAM. The workloads in the tracked VMs are mission-critical business applications from well-known organizations

throughout the world. It is studied using the LSTM deep learning concept as an Explorative Data Analysis (EDA) to forecast the resource needed by means of predictive scaling, having a minimum optimum capacity to auto-scale in and out to the Dev-Ops demand quickly in advance.

The steps involved in EDA has progressed LSTM algorithm by importing libraries and setting the seeds for generating random numbers by fixing a starting number. The collected raw data is made to data cleansing which removed and imputed the missing data. The data processing is done by min max scalar splitting the cleaned dataset to 60% of train dataset and 40% of validation (test) dataset which can be executed through EDA as shown in Fig. 3. Once the EDA process is done, the dataset is train to fit LSTM model based on the layer of optimizer ADAM (ADaptive Moment estimation), sequential and ReLu. Finally, the output layer of LSTM defined the predicted values through visualization report. The working principle of LSTM model as well as predictive auto-scaling algorithm using LSTM model is discussed.

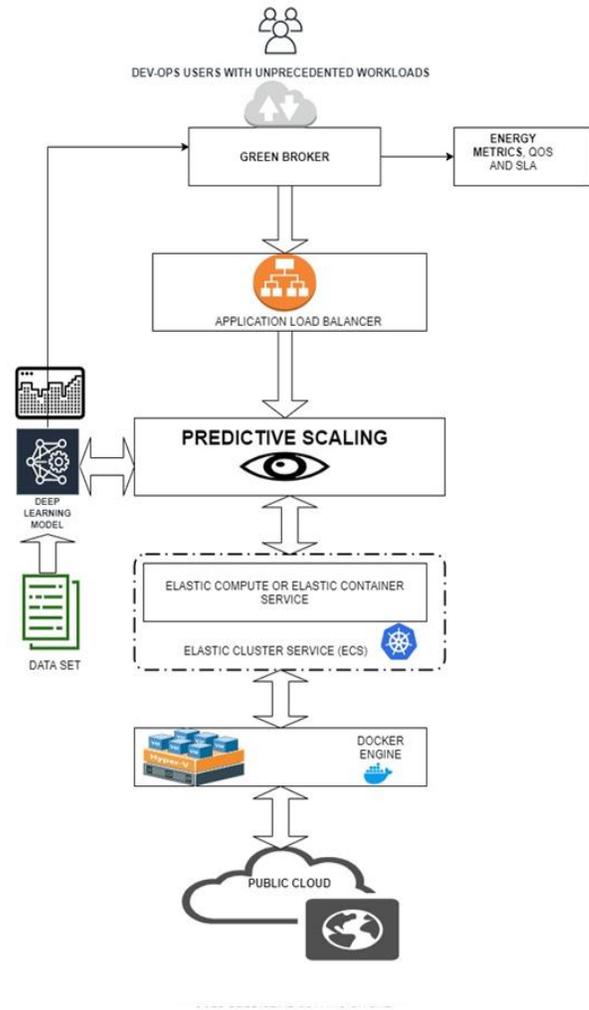


Fig. 2. Proposed Predictive Scaling on Public Cloud Infrastructure.

TABLE I. COLLECTION OF DEV-OPS USERS TRANSACTION AS DATASET

Timestamp	CPU cores	CPU capacity provisioned [MHZ]	CPU usage [MHZ]	CPU usage [%]	Memory capacity provisioned [KB]	Memory usage [KB]	Memory usage [%]	Disk read throughput [KB/s]	Disk write throughput [KB/s]	Disk size [GB]
11.01.2016 15:00:00	8	0	214	1,49	25165824	17407200	69,17	734	373	300
11.01.2016 17:00:00	8	0	137	0,95	25165824	251658	1	42	9	300
11.01.2016 19:00:00	8	0	45	0,31	25165824	42782	0,17	0	3	300
11.01.2016 21:00:00	8	0	44	0,31	25165824	42782	0,17	0	3	300
11.01.2016 23:00:00	8	0	44	0,31	25165824	108213	0,43	0	3	300
12.01.2016 00:00:00	8	0	43	0,3	25165824	166094	0,66	0	3	300
12.01.2016 00:05:00	8	0	44	0,3	25165824	47815	0,19	0	3	300
12.01.2016 00:10:00	8	0	47	0,32	25165824	148478	0,59	0	3	300
12.01.2016 00:15:00	8	0	47	0,33	25165824	47815	0,19	0	3	300

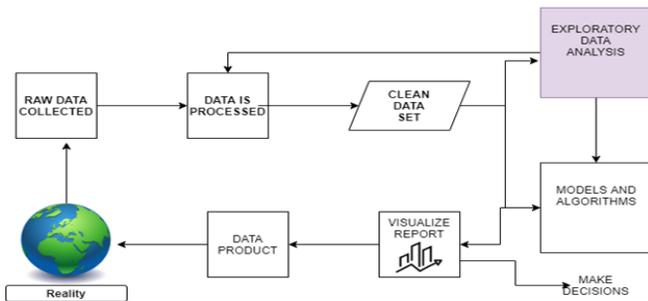


Fig. 3. Work flow of Exploratory Data Analysis (EDA).

#### IV. WORKING OF LSTM AND GRU METHOD IN DEEP LEARNING

Deep Learning methods executes well on large and multivariate time-series prediction problems. The performance of learning model is better after training in complex and more non-linear data. LSTM is more accurate for large dataset with long-term predictions and ultimately deep learning has automatic feature extraction on comparing flat machine learning [28].

The working mechanism of the LSTM is illustrated in Fig. 6, and the LSTM is a kind of modern Recurrent Neural Network (RNN) architecture that remembers information at variable intervals. The LSTM algorithm is well-known for classification and forecasting time series requires lagging of timestamps with uncertain periods. One of the major advantages of LSTM is about gap length over relative insensitivity that provides better solution compared to alternative RNNs, Hidden Markov Models (HMM) and various traditional techniques. However, the case of RNN and HMM are completely depend upon the hidden state which initiated before emission and sequence results in vanishing gradient problem. Instead of predicting 10 intervals, the application is predicting 1000 intervals of sequences, the model may forgot the initial points from other technique like RNN and HMM, because the last hidden state doesn't have any information of past to remember, but it can be resolved by LSTM.

GRU (Gated Recurrent Unit) can predict well and performs fast on small datasets. The architecture of GRU which was shown in the Fig. 5 is simpler on comparing LSTM structure. The flow of information in a sequence chain can be regulated by gate structure. The GRU has only two gates known as Reset and Update gates. GRU do not use memory unit like LSTM. GRU is easier to modify. But LSTM and GRU perform moreover equal but LSTM remembers long sequences. The Full GRU Unit has shown in Fig. 4.

#### FULL GRU Unit

$$\tilde{c}_t = \tanh(W_c[G_r * c_{t-1}, x_t] + b_c)$$

$$G_u = \sigma(W_u[c_{t-1}, x_t] + b_u)$$

$$G_r = \sigma(W_r[c_{t-1}, x_t] + b_r)$$

$$c_t = G_u * \tilde{c}_t + (1 - G_u) * c_{t-1}$$

$$a_t = c_t$$

Fig. 4. GRU Unit.

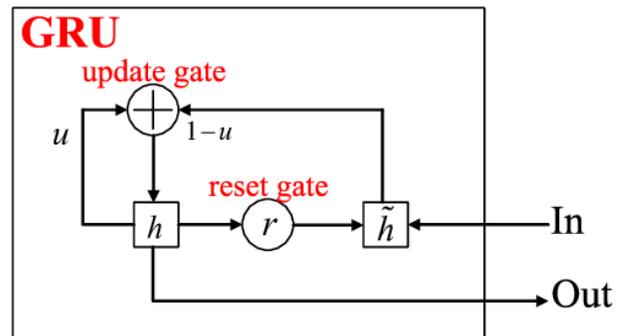


Fig. 5. GRU Working Process.

The cell state that consists of looping arrows that reference the recursive cell nature is believed to constitute the long-term memory in general. In equation 1, the long term memory acknowledges that data from previous intervals that has been stored in LSTM cell shown in Fig. 6.

$$c_t = f_t \circ c_{t-1} + i_t \circ \tilde{c}_t \quad (1)$$

The forget gate, which is below the cell state and adjacent to the input modulation gate has changed the cell state. The previous cell state is forgotten, which is multiplied by the forget gate and the latest information is gathered via the input gates output, according to equation (2).

$$f_t = \sigma(W_f[h_{t-1}, x_t] + b_t) \quad (2)$$

The remember vector is commonly referred to as the forget gate, since its output has shown the cell state, which comprises of information contained in forgot multiplied by 0 to the matrix position. When the forget gate output is 1, the information in the cell state is retained as it is indicated in equation (3). As a result, the input gate is represented as a sigmoid function that is applied to the weighted input for observation as well as the previously concealed state.

$$i_t = \sigma(W_i[h_{t-1}, x_t] + b_i) \quad (3)$$

Furthermore, these gates can determine what data has to be put in the cell state, with the activation functions for each gate accounting for a considerable percentage of the total. As a result, the input gate is modeled as a sigmoid function with a range of [0,1]. If the summing of cell states among the previous cell states is supplied, the sigmoid function can only accumulate memory and not erase forgotten memories. Similarly, the float number is summation among [0, 1] which may never considered to be zero or forget. The input modulation gate in this example has been modeled after the tanh activation function indicated in equation (4) whereas the range of tanh is [-1, 1] which admit the forget memory present in the cell state shown in Fig. 6.

$$\tilde{c}_t = \tanh(W_c[h_{t-1}, x_t] + b_c) \quad (4)$$

Thus, the focus vector is generally named as the output gate. There are several potential values in the matrix are made to move forward to the subsequent hidden state is expressed in equation 5.

$$o_t = \sigma(W_o[h_{t-1}, x_t] + b_o) \quad (5)$$

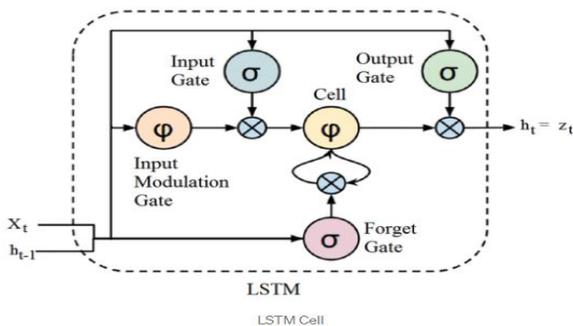


Fig. 6. LSTM Working Process.

The memory usage is generally named as hidden state whereas the data is considered for the next sequence which is illustrated in equation (6) that performs as an analog for the hidden state in RNN.

$$h_t = o_t \circ \tanh(c_t) \quad (6)$$

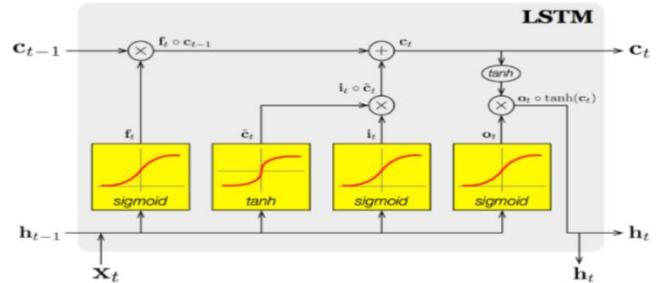


Fig. 7. LSTM Cells Activation Function.

The forget gate that aids in the forgetting of information from a previous cell state, is the sigmoid's initial activation function (Ct-1). Furthermore, the following sigmoid and initial tanh activation functions are used as input gates, and the information is either stored to the cell state or elapsed. As a result, the preceding sigmoid serves as an output gate, determining which information must be sent on to the next hidden state as shown in the Fig. 7.

#### Algorithm for Predictive auto-scaling using LSTM

**Inputs:** Resource utilization from DevOps users, VMs, Load balancer with RR technique, Data Set, CPU load capacity.

**Output:** Predicted CPU Resource utilization for auto-scaling the nodes.

- Step 1:** Request the instances by Dev-ops users for cyclic workloads.
- Step 2:** On user request the cloudlets can be sent through RR technique for further escalation to Predictive Scaling Engine to forecast the future workload demand using LSTM Model.
- Step 3:** Load the dataset for Data preprocessing which can be done through min max scalar through EDA and fit the LSTM model and GRU model for further execution to train and test.
- Step 4:** Based on the CPU workload, the data acknowledged with long term memory from earlier interval is stored in LSTM cells as per equation 1.
- Step 5:** Modification of cell state is done through forget gate as per equation 2 and the recent information gets accumulated in the output of input gate.
- Step 6:** If the forget gate is set to 1, the data is kept on its own as shown in equation 3, else the information present in the forget gate is multiplied by 0 in the matrix position.
- Step 7:** The weighted input has been applied to the optimized ADAM layer as a sigmoid function with the range [0, 1] for observation as well as prior concealed state.
- Step 8:** The forgotten memory existent in the cell state is accepted by the input modulation gate, which is a tanh activation function performed on the ReLu (Rectified Linear Unit) layer as per equation 4 with a range of [-1, 1].
- Step 9:** The hidden state representing memory usage with data is considered for the next sequence as per equation 6 that performs as sequential layer.
- Step 10:** The process of LSTM is executing the current VMs based on VM list provided through proper VM instance type by EDA.
- Step 11:** If CPU actual load\_capacity > predictive workload, trigger auto-scale in policy (VM-1) else scale-out (VM+1) with cool down time and also by enabling dynamic scaling for cost optimization.
- Step 12:** Update the provisioning instance count and repeat the steps 3 to step 11
- Step 13:** Terminate VMs and return.
- Step 14:** Visualize the Results for further auto-scaling of right instances to be deployed for running the workloads in public cloud.

Auto-Trigger Policy For Predict and Scale:

```
Cat<<EOF>> predict_sclae_policy_cpu.csv // Load History of traces
{
  Region: me-south-1
  {"Metrics": [CPU], "Instance Type":t2, "Cores":8, "Unit"=MHZ}
}
if{"Actual_Target_Value:123>Predicted_Targeted_value=109, VM-1 else
VM+1 "Predefined Metric Type: ASGCPUtilization"}}
{"Mode": Predict and Scale, "Cool down time":300 seconds} EOF
```

However, the request from the Dev-Ops user’s workload are balanced through dynamic weighted RR technique and analyzed by EDA. The process of EDA workloads are performed with predictive auto scaling as auto-scale in of VMs and auto-scale out of VMs are progressed. The progressed VMs are assigned to the respective CSP users precisely with less usage of CPU capacity as well as minimized memory usage. The proposed predictive scaling by LSTM is evaluated by comparing it with Gated Recurrent Unit (GRU) method.

V. RESULT AND DISCUSSION

This research experiment has utilized the AWS platform and simulated real-world workloads to evaluate the predictive scaling approach through Amazon Sagemaker or Google Colab compatible. The CPU core utilized is 8 with 32 GiB of memory, EBS storage, 2.20GHz Intel(R) Xeon(R) turbo boost and 6 bit platform. The host machines for this experimental instance are t2.large, t2.xlarge and t2.2xlarge of same family with burstable performance instances, all of which feature Intel scalable CPUs with speeds up to 3.0 GHz. In this paper, the implementation of the elastic resource allocation strategy is based on the Quality of Service (QoS) performance criterion. However, the recommended method has the ability to meet an appropriate demand in different kinds of varied workloads. Hence, the proposed approach has considered both reducing the CPU utilization and memory usage which progressively reduced the cost of resources utilization. The optimization outcome of QoS parameters for the proposed predictive auto-scaling by LSTM is shown in Table II reveals that the actual CPU and memory usage is high but the recommended CPU and memory usage is low and hence we can save the bill cost in usage of Compute as well as memory instances.

TABLE II. PERFORMANCE RESULTS OF PREDICTIVE AUTO-SCALING FROM LSTM METHOD

DateTime	CPU usage [MHZ]_Actual	Memory usage [KB]_Actual	CPU usage [MHZ]_Predicted	Memory usage [KB]_Predicted
2016-02-02 00:00:00	58	115763	81.240875	136286.890625
2016-02-02 00:05:00	123	332189	106.497734	405408.000000
2016-02-02 00:10:00	62	148478	67.060234	163492.187500
2016-02-02 00:15:00	49	198810	66.726730	151165.390625
2016-02-02 00:20:00	60	0	66.162521	140813.171875

VI. PERFORMANCE ON CPU UTILIZATION

Fig. 8 and Fig. 9 have illustrated the actual and predicted usage trends of CPU based on the date time through visualization insights. The range obtained in the LSTM CPU usage is from 45 to 125MHZ.

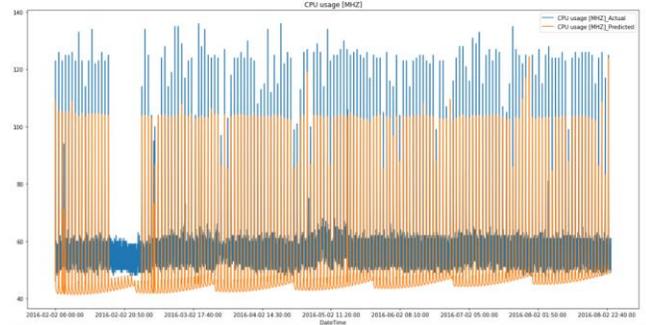


Fig. 8. CPU usage of Actual vs Predicted for LSTM Technique.

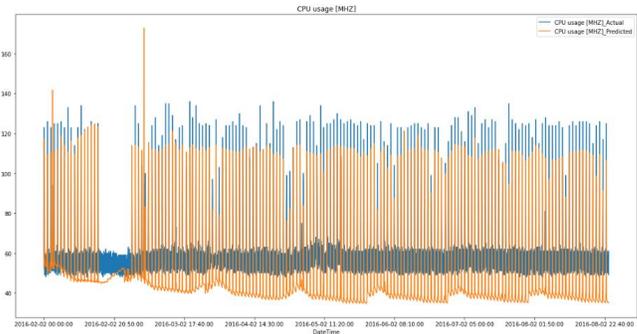


Fig. 9. CPU usage of Actual vs Predicted for GRU Technique.

The maximum CPU resource utilization of actual and predicted for LSTM at 2016-02-02 00:05:00 are 123 MHZ and 109.12 MHZ respectively but in the case of GRU, the CPU utilization at the same datetime is 123 MHZ in actual and 117.18 MHZ in prediction. When comparing the predicted CPU usage of LSTM shows that it is lesser resource utilization than GRU. Therefore, the instance provisioning of LSTM is less while compared to GRU method.

VII. PERFORMANCE ON MEMORY USAGE

Fig. 10 and Fig. 11 have illustrated the actual and predicted usage of memory based on the datetime. The range obtained in the CPU usage is from 45 to 125MHZ. The maximum memory utilization of actual and predicted for LSTM at 2016-02-02 00:05:00 are 332.19 MB and 422.45 MB respectively but in the case of GRU, the memory utilization at the same datetime is 332.19 MB in actual and 398.35 MB in prediction.

However, when comparing the predicted memory utilization of LSTM is higher in resource utilization than GRU but in the other datetime, predicted memory utilization of LSTM is very less than GRU. Therefore, the instance provisioning of LSTM is less as well as avoiding traffic while compared to GRU method.

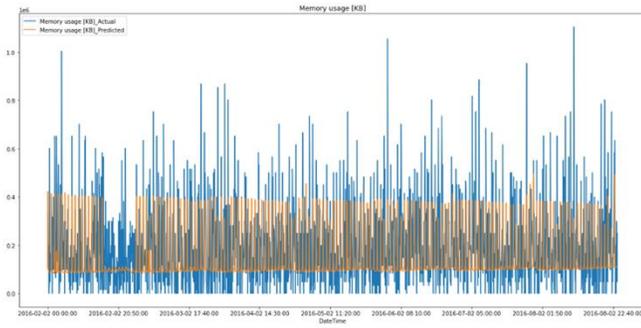


Fig. 10. Memory usage of Actual vs Predicted for LSTM Technique.

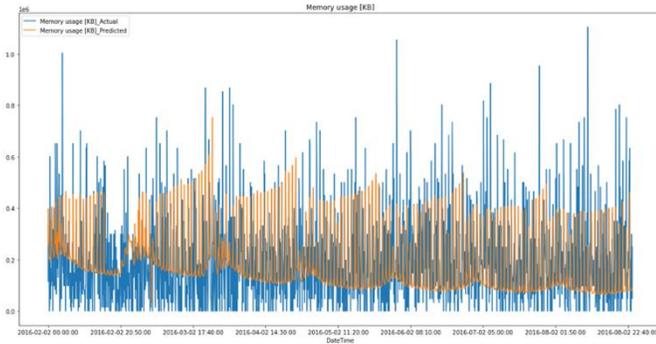


Fig. 11. Memory usage of Actual vs Predicted for GRU Technique.

Moreover, the error rate calculation is done through RMSE value and it is a standard procedure to measure the error of the model in forecasting the quantitative data. It can be measured with the given formula shown in the Fig. 12.

$$RMSE = \sqrt{\frac{\sum_{i=1}^n (\hat{y}_i - y_i)^2}{n}}$$

Fig. 12. RMSE SCORE.

The proposed predictive scaling in LSTM technique is 0.0081 whereas in the case of GRU is 0.0095 that affect the accuracy of the predictive scaling of GRU while comparing to LSTM. Thus, the accuracy of predictive scaling in LSTM is higher may assist in reducing the usage of instance provisioning by minimizing the energy consumption and reduction in bill cost.

### VIII. CONCLUSION

The essential factor required for current situation is green computing which provides the environment with beneficial computing power that believes on energy efficient computing. This paper has presented few basic concepts of predictive auto-scaling with EDA and LSTM algorithm. The working principle of tanh and sigmoid activation function as input has assisted to predict and forecast the predictive scale in and scale out process exactly and accurately. The pitfalls performance has followed the predictive nature to the web application in public cloud. Moreover, the avoidance of these pitfalls can be done through predictive auto-scaling by LSTM technique and validated in a real-time environment. Hence, the result of CPU

usage and memory utilization performances defines the performance of ReLu layer and sequential layer of LSTM technique in cloud computing application. Thus, the comparison of LSTM method is compared with GRU technique for evaluating the performance of CPU usage and memory utilization. The evaluation results determined that CPU utilization and memory usage of LSTM is lesser than GRU method and RMSE value of LSTM is 0.0081 but in GRU is 0.0095 illustrated that error rate is higher in GRU. Moreover, the utilization of predictive scaling method has illustrated an improved performance in terms of energy efficiency by determining the better and reduced utilization of CPU as well as less memory usage while compared to GRU in large data set. This presented innovative idea for Dev-Ops users for unprecedented and cyclic workloads with green cloud brokers through predictive auto-scaling by LSTM has provided the CDC to reduce power consumption without violating QOS and SLA.

### REFERENCES

- [1] N. Serrano, G. Gallardo, and J. Hernantes, Infrastructure as a service and cloud technologies. *IEEE Software*, 32(2):30–36, Mar 2015.
- [2] D. Moldovan, H. L. Truong, and S. Dustdar, Cost-aware scalability of applications in public clouds. In *2016 IEEE International Conference on Cloud Engineering (IC2E)*, pages 79–88, April 2016.
- [3] D. Jayasinghe, S. Malkowski, J. Li, Q. Wang, Z. Wang, and C. Pu. Variations in performance and scalability: An experimental study in iaaS clouds using multi-tier workloads. *IEEE Transactions on Services Computing*, 7(2):293–306, April 2014.
- [4] Liu, Jinwei, Haiying Shen, and Lihua Chen, "CORP: Cooperative opportunistic resource provisioning for short-lived jobs in cloud systems," In *2016 IEEE International Conference on Cluster Computing (CLUSTER)*, pp. 90-99, IEEE, 2016.
- [5] Bi, Jing, Libo Zhang, Haitao Yuan, and MengChu Zhou. "Hybrid task prediction based on wavelet decomposition and ARIMA model in cloud data center." In *2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC)*, pp. 1-6, IEEE, 2018.
- [6] Amiri, Maryam, and Leyli Mohammad-Khanli, "Survey on prediction models of applications for resources provisioning in cloud," *Journal of Network and Computer Applications* 82 (2017): pp. 93-113.
- [7] Yu, Yongjia, Vasu Jindal, Farokh Bastani, Fang Li, and I-Ling Yen, "Improving the smartness of cloud management via machine learning based workload prediction," *IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, vol. 2, pp. 38-44, IEEE, 2018.
- [8] Kaur, Gurleen, Anju Bala, and Inderveer Chana. "An intelligent regressive ensemble approach for predicting resource usage in cloud computing." *Journal of Parallel and Distributed Computing* 123 (2019): pp. 1-12.
- [9] Borkowski, Michael, Stefan Schulte, and Christoph Hochreiner, "Predicting cloud resource utilization," In *Proceedings of the 9th International Conference on Utility and Cloud Computing*, pp. 37-42, 2016.
- [10] Anupama, K. C., R. Nagaraja, and M. Jaiganesh, "A Perspective view of Resource-based Capacity planning in Cloud computing," *1st International Conference on Advances in Information Technology (ICAIT)*, pp. 358-363, IEEE, 2019.
- [11] K. B. Bey, F. Benhammedi, A. Mokhtari, Z. Guessoum, "CPU load prediction model for distributed computing," in *Proc. 8th Int. Symp. Parallel Distrib. Comput.*, Jun. 2009, pp. 39-45.
- [12] K. Mason, M. Duggan, E. Barrett, J. Duggan, and E. Howley, "Predicting host CPU utilization in the cloud using evolutionary neural networks," *Future Gener. Comput. Syst.*, vol. 86, pp. 162-173, Sep. 2018.
- [13] Z. Ullah, S. H. Qazi, and G. M. Khan, "Adaptive resource utilization prediction system for infrastructure as a service cloud," *Comput. Intell. Neurosci.*, vol. 2017, Jul. 2017.

- [14] S. Ismaeel and A. Miri "Multivariate time series ELM for cloud data centre workload prediction," in Proc. Int. Conf. Hum.-Comput. Interact. Cham, Switzerland: Springer, Jul. 2016, pp. 565-576.
- [15] Bi, Jing, Libo Zhang, Haitao Yuan, and MengChu Zhou. "Hybrid task prediction based on wavelet decomposition and ARIMA model in cloud data center." In 2018 IEEE 15th International Conference on Networking, Sensing and Control (ICNSC), pp. 1-6. IEEE, 2018.
- [16] Janardhanan, Deepak, and Enda Barrett. "CPU workload forecasting of machines in data centers using LSTM recurrent neural networks and ARIMA models." In 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), pp. 55-60. IEEE, 2017.
- [17] Cetinski, Katja, and Matjaz B. Juric. "AME-WPC: Advanced model for efficient workload prediction in the cloud." Journal of Network and Computer Applications 55 (2015): pp. 191-201.
- [18] M. U. Farooq, A. Shakoor, and A. B. Siddique, — An Efficient Dynamic Round Robin Algorithm for CPU scheduling, || no. March, 2017.
- [19] B. Dave, P. S. Yadev, M. Mathuria, and Y. M. Sharma, — Optimize Task Scheduling Act By Modified Round Robin Scheme with Vigorous Time Quantum, || 2017 Int. Conf. Intell. Sustain. Syst., no. Iciss, pp. 905 - 910, 2017.
- [20] D. Khokhar and A. Kaushik, — BEST TIME QUANTUM ROUND ROBIN CPU, || no. 5, pp. 3 - 7, 2017.
- [21] Priyanka Singh, Palak Baaga & Saurabh Gupta (2016), Assorted Load Balancing Algorithm in Cloud Computing: A Survey. International Journal of Computer Applications. 143-No 7, June 2016. pp.34-40.
- [22] Asha, M. L. & Neethu Myshri, R. (2014), Performance Evaluation of Round Robin Algorithm in Cloud Environment. International Journal of Computer Applications ( pp.12-16 ). ICICT-2014.
- [23] Yan, M.; Liang, X.; Lu, Z.; Wu, J.; Zhang, W. HANSEL: Adaptive horizontal scaling of microservices using Bi-LSTM. Appl. Soft Comput. 2021, 105, 107216.
- [24] Imdoukh, M.; Ahmad, I.; Alfaiakawi, M.G. Machine learning-based auto-scaling for containerized applications. Neural Comput. Appl. 2019, 32, 9745–9760.
- [25] Tang, X.; Liu, Q.; Dong, Y.; Han, J.; Zhang, Z. Fisher: An Efficient Container Load Prediction Model with Deep Neural Network in Clouds. In Proceedings of the 2018 IEEE Intl Conf on Parallel Distributed Processing with Applications, Ubiquitous Computing Communications, Big Data Cloud Computing, Social Computing Networking, Sustainable Computing Communications (ISPA/IUCC/BDCLOUD/SocialCom/Sustain Com), Melbourne, Australia, 11–13 December 2018; pp. 199–206.
- [26] Mahmoud Imdoukh, Imtiaz Ahmad, Mohammad Gh. Alfaiakawi: Machine Learning –based auto-scaling for containerized applications 2019, Neural Computing and Applications, springer, <https://doi.org/10.1007/s00521-019-04507-z>.
- [27] <http://gwa.ewi.tudelft.nl/datasets/gwa-t-13-materna>.
- [28] Anupama KC, Shivakumar BR, Nagaraja R, "Resource Utilization Prediction in Cloud Computing using Hybrid Model", International Journal of Advanced Computer Science and Applications (IJACSA), vol.12, No.4, 2021.

# Highly Efficient Parts of Speech Tagging in Low Resource Languages with Improved Hidden Markov Model and Deep Learning

Diganta Baishya, Rupam Baruah

Department of Computer Science and Engineering  
Jorhat Engineering College  
Jorhat, India

**Abstract**—Over the years, many different algorithms are proposed to improve the accuracy of the automatic parts of speech tagging. High accuracy of parts of speech tagging is very important for any NLP application. Powerful models like The Hidden Markov Model (HMM), used for this purpose require a huge amount of training data and are also less accurate to detect unknown (untrained) words. Most of the languages in this world lack enough resources in the computable form to be used during training such models. NLP applications for such languages also encounter many unknown words during execution. This results in a low accuracy rate. Improving accuracy for such low-resource languages is an open problem. In this paper, one stochastic method and a deep learning model are proposed to improve accuracy for such languages. The proposed language-independent methods improve unknown word accuracy and overall accuracy with a low amount of training data. At first, bigrams and trigrams of characters that are already part of training samples are used to calculate the maximum likelihood for tagging unknown words using the Viterbi algorithm and HMM. With training datasets below the size of 10K, an improvement of 12% to 14% accuracy has been achieved. Next, a deep neural network model is also proposed to work with a very low amount of training data. It is based on word level, character level, character bigram level, and character trigram level representations to perform parts of speech tagging with less amount of available training data. The model improves the overall accuracy of the tagger along with improving accuracy for unknown words. Results for “English” and a low resource Indian Language “Assamese” are discussed in detail. Performance is better than many state-of-the-art techniques for low resource language. The method is generic and can be used with any language with very less amount of training data.

**Keywords**—Hidden markov models; viterbi algorithm; machine learning; deep learning; text processing; low resource language; unknown words; parts of speech tagging

## I. INTRODUCTION

Parts of speech tagging can be viewed as the problem of word classification. Each such class contains words having some common properties regarding their usage in the sentences. For example, the English language contains the following parts of speech: ‘noun’, ‘pronoun’, ‘verb’, ‘adjective’, ‘preposition’, ‘conjunction’, and ‘interjection’. The meaning of a sentence and its grammatical correctness depends on the kind of parts of speech being used in the sentence. The

accurate parts of speech tagging can only determine the correct interpretation of the text. Any Language Processing task, therefore, depends heavily on the accuracy of tagging. Information in natural languages like parts of speech can be helpful in many language-related tasks. But, most of the developments of natural language processing are observed for a few dominant languages spoken widely in the world. This is because of a lack of extensive research and the non-availability of computable resources for other languages. It is therefore very important to identify the key factors that affect the accuracy and to make proper use of them so that such languages can also benefit from the advancements of natural language processing techniques. The concern is to find the innovative idea to improve accuracy for languages with fewer amounts of data available for use. With the availability of methods to work well with low training, we can develop NLP applications for languages that are poor in terms of computable resources. Also, it is important to design systems that can be used across any language so that the benefit can be transferred to any language.

The Hidden Markov model is one of the most popular stochastic models used for natural language processing. The Viterbi algorithm uses Hidden Markov Model to find the most likely sequence of hidden states. It is used to derive an observed sequence. Thus, the algorithm can be used to predict parts of the speech tags of a sequence of words [1]. The model is trained with a large amount of already tagged training data. Such a model does not work properly when training data is less in volume. The model fails to learn the behaviour due to less training and also due to unknown words that were not used during training. The accuracy is further low in the cases of languages for which adequate training data are not available for training the model. A lot of research has been carried out to overcome this by modifying the hidden Markov model for unknown words but there is a lot of scope for improvement. Most of the research has been carried out to improve the Hidden Markov Model and Viterbi Algorithm using a large training dataset and with the imposition of some rules. Usage of huge training datasets limits the scope of the methods only to those languages that are very rich in computable resources. Also, rule-based methods limit the scope only to the specific language in context because rules are language-dependent. Hence, a language that is not studied in many details cannot get the benefit of rules-based NLP methods. This paper describes

two specific works to improve performance automatic parts of speech tagging for languages with low quantity of resources in computable form. At first, we introduce a new method to calculate the probability for unknown words. We use bigram and trigram of characters for this purpose and we have also made modifications to the Viterbi algorithm accordingly. The bigram and trigram combinations of characters are used as resources during training for the Hidden Markov model. Bigram and trigram of characters help to model unknown words and also to improve recognition for untrained words. Improving accuracy for unknown words improves the performance for languages with fewer amounts of computable resources available for training. Experiments have been conducted in English languages. We have also tested the same with a small set of Assamese, a low resource language spoken widely in North East India. We have reported results that show considerable improvement. The concept is generic and can be used with any language. This is helpful especially for languages with very less amount of computable resources. Such languages cannot be trained with a huge amount of vocabulary due to lack of data and it results in many unknown words being encountered while testing the system.

Next, a deep learning method is proposed to improve recognition for words using bigram and trigram of characters. Machine Learning and deep learning models are very much popular these days. This kind of model learns the behaviour of the system after being trained with enough labeled datasets. The model learns the association of training datasets and applies it to the real data with good accuracy. Such a model needs to be trained with a huge amount of training data to learn the behaviour well. Challenge is to make the system learn from the least amount of available data so that it works for low-resource languages. We have therefore discussed the proposed deep learning architecture that is capable of classifying the words into defined parts of speech with considerable accuracy. It is based on word level, character level, character bigrams, and character trigram level representation.

The rest of the paper is organized as follows: Section II next describes some of the earlier works and popular methods used for automatic parts of speech tagging, the Hidden Markov Model, parts of speech tagging related to low resource languages, and machine learning methods. Section III describes the research objective in brief. Section IV describes the proposed methods and the data sets used for the purpose. Section V outlines the experiments and results. Section VI discusses the outcomes and Section VII concludes with the future scope of improvements. The reference section outlines the references used in the paper.

## II. EARLIER WORK

### A. Works Related to Parts of Speech Tagging

The automatic parts of speech tagging is one of the key areas of research since people started working on processing natural languages. Rule-based methods, stochastic methods, and transformation-based learning approaches are the most widely used supervised techniques for parts of speech tagging. The stochastic or probabilistic methods use a training set and calculate the probability of a word belonging to all possible tags. Based on this calculation, it then assigns the tag with the

highest value of probability. As outlined by Martinez (2011), one of the popular methods involved in POS tagging is the Rule-Based Method which is based on a set of rules set by humans [2]. However, it requires too much manual intervention and also requires in-depth knowledge of grammatical rules that varies from language to language. Transformation Based Learning is also used recently to automatically tag POS where the rules are learned from an initially annotated corpus. This method requires a huge amount of training to make the system learn and provide accurate results. The most popular method for POS tagging is Markov Model Taggers that are based Hidden Markov Model. It works on statistical methods to find the best possible sequence of tags out of the possible tag sequences. It consists of three components: outputs, transitions, and states where states represent the tags in case of POS tagging. Maximum Entropy Methods, Support Vector Machines, Neural networks, Decision trees, etc. are some of the other methods used for this purpose. Accuracy can be obtained above 95%, but the model needs to be trained with a huge training dataset [2]. Among the early works, Janas [3] in 1977 proposed a two-step method based on knowledge of linguistic regularities for English texts. He used a large corpus to get 84% of words tagged correctly. Research into parts of speech tagging for languages other than English has also progressed a lot recently. Fernando et. al (2016) recently presented a Support Vector Machine-based Part-Of-Speech tagger for the Sinhala language [4]. Application of Hidden Markov Models based tagger for the language is far behind as stated by the authors. They reported an overall accuracy of 84.68%, and unknown word accuracy of 59.86%. Better use of techniques like the hidden Markov model will be helpful to improve accuracy for the Sinhala language. But unavailability of a huge corpus like that of English is a concern to do so. Hyun-Je Song and Seong-Bae Parkhave (2020) have recently addressed two of tagging for Korean Language problems using a two-step mechanism [5]. Udomcharoenchaikit, Boonkwan, and Vateekul (2020) have introduced an evaluation scheme of Sequential Tagging Methods based on an example-based system using known spelling errors for the Thai language [6].

### B. Related Works using Hidden Markov Model

The Hidden Markov Model is the most popular stochastic method for automatic parts of speech tagging. Cutting et al. described [1] some initial works on automatic parts of speech tagging based on the Hidden Markov Model (HMM). They reported an accuracy of 96% using Brown corpus [7], developed by Francis et al. (1979) for English. Cing et. al. (2019) presented a comparison of using HMM only, and HMM with morphological analysis for parts of speech tagging of Myanmar Language. Morphological rules are used to improve performance for unknown words. They have stated in conclusion that using only HMM for a small dataset has no scope at all. A large training dataset or rule-based method in combination with HMM is the only solution [8]. Jurgen et al. (2011) used infinite HMM for parts of speech tagging in an unsupervised manner [9]. Myint et al. [10] proposed to use lexical information with HMM for the Myanmar language as HMM is only capable of using in contexts, not lexical information. They have therefore proposed Lexicalized Hidden Markov Models (L-HMMs) for improving recognition.

Thorsten Brants [11] reported that a Markov model-based tagger performs at least as well as other approaches, including the Maximum Entropy framework. He has used some rules on top of HMM for unknown words and found an accuracy of up to 81%. Ferran PLA and Antonio Molina [12] applied Lexicalized Hidden Markov Models and reported improvement of accuracy for part-of-speech tagging. They reported 6% improvement for unknown words. Recently Tham et. al. (2020) have reported the usage of hybrid POS tagger for the Khasi language. A tagger is developed using the Hidden Markov Model (HMM). It is then integrated with conditional random fields (CRF) rules. The errors obtained from the first tagger are used to improve accuracy [13]. Rule-based features are very much dependent on language. Jassim et. al(2021) have used an N iterative HMM model for parts of speech tagging in Iraqi National Song. The iterative approach has improved accuracy as claimed by the authors [14]. Since HMM uses a huge amount of training data, it can very well map the context of the words and provide high accuracy as seen in the works conducted by the researcher discussed above. However, the model suffers in the case of words that are not trained during training. Among the early works, Ratnaparkhi (1996) proposed a maximum entropy model [15] to successfully tag unseen words with accuracy up to 96%. It uses some specialized features to take decisions and uses approximately 900 thousand of words from Wall Street Journal corpus as a training data set taken from the Treebank project (Marcus et al., 1994) [16]. Robert M. Losee [17] used tagging for improving decision-making with the help of linguistic information. Toutanova et al. [18] proposed a part-of-speech tagging using lexical features, preceding and following text context with fine-grained modeling for features of unknown words. Martin Haulrich reported [19] the implementation of a part-of-speech tagger based on the first-order Hidden Markov Model and compared different strategies to improve the result for unknown words. Other rule-based techniques take decisions based on the presence or absence of a number, upper-case letter, etc as proposed by researchers [15]. Rules may be added to improve accuracy for the unknown word. But these rules are language-dependent. Scott M.Thede [20] proposed a few statistical methods for predicting unknown words. The methods are applicable to any language. The author used Brown corpus [7] in this case too. Mikheev (1996) used the beginning and end of a word to predict the parts of speech for unknown words [21]. They used certain morphological rules: Prefix rules, suffix rules, and ending-guessing rules. Anastasyev et. al [22] described rules for detecting unknown word tagging for rich languages. Use of context, word endings are used as clues for detecting parts of speech. The following sections detail the basics principle of the Viterbi Algorithm and Hidden Markov Model.

### C. Basic Principle of Hidden Markov Model

The Hidden Markov Model (HMM) basically comprises of two kinds of events: observed events and hidden events. For the part of speech tagging problem, observed events are the words that appear in the input text and hidden events are the parts of speech that are to be predicted. Components of hidden Markov model are: a matrix of state transition probability, sequence of observation, sequence of emission probabilities and initial probability distribution [23] [24].

1) *Transition probability*: It is the first Markov assumption which implies that the current state depends only on the previous state. We will call this as transition probability. A transition probability matrix is to be calculated based on training data for all pairs of tags (states). Mathematically it is represented by:

$$P(q_i|q_1...q_{i-1}) = P(q_i|q_{i-1}) \quad (1)$$

where,  $q_i$  is the state at  $i^{\text{th}}$  instance.

### 2) *Emission probability*

$$P(o_i|q_1...q_i,...,q_T, o_1,...,o_i,...,o_T) = P(o_i|q_i) \quad (2)$$

Here,  $o_i$  is the observation at  $i^{\text{th}}$  instance.

This second Markov assumption implies that the observation at any instant depends only on the present state. We will term it as emission probability. An emission probability matrix is to be calculated based on training data for all pairs of tags (states) and words (observations).

3) *Viterbi algorithm*: It is used to predict the part of speech of a word based on maximum likelihood calculated as:

$$V(t(j)) = \max : V(t-1) * a(i,j) * b_j(O_t), \quad (3)$$

$V(t(j))$  is the Viterbi path probability of the model being at state  $j$  at any instance, after observing the first  $t$  number of observations. Here  $a$  is transition probability matrix and  $b$  is emission probability matrix [25] [26].

The problem with this basic algorithm is the fact that the emission probability  $P(o_i|q_i)$  is zero for an unknown word. It is because.

$$P(o_i|q_i) = N(o_i|q_i) / Nq_i = 0 \quad (4)$$

where,  $N(o_i|q_i)$  is the number of time observation  $o_i$  appears in training set as state  $q_i$  and  $Nq_i$  is the number of time state  $q_i$  appears in training set. Hence, over the years scientists have come up with different methods to improve accuracy for such words. One simple method is Laplace smoothing, where the following modification is made:

$$P(o_i|q_i) = (1+N o_i|q_i) / (Nq_i + V)$$

where  $V$  is the length of vocabulary trained.

Considering only the transition probability for calculation in case of unknown words is another option to overcome it by replacing the value zero by one .A brief discussion on earlier works in this area is discussed above in this section.

### D. Related Work for Low Resource Languages

The resources available for the available languages in the world are extraordinarily unbalanced [27]. There are many organizations that are working dedicatedly for technology development on low resource language. Under the LORELEI (Low Resource Languages for Emergent Incidents) Program of Linguistic Data Consortium for DARPA, researchers are working on developing NLP technologies for natural disaster management for almost three dozen low resource languages [28]. NLP research teams are working seriously on approximately 20 of the almost 7000 languages of the world

leaving a majority of the population not reachable to advanced NLP applications [29]. Low resource languages are those language that are less computerized, less privileged resource scarce languages. These are languages where statistical methods cannot be applied due to the availability of fewer data [29], [30], [31], [32]. As Simpson et. al. [33] reported that a low resource language: "All meet the basic criteria of being significant in terms of the number of native speakers but poorly represented in terms of available language resources." Christopher et. al. states that defining a language as "low resource language" depends on the Demography, Linguistics, and Resource availability of the language and the speakers [31]. Some amount of work has been done for low resource languages, but the researchers are not yet able to develop NLP applications for majority of the languages. This is because a strong language-independent method is highly essential to work with languages with fewer amounts of training data to develop NLP applications. With the low amount of training, testing always encounters more and more unknown data and it eventually makes the hidden mark model not much useful for such cases. Recently, some works [34] [35] for resource-poor language and rule-based methods have shown some improvement. But still, rule-based NLP applications are language-specific and the advantages are limited. Researchers have used unsupervised techniques for low resource languages. N-gram Models [36] can be also very useful for of processing many natural language processing tasks. Authors reported some considerable result taking help from another resourceful language as parent language and with standardized text for the two languages [37], [38]. But they also reported difficulty in choosing the parent language because typologically close languages do not always work best. Researchers have used modern days supervised techniques based on long short-term memory networks (LSTM) on multilingual embeddings to get good results. But that also requires quite a large training dataset [39], which is not available for most of the languages. Some Researchers have used bilingual lexicon available to some extent for few languages to investigate the possibility of designing language models with limited training data. The method uses the learning of cross-lingual word embeddings to train monolingual language models. The training shows improvements due to the pre-training process [40]. Some amount of work has also been done for Assamese using some stochastic methods [41], [42], [43] [44] [45]. Recently authors have discussed the key areas of NLP research in Assamese [46]. Researchers have also been working recently on parts of speech and other nlp issues on Arabic languages [47] [48].

#### E. Related Work using Machine Learning

Recently deep learning methods have gained high popularity. The same is being used for Indian and other low-resource languages. Sequential deep learning methods are very popular in this regard. Some of them are long short-term memory (LSTM), bidirectional LSTM, gated recurrent units (GRU), recurrent neural network (RNN), etc. Authors in [49], have applied deep learning for tagging the Chinese Buddhist language. Their learning model is based on RNN. The model as informed by the author is more effective than traditional methods. Bidirectional LSTM is another popular method in this regards authors in [50], experimented with

BLSTM and auxiliary loss over a set of 22 languages. They used the auxiliary loss to improve the performance for rare words. Techniques of using character level along with word-level representation are used recently for POS tagging using deep neural networks. Authors in [51] used the method for English and Portuguese. A convolutional layer was used to prepare the data with character representation. Authors in [52] discussed in detail, how to represent character-level information from raw text. They successfully did it to predict the next character from a given sequence of characters. They used a simple recurrent network for this purpose.

Authors in [53], reported using the character level outputs of convolutional neural network (CNN) as inputs to an LSTM RNN model. The authors have stated that it highly improves the performance in the case of morphologically rich languages like Russian, Spanish, French, Czech, Arabic, German. Machine learning approaches have recently been used with many low-level languages. Authors in [54] described their architecture for Korean POS tagging. They addressed the issue of rare word detection by input-feeding and copying mechanism and got considerable results. Authors in [55] used machine learning models for POS tagging of Sanskrit language. They represented each word as a point and then used clustering with LSTM autoencoder to get the tagging. Authors in [56] used deep learning methods for the Nepali language. They used Long Short-Term Memory Networks (LSTM), Recurrent Neural Network (RNN), Gated Recurrent Unit (GRU), and bidirectional variants to successfully tag Nepali words with high accuracy.

### III. RESEARCH OBJECTIVES

Parts of speech is the preliminary pre-processing step that requires to be executed for any NLP application. But the popular methods available for tagging require a huge amount of training data. They perform very poorly for languages for which a huge amount of training data is not available. The problem is to develop parts of speech tagging methods that are applicable to any language in the world with a very low amount of computable resources.

Most common methods like the Hidden Markov Model and Machine Learning are not well applicable to languages where large amounts of computable data resources are not available. Accuracy is also not very high for words that are not trained earlier because the models cannot read much information for such words. Some of the rule-based methods are mainly used to address these issues. But the scope of such a rule is limited and dependent on the language for which rules are set. The need is to develop systems that can improve accuracy, especially for unknown words, with low training and applicable to any language. This paper concentrates on language-independent approaches towards using the Hidden Markov Model and deep learning techniques with a very small amount of training data so that it can be used for any low resource language with considerable performance. Main focus is to devise language-independent methods to improve accuracy especially, the accuracy of unknown words which is the major concern for any supervised method trained with a low training dataset.

#### IV. PROPOSED METHOD

##### A. Using Modified Viterbi Algorithm

We have proposed modifications to Hidden Markov Model to improve accuracy for untrained words with a small set of training data. We have used Subset from Brown Corpus [7], which is mostly used by researchers in this area. This will give a better platform for comparing proposed modifications with exiting methods. Proposed method is based on probability of character bigrams and character trigrams. The emission probability of a character bigram  $b_i$  given tag  $t_i$  is calculated as follows:

$$P(b_i | t_i) = N(b_i | t_i) / N(t_i) \quad (5)$$

where  $N(b_i | t_i)$  is number of time bigram  $b_i$  appears in training set as tag  $t_i$  and  $N(t_i)$  is Number of time tag  $t_i$  appears in training set. Similarly

$$P(tr_i | t_i) = N(tr_i | t_i) / N(t_i) \quad (6)$$

where  $N(tr_i | t_i)$  is the number of time trigram  $tr_i$  appears in training set as tag  $t_i$  and  $N(t_i)$  is Number of time tag  $t_i$  appears in training set.

The probability of unknown words is calculated based on the fact that bigrams (and trigrams) constituting the unknown word may have already appeared in some trained words, and thus this information may be used to predict the possible tag of the unknown word being tested. We assume that the probability of a word given a tag is proportional to the product of probabilities of sequences of character bigrams (also trigrams) of the word given the tag. Thus instead of considering the emission probability of unknown word as zero or one, we make the following changes:

$$P(o_i | q_i) \propto c * P(b_1 | t_i) * P(b_2 | t_i) * \dots * P(b_n | t_i) \quad (7)$$

where  $c$  is a constant and  $b_1, b_2 \dots b_n$  are the bigrams of the characters constituting the word  $o_i$ .

Hence, equation (3) can be rewritten as

$$V(t_j) = \max: V(t-1) * P(b_1 | t_i) * P(b_2 | t_i) * \dots * P(b_n | t_i) * b_j(O_i) \quad (8)$$

If any value of  $P(b_k | t_i)$  turns out to be zero, it is considered to be a very small value to avoid zero product.

Similarly the same kind of modifications can be made for trigrams of characters:

$$V(t_j) = \max: V(t-1) * P(tr_{i1} | t_i) * P(tr_{i2} | t_i) * \dots * P(tr_{in} | t_i) * b_j(O_i) \quad (9)$$

If any value of  $P(tr_{ik} | t_i)$  turns out to be zero, it is considered to be a very small value to avoid zero product. This is an alternative to considering a zero or one value for the emission probability for the entire word as discussed in the previous section. This helps us to guess the probability of an unknown word, by using the probabilities of bigrams that may have occurred with other words that are already trained.

##### B. Using Deep Learning Architecture

The recent usage of neural network and machine learning methods has proved to be very much useful in modern technology. One of the most popular neural networks used for this purpose is a recurrent neural network (RNN). It feeds the

output of one stage as input to the next. The states in RNN can store input of variable length of sequences. This particular property makes it very much useful for inputs with variable lengths like text sentences, speech processing, etc. LSTM is a kind of RNN that uses a special unit that can store memory for the long term. This kind of model can keep information retained for a long time because of its ability to select the kind of information to retain.

We have designed an architecture for the deep learning model and have successfully implemented it to work considerably well with less amount of training data. The work is inspired by [57], [58], and [59], where authors have used character-level representation along with word-level representation to train the model. We take a sequence of tagged words and feed the words, characters, bigrams and trigrams of characters of words into the first layer of the learning model. We have experimented with different parameters of the layers to get the best-suited architecture. The first layer of the learning network transforms words into feature vectors. It captures information about words' semantic and their morphological characteristics. Every word is converted into a vector of sub vectors of word-level embedding, character-level embedding, bigram character-level wording, and trigram character-level wording.

1) *Word-level embeddings*: Word-level embeddings are encoded in an embedding matrix by column vectors where each column represents the word-level embedding of the corresponding word in the vocabulary. Every word thus is converted into its word-level embedding. A word is first encoded as a one-hot column vector. It is then fed to the input layer. A word embedding matrix is used to multiply it to finally get the word embedding. A word vector at time instant  $t$ ,  $WV_t$  is multiplied with embedding matrix  $WM_w$  to get the Word Embedding  $E_w$  as follows:

$$E_w = WV_t \times WM_w \quad (10)$$

2) *Character-level embeddings*: All characters in a word are represented by a character level embedding. Like, word-level embedding, Character-level embeddings are encoded in an embedding matrix by column vectors where each column represents the character-level embedding of the corresponding character in the character vocabulary. The word embedding is calculated by concatenating word and character embeddings.

$$E_w = (WM_w \times WV_t) \epsilon (CM_c^1 \times CV_t^1) \epsilon (CM_c^2 \times CV_t^2) \dots \epsilon (CM_c^n \times CV_t^n) \quad (11)$$

where,  $\epsilon$  is concatenation symbol. A character vector at time instant  $t$  and position  $i$ ,  $CV_t^i$  is multiplied with embedding matrix  $CM_c$  to get the Character Embedding.

3) *Bigram-character-level embeddings*: All bigram combinations of characters in a word are represented by a bigram-character level embedding. Like, word-level embedding, bigram-character level embeddings are encoded in an embedding matrix by column vectors where each column represents the bigram character-level embedding of the

corresponding bigram-character in the bigram-character vocabulary. The word embedding is then calculated by concatenating word, character embeddings, and bigram character embeddings.

$$E_w = (WM_w \times WV_t) \epsilon (CM_c^1 \times CV_t^1) \epsilon \dots \epsilon (CM_c^n \times CV_t^n),$$

$$\epsilon (BM_c^1 \times BV_t^1) \epsilon \dots \epsilon (BM_c^m \times BV_t^m) \quad (12)$$

where  $\epsilon$  is concatenation symbol. A bigram character vector at time instant  $t$  and position  $i$ ,  $BV_t^i$  is multiplied with embedding matrix  $BM_c$  to get Bigram Character Embedding.

4) *Trigram-character-level embeddings:* Similarly, trigram combination of characters in a word is represented by a trigram level embedding. It is encoded in an embedding matrix by column vectors where each column represents the trigram character-level embedding of the corresponding trigram-character in the trigram-character vocabulary.

$$E_w = (WM_w \times WV_t) \epsilon (CM_c^1 \times CV_t^1) \epsilon \dots \epsilon (CM_c^n \times CV_t^n),$$

$$\epsilon (TM_c^1 \times TV_t^1) \epsilon \dots \epsilon (TM_c^m \times TV_t^m) \quad (13)$$

where  $\epsilon$  is concatenation symbol. A trigram character vector at time instant  $t$  and position  $i$ ,  $TV_t^i$  is multiplied with embedding matrix  $TM_c$  to get Trigram Character Embedding.

The addition of bigram combinations and trigram combinations helps the model to learn the inflections and morphological patterns related to tagging very well. The results are discussed in the next section. The basic principle of concatenating the different kind of embedding is illustrated in Fig. 1.

The difference with the usual LSTM applied is in the fact that word embedding in proposed model is a concatenation of word embedding, character embedding, and bigram character embedding or trigram character embedding. The order of characters is the same as the order in which they appear in the word. Similarly, the order of bigram and trigrams of characters are also in the same order in which they appear in the word. The embedding dimensions are decided after repeated experiments to get the most suitable value.

### C. Data Sets

The English dataset is based on already tagged Brown Corpus [7]. The corpus is based on the current American English language containing about a million words. It comprises elements of statistics, psychology, linguistics, and sociology. Kučera and Francis (1967) reported their initial work on basic statistics on the corpus which eventually turned into Brown Corpus [7] [60].

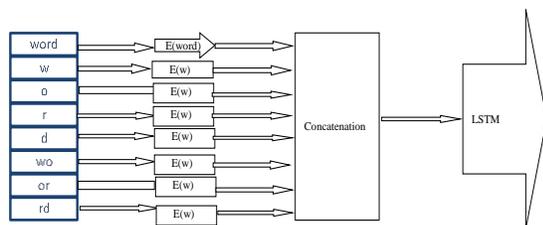


Fig. 1. Concatenating the Embeddings to Feed into LSTM.

The dataset considered for Assamese is developed in-house. Assamese is the language spoken over the state of Assam and entire North-East India. However, not much information is available in computable form. A publicly available set of tagged words is not available in Assamese. Hence it is prepared in-house. It comprises an annotated text of approximately ten thousand words. The dataset is prepared from a corpus collected from TDIL (Technology Development for Indian Languages). It contains articles of different categories like storybooks, scientific articles, health articles, drama, etc. The corpus was tagged into different kinds of parts of speech as per Assamese grammar.

## V. EXPERIMENTS AND RESULTS

We have prepared three small datasets of three different sizes of words taken from already tagged Brown Corpus. The original implementation of the Viterbi algorithm performs poor due to low training data. Due to low training, it cannot approximate the transition matrix accurately. Also, it encounters many unknown words during testing because of the small training size. In the original Viterbi algorithm, due to zero utterances of unknown words in training data, the emission probability evaluates to zero, thus resulting in zero value for the observation. This is already stated in equation (4)

$$P(o_i|q_i) = N(o_i|q_i) / Nq_i = 0$$

The transition probability is only considered by many researchers for the multiplication of transition probability and emission probability. It is equivalent to consider emission probability as one for unknown words. This is obviously a biased method, thus resulting in poor performances for both unknown and known words. Again, if zero value for emission probability is considered for unknown words, then the calculated value becomes zero for all unknown words, which is an obvious fault.

For small training data, this is a big challenge because, with a small training data, the transition history cannot be learnt properly and so it can never accurately measure the transition matrix. Therefore, the performance is very poor especially for unknown words. Proposed method replaces the transition probability with the probability of multiplication of individual emission probability of bigrams. The result shows improvement as it gives the word a tag based on the probability distribution of its constituent bigrams towards the tags as per corpus. The product of individual probabilities of bigrams is multiplied with transition probability, thus considering both emission and transition rather than considering none or only transition probability.

First, experiment was conducted for 5000 words as Training Set and 1250 words as Test Set for the very basic Viterbi Algorithm. The performance is poor because the system was trained with too low data. Similarly, the same was done with 10,000 and 20,000 words of training and test them with 2,500 and 5,000 words respectively for the basic Viterbi algorithm as a baseline for comparison.

The result of the implementation of the basic Viterbi algorithm on the three small sequences only tagged words (4:1 ratio for trained and tested words) used for training is tabulated

in Table I. The result shows improvement with more training data due to better guess of transition probability because of more training.

TABLE I. RESULT OF THE BASIC VITERBI ALGORITHM TRAINED WITH SMALL SET OF TAGGED WORDS

<b>Training Size(words)</b>	5000	10000	20000
<b>Number of word tested</b>	1250	2500	5000
<b>unknown word tested</b>	318	552	1131
<b>Unknown Word accuracy</b>	35.53%	39.86%	40.58%
<b>Overall Word accuracy</b>	79.68%	82.48%	81.06%

As discussed earlier, the evaluation of the correct tag(state) is based upon the equation:

$$V(t(j)) = \max : V(t-1) * a(i,j) * b_j(O_t)$$

It can be simplified as finding maximum likelihood of state over all possibility based upon the equation.

$$P(\text{State}) = P(\text{Tag/PrevTag}) * P(\text{Word/Tag}) \quad (14)$$

In simple term, it can be written as:

$$P(\text{State}) = P(\text{emission}) * P(\text{transition})$$

Next, two modifications are made on the following basic formula:

$$P(\text{State}) = P(\text{emission}) * P(\text{transition})$$

#### A. Modification Method1

It is based on emission probability of character bigrams and trigrams. The probability of a state is calculated based upon the following equation:

$$P(\text{State}) = \text{Product of emission probabilities of bigrams (trigrams)} \quad (15)$$

The transition probability is discarded as work is concentrated on small set of training data.

#### B. Modification Method2

It is based on emission probability of character bigrams and trigrams and transition probability of tags. The probability of a state is calculated based upon the following equation:

$$P(\text{State}) = \text{Product of emission probabilities of bigrams (trigrams)} * P(\text{transition}) \quad (16)$$

A part of the bigram probability matrix is also shown in Table II. It is calculated from first 5000 words of Brown corpus. The table shows probabilities of BIGR(Bigram) for the following parts of speech: NOU(Noun), VRB (Verb), ADJ(Adjective), DET (Determinant), ADP(Adposition), PRO (Pronoun), ADV(Adverb) and CON(Conjunction). Matrix for only five bigram combinations are shown.

The basic algorithm performs better with the larger size of the training data set. The accuracy value above 96% has been reported [1] using entire Brown Corpus [7] of approximately 540 thousand words. However, unknown word accuracy is not good. Then the proposed modifications are applied upon the same set of data. The goal is to improve the results with a small set of training data. The trigram character probability has also been used instead of using bigram probability for the same sets of data. The results with the four datasets of different sizes are described in Table III, Table IV, Table V and Table VI, respectively.

A comparison of the results for the four different sizes of training data with the same 4:1 ratio of different testing and training dataset are shown in Fig. 2. Improvement is more visible with bigram characters than that of trigrams. For subsequent experiments, bigram characters are used.

Next, Experiments were also conducted for bigrams with increased rate of testing data (50% training and 50% testing) and the results are tabulated below in Table VII. In this case three different sizes of text were taken from Brown corpus and then the systems were trained using them. Equal volume of data was used to test each of the systems. The test dataset was selected from a different part of the corpus.

TABLE II. PART OF THE BIGRAM PROBABILITY MATRIX

<b>BIGR</b>	<b>NOU</b>	<b>VRB</b>	<b>ADJ</b>	<b>DET</b>	<b>ADP</b>	<b>PRO</b>	<b>ADV</b>	<b>CON</b>
<b>Aa</b>	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000
<b>Ab</b>	0.0012	0.0022	0.0098	0.0000	0.0000	0.0000	0.0130	0.0000
<b>Ac</b>	0.0045	0.0053	0.0033	0.0084	0.0015	0.0000	0.0047	0.0000
<b>Ad</b>	0.0034	0.0075	0.0025	0.0000	0.0000	0.0000	0.0083	0.0000
<b>Ae</b>	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000	0.0000

TABLE III. SUMMARY OF THE RESULTS FOR TRAIN SIZE OF 5000

	<b>Original Method</b>	<b>Modification Method1 (Equation 11)</b>		<b>Modification Method2 (Equation 12)</b>	
		<b>Bigram</b>	<b>Trigram</b>	<b>Bigram</b>	<b>Trigram</b>
<b>Size of Test Set</b>	1250	1250	1250	1250	1250
<b>Unknow word</b>	318	318	318	318	318
<b>Unknown Word accuracy</b>	35.5%	55.9%	54.1%	56.6%	55.6%
<b>Overall Word accuracy</b>	79.7%	85.0%	84.8%	85.3%	85.2%

TABLE IV. SUMMARY OF THE RESULTS FOR TRAIN SIZE OF 10000

	Original Method	Modification Method1 (Equation 11)		Modification Method2 (Equation 12)	
		Bigram	Trigram	Bigram	Trigram
Size of Test Set	2500	2500	2500	2500	2500
Unknow word	552	552	552	552	552
Unknown Word accuracy	39.9%	58.7%	57.6%	65.4%	59.0%
Overall Word accuracy	82.5%	86.8%	86.6%	88.4%	87.0%

TABLE V. THE COMPARATIVE SUMMARY OF THE RESULTS FOR TRAIN SIZE OF 20000

	Original Method	Modification Method1 (Equation 11)		Modification Method2 (Equation 12)	
		Bi gram	Tri gram	Bi gram	Tri gram
Size of Test Set	5000	5000	5000	5000	5000
Unknow word	1131	1131	1131	1131	1131
Unknown Word accuracy	40.6%	52.4%	51.9%	60.7%	55.6%
Overall Word accuracy	81.1%	83.7%	83.9%	85.7%	84.7%

TABLE VI. THE COMPARATIVE SUMMARY OF THE RESULTS FOR TRAIN SIZE OF 50000

	Original Method	Modification Method1 (Equation 11)		Modification Method2 (Equation 12)	
		Bigram	Trigram	Bigram	Trigram
Size of Test Set	12500	12500	12500	12500	12500
Unknow word	2076	2076	2076	2076	2076
Unknown Word accuracy	42.3%	46.4%	51.6%	60.4%	55.7%
Overall Word accuracy	85.8%	86.5%	87.5%	88.8%	88.2%

TABLE VII. RESULTS WITH 50:50 RATIO OF TRAINING AND TEST DATASET USING BIGRAM CHARACTERS

	Original Method		Modification Method1 (Equation 11)		Modification Method2 (Equation 12)	
	10000	20000	10000	20000	10000	20000
Size of Train Set	10000	20000	10000	20000	10000	20000
Size of Test Set	10000	20000	10000	20000	10000	20000
Unknow word	2723	4328	2723	4328	2723	4328
Unknown accuracy	38.6%	43.2%	55.4%	49.9%	63.2%	59.9%
Overall accuracy	78.5%	82.3%	83.3%	83.8%	85.4%	86.0%

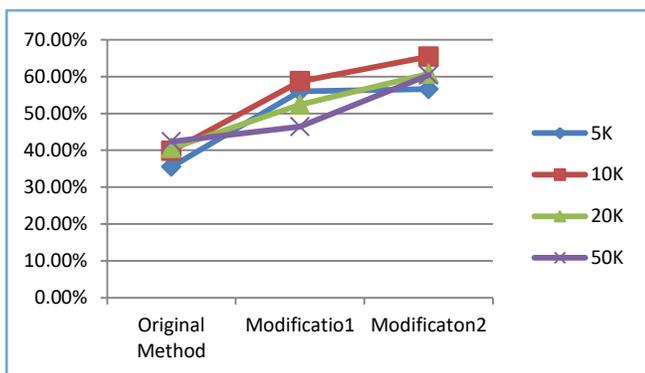


Fig. 2. Comparison of the Three Methods for unknown Words with 4:1 Ratio of different Testing and Training Dataset Bigram Characters.

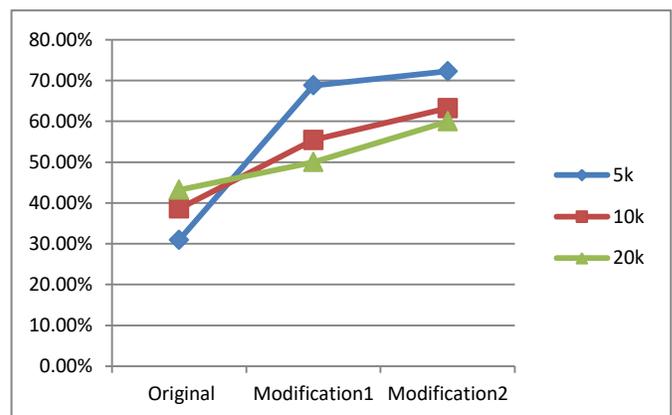


Fig. 3. Comparison of the Three Methods for unknown Words with 1:1 Ratio of different Testing and Training Dataset.

With the size of test dataset being almost double than the previous experiments, the results are seen to be consistent for unknown words. A comparison is detailed in Fig. 3.

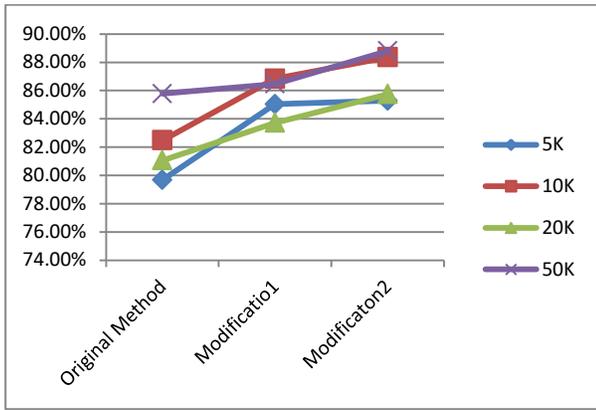


Fig. 4. Overall Accuracy for different Sizes of Train and Test Data (4:1) with Bigram of Characters.

The accuracy for unknown words is only detailed above. The overall accuracy is not any issue with Hidden Markov Model, which is high in this case too even with very low size of training data. The overall accuracy for the different sizes using bigram characters are depicted in Fig. 4.

The system is also tested with “Assamese” language with low training data. Assamese is a low resource language spoken in the state of Assam located in North East India. The findings are tabulated below in Table VIII and a brief comparison is shown in Fig. 5 and Fig. 6.

The system is also tested with “Assamese” language with 1:1 ratio of training and testing data. The findings are tabulated below in Table IX and Fig. 5.

The Assamese corpus was collected from TDIL (Technology Development for Indian Languages), which can be procured from their website after due permission. The corpus was tagged as per Assamese grammar rules to prepare train and test dataset. The result shown here is based on a train and test size of 10k words each that are non-overlapping. The

results are satisfactory even with large proportion of unknown words.

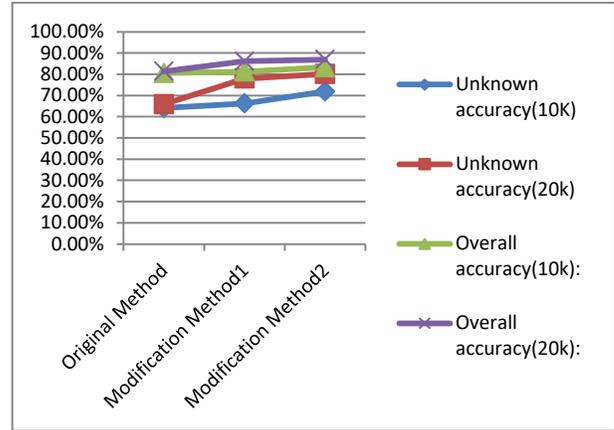


Fig. 5. Accuracy for 10K and 20 K of Training with 2.5 K and 5 K Testing Data respectively (4:1) using Bigram Characters for Assamese.

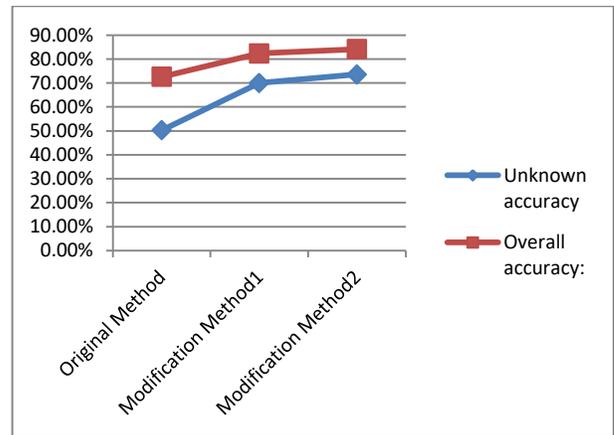


Fig. 6. Accuracy for 10K of Training and 10 K Testing data (1:1) using Bigram Characters for Assamese.

TABLE VIII. RESULTS WITH 4:1 RATIO OF TRAIN AND TEST SET USING BIGRAM CHARACTERS FOR ASSAMESE

	Original Method		Modification Method1 (Equation 11)		Modification Method2 (Equation 12)	
Size of Train Set	10000	20000	10000	20000	10000	20000
Size of Test Set	2500	5000	2500	5000	2500	5000
Unknow word	907	1960	907	1960	907	1960
Unknown accuracy	64.1 %	65.9%	66.3%	77.9%	71.9%	80.2%
Overall accuracy	80.6%	81.4%	81.2%	86.1%	83.3%	86.9%

TABLE IX. RESULTS OF 1:1 RATIO OF TRAIN-TEST SET USING BIGRAM CHARACTERS FOR ASSAMESE

	Original Method	Modification Method1 (Equation 11)	Modification Method2 (Equation 12)
Size of Train Set	10000	10000	10000
Size of Test Set	10000	10000	10000
Unknow word	5034	5034	5034
Unknown accuracy	50.26%	69.98%	73.60%
Overall accuracy	72.56%	82.34%	84.17%

C. Result with Deep Learning Model

The proposed deep learning model is then applied to automatically tag the same set of English words used above. The result obtained is satisfactory and described in Table X and Fig. 7. The training dataset used is much smaller to check its usefulness for low resource languages. Datasets of sizes 10k and 20 k are used to train the system and it is tested with the equal size of different data.

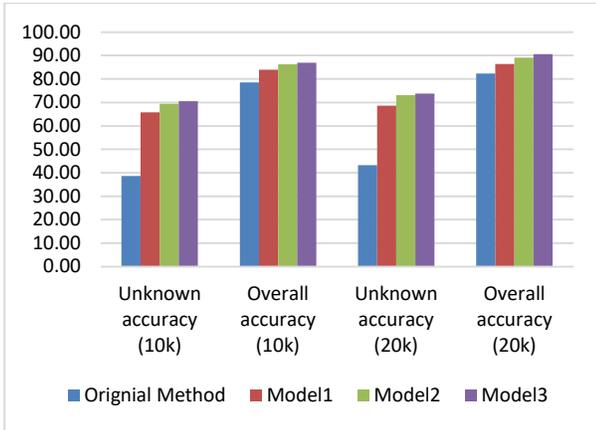


Fig. 7. Accuracy for 10K of Training and 10 K Testing Data (1:1) using Deep Learning for English.

Next, proposed deep learning model is used for the same purpose for the Assamese Language. Initially, only the traditional machine learning method of using word-level is

applied embedding to get an accuracy of 72.51% which is comparable to the proposed traditional stochastic model. Next, the system is trained with word and character level embedding (Model1) and the accuracy jumps to 88.21%. Next, the model combining word and character sequences with tigrams (Model2) and trigrams (Model3) is implemented. As the models learn the morphological behaviours much better than before, the accuracy goes up to 93.52% for bigrams and 94.51% for trigrams. The accuracy of unknown words also raises due to better learning. Table XI and Fig. 8 compares the result of applying the proposed deep learning models for Assamese.

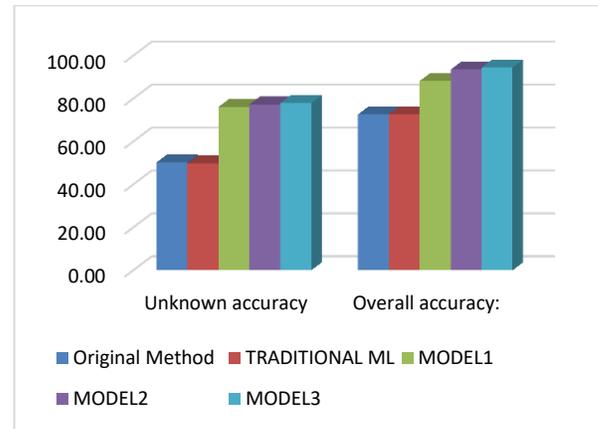


Fig. 8. Accuracy for 10K of Training and 10 K Testing Data (1:1) using Deep Learning for Assamese.

TABLE X. RESULT WITH 50:50 RATIO OF TRAIN AND TEST SET USING DEEP LEARNING FOR ENGLISH

	Original Method		Model1		Model2		Model3	
<b>Train Set:</b>	10000	20000	10000	20000	10000	20000	10000	20000
<b>Test Set</b>	10000	20000	10000	20000	10000	20000	10000	20000
<b>Unknown word</b>	2723	4328	2723	4328	2723	4328	2723	4328
<b>Unknown accuracy</b>	38.6%	43.2%	65.8%	68.6%	69.5%	73.1%	70.6%	73.8%
<b>Overall accuracy</b>	78.5%	82.3%	84.0%	86.4%	86.3%	89.1%	86.9%	90.6%

TABLE XI. RESULTS WITH EQUAL SIZE TRAIN AND TEST SET USING DEEP LEARNING FOR ASSAMESE

	Original Method	Traditional ML Method	Model1	Model2	Model3
<b>Train Set Size</b>	10000	10000	10000	10000	10000
<b>Test Set Size</b>	10000	10000	10000	10000	10000
<b>Unknown word</b>	5034	5034	5034	5034	5034
<b>Unknown accuracy</b>	50.26%	45.82%	76.08%	77.27%	77.89%
<b>Overall accuracy</b>	72.56%	72.41%	88.21%	93.52%	94.51%

## VI. DISCUSSION

The results of the experiments with modified HMM methods clearly state improvement of accuracy for unknown words. The training sets of 5k, 10k, 20k, and 50k are used on an experimental basis and the system can also be tested with a large dataset. However, as the goal is to improve accuracy with a small training set, so the limited sizes of data are considered for training. The methods do not use any specific rule, and hence can be implemented for any language. The initial experiments are based on a 4:1 ratio of training and testing dataset, which shows considerable improvement with Modifications even though the test size increased with an increase in training size to maintain the ratio. The results are also encouraging for the next set of experiments that are based on a 1:1 ratio of training and testing dataset. Even with equal sizes of testing and training datasets, the system performs considerably well specially for a second modification. In the experiments conducted, it is observed that the accuracy has improved with an increase in the training set from 5,000 to 50,000 particularly in the case of modification method2. This happens because, with an increase in the size of the training set, the transition probability starts contributing along with emission probability, thus increasing accuracy. The improvement observed is less in Method1 as it only considers emission probability. Table VII and Table IX clearly show that the accuracy does not degrade even after increasing test size and unknown words. The system maintains overall accuracy of above 85% in all cases, which is considered good with such a low amount of training. The overall accuracy is higher than 80% even when it is exposed to a test dataset of size equal to that of the training set.

The accuracy further improves with the proposed deep learning model. The words when trained with characters and bigram or trigrams of characters improve the accuracy further as shown in Table X and Table XI. The model learns better when bigram and trigrams of characters are fed into the input along with character sequences. The bigrams and trigrams of characters allow the model to learn better the inflections and hence accuracy improves. The improvement is more obvious for Assamese because of high inflections.

Table XII compares some of the works carried for Assamese in recent times.

TABLE XII. COMPARING THE RESULT WITH OTHER RECENT WORKS IN ASSAMESE

Reference Paper	Accuracy
[41]	89.21%
[42]	87.17%
[43]	87%
Work referred in this Paper	94.51%

## VII. CONCLUSION

It is observed that the accuracy of transition probability increases with an increase in the size of the training dataset. The transition among the different parts of speech can easily be computed in the form of transition probability with the help of a very large training set. But, for a small set of training data,

the transition probability is not predictable. Hence, for a small set of training data, emission probability plays the most important role to decide the total probability. Due to non-appearance in the training set, the emission probability for unknown words is zero and this is the root cause of the problem for detecting correct tags of unknown words. With the usage of bigram and trigram of characters in proposed modifications, unknown words may also have non-zero emission probability if such bigrams and trigrams have ever occurred during training other words. This increases the accuracy while classifying unknown words. The experiments conducted for English with low training data prove that the results are comparable with other methods used with large training data. The same technique of character sequences, bigrams sequences of characters, and trigrams sequences of characters applied to design a deep learning model also makes the system learn the behaviour so well that accuracy level increases up to a great extent. The system also performs well for low resource language like "Assamese" when used with a very small volume of training data. The methods are language independent and we hope that the methods will be useful for future implementation for any low resource language. More in-depth research on this will further improve accuracy for low resource language.

## REFERENCES

- [1] Doug Cutting and Julian Kupiec and Jan Pedersen and Penelope Sibun, "A Practical Part-of-Speech Tagger", <https://www.aclweb.org/anthology/A92-1018.pdf>.
- [2] A. R. Martinez (2011), "Part-of-speech tagging. Wiley Interdisciplinary Reviews" Computational Statistics, 4(1), 107–113. doi:10.1002/wics.195.
- [3] Jürgen M.Janas, "Automatic recognition of the part-of-speech for English texts", Information Processing & Management, Volume 13, Issue 4, 1977, Pages 205-213.
- [4] Fernando, Sandareka, Surangika Ranathunga, Sanath Jayasena, and Gihan Dias, "Comprehensive part-of-speech tag set and svm based pos tagger for sinhala." In Proceedings of the 6th Workshop on South and Southeast Asian Natural Language Processing (WSSANLP2016), pp. 173-182. 2016.
- [5] Hyun-Je Song and Seong-Bae Park, "Korean Part-of-speech Tagging Based on Morpheme Generation", ACM Trans. Asian Low-Resour. Lang. Inf. Process. 19, 3, Article 41 (April 2020), 10 pages. DOI:<https://doi.org/10.1145/3373608>.
- [6] Can Udomcharoenchaikit, Prachya Boonkwan, and Peerapon Vateekul., "Adversarial Evaluation of Robust Neural Sequential Tagging Methods for Thai Language", ACM Trans. Asian Low-Resour. Lang. Inf. Process. 19, 4, Article 53 (July 2020), 25 pages. DOI:<https://doi.org/10.1145/3383201>.
- [7] Francis, W. Nelson & Henry Kucera, "BROWN CORPUS MANUAL: Manual of Information to Accompany a Standard Corpus of Present-Day Edited American English for Use with Digital Computers.", 1979 <http://icame.uib.no/brown/bcm.html>.
- [8] D.L Cing., and K.M Soe, "Joint word segmentation and part-of-speech (POS) tagging for Myanmar language", Seventeenth International Conference on Computer Applications (ICCA 2019).
- [9] Jurgen Van Gael, Andreas Vlachos and Zoubin Ghahramani, "The infinite HMM for unsupervised PoS tagging.", EMNLP (2009).
- [10] Phyu Hninn Myint, Tin Myat Htwe, and Ni Lar Thein, "Lexicalized HMM-based Part-of-Speech Tagger for Myanmar."
- [11] Thorsten Brants, "TnT-a statistical part-of-speech tagger." arXiv preprint [cs/0003055](https://arxiv.org/abs/cs/0003055) (2000).
- [12] Antonio Molina, & Ferran Pla, (2001), "Clause Detection using HMM" 10.3115/1117822.1455688.

- [13] Tham, Medari Janai. "A Hybrid POS Tagger for Khasi, an Under Resourced Language." *International Journal of Advanced Computer Science and Applications(IJACSA)* 11, no. 10 (2020): 333-342.
- [14] Jassim, Abbood Kirebut, and Boshra F. Zopon Al Bayaty. "A Stochastic Approach to Identify POS in Iraqi National Song using N-Iterative HMM using Agile Approach.", *IOP Conference Series: Materials Science and Engineering*. Vol. 1094. No.1.IOP Publishing, 2021.
- [15] Ratnaparkhi, Adwait, "A Maximum Entropy Model for Part-Of-Speech Tagging", *Conference on Empirical Methods in Natural Language Processing, 1996*, available "https://www.aclweb.org/anthology/W96-0213.
- [16] Mitchell Marcus, Grace Kim, Mary Ann Marcinkiewicz, Robert MacIntyre, Ann Bies, Mark Ferguson, Karen Katz, Britta Schasberger "The Penn Treebank: annotating predicate argument structure." In *HUMAN LANGUAGE TECHNOLOGY: Proceedings of a Workshop held at Plainsboro, New Jersey, March 8-11, 1994*. 1994.
- [17] Robert M.Losee, "Natural language processing in support of decision-making: phrases and part-of-speech tagging", *Information Processing & Management* Volume 37, Issue 6, November 2001, Pages 769-787.
- [18] Kristina Toutanova, Dan Klein, Christopher D. Manning, and Yoram Singer. 2003, "Feature-rich part-of-speech tagging with a cyclic dependency network", In *Proceedings of the 2003 Conference of the North American Chapter of the Association for Computational Linguistics on Human Language Technology - Volume 1 (NAACL '03)*. Association for Computational Linguistics, USA, 173-180. DOI:https://doi.org/10.3115/1073445.1073478".
- [19] Martin Haulrich, "Different Approaches to Unknown Words in a Hidden Markov Model Part-of-Speech Tagger", 2009. available at: <https://cl.lingfil.uu.se/~nivre/statmet/haulrich.pdf>.
- [20] Scott M. Thede. "Predicting part-of-speech information about unknown words using statistical methods.", *Proceedings of COLING-ACL '98*, pages 1505-1507.
- [21] Andrei Mikheev. 1997, "Automatic rule induction for unknown-word guessing", *Comput. Linguist.* 23, 3 (September 1997), 405-423.
- [22] Daniil Anastasyev, Andrew Andrianov, and Eugene Indenbom. "Part-of-speech tagging with rich language description." In *Computational Linguistics and Intellectual Technologies. Proceedings of the International Conference "Dialogue"*, vol. 16, no. 23, pp. 2-13. 2017.
- [23] L R Rabiner (1989) "A tutorial on hidden Markov models and selected applications in speech recognition." *Proc IEEE* 77(2):257-286.
- [24] Daniel Jurafsky, James H Martin. 2000. "Speech and Language Processing. Pearson Education".
- [25] A J Viterbi (April 1967). "Error bounds for convolutional codes and an asymptotically optimum decoding algorithm". *IEEE Transactions on Information Theory*. 13 (2): 260-269. doi:10.1109/TIT.1967.1054010.
- [26] G. David Forney Jr, "The Viterbi Algorithm: A Personal History", 2005.
- [27] Daniel Nettle, "Explaining Global Patterns of Language Diversity", *Journal of Anthropological Archaeology*, Volume 17, Issue 4, 1998, Pages 354-374, ISSN 0278-4165.
- [28] S Strassel. and J Tracey "Lorelei language packs: Data, tools, and resources for technology development in low resource languages", In *Proceedings of the Tenth International Conference on Language Resources and Evaluation (2016)*, pages 3273-3280.
- [29] Magueresse, Alexandre, Vincent Carles and Evan Heetderks, "Low-resource Languages: A Review of Past Work and Future Challenges." *ArXiv abs/2006.07264* (2020).
- [30] Anil Kumar Singh. 2008, "Natural language processing for less privileged languages: Where do we come from? where are we going?" In *Proceedings of the IJCNLP-08 Workshop on NLP for Less Privileged Languages*.
- [31] Christopher Cieri, Mike Maxwell, Stephanie Strassel, and Jennifer Tracey. 2016. "Selection criteria for low resource language programs.", In *Proceedings of the Tenth International Conference on Language Resources and Evaluation (LREC'16)*, pages 4543-4549.
- [32] Yulia Tsvetkov. 2017, "Opportunities and challenges in working with low-resource languages". Carnegie Mellon University.
- [33] Simpson, Heather, Christopher Cieri, Kazuaki Maeda, Kathryn Baker, Boyan Onyshkevych. 2008. *Human Language Technology Resources for Less Commonly Taught Languages: Lessons Learned Toward Creation of Basic Language Resources*, paper presented at the SALTML Workshop: Free/Open-Source Language Resources for the Machine Translation of Less Resourced Languages satellite to the 7th International Conference on Language Resources and Evaluation, Marrakesh, May 28-30.
- [34] Vamshi KG Reddy, Pratibha Rani, Vikram Pudi, and Dipti M. Sharma. "Decision tree ensemble for parts-of-speech tagging of resource-poor languages", In *Proceedings of the 10th annual meeting of the Forum for Information Retrieval Evaluation*, pp. 41-47. 2018.
- [35] Elaheh Sadredini, Deyuan Guo, Chunkun Bo, Reza Rahimi, Kevin Skadron, and Hongning Wang. "A scalable solution for rule-based part-of-speech tagging on novel hardware accelerators." In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining*, pp. 665-674. 2018.
- [36] Peter F Brown, Peter V Desouza, Robert L Mercer, Vincent J Della Pietra, and Jenifer C Lai. 1992. *Class-based n-gram models of natural language*. *Computational linguistics*, 18(4):467-479.
- [37] Jan Buys and Jan A Botha. 2016. "Cross-lingual morphological tagging for low-resource languages", *arXiv preprint arXiv:1606.04279*.
- [38] Ronald Cardenas, Ying Lin, Heng Ji, and Jonathan May. 2019. A grounded unsupervised universal part-of-speech tagger for low-resource languages. *arXiv preprint arXiv:1904.05426*.
- [39] Othman Zennaki, Nasredine Semmar, and Laurent Besacier. 2015. Utilisation des réseaux de neurones récurrents pour la projection interlingue d' étiquettes morpho-syntaxiques a partir d'un corpus parallèle. *TALN 2015*.
- [40] Oliver Adams, Adam Makarucha, Graham Neubig, Steven Bird, and Trevor Cohn. 2017, "Cross-lingual word embeddings for low-resource language modeling", In *Proceedings of the 15th Conference of the European Chapter of the Association for Computational Linguistics: Volume 1, Long Papers*, pages 937-947.
- [41] Surjya Kanta Daimary & Vishal Goyal & Madhumita Barbor & Umrinderpal Singh, "Development of Part of Speech Tagger for Assamese Using HMM," *International Journal of Synthetic Emotions (IJSE)*, IGI Global, vol. 9(1), pages 23-32, January. (2018).
- [42] A. K. Barman, J. Sarmah and S. K. Sarma, "POS Tagging of Assamese Language and Performance Analysis of CRF++ and fnTBL Approaches," *UKSim 15th International Conference on Computer Modelling and Simulation*, 2013, pp. 476-479, doi: 10.1109/UKSim.2013.91.
- [43] S Navanath Saharia, Dhrubajyoti Das, Utpal Sharma, and Jugal Kalita. 2009. Part of speech tagger for Assamese text. In *Proceedings of the ACL-IJCNLP 2009 Conference Short Papers (ACLShort '09)*. Association for Computational Linguistics, USA, 33-36.
- [44] D. Baishya and R. Baruah, "Improving Hidden Markov Model for very low resource languages: An analysis for Assamese parts of speech tagging," *2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence)*, 2021, pp. 142-146, doi: 10.1109/Confluence51648.2021.9377146.
- [45] D. Baishya and P. K. Das, "Improving windows tasks recognizer for Assamese using bigram analysis," *2014 International Conference on Audio, Language and Image Processing*, 2014, pp. 470-475, doi: 10.1109/ICALIP.2014.7009838.
- [46] D. Baishya, R. Baruah and A. Neog, "Present state and future scope of Assamese text processing," *2021 International Conference on Computer Communication and Informatics (ICCCI)*, 2021, pp. 1-6, doi: 10.1109/ICCCI50826.2021.9402617.
- [47] Imad Zeroual, Abdelhak Lakhouaja, Rachid Belahbib "Towards a standard Part of Speech tagset for the Arabic language", *Journal of King Saud University-Computer and Information Sciences*, vol. 29, pp 171-178, 2017.
- [48] V. Pirrelli and A. Zarghili, "Arabic Natural Language Processing: Models systems and applications", *Journal of King Saud University-Computer and Information Sciences*, vol. 29, pp. A1-A3, 2017.
- [49] L. Qin, POS tagging of Chinese Buddhist texts using Recurrent Neural Networks, report, 2015.

- [50] Plank, A. Søgaard and Y. Goldberg, Multilingual part-of-speech tagging with bidirectional long short-term memory models and auxiliary loss, arXiv:1604.05529, 2016.
- [51] C. D. Santos and B. Zadrozny, Learning character-level representations for part-of-speech tagging, in: Proceedings of the 31st International Conference on Machine Learning (ICML-14), pp. 1818–1826, 2014.
- [52] G. Chrupala, Text segmentation with character-level text embeddings, in: Proceedings of the ICML Workshop on Deep Learning for Audio, Speech and Language Processing, 2013.
- [53] Y. Kim, Y. Jernite, D. Sontag and A. M. Rush, ,”Character-Aware Neural Language Models”,arXiv:1508.06615,2015.
- [54] Sangkeun Jung, Changki Lee, and Hyunsun Hwang. 2018. End-to-End Korean Part-of-Speech Tagging Using Copying Mechanism. ACM Trans. Asian Low-Resour. Lang. Inf. Process. 17, 3, Article 19 (May 2018), 8 pages. DOI:<https://doi.org/10.1145/3178458>.
- [55] Prakhar Srivastava, Kushal Chauhan, Deepanshu Aggarwal, Anupam Shukla, Joydip Dhar, and Vrashabh Prasad Jain, “Deep Learning Based Unsupervised POS Tagging for Sanskrit” In Proceedings of the 2018 International Conference on Algorithms, Computing and Artificial Intelligence (ACAI 2018). Association for Computing Machinery, New York, NY, USA, Article 56, 1–6. DOI:<https://doi.org/10.1145/3302425.3302487>.
- [56] G. Prabha, P. V. Jyothisna, K. K. Shahina, B. Premjith and K. P. Soman, "A Deep Learning Approach for Part-of-Speech Tagging in Nepali Language," 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018, pp. 1132-1136, doi: 10.1109/ICACCI.2018.8554812.
- [57] Collobert, R., Weston, J., Bottou, L., Karlen, M., Kavukcuoglu, K., and Kuksa, P. Natural language processing (almost) from scratch. Journal of Machine Learning Research, 12:2493–2537, 2011.
- [58] Dos Santos, Cicero & Zadrozny, Bianca. (2014). Learning Character-level Representations for Part-of-Speech Tagging. 31st International Conference on Machine Learning, ICML 2014.
- [59] Verwimp, Lyan & Pelemans, Joris & Van hamme, Hugo & Wambacq, Patrick. (2017). Character-Word LSTM Language Models. 10.18653/v1/E17-1040.
- [60] Francis, W. Nelson & Henry Kucera. 1967. Computational Analysis of Present-Day American English. Providence, RI: Brown University Press.

# Critical Success Factors Associated to Tourism e-Commerce: Study of Peruvian Tourism Operators

Sussy Bayona-Oré<sup>1</sup>

Universidad Autónoma del Perú, Panamericana Sur Km.  
16.3, Villa el Salvador, Lima-Perú

Romy Estrada<sup>2</sup>

Universidad San Martín de Porres, Av. La Fontana 1250.  
Urb. Santa Patricia, La Molina, Lima-Perú

**Abstract**—The incorporation of information and communication technologies (ICT) has generated new opportunities and innovation in business models, such as electronic commerce (EC). Despite the benefits that the EC offers PYMEs, its adoption is low. Several authors have argued that many factors condition the adoption of EC in developing countries. This study proposes a model of factors associated with the adoption of EC by tourism operators based on factors categorized into organizational, individual, environmental, and technological factors. In this study, a structural equation modeling and confirmatory factor analysis tools were used to analyze the data. The data collected from 116 participants (69% males and 31% females, managers of tourism operators). The results reveal that 11 factors influence the adoption of EC. Also, the operators currently using EC consider that the most influential factor are related with organizational factors operators that have not implement EC value factors involving skills, knowledge and experience in technology. This study can be used to establish policies on ICT adoption in tourism PYMEs.

**Keywords**—Adoption; e-commerce; tourism operators; PYMEs; critical factors; TOE

## I. INTRODUCTION

The tourism sector is an emerging sector that has recently experienced diversification. Tourism is key to countries' economies, contributing to job creation [1], and is one of the premier export industries in developing countries [2]. The tourism sector plays the role of a catalyst for innovation and entrepreneurship and contributes to improving the lives of millions of people and transforming entire communities [3].

Information and communication technologies (ICTs) and the expansion of the internet have generated new opportunities and innovation in business models, changing the business structure and creating new ways of doing things. Likewise, the benefits of ICT in improving efficiency, reducing costs, and increasing productivity in organizations have been recognized. One of the sectors affected by ICT is the tourism sector, which has adopted new technologies with a growing trend in the future. This sector has remained at the forefront of the digital transformation due to the changes in how the sector operates and people travel [4]. Tourism in Peru is the third-largest industry behind fishing and mining.

A technology that has been used and is becoming more critical is electronic commerce (EC) [5], which is used in several sectors, such as the tourism sector. PYMEs in the tourism sector are not oblivious to these changes and are recognized as providers of job opportunities [6]. Despite the

benefits of ICTs, such as reduced costs per transaction, increased speed, and operational efficiency, not all PYMEs have incorporated EC. Although the global turnover of EC continued to grow steadily by about 11% in 2019, in the case of Latin America, it constitutes only 2% [7]. Moreover, EC has grown almost 15 times in revenue since 2009 [8].

In the tourism sector, EC is conducted in tourism-related activities using ICT tools by tourism organizations [9]. In developing countries, EC adoption in PYMEs is below that of large enterprises [10, 11]. One aspect that hinders adoption is that most PYMEs do not know how information technology (IT) can benefit their businesses and support them in achieving their goals; therefore, they do not invest in EC [12]. Some countries lag in adopting ICT due to poor economies, lack of infrastructure, and an unskilled workforce [9].

The process of ICT adoption has been studied by several authors [6, 13]. Some factors have been mentioned as enablers of EC in tourism PYMEs: pressure from external agents, perceived usefulness, perceived ease of use, technological readiness, ICT skills of employees, organizational readiness, management capacity, and government support, among others. Tourism is an activity that energizes the Peruvian economy, so it is essential to study how tourism PYMEs adopt EC.

The main contribution of this paper is determining the critical success factors positively associated with the EC adoption according to the perception of tour operations managers. With the recent events of the coronavirus disease 2019 (COVID-19) pandemic, an opportunity has been created for tour operators to reassess the business model. The general challenges for the tourism sector are innovating and digitizing as many activities as possible (i.e., organizations must invest in digital transformation to improve the management and planning of tourism destinations) [1].

Once the critical enabling factors of EC are known, an adoption model adapted from the technology and organizational environment (TOE) framework is proposed.

The managers of PYMEs, researchers and tourism institutions can benefit from the findings of this research.

The article is structured into five sections, including the introduction. Section II presents a comprehensive background and research hypotheses. Section III presents the material and methods. Section IV describes the results. Section V presents the discussion of the results and suggests future studies. Finally, in Section VI, the conclusions are presented.

## II. LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

This study aims to determine which factors, based on the literature review, are positively associated with the adoption of EC from the tour operator manager’s viewpoint and to increase understanding of the topic. Tourism is a sector that energizes the economy through creating jobs, for which ICT can be a strategic ally, especially for PYMEs dedicated to tourism. With the COVID-19 pandemic, new challenges have arisen for these companies, such as reassessing the business model and innovating and digitizing activities, which many PYMEs have not considered.

### A. Technology, Organizational and Environment

The Technology Acceptance Model (TAM) and Technology Organization Environment (TOE) framework can be used to measure the adoption of a technology in organizations. The TOE framework was developed by Tornatzky and Fleischer [14]. This framework describes the influence of contextual factors in adopting an innovation. Three aspects of the context of an enterprise influence the adoption of technological innovations: technological context, organizational context, and environmental context [10].

Technological context is related to technologies in the organization (internal) and those available for adoption that are not used by the organization (external). In the adoption process the technology existing in the organization is important because is related to technological change. One of the factors that affect the use of technology is usability.

Organizational context refers to the nature and resources of the organization, specifically its size, decentralization, formalization, management-structure complexity, and human resources. Environmental context refers to the aspects surrounding the organization, such as competitors and suppliers and the relationship with government entities.

This framework was adapted considering the factors identified in the literature, such as perceived utility, ease of use, and managerial skills, among others, and a new context called individual was added. Individual context refers to aspects related to people, skills, knowledge, and experience. Thus, it is possible to understand how these determinants can influence the adoption of ICT from the context of the adapted TOE framework. The following section reviews studies related to technology adoption factors.

### B. Critical Factors in the Adoption of EC

ICT play a vital role in developing the tourism sector and positive contribution to sustainable development [15]. Despite the rapid growth in the number of travelers using technology, challenges to adopting technology exist in all tourism segments. Several factors condition the adoption of EC. In a previous study [16], the systematic review method was used to determine the critical success factors for EC adoption.

The summary of the identified, prioritized, and categorized factors in this study is presented in Table I. The first column of Table I presents the categories, and the second column presents the factors that correspond to each of the identified categories. The factors in the Table I were presented with a frequency greater than two. Among the factors are the expansion of the

internet in society, positioning, distributed product types, perceived risks, subjective norms, perceived needs, socio-cultural practices of sharing information among PYMEs, and the e-readiness of government and socio-cultural practices.

TABLE I. CATEGORIES AND CRITICAL FACTORS

Category	Critical Factors
Technology (FT)	EC is perceived as useful in the business (FT1), perceived cost of e-commerce implementation (FT2), perceived ease of use (FT3), and perceived security and reliability of payment methods (FT4)
Organizational (FO)	Organizational readiness (FO1), technological readiness (FO2), and management capability (FO3)
Environmental (FA)	Customer pressure (FA1), stakeholders demand for EC (FA2), government support (FA3), access to quality information technology services and infrastructure (FA4), and expansion of the internet in society (FA5)
Individual (FI)	Employee information technology skills, knowledge, and experience (FI1), employee attitudes toward using information technology (FI2), manager information technology skills, knowledge, and experience (FI3), and manager's attitude toward using information technology (FI4)

Factors mentioned by previous authors include whether the company staff have previously used ICT, the national policies that support EC, the size of the business, the maturity level in implementing ICT in organizations, technological resources for the EC implementation process, the external pressure or the possibility of external assistance (advice and support) to implement EC platforms [17].

According to Dahbi and Benmoussa [18], the categories that group the factors are organizational, technological, cultural, financial, and external (called environmental in other studies). Among the organizational factors, management support and the perceived need for EC are mentioned.

The mentioned technological factors are employee ICT knowledge, client confidence in technology, client confidence in transactions, and client knowledge of technology. Among the cultural factors, some authors have mentioned the attitude toward changes in conducting business, the need for human contact, and the need to feel/touch the product. Financial factors include implementation costs, logistics costs, financial resources, and price transparency. External factors include government support, customs regulations, and pressure from competitors, customers, and suppliers.

The technological factors most mentioned in the literature review were perceived utility, perceived ease of use, perceived cost of EC implementation, perceived ease of use, and perceived security and reliability of payment methods. The organizational factors were perceived organizational readiness, perceived technological readiness of the enterprise, and perceived management capability of the enterprise.

The environmental factors were customer perception for successful adoption of EC, perception of pressure from business partners, suppliers, and competitors for EC implementation, perception of government support for EC implementation, perception of access to quality ICT services and infrastructure, and perception of the expansion of the internet in society. The individual factors are the perception of

the employee and manager's ICT skills, knowledge, experience, and attitudes toward ICT use and the manager's education level.

### C. Technological Factors

Due to challenges related to ICT infrastructure and services, the percentage of ICT use is not equally distributed in large cities and the country's interior. In addition, ICT is fundamental to the expansion of EC. In this regard, Carvalho and Mamede [19] found that the infrastructure cost factor contributes positively to adopting ICT, which is in line with their findings [18]. As new technologies emerge, an essential aspect for EC is the confidence that online transactions and payments are secure.

Iddris [20] mentioned that EC security and the initial cost of EC negatively influence the adoption of EC by PYMEs. In contrast, AlGhamdi et al. [21] noted that the reliability and security of online payment options positively influence the adoption of EC. The perceived cost of implementation is considered a contributing factor to EC adoption. From the researcher's viewpoint, the security of a transaction is a barrier in the case of security problems. Taylor and Eshun [22] indicated that, although EC is perceived to have benefits, as identified by Shaharudin et al. [23], online payment processes and pricing structures influence the adoption of EC by PYMEs.

Perceived useful in the business has been mentioned in several studies as a factor related to EC adoption [24, 25]. Several authors have mentioned perceived usability as a contributing factor in EC adoption [23, 24, 25, 26].

For Ochola [27], the characteristic factors of innovation complexity and relative advantages have a significantly positive effect on adopting EC by PYMEs. Other factors, such as innovation and perceived benefits, have been mentioned in the studies. Le et al. [28] found that innovation compatibility, innovation complexity, and perceived risks influence the adoption of EC by PYMEs in Vietnam. Shaharudin et al. [23], Rahayu and Day [10], and Syah et al. [26] found a positive relationship between the perceived benefits and EC adoption by PYMEs. Al-Alawi and Al-Ali [12] indicated that the perceived benefit factor is positively related to the adoption of EC by PYMEs. Based on the identified constructs, the following hypothesis was proposed.

Hypothesis 1 (H1): Technology factors (FT) are positively associated with EC adoption.

### D. Organizational Factors

Abbasi et al. [24] found that the company's innovative character has a significantly positive effect on EC adoption. One factor is organizational readiness, which positively correlates with EC adoption [19, 25, 26, 29]. Walker, Saffu, and Mazurek [30] found that organizational readiness and decision-making were important in discerning EC adoption. Kenneth et al. [31] noted that infrastructure and competition significantly influence the adoption of EC by Kenyan tourism PYMEs.

Villa et al. [17] identified factors related to the adoption of the EC, such as ICT and the level of maturity and the resources for the EC implementation process. Rahayu and Day [10]

found that the technological readiness factor is a determinant for adopting ICT in PYMEs in Indonesia. Ochola [27] noted that the company's seniority factor has a significant positive effect on the adoption of EC by PYMEs in Kenya. Lama, Pradhan, and Shrestha [9] concluded that barriers to adopting EC include a lack of adequate infrastructure and resources. Frasquet et al. [32] argued that the organization's size is a critical factor, and Villa et al. [17] related the size of the business to the adoption of EC.

Kenneth et al. [31] found that the factors with a significant influence on the adoption of EC by PYMEs in the Kenyan tourism sector are leadership style and positioning. Iddris [20] proposed that factors with a negative influence on the adoption of EC by PYMEs in Ghana include management culture and interest. Al-Alawi and Al-Ali [12] argued that the support factor of senior management is positively related to the adoption of EC by PYMEs in Kuwait. Chee et al. [33] stated that the senior management support factor is significantly related to adopting EC by PYMEs. Lama, Pradhan, and Shrestha [34] concluded that the key drivers include awareness, value proposition, and the role of the owner or senior management.

Dahbi and Benmoussa [18] agreed with the previous authors and mentioned logistics and financial resources as critical factors for adoption, as did Kenneth et al. [31], who supported that resources [28] influence adopting EC. Taylor and Eshun [22] indicated that company resources influence the adoption of EC. Based on the identified constructs, the following hypothesis was formed.

Hypothesis 2 (H2): Organizational factors (FO) are positively associated with EC adoption.

### A. Environmental Factors

Saffu et al. [25] indicated that the external pressure factor (competitors, buyers, business partners, and suppliers) is related to the adoption of EC by PYMEs in Slovakia, whereas Shaharudin et al. [23] found that the factor influencing EC adoption by PYMEs is external pressure from customers. Chee et al. [33] noted that pressure factors from competitors influence SME adoption of EC, whereas Shaharudin et al. [23] suggested it is pressure from competitors, business partners, and suppliers.

Lama, Pradhan, and Shrestha [34] concluded that market strength is among the key motivators. For Carvalho and Mamede [19], the business partner factor contributes positively to adopting EC. Matsinhe and Kabanda [6] argued that such aspects as international market strength condition the adoption of EC. Syah et al. [26] found a positive relationship between external pressure (partners, competitors, customers and suppliers) and the adoption of EC by PYMEs. Frasquet et al. [32] supported that EC adoption by retailers in Spain, the UK, and France is influenced by such factors as the competitive environment. Le et al. [28] found that the intensity of competition, industry support, supplier behavior, buyer behavior, and government support influence EC adoption by PYMEs in Vietnam. Walker, Saffu and Mazurek [30] noted that operational support and external pressure were vital in discerning EC adoption.

Dahbi and Benmoussa [18] mentioned external factors, such as government support, customs regulations, and pressure from competitors, customers, and suppliers. Al-Alawi and Al-Ali [12] proposed the factor of government regulations. Villa et al. [17] identified factors related to the adoption of EC, including national policies that support EC, external pressure to be part of this commerce type, and the possibility of external assistance (advice and support) to implement EC platforms.

Taylor and Eshun [22] indicated that IT service providers, online banking service availability, energy service reliability, and industry competition influence the adoption of EC by Ghanaian PYMEs. Ardjouman [35] identified that infrastructure and maintenance factors, such as limited internet access and limited and unreliable power sources, negatively affect adopting EC by PYMEs in Côte d'Ivoire. For AlGhamdi et al. [21], the factors include government support and assistance in EC and developing a strong ICT infrastructure. AlGhamdi et al. [21] also found that developing a strong ICT infrastructure is an enabler for the adoption of EC. Al-Alawi and Al-Ali [12] proposed that the government regulatory factor is positively related to the adoption of EC by PYMEs in Kuwait. Based on the identified constructs, the following hypothesis was formed.

Hypothesis 3 (H3): Environmental factors (FA) are positively associated with EC adoption.

#### E. Individual Factors

Abbasi et al. [24] proposed that the subjective standards variable significantly affects EC adoption by PYMEs in Iran. Le et al. [28] found that the factors of employee knowledge of EC and the manager's attitude toward innovation influence the adoption of EC by PYMEs. Iddris [20] noted that the factors that negatively influence the adoption of EC by PYMEs are the lack of technical skills of employees and the resistance of people. Hajli et al. [29] suggested that the EC awareness factor positively correlates with EC adoption by PYMEs in Iran. Taylor and Eshun [22] indicated that such factors as skilled personnel in EC solutions and company resources influence the adoption of EC by Ghanaian PYMEs.

Carvalho and Mamede [19] noted that managers' perception of the return on investment contributes positively to EC adoption. Ardjouman [35] identified that employee technical skills are related to the adoption of EC. Ochola [27] noted that employee IT skills and education level significantly positively affect adopting EC by PYMEs in Kenya. Villa et al. [17] identified the previous use of ICTs by company staff as a factor related to adopting EC. Carvalho and Mamede [19] found that human resources contribute positively to EC adoption.

Rahayu and Day [10] argued that the innovation, IT capacity, and IT experience of the owner/manager are determinants for adopting EC in PYMEs in Indonesia. Matsinhe and Kabanda [6] determined that the characteristics of the manager, previous experience in EC, and sharing of experiences condition the adoption of EC. Based on the identified constructs, the following hypothesis was formed. Table II presents the proposed hypotheses.

Hypothesis 4 (H4): Individual factors (FI) are positively associated with EC adoption.

TABLE II. PROPOSED HYPOTHESIS

Hypothesis	Factors	Association*
H1	Technological factors are positively associated with EC adoption	(H1: FT → IMP)
H2	Organizational factors are positively associated with EC adoption	(H2: FO → IMP)
H3	Environmental factors are positively associated with EC adoption	(H3: FA → IMP)
H4	Individual factors are positively associated with EC adoption	(H4: FI → IMP)

Based on the research conducted in the literature review and the proposed hypotheses, the association between critical success factors and EC adoption for tourism operators is represented in Fig. 1.

### III. MATERIALS AND METHODS

The details regarding the research method, data collection, the instrument used, the pilot study, the study sample and demographic data are presented in this section.

#### A. Research Method

In this research, factors associated with EC adoption are analyzed using the quantitative research method to measure the variables. The research is transversal because the data were collected at a single moment. The study population comprises 2,692 managers of tourism operations located in various regions in Peru. A nonprobabilistic sample was applied. In total, 116 managers of tourism operations (31% male and 69% female) from different cities in Peru were asked to complete a questionnaire.

#### B. Data Collection

A questionnaire was designed as a data collection instrument. The questionnaire had two sections: sociodemographics and questions on each factor. Moreover, 10 and 16 items were evaluated to measure the qualifying factors for adopting the EC in tourism PYMEs. All items for this study were rated on a five-point Likert scale from 1 (strongly disagree) to 5 (strongly agree). The instrument was subjected to a validity check using a pilot test with four operator managers from outside the selected sample to check the validity and reliability of the instrument. A total of 116 questionnaires were distributed to the managers of tourism operations who completed and returned them. Table III lists the items on the questionnaire.

#### C. Data Analysis

The proposed model and hypotheses were tested using SEM (Structural Equation Modeling). The IBM SPSS Amos 22 tools were applied to analyze the data. Concerning SEM this study confirmed the prerequisites for item parceling. Cronbach's alpha was used to determine the internal consistency.

D. Structural Model

Based on the research conducted in the literature review and the proposed hypotheses, the association between critical success factors and EC adoption for tourism operators is represented in Fig. 1 as a causal diagram. Fig. 1 illustrates the causal diagram of the assessment of qualifying factors for adopting EC in tourism PYMEs. The variables are technological factors (FT), organizational factors (FO),

environmental factors (FA), and individual factors (FI). One variable adoption is EC (IMP).

The conceptual model presents 16 critical success factors organized in four categories (Table I). Cronbach’s alpha was used to assess the internal consistency of the factors. A Cronbach’s alpha value greater than 0.70 is recommended for confirmatory research [36]. Table IV lists the statistics of all elements of the model.

TABLE III. VARIABLES OF THE INSTRUMENT

Module	Items
Sociodemographics	Age, gender, and location
Technological factors	EC is useful, implementation cost and maintenance are affordable, EC is easy to use, payment method is secure and trustworthy
Organizational factors	Functions and processes are understood, information management is automated, company management capacity
Environmental factors	Customer demand the implementation of EC, stakeholders demand the implementation of EC, government support, services, and infrastructure are accessible, internet access.
Individual factors	Employees have knowledge, skills, abilities, and employees have a positive attitude,
E-commerce	EC implementation

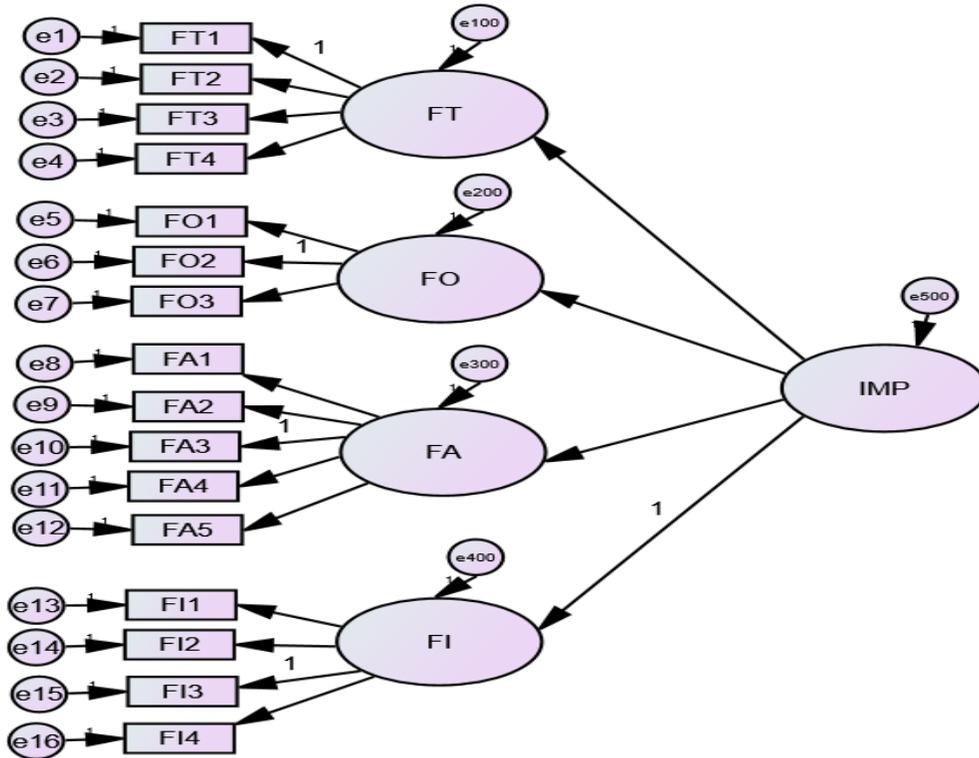


Fig. 1. Causal Diagram.

TABLE IV. STATISTICS OF ALL ELEMENTS

Factor	Scale average if the element is deleted	Scale variation if the element is deleted	Total correlation of elements corrected	Multiple square correlation	Cronbach's Alpha if the element is deleted
FT Technological Factors					
FT1	10.90	6.67	0.57	0.34	0.78
FT2	11.68	6.74	0.61	0.39	0.76
FT3	11.44	6.44	0.69	0.48	0.72
FT4	11.55	7.15	0.61	0.38	0.76
FO Organizational Factors					
FO1	8.31	4.22	0.78	0.61	0.84
FO2	8.10	3.78	0.77	0.59	0.85
FO3	8.05	4.07	0.80	0.64	0.82
FA Environmental Factors					
FA1	13.42	5.69	0.49	0.49	0.41
FA2	13.46	6.02	0.60	0.52	0.37
FA3	14.66	8.19	0.03	0.12	0.69
FA4	13.53	7.21	0.43	0.29	0.48
FA5	12.83	7.36	0.23	0.32	0.57
FI Individual Factors					
FI1	13.01	6.36	0.81	0.77	0.90
FI2	13.01	6.43	0.82	0.78	0.89
FI3	12.94	6.14	0.78	0.72	0.91
FI4	12.84	5.96	0.85	0.78	0.88

#### IV. RESULTS

##### A. Participants Demographics

Table V provides the demographics of the sample, including education and the use of EC. Regarding the characteristics of the respondents, 31% of the respondents were male, and 69% of the respondents were female. The majority of the managers (63.7%) were over 37 years old, and 21.6% were in the age group of 33 to 37 years old. In addition, 27.6% of the respondents have considered implementing EC at some point, 25% have decided to implement EC, and 41.4% are currently using EC.

##### B. Structural Model and Hypothesis Testing

When observing the reliability analysis results, environmental factors are qualified as questionable; therefore, were analyzed the answers collected on those factors through a frequency analysis. More than one-third of the interviewees answered “neither agree nor disagree” on the frequency analysis, which affects the overall analysis. In this sense, these factors should be excluded from the analysis.

Validation steps were followed before validating the proposed theoretical model using the SEM technique of the AMOS SPSS software and analyzing the measurement estimates of the observed variables. As a first step, the confirmatory factor analysis validates the factor composition (constructs) to identify which indicators (observed variables) load to establish the number of factors and their intercorrelations. The second step was to convergent validity.

- The validation of the convergence of items and constructs refers to the fact that a variable measure what

it is supposed to measure. The erroneous assignment of latent variables to certain observed variables produces validity problems. Two conditions exist for the validity of an observed variable. First, the observed and latent variables must have a direct relationship with each other. Second, the latent factors excluded from the model must not directly affect the observed variable. The indices of convergent validity are greater than 0.70, and the average of the extracted variance (AVE) is greater than or equal to 0.50 (see Table VI).

- The validation of the hypotheses through a causality analysis determines whether the structural model is correct and approximates the actual phenomenon. The goodness-of-fit statistics, which refer to the accuracy of the assumptions of the specified model were analysed. Considerations for the evaluation of the SEM of the research include the following: (1) due to the small sample (116 surveys), the procedure for estimating the model was the maximum likelihood and (2) the multivariate distribution of the statistics used in the model is assumed to be normal. Table VI presents the results of the model estimation.

From the results in Table VI, causal Model 2 is observed, where the factor loads of the items are greater than or equal to 0.70 (factor loading or standardized regression weights  $\geq 0.70$ ), and the mean variances extracted (AVE) are greater than or equal to the recommended value of 0.50. Thus, the conformation of factors fulfills the criteria of convergent validity. The indices of adjustment of causal Model 2 are acceptable. Table VII lists the model fit indices.

TABLE V. FREQUENCY ANALYSIS

Characteristics		N	Percent
Gender	Female	80	69.0%
	Male	36	31.0%
Age	Over 37	74	63.8%
	33–37	25	21.6%
	28–32	9	7.8%
	23–27	7	6.0%
	< 23	1	0.9%
Manager education	University superior	83	71.6%
	Technical superior	30	25.9%
	High school	3	2.6%
Use EC	Don't know EC	3	2.6%
	Implementing EC has not been considered	4	3.4%
	Implementing EC has been considered at some time	32	27.6%
	Implementing EC has been decided	29	25.0%
	Currently using EC	48	41.4%

Source: Research data; N: Number; EC: e-commerce

TABLE VI. MODEL ESTIMATION

Factors	Variables	Causal Model 1			Causal Model 2		
		Factor Loading *	Loading Squared	AVE	Factor Loading *	Loading Squared	AVE
Technological Factors (FT)	FT1	0.75	0.57	0.51	0.76	0.58	0.51
	FT2	0.65	0.42				
	FT3	0.77	0.60		0.74	0.55	
	FT4	0.67	0.44		0.64	0.41	
Organizational Factors (FO)	FO1	0.83	0.69	0.73	0.82	0.68	0.72
	FO2	0.83	0.69		0.83	0.68	
	FO3	0.90	0.80		0.90	0.81	
Environmental Factors (FA)	FA1	0.88	0.77	0.70	0.89	0.79	0.70
	FA2	0.79	0.63		0.78	0.61	
	FA3						
	FA4						
	FA5						
Individual Factors (FI)	FI1	0.87	0.75	0.7	0.91	0.84	0.8
	FI2	0.88	0.77		0.94	0.88	
	FI3	0.82	0.68				
	FI4	0.88	0.78		0.80	0.63	

\* Standardized regression weights

TABLE VII. MODEL FIT INDICES

Fit Indices	Acceptable Fit	Causal Model 1		Causal Model 2	
		Indices	Fit situations	Indices	Fit situations
Chi-square	>1 and < 5	2.52	Acceptable	1.73	Acceptable
Goodness-of-fit index	≥ 0.8	0.82	Acceptable	0.90	Acceptable
Comparative fit index	≥ 0.9	0.91	Acceptable	0.96	Acceptable
Root mean square error of approximation	≤ 0.08	0.12	Not Acceptable	0.08	Acceptable

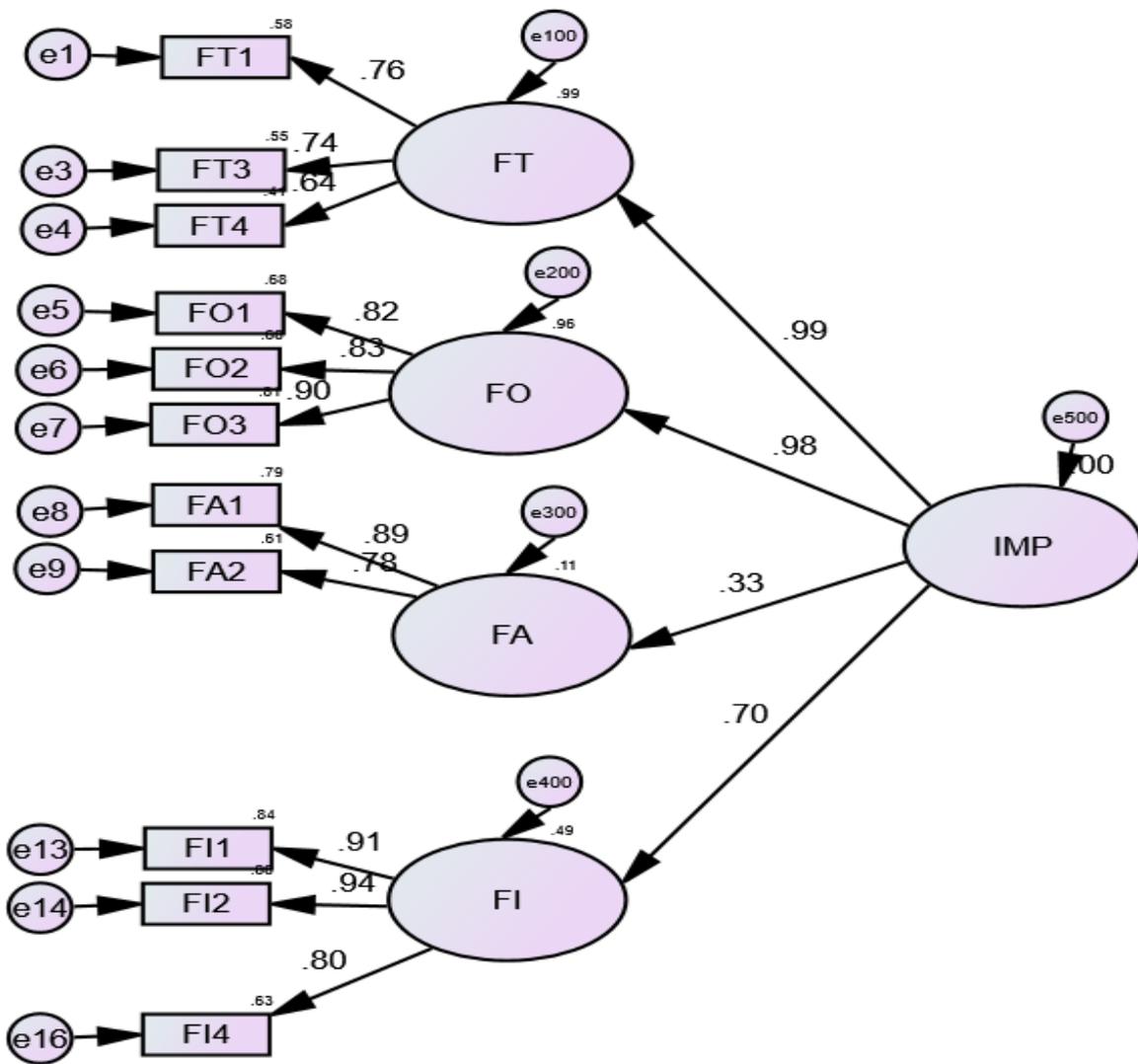


Fig. 2. Assessment of Qualifying Factors for e-commerce Adoption.

TABLE VIII. RESULTS OF HYPOTHESIS TESTING

Hypotheses	Factors	Association
H1	Technological factors are positively associated with EC adoption	33.0%
H2	Organizational factors are positively associated with EC adoption	32.7%
H3	Environmental factors are positively associated with EC adoption	11.1%
H4	Individual factors are positively associated with EC adoption	23.2%

Notes: EC: e-commerce.

According to the general modeling in structural equations regarding the qualifying factors for adopting EC in tourism operators, the most influential factors are the technological and organizational factors. Fig. 2 presents the final causal model on the evaluation of the qualifying factors for adopting EC.

Table VIII presents the results of the hypotheses.

The following observations were made when analyzing groups according to the company situation where the interviewees work concerning adopting EC:

- Group 1: Tourism operators currently using EC consider that the most influential factor is the organizational factor, mainly information management in the company.
- Group 2: Tourism operators that have not yet implemented EC equally value factors involving skills, knowledge, and experience in technology and the technological and organizational factors of the company.

## V. DISCUSSION AND FUTURE STUDIES

In a context of pandemic COVID-19 the adoption of ICT, in special EC has been recognized a key factor to give continuity with business activities due to social isolation, distancing and border closures. Also, the research on adopting ICTs has a great interest, especially business. EC is a very potent strategy to beat competitors and generate profits. Despite the benefits of the adoption of EC, the adoption of EC by SEM is low. The reasons, factors or determinants have been amply documented in the literature and several explanations such as organizational factors, environmental factors, technological factors and individual factors are mentioned. The studies corresponding to different countries and not evidences have been founded about impact of factors in the EC in Peruvian tourism operators. In this study, a total of four hypotheses were tested.

Accordingly, the results the technological factors were positively associated with EC adoption. EC is perceived useful in the business, and perceived ease of use. Are two constructs of ICT models adoption. An Information System that presents difficulties in their use discourages its use. Perceived usefulness is related to use of technology enhance the job performance and Perceived ease of use is related effort necessary to use of technology. Then individuals will be more willing to adopt EC if it is easy of use. Perceived ease of use is consistent with the studies by Ochola [27] and Syah et al. [26]. The perceived security and reliability factor, related to secure and reliable payment methods, was also consistent with the research by Ochola [27]. Today, the development of technologies and components for the EC encourages tourism operation managers to trust it and naturally adopt ICT. Specifically, if the managers of tourism operators believe that the method of payment used and the transactions are secure then they are more likely to support the adoption of EC. Technological factors were founded as influencing factors for EC.

Organizational factors are positively associated with the adoption of EC. Organizational factors include organizational readiness with clearly understood functions and processes, technological readiness due to automated information management, and management capability that enables change. Organizational readiness is related to EC adoption, which is consistent with the research by Syah et al. [26]. Only organizational readiness is associated with EC adoption. Tour operation managers may consider EC adoption the necessary next step for their businesses to grow and evolve.

Environmental factors are positively associated with EC adoption. In this case, only two out of five factors were considered: customer and stakeholders demand for EC. In the pandemic, these two environmental factors have a more significant influence, considering the immobilization in some cases and the distance and sanitary measures required by regulatory organizations. In this regard, customer pressure is a factor highlighted in the research by Syah et al. [26], Saffu et al. [25], Le et al. [28] and Sánchez-Torres et al. [37]. The fact that pressure from customers and external agents is correlated with EC adoption indicates that tour operator customers, suppliers, competitors, and business partners are increasingly

using electronic media in buying and selling transactions. This situation may increase the motivation of tour operation managers to adopt this technology to meet the need for immediacy in transactions with customers, suppliers, competitors, and business partners.

External pressure of stakeholders was related to EC adoption, which is consistent with the research by Syah et al. [26] and Saffu et al. [25]. The government support was not empirically validated which is consistent with other studies. Regulatory policies that are not clear and not significative for EC adoption could be a reason. Also, this result can be explained for the highest rates of entrepreneurship. The expansion of the internet in society is not related to the adoption of EC. This result can be explained due to internet is part of our lives and has been incorporated in the organizations.

Individual factors are positively associated with e-business adoption, such as employee ICT skills, knowledge, experience, and attitudes toward ICT use, and managers' attitudes toward ICT use. Furthermore, these factors could guarantee, to some extent, the success of the implementation of this technology and the design and execution of the processes. In PYMEs, the primary decision maker is the owner of the business [38] and top management support is statistically significant determinant of e-commerce adoption.

When comparing the manager group of tour operators that already has EC, the most influential factor is the organizational factor, mainly the information management of the company. In contrast, in groups that have not yet implemented EC, they equally value the skills, knowledge, and experience in technology and the technological and organizational factors.

This study provides an understanding of the factors considered by tour operators for adopting EC. A sample of 116 tour operators was used to conduct this study, which presents the limitation of the generalizability of the results. Although most departments were represented in the sample, further research is needed to assess factors faced during the COVID-19 pandemic. The study represents the characteristics of tour operators in Peru, so it is crucial to conduct empirical studies in other developing countries to generalize the findings. With the COVID-19 pandemic measures, such as closed airport and flight bans to prevent widespread infection, many tour operators were forced to suspend operations. Future work would include assessing the effect of COVID-19 on tour operators and adopting ICT to address new regulations.

## VI. CONCLUSION

For all kinds of organizations in different sectors, ICT has become a strategic ally. The tourism sector is considered a driving force in the economy. Despite the benefits offered by ICT, the incorporation into the tourism sector has been very slow. Several authors have argued that a set of factors influence adopting EC in tourism companies. The purpose of this research was to develop and propose a model for adopting ICT by tourism operators. The first task was to determine critical factors from the literature review and establish the identified and selected factors. The research was quantitative, with a sample of 116 tour operators surveyed using Google Forms. Confirmatory factor analysis was used to determine the

factors influencing ICT adoption. Technological, organizational, environmental, and individual factors are positively associated with the adoption of EC. Disseminating the results to tourism operators facilitates their understanding and the need to consider these factors to reinvent themselves. As future work, a plan to review the critical factors and their behavior concerning the changes due to COVID-19 through a longitudinal study to determine whether significant differences exist in the process of adopting ICT.

#### REFERENCES

- [1] UNWTO, International tourism highlights. <https://www.unwto.org/doi/epdf/10.18111/9789284422456>, 2020.
- [2] UNWTO, Tourism and the world economy, in the facts and figures. World Tourism Organization, 2016. <http://www.unwto.org/index.php>.
- [3] World Tourism Organization. Panorama del Turismo Internacional. Madrid, Spain, 2019.
- [4] S. Reinhold, F. Zach, and C. Laesser, E-business models in tourism. In Handbook of E-tourism, Xiang, Z., Fuchs, M., Gretzel, U., Höpken, W., Eds.; Springer, Cham, Switzerland, 2020, (pp. 1–30).
- [5] J. Habel, S. Alavi, and K. Linsenmayer, “From personal to online selling: How relational selling shapes salespeople’s promotion of e-commerce channels,” *J. Bus. Res.*, vol. 132, pp. 373–382, 2021.
- [6] F. Matsinhe, and S. Kabanda, E-commerce institutionalisation in Mozambique: Enablers and barriers. In ICT4D 2019, IIFIP AICT, Nielsen P.; Kimaro, H.C., Eds., 2019, Vol. 551, pp.140–151.
- [7] Ecommerce Foundation, Ecommerce Report Global 2019. Amsterdam, The Netherlands. Ecommerce, 2019.
- [8] CAPECE, Cámara Peruana de Comercio Electrónico; Reporte Oficial de la Industria Ecommerce en Perú. Crecimiento de Perú y Latinoamérica 2009-2019. Observatorio Ecommerce, 2019.
- [9] S. Lama, S. Pradhan, and A. Shrestha, “A. Exploration and implication of factors affecting e-tourism adoption in developing countries: A case of Nepal,” *Inf. Technol. Tourism*, vol. 22, pp. 5–32, 2020.
- [10] R. Rahayu, and J. Day, “Determinant factors of e-commerce adoption by SMEs in developing country: Evidence from Indonesia,” *Procedia - Soc. Behav. Sci.*, vol. 195, pp. 142–150, 2015.
- [11] H. Khan, and S. Uwemi, “What are e-commerce possible challenges in developing countries: A case study of Nigeria,” *Int. J. Bus. Syst. Res.*, vol. 12, no. 4, pp. 454–486, 2018.
- [12] A. Al-Alawi, and M. Al-AliF, “Factors affecting e-commerce adoption in SMEs in the GCC: An empirical study of Kuwait,” *Res. J. Inf. Technol.*, vol. 7, no. 1, pp. 1–21, 2015.
- [13] M. Aboelmaged, “Predicting e-readiness at firm-level: An analysis of technological, organizational and environmental (TOE) effects on e-maintenance readiness in manufacturing firms,” *Int. J. Inf. Manag.*, vol. 34, no. 5, pp. 639–651, 2014.
- [14] L. Tornatzky, M. Fleischer, and A. Chakrabarti, Processes of Technological Innovation. Lexington Books, 1990.
- [15] S. Gössling, “Tourism, technology and ICT: a critical review of affordances and concessions,” *Journal of Sustainable Tourism*, vol. 29, no. 5, pp. 733-750, 2021.
- [16] S. Bayona-Oré, and R. Estrada, “Critical Factors to Adoption of Electronic Commerce in Tourism SMEs,” *Revista Ibérica de Sistemas e Tecnologías de Informação*, vol. E28, pp. 961–971, 2020.
- [17] E. Villa, V. Valencia, and L. Ruiz, “Picón Electronic commerce: Factors involved in its adoption from a bibliometric analysis,” *J. Theoretical Appl. Electr. Comm. Res.*, vol. 13, no. 1, pp. 39–70, 2018.
- [18] S. Dahbi, and C. Benmoussa, “What hinder SMEs from adopting e-commerce? A multiple case analysis,” *Procedia Comput. Sci.*, vol. 158, pp. 811–818, 2019.
- [19] M. Carvalho, and H. Mamede, “The impact of e-commerce on the success of microenterprise retail sector of the Pinhal Interior Norte sub-region of Portugal. *Procedia Comput. Sci.*,” vol. 138, pp. 571–579, 2018.
- [20] F. Iddris, “Adoption of e-commerce solutions in small and medium-sized enterprises in Ghana,” *Eur. J. Bus. Manag.*, vol. 4, no. 10, pp. 48–57, 2012.
- [21] R. AlGhamdi, J. Nguyen, A. Nguyen, and S. Drew, “Factors influencing e-commerce adoption by retailers in Saudi Arabia: A quantitative analysis,” *Int. J. Electron. Comm. Stud.*, vol. 3, no. 1, pp. 83–100, 2012.
- [22] T. Taylor, and E. Eshun, “Factors affecting internet and e-commerce adoption among small and medium-sized enterprise non-traditional exporters: Case studies of Ghanaian handicraft exporters,” *Eur. J. Bus. Manag.*, vol. 4, no. 13, pp. 25–37, 2012.
- [23] M. Shaharudin, M. Omar, S. Elias, and M. Fadzil, “Determinants of electronic commerce adoption in Malaysian SMEs furniture industry,” *Afr. J. Bus. Manag.*, vol. 6, no. 10, pp. 3648–3661, 2012.
- [24] M. Abbasi, M. Sarlak, A. Ghorbani, and H. Esfanjani, “CSFs of e-commerce admission in small and medium size enterprises (SMEs),” *Afr. J. Bus. Manag.*, vol. 4, no. 16, pp. 3480–3490, 2010.
- [25] K. Saffu, J. Walker, and M. Mazurek, “Perceived strategic value and e-commerce adoption among SMEs in Slovakia,” *J. Internet Comm.*, vol. 11, no. 1, pp.1–23, 2012.
- [26] D. Syah, R. Lupiyoadi, and A. Tjiptadi, “Factors affecting the use of e-commerce in creative industries: Empirical evidences from SMES in Jabodetabek-Indonesia,” *Jurnal Siasat Bisnis*, vol. 20, no. 2, pp. 143–160, 2016.
- [27] P. Ochola, “An empirical study of determinants of e-commerce adoption amongst micro, small and medium enterprises (MSMES) in Kenya,” *Int. J. Econ., Comm. Manag.*, vol. 3, pp. 223 –240, 2015.
- [28] V. Le, F. Rowe, D. Truex, and M. Huynh, “An empirical study of determinants of e-commerce adoption in SMEs in Vietnam: An economy in transition,” *J. Global Inf. Manag.*, vol. 20, no.3, pp. 1–35, 2012.
- [29] M. Hajli, H. Bugshan, M. Hajli, and A. Kalantari, “E-commerce pre-adoption model for SMEs in developing countries,” In Proceedings of the International Conference on e-Learning, e-Business, Enterprise Information Systems, and e-Government (EEE) (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp), 2012.
- [30] J. Walker, K. Saffu, and M. Mazurek, An empirical study of factors influencing e-commerce adoption/non-adoption in Slovakian SMEs, “*J. Internet Comm.*,” vol. 15, no. 3, pp. 189–213, 2016.
- [31] W. Kenneth, M. Rebecca, and A. Eunice, “Factors affecting adoption of electronic commerce among small medium enterprises in Kenya: Survey of tour and travel firms in Nairobi,” *Int. J. Bus., Humanities Technol.*, vol. 2, no. 4, pp. 76–91, 2012.
- [32] M. Frasquet, Molla, A., and M. Ruiz, “Determining factors and consequences of the adoption of B2C e-commerce: An international comparison,” *Estudios Gerenciales*, vol. 28, no. 123, pp.101–120, 2012.
- [33] L. Chee, B. Suhaimi, and L. Quan, “Understanding the determinants of e-commerce adoption: Evidence from manufacture sector in West Malaysia,” *Indian J. Sci. Technol.*, vol. 9, no.10, pp. 1–8, 2016.
- [34] S. Lama, S. Pradhan, and A. Shrestha, “An e-tourism adoption model & its implication for tourism industry in Nepal,” In *Information and Communication Technologies in Tourism 2019* (pp. 291–303). Springer, Cham.
- [35] D. Ardjouman, “Factors influencing small and medium enterprises (SMEs) in adoption and use of technology in Cote D’ivoire,” *Int. J. Bus. Manag.*, vol 9, no. 8, pp. 179-190, 2014.
- [36] D. Straub, M. Boudreau, and D. Gefen, “Validation guidelines for IS positivist research,” *Commun. Assoc. Inf. Syst.*, vol. 13, no. 1, pp. 380-427, 2004.
- [37] J. Sánchez-Torres, S. Berrío, and P. Rendón, “The adoption of e-commerce in SMEs: the Colombian case,” *Journal of Telecommunications and the Digital Economy*, vol. 9, no. 3, pp. 110-135, 2021.
- [38] R. Sujatha, R., and M. Karthikeyan, “Determinants of E-Commerce Adoption: Evidence from Small and Medium-Sized Enterprises in India,” *International Journal of Business and Society*, vol. 22, no. 2, 574-590, 2021.

# A Survey on Computer Vision Architectures for Large Scale Image Classification using Deep Learning

D. Dakshayani Himabindu<sup>1</sup>  
Department of IT, VNRVJIET  
Hyderabad-90, T.S, India

S. Praveen Kumar<sup>2</sup>  
Department of Computer Science,  
GITAM, Visakhapatnam-45,  
Andhra Pradesh, India

**Abstract**—The advancement in deep learning is increasing day-by-day from image classification to language understanding tasks. In particular, the convolution neural networks are revived and shown their performance in multiple fields such as natural language understanding, signal processing, and computer vision. The property of translational invariance for convolutions has made a huge advantage in the field of computer vision to extract feature invariances appropriately. When these convolutions trained using back-propagation tend to prove their results ability to outperform existing machine vision techniques by overcoming the various hand-engineered machine vision models. Hence, a clear understanding of current deep learning methods is crucial. These convolution neural networks have proven to show their performance by attaining state-of-the-art performance in computer vision over years when applied on humongous data. Hence in this survey, we detail a set of state-of-the-art models in image classification evolved from the birth of convolutions to present ongoing research. Each state-of-the-art model evolved in the successive year is illustrated with architecture schema, implementation details, parametric tuning and their performance. It is observed that the neural architecture construction i.e. a supervised approach for an image classification problem is evolved as data construction with cautious augmentations i.e., a self-supervised approach. A detailed evolution from neural architecture construction to augmentation construction is illustrated by provided appropriate suggestions to improve the performance. Additionally, the implementation details and the appropriate source for the execution and reproducibility of results are tabulated.

**Keywords**—Image classification; deep learning; computer vision survey; convolution neural networks; IMAGENET dataset

## I. INTRODUCTION

Previous machine vision methods mostly use hand-engineered features. They mostly rely on the morphology of the image sometimes [1]. This can eventually cause a problem in designing a model to capture essential features. To overcome this deep learning models are adapted. Deep learning is advancing in numerous domains such as image recognition, speech recognition [2-6], signal processing [7-12], language processing [13-18], and graphs [19-24]. This leverage in the use of deep learning-initiated advancements in the development of highly scalable hardware architectures which perform large computations. The availability of huge data with high computing resources eventually helped in developing deep architectures which are utilized for large scale tasks. Specifically, in computer vision, deep learning has

advanced in numerous subdomains such as image classification [25-30], object recognition [31-43], pose estimation [44-48], image segmentation [49-54], and visual question answering [55-60]. The previous research states that these advancements are held on a large scale to attain state-of-the-art results. In most of the tasks, the generic method applied is convolution neural networks (convnets). There are variant hyperparameters involved in building an effective neural architecture. There are definite properties of convolution neural networks and these properties act as advancements to the current research building large scale architectures. Hence, in this introduction a certain set of relevant concepts regarding Convnets are detailed. In the next section, a set of contributions are detailed explicitly.

## II. CONTRIBUTION

The contributions of this survey to the present existing literature are described as,

- 1) Firstly, a prerequisite introduction to convnets is provided and the successive advancements and the individual parameters involved in architecture are detailed.
- 2) The evolution of the convnets from its beginning is explained and a sequential state-of-the-art advancement in image classification utilizing the convnets are elaborated in detail.
- 3) Finally, a set of recommendations are provided to enhance the neural architectures to obtain successive state-of-the-art performance and pave a path to future advancements.

## III. ORGANIZATION OF THE SURVEY

The organization of this survey is described in three phases. Further, Fig. 1 describes the complete flow of this survey.

- 1) The first phase gives a complete description of the convolution neural networks i.e. specifically describing the components involved in convolutions and their visual illustrations are provided equivalently. This section provides a clear intuition of the working of convnets with a glimpse of the terminology used. Finally, the advantages and disadvantages are equally provided to understand where convnets can perform best and fail.

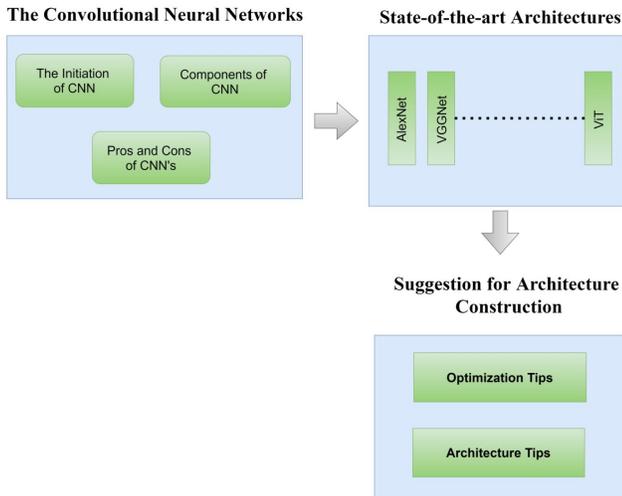


Fig. 1. The Visual Illustration of the Complete Organization of the Survey.

- 2) In the second phase, a clear understanding of the state-of-the-art networks is provided. Each architecture is described in detail by detailing the method implied and hyperparameters tuned for variant settings. This gives insights to the reader to understand the flow and the evolution of convnets and its developing aspects in the current research.
- 3) 3. The final phase provides suggestions to construct a novel architecture to provide a good transferability of features with low computational expense by considering various factors.

#### IV. THE CONVOLUTION NEURAL NETWORKS

First, it is aimed to discuss the mathematical intuition of convolution neural networks and next, the first implementation of convnets is described. Next, a set of components involved in the construction of convolution architecture are described accordingly. Subsequently, a set of properties for convnets are detailed. Finally, the advantages and the disadvantages carried by convolution neural networks are specifically mentioned [61, 62].

##### A. The Initiation of Convnets

The convnets are inspired by the convolution theorem. Convolution is a combinatory operating between two functions where their arguments are real.

$$Conv(y) \leftarrow \int f(x).g(y-x)dx$$

The equation above, Conv(.) is a convolution operation. This convolution operation is mentioned typically<sup>1</sup> as,

$$Conv(y) \leftarrow (f * g)(y)$$

The first function f(.), denotes a probability density function which is referred to as input. The second argument, g(.) is

referred to as kernel. Hence, these mathematical implications are helped in building the first convolution neural network.

The first convolution neural network was observed in the literature by LeCun. Y et al. [63]. The main object of this research was to implement a convnets to recognize handwritten postal zip codes. To train the model, backpropagation was implied and then successively able to extract variant features. The complete architecture has 1 input layer, two convolution layers and two fully connected layers. This first work helped revolutionize the convnets to a greater extent.

Subsequently, work by LeCun. Y et al. [64] implemented multi-layered NN by training the model end-to-end using backpropagation. This helped to learn and implement gradient-based optimization. In addition to the previous work, this work implemented a graph transformer network for language understanding which utilizes convnets by training with global techniques. The convolution architecture proposed is known as LeNet-5 which had 4 convolution layers and 3 fully connected layers. The final fully connected layer i.e. final activations are Gaussian connections. This initial conceptualization of convnets produced rigorous outcomes after the evolution of large computational devices to obtain state-of-the-art performance every year in large scale visual recognition challenge ILSVRC-12.

##### B. Components in Convnets

There are a set of components involved in convnets and this help understand the terminology regarding the convnets. A visual illustration of individual components is provided accordingly.

a) *Kernel*: The kernel is described as a grid or a matrix that convolves on the input.

b) *Stride*: The stride is a step taken after each convolution i.e., the number of steps moved by the kernel on the input.

c) *Feature Map*: The feature map is considered as the output activation incurred after completion of the convolution operation.

d) *Padding*: The padding is the process of filling the borders of the input equivalently in every dimension i.e., mathematically the input is surrounded by zero eventually increasing the size of the input.

Hence, In Fig. 2 these components involved in convolution are explained in detail. The blue component which is of size 2x2 is input. The grey 3x3 size matrix refers to the kernel. Next, the dotted square grid bordered around the input is called padding. The dark green component which is projected on the top of the input is a feature map obtained. Hence, the convolution operation is carried by moving the kernel onto the input. This kernel applies dot product on the input and a set of values are obtained. Further, these values are aggregated using a sum function. Then, a feature map is obtained accordingly. This process is iterated till the complete input is convolved. In a convnet, kernel size determines the shape of the kernel to perform the convolution operation. The number of kernels determines the number of variant types of kernels with varying values inserted into them. Next, padding

<sup>1</sup>The \* mentioned denotes the convolution operation.

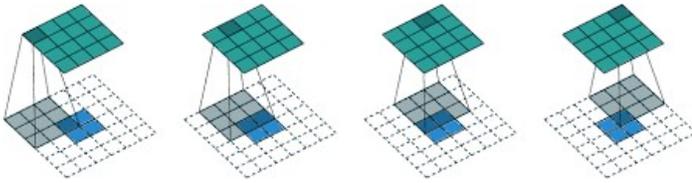


Fig. 2. Visual Illustration of Convolution Operation.

is generally used to produce similar dimensional output. In the next section, a set of advantages and disadvantages involved in convolutions are detailed. Further, a detailed explanation is provided by considering varying situations and altering the above-mentioned components in the work [65].

### C. Pros and Cons of Convnets

The convnets do have certain abilities which provide higher performance on multi-domain tasks. Even having definite advantages, convolutions carry a set of disadvantages which are discussed in detail.

#### a) Advantages:

- **Transferability:** The previous deep networks such as Restricted Boltzmann Machines, deep belief networks and fully connected neural networks do not persist with transferability of weights. But, the convnets are provided with transferability of features. Hence, a certain layer in architectures can be extracted to reproduce the weights for variant tasks. It can be further implicated in architecture pruning for improving the feature extraction for variant tasks.
- **Sparse Connections:** The connections in most of the previous existing neural networks have dense connections i.e. having an extreme number of connections which in turn increases the computational budget of the model. But, whereas convnets have sparse connections reducing the redundant connectivity and reducing the computational expense.

#### b) Disadvantages:

- **Rotational Sensitivity:** The convnets cannot extract the features of the entity residing an input which is rotated until and unless the objects in the images are rotationally symmetrical. Hence, to overcome these many techniques are implied such as augmentation. Horizontal flip, vertical flip and angular rotations are provided to an individual image to extract features even having rotational changes.
- **Time-Variant signals:** The convolutions lack in understanding the signal processed during a variant time pattern to that of a non-linear system. This can lead to the problem is speech specifically problem underlying the acoustic detections. But this problem is not seen in image recognition.

## V. STATE-OF-THE-ART VISION MODELS

### A. Alex-Net

Krizhevsky et al. [66] proposed an end-to-end trainable deep convolutional network for large scale image classification

i.e., on IN12. They observed the problem of using ML methods for image classification. They developed an eight layered deep NN which has 5 conv layers and 3 fully connected layers. The kernel size and stride implied are clearly illustrated in figure.3.

Firstly, they used relu [67] as non-linearity to forward the activations from one layer to another where they observed speeding up of convergence when relu is used as non-linearity. Second, they used GPU's for training their network in which, two GPU's are used with parallelized computing and having communication mutually layer to layer. This improved the performance of the model by reducing T-1 error and T-5 error by 0.017 and 0.012 respectively. Next, for normalization a technique (which is a similar normalization technique to that of [68]), named local response normalisation, is operated for conv layers which are tuned while validation procedure. This improved the performance of the model by reducing the T-1 error and T-5 error by 0.014 and 0.012 respectively. Next, the overlapping pooling technique is utilized which pools the pixels which are not only adjacent but also which are overlapping with correspondence. It is achieved by reducing the step during convolution. This reduced error-rate of T-1 and T-5 activations by 0.004 and 0.003 respectively.

The constructed architecture has consumed 60 M parameters which are mentioned in Fig. 3. To have good generalization a sequence of tasks was done to reduce the problem of overfitting in the networks. Firstly, data augmentation is done. In this step, the samples regarding an image are increased either translating the image in horizontal (or vertical) directions or the pixels of the images are changed in terms of colour intensities. This is done by considering the principal components of images and adding weight to pixels accordingly. This procedure led to an increment of T-1 accuracy by 1%. Secondly, the fully connected layers are attached with two dropout layers [69] (for the last two layers excluding class activations) with a drop ratio of 50% i.e. 50% of the neurons are inactive during the training and the network tend to learn during validation.

The complete model was trained on 90 epochs. It is optimized using SGD with an initial learning rate of  $10^{-2}$  and  $9 \times 10^{-1}$  as momentum through 128 batches (batches considered per iteration). When no convergence invalidation was observed in the learning, the rate was decreased 10 times to that of initial learning. The model achieved a T-1 error rate of 37.5% and a T-5 error rate of 17%. Further, the model was altered in various types and different accuracy score are obtained. These details are tabulated in the Table I.

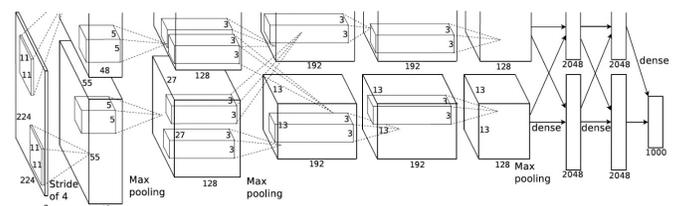


Fig. 3. Alex-Net Architecture with Varying Strides and Filters.

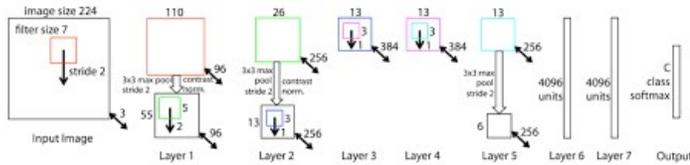


Fig. 4. Ze-Net Architecture with Varying Strides and Filters [5].

## B. Ze-Net

Matthew D. Zeiler et al. [70] proposed a Conv NN which is very similar to Alex-Net by visualizing the feature maps and kernels for better understanding internal computations of the convnets. They developed an eight layered deep NN which has 5 conv layers and 3 fully connected layers. The kernel size and stride implied are clearly illustrated in figure.4.

The architecture of the model is designed with a decoder and an encoder which extracts latent representations and reconstructs the image respectively. Several conv layers are used to extract the spatial features with ReLu as activation throughout the network. The decoder helps in unspooling the visual representations by a switch variable. This switch variable is used for memorizing the pooled information in the encoder structure and mapping it on the decoder structure. Further, to observe feature extraction, translation scaling and rotation mechanisms are performed in which the convnets were invariant to translation and scaling but not for the rotation. Finally, to observe the localization ability of convnets a certain part of the image consisting of important feature is occluded. It is observed that convnets significantly degraded in terms of performance due to occlusion.

The model implied is very similar to that of AlexNet with two variations, the filter size is reduced in the first layer from 11x11 to 7x7 and stride 4 of convolution is reduced to stride 2. Augmentation is performed by subtracting the input with individual pixel mean and used 10 variant sub crops techniques such as horizontal flip, vertical flip etc. The learning rate with which the SGD optimizer was initialized as 0.01. A momentum of 0.9 was implied for faster training. The bias components were initialized with zero and 50% of the densely connected layers are dropped during the training process. The model acquired T-1 and T-5 error rates of 36% and 14.7% respectively. Further, the network pre-trained on ImageNet is implied on Caltech-101 dataset with an accuracy score of 83.8 for 15 images per class whereas increasing 30 images per class it obtained an accuracy score of 86.5%.

## C. OverFeat

This work was inspired by the standard concepts that injected good improvement in the field of classification [71-74]. Sermanet et al. [75] proposed a framework implying CNN's not only for classification but also for detection and localization. The novel localization criterion in this work is obtained by capturing and aggregated to multiple object boundaries. When the localization task is performed on ImageNet the best performing OverFeat model secured the first position in the 2013 challenge.

The main objective of the OverFeat is to perform classification by simultaneously locating and detecting the objects

with the use of a single conv architecture. A novel method is implied to detect and localize the bounding boxes of the image which is predicted by the neural architecture. With a combination of various localization predictions, the process of detection acquires good features and hence the performance is increased and eventually training time can be reduced. This method not only helps to provide less computation but also with greater performance acquiring higher accuracy scores.

The complete OverFeat model has three ideologies and the methodology is implemented accordingly,

- 1) Initially, a conv net is applied at variant locations captured in the specified image. Sequentially, a sliding window approach is implied using different scales. This eventually helped to provide a better classification model but, the localization performance was degraded.
- 2) The system was not only trained to produce distribution for the set of categories but also improved localization by properly constructing the size of the bounding box to capture the region of interest for that specified category.
- 3) Lastly, a proof of concept was provided for a specific category at individual locations.

The implementation works by training a conv net by using a sliding window as the decision box by choosing the centre pixel and classifying it accordingly to a definite object. The advantages of this method are the bounding contours utilized for localization need not be rectangular. The disadvantage of the model is that it acquires numerous pixel-level labels which in turn increases computations cost. This work was the first implementation of localization, and the detection task for ImageNet by using a unified framework. The localization and detection task performed by overfeat is done by allowing the model to guess the labels for the specified object five times and if the probability of the guess turns to be 0.5 and above (matching the ground truth label) then, a definite label for the object is assigned to definite class accordingly. The five times guess the pattern is chosen to specify the correct object in the presence of multiple objects without labels.

During the construction of the OverFeat, a set of hyperparameters are tuned and are mentioned individually. The optimizer implied in this method is SGD with an initial learning rate of  $5 \times 10^{-2}$ . A momentum was used to faster the training procedure (an initial momentum of 0.6 was implied). Weight decay for the L2 regularization is initialized as  $10^{-5}$ . ReLU is used as an activation function at the utmost every layer. The initial five layers of the model implied are very similar to AlexNet with ReLU activations and successive pooling layers (max-pooling layers). But with many similarities, certain differences are to be noted and they are mentioned. No local response normalization is utilized in this work as it did not improve performance. The pooling layers implemented do not overlap as they depicted better performance. Further, implying small stride in the first two layers, better invariances was obtained i.e., large stride speedups the training process but performance in terms of accuracy can be degraded.

The OverFeat proposed 8 models of which, two are ensemble models. The fast ensemble model with four scales and fine stride acquires a T-1 error rate of 35.10% and a T-5 error

rate of 13.86%. Whereas, an accurate model acquired a T-1 error rate of 33.96% and a T-5 error rate of 13.24%.

#### D. VGGNets

Simonyan et al. [76] worked on deep neural networks with different depth of layer's in them to know the changing rate of accuracy concerning the depth of the neural network. The depth of the neural networks proposed in this paper varied from 11 to 19 layers. Six different types of networks were used by the author to know how the models perform based on different configurations in it. The kernel size or the receptive field is set to the size of 3X3 rather than 5X5 or 7X7 because a smaller receptive field help in capturing the details of the image in a more specific way and use fewer parameters. The six types of networks built in this paper have been given the following names A, A-LRN, B, C, D and E. These networks differ by the depth of layers. An A-LRN is the two networks with a depth of 11 layers, the only difference is that in A-LRN, Local Response Normalization (LRN) is used to check how the accuracy is varied when LRN is used in a network. It was observed that adding LRN to the network was not much of use to improve the accuracy score. B has a depth of 13 layers, C is just an extension of B where there are 3 extra 1X1 convolutional layers in it. D and E have 16 and 19 layers of depth in their network configurations respectively.

In the aforementioned networks, a max-pooling layer is present after a few convolutional layers or a block of these layers. Inside each block, there is a combination of 3X3 and 1X1 convolutional layers accordingly. The input image is of size 224X224 pixels, which is downsampled by the convolution and max-pooling layers next the extracted features are passed into the dense layer for the classification or detection task of the image. These architectures used Stochastic Gradient Descent (SGD) with 0.9 momentum and has a batch size of 256. Drop out was also used in two fully connected layers followed by a dense layer and a softmax layer to predict the class of the image. The learning rate was set to 10<sup>-2</sup> and this was decreased by a factor of 10 if the accuracy got saturated at a point. Training of these networks was completed after 74 epochs. During the training time, Lr was decreased by a factor of 10 for 3 times in total. First, the networks (A, A-LRN, B) were trained on a single scale of 256 and the remaining networks (C, D, E) were trained using multiple scaled images (scale jittering) with the scale ranging from 256 to 512. It was observed that the performance of these networks improved significantly with the use of scale jittering and by increasing the depth of the network, E convnet got a top-5 Val-error of 8% which is a competitive score.

To further assess the capabilities of the network, the VGG team used scale jittering even more aggressively on the train-test set this time and saw that convnets D and E got a top-5 Val-error of 7.5%. Multiple crops were also used in the next experiment and it was compared with the dense evaluation method. From this experiment, it is concluded that the multiple crop method outperforms the dense method. The testing method shown by the VGG team was very different from the previously mentioned works, where the last FC layer was converted into a convolutional layer and this receptive field was put on a whole image and then obtained a single vector

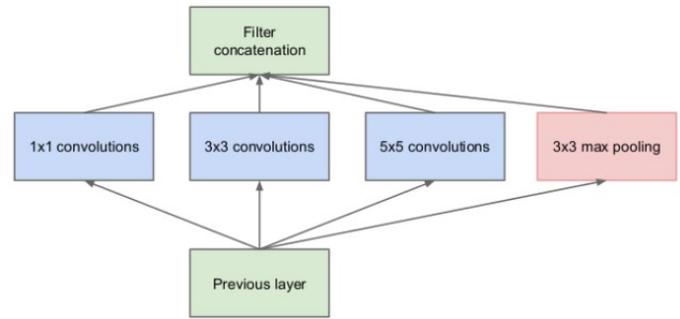


Fig. 5. Naive Inception Module.

with the individual class score. The vector was pushed into the softmax layer to get the prediction score.

An ensemble of all these convnets was made and it was seen that the seven networks ensemble model has a test error of 7.3% and the ensemble of D and E convnets had a test error of 6.8%. The 2 convnet ensemble networks secured second place in the ILSVRCV-2014 challenge. But the margin between the scores was very close when compared to Google Net (first place). The single net performance of VGG architecture outperforms all the other architectures (even Google Net) with a large margin of 0.9%.

#### E. Google-Net and InceptionV2

Szegedy et al. [77] presented a deep learning model which has an inception module in it. Google-Net mainly focuses was to develop a deep neural network architecture with a less computational expense. As the network goes deeper the arithmetic operations performed by the models also increases and this gives scope for newer error that occurs with computing gradients. Because of the previously mentioned reasons the author suggests creating a sparse network rather than a fully connected network. The goal is very simple all we have to do is find optimal weights through a sparse network that could approximate or predict an image. Translation invariances added in this work by building a network through several convolution layers.

Fig. 5 shows the naïve inception module which applies convolution to the input image with a kernel size of 1x1,3x3,

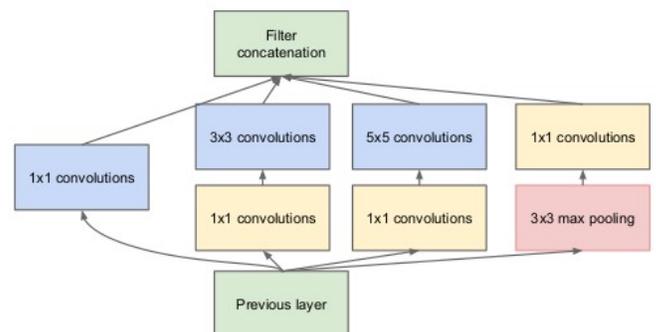


Fig. 6. Dimensionality Reduced Inception Module.

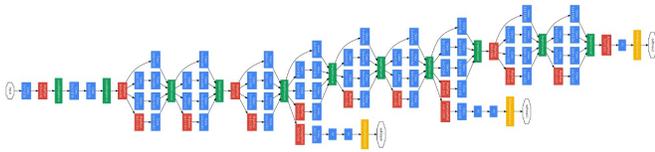


Fig. 7. Detailed Architecture of Google-Net.

and 5x5. Next, pooling is done to the input image and these activations are concatenated using correlation statistics instead of stacking up the layers can increase computational expense. With this understanding, a new inception module is created, and the dimensions are reduced by bottleneck convolutions i.e., 1x1 convolution kernel to the input image and it is observed that lower-dimensional space preserve the information of the corresponding image. These dimensionality reduced inception modules are now stacked on each other by applying max pooling layer of stride 2 in between the modules occasionally. The proposed Google-Net architecture consists of 22 layers in total. An ensemble of 7 such models was created and tested on IL-14 for classification as well as detection.

Fig. 6 shows the architecture of GoogleNet. In between this network for few inception modules, a classifier was assigned to them. This has helped to generalize images more precisely. These classifiers contain a 1x1 convolutional filter with 128 filters in it. Next, the convolutional layer is stacked with a fully connected layer with 1024 neurons in it. Followed by a dropout layer and a SoftMax layer to provide the probabilities of each class and then predict the image class. In this network, every layer uses the ReLU non-linearity function for the activation of each neuron in the network.

Seven distinct types of networks were built based on the new inception module to train them on the ImageNet dataset with different learning rates and sampling methodologies. The probabilities of all these networks were averaged to get the output. With this ensemble method, Google Net got a top-5 error rate of 6.67% on testing and validating set. An ensemble of 6 models was used in the ILSVRC 2014 detection challenge which achieved map of 43.9% and secured first place in both the classification and detection challenges. From this work, it can be deduced that the sparse network can be useful in deep neural networks to know the deep representation of the image while using less computational resources. Kindly refer Fig. 7 for detailed understanding of architecture.

A certain problem, covariant shift is observed while training a deep neural network is addressed and solved by implementing the Batch Normalization (BN) procedure. This paradigm was proposed by Sergey Ioffe and Christian Szegedy [78-80]. BN procedure was implemented on Inception ensemble with an Image resolution of 224x224 produced a T-1 accuracy score of 79.9% and T-5 accuracy score of 95.1%.

#### F. InceptionV3

Szegedy et al [81] implied the aforementioned Inception architecture and scaled the convolution layer to provide higher performance by decreasing computational expense. This is the upgraded version of GoogleNet and maintained appropriate

convolution by doing defiant regularization throughout the network. The authors illustrated the work by defining a set of principles and scale the conv layer by optimizing techniques. The principles are defined in such a way that they performed experimentation on different datasets by considering much architecture. The principles of the network are

- A cautious decrement in representation is preferable, instead of bottleneck layers at the beginning of the network.
- Higher dimensions in the network are easier to process with piling up the activations in a conv network for extracting invariant features.
- Even though pooling provides faster learning, spatial aggregation in the network holds the representational features without any loss in the lower dimensions.
- The width and depth of the network must be optimally selected with a balanced criterion.

Generally, a 5x5 or large conv layers can capture the activations of the previous layers. Reducing the feature map size would decrease the no of parameters, training time and computational cost of the network. The inception module consists of 5x5 conv layers, instead of these, the authors have replaced 5x5 conv layers with two 3x3 conv layers which are shown in Fig. 8 with 28% relative gain. But this method has a problem of loss of expressiveness or using a low filter size (below 3x3) which may produce the best outcome. So, the authors have come up with an idea of using asymmetric convolutions. The concept of asymmetric convolution is any nxn convolution can be replaced by 1xn convolution which is followed by nx1 convolution. As n increases the computation of the model decreases. The 3x3 convolutions in the network are replaced by 1x3 and 3x1 as shown in the figure.9. By using this method, it reduces the computation cost by 33%. The activation maps in the network filters are improved because to get rid of the bottleneck representation. The network consists of 42 layers and has 2.5% more computation than GoogLeNet.

The concept of asymmetric convolution is any nxn convolution can be replaced by 1xn convolution which is followed by nx1 convolution. As n increases the computation of the model decreases. The 3x3 convolutions in the network are replaced by 1x3 and 3x1 as shown in the figure.9. By using this method, it reduces the computation cost by 33%. The activation maps in the network filters are improved because to get rid of the bottleneck representation. The network consists of 42 layers and has 2.5% more computation than GoogLeNet.

The model takes SGD as an optimizer with a batch size of 32 which is trained across 100 epochs by considering a learning rate of 0.045. The model achieves the state-of-the-art results with T-1 and a T-5 error rate of 21.2% and 5.6% respectively. By ensembling 4 Inception-v3 models they got a T-1 and T-5 error rate of 17.2% and 3.58% respectively.

#### G. Inception-v4, Inception-ResNet

Szegedy et al [82]. has extended the idea of Inception-v3 by combining residual connections to it with accelerating training. This model has won the 2015 ILSVRC challenge by acquiring state of the art performance. The authors have

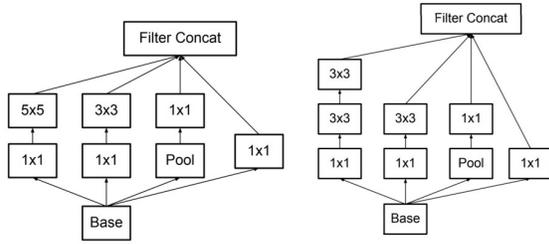


Fig. 8. Illustration of the Variation of Bottleneck from 5x5 to two 3x3 Convolution Blocks.

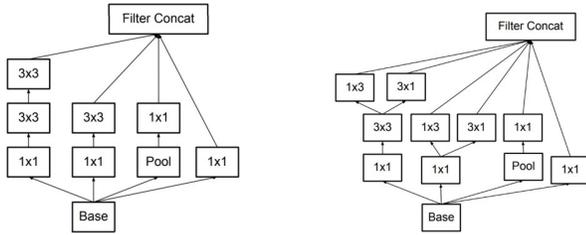


Fig. 9. Illustration of the Variation of Bottleneck from a 3x3 to 1x3 and 3x1 Convolution Blocks.

provided proof of the residual connections speed up the training of Inception networks. As the Inception networks are very deep, the filter concatenation stages in the network are replaced by residual connections. By increasing the depth and width of the Inception-v3 networks they proposed another network called Inception-v4. To provide an optimised network, the layers are tuned cautiously. To connect Residual versions with the Inception network, a cheaper Inception block is implied rather than the original Inception. Fig. 10 shows the whole architecture with residual connections inside an Inception network. There are filter expansion layers (1x1 convolutions with no activation) inside the network. Batch-normalizations are omitted on the top of the network and overall the no of inception blocks was added subsequently. While experimentation the authors have found that if the networks have more than 1000 filters, the model has died before the training has started. There is no use in increasing the batch size or lowering the learning rate. It seemed to stabilize the training process by scaling the residuals and then adding to the before layers.

Using RMSProp [83] as an optimizer and learning rate of 0.045 they achieved a T-1 and T-5 error rate of 19.9% and 4.9% respectively on ILSVRC 2012 by considering Inception-ResNet-V2 as the base model. By combining three residual and one Inception-v4 they achieved a T-5 error rate of 3.08% on the ImageNet classification challenge.

H. ResNext

Saining Xie et al [84] has developed a model succeeding the ResNet model which is known as “ResNext”. This model is the 1<sup>st</sup> runner-up in ILSVRC 2016 competition. This model contains extra dimensionality called cardinality which deals with the depth and width of the network. The ResNext

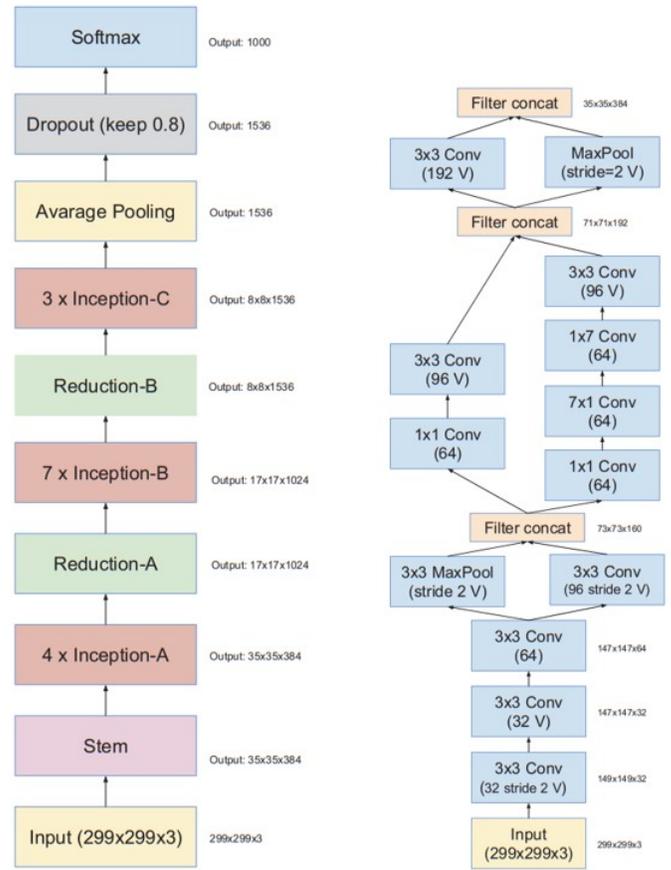


Fig. 10. The above Figure Illustrates the Complete Architectural Details of Inceptionv4.

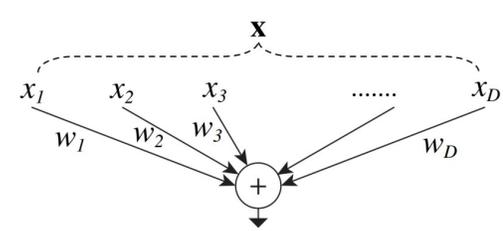


Fig. 11. The Neural Weight Transformation with Varying Inputs and Weights.

architecture consists of aggregated transformations by splitting, transforming and aggregating a single neuron.

The model embraces the method of repeating layers in VGG and ResNet’s by making use of the split-transform-merge strategy in the Inception model. The neuron in the network splits the input and transforms the weighted sum to low dimensions by aggregating through summation fig(11).

Each neuron in the network carries out a non-linear function due to the addition of the new dimension (cardinality). The ResNext model replaces the elementary transformation with a signified function and constructed by combing a set of residual

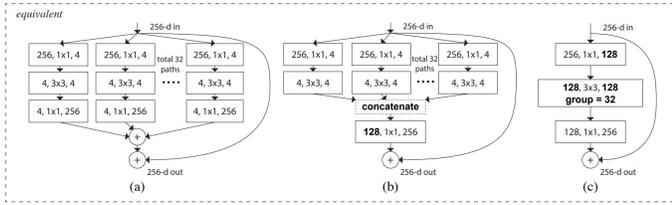


Fig. 12. Three Variant Architecture Designs Implemented in the ResNeXt.

blocks which are subjected by two rules first, maintaining the same shape in the spatial maps i.e. ensuring width size and a filter size of each block are the same. Second, it maintains the complexity of the network where width is multiplied by 2 when the spatial maps are down sampled. This model takes fewer parameters when compared to existing ResNet's with  $4.2 \times 10^7$  FLPOs.

Each block in the ResNext network has the same number of internal dimensions. ResNext-50 (32x4d) indicates four internal dimensions with 32 paths (cardinality=32). When compared with the Inception-ResNet block ResNext model is designed with less effort in each path and implemented in different forms illustrated in the figure.12. The third form of the network is chosen because it is much faster and has grouped convolutions than the other two models. The grouped convolutions consist of 32 convolutions with input and output of 4 dimensions. The experiments were carried out with increasing the cardinality and width which results in the increase of FLOPs by a factor of 2. By increasing the cardinality, the error is reduced by 1.3% to 20.7% rather than increasing the width of the network. The ResNext-101 (64x4d) has obtained a T-1 error rate of 20.4% and a T-5 error rate of 5.3% with an image size of 224x224. They also evaluated this model on different dataset like ImageNet-5K and got an error rate of 40.1% which reduces the error by 2.3% when compared to ResNet-101.

### I. Dual Path Networks

Y. Chen et al [85] proposed an architecture Dual path network (DPN). It is the combination of a residual network (ResNet) and a Densely connected network (DenseNet). The proposed architecture takes the feature reuse from ResNet and feature exploration from DenseNet by maintaining low complexity and more number of parameters. DPN includes higher-order recurrent neural networks (HORNN) which benefit from sharing weights throughout the network and also proves that ResNets and DenseNets are the same by using HORNN. By optimizing the network they had achieved a state of the art results on ImageNet-1k.

To understand the connection between the two networks they formulated the HORNN as

$$i^j = p^j \sum_{Q=0}^{j-1} R_Q^j(i^Q)$$

Where  $i^j$  is the state which is hidden in RNN at a particular step which is denoted by Q, the current step is indicated by j.  $R_Q^j(\cdot)$  function is for extracting features.  $R_Q^j(\cdot)$  and  $p^j(\cdot)$  do not share weights but extracts the same features more times. So that it may lead to feature redundancy this is one of the drawbacks of the network. ResNet has the problem with

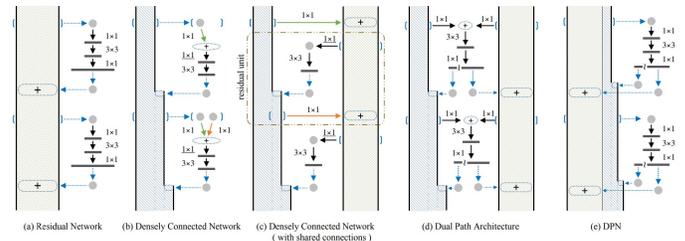


Fig. 13. Visual Illustration of Networks from Deep Residual Network to Dual Path Networks (DPN).

finding new features while DenseNet has the problem with high feature redundancy. The DPN architecture has a 1x1 conv layer, 3x3 conv layer and 1x1 conv layer as last layer figure. 13. The output of the network has divided into two parts first, the element-wise addition of residual combinations. Second, adjoined with DenseNets to improve the learning ability of individual micro-block. The second conv layer in the network is replaced by ResNext. ResNet is widely used so the authors choose it as the main part of the network which is combined with DenseNets to construct the architecture. A DPN can implement either by adding a "slice layer" or "concat layer" to the residual network which consumes extra memory usage and computational cost. DPN has 26% fewer parameters when compared to ResNext-101 (64x4d). The model is implemented on 40 k80 graphic cards with a batch size of 32 on individual GPU. The proposed architecture DPN-131 (40x4d) has got a T-1 error rate of 18.55% and a T-5 error rate of 4.16%. The model is also evaluated on different dataset like places 365 standard datasets where it got T-1 and T-5 accuracy scores of 56.84% and 86.69

### J. NASNets

Zoph et al. [86] contribute a new search space for constructing neural architectures by transferring the weights from a smaller dataset to that of the larger one. This research introduces a new regularization method (known as scheduled-drop-path) for the models developed through their proposed search space which improves generalization. The efficient model developed through this search space attains SOTA results in classification (IN-12 dataset). Additionally, utilizing the R-CNN framework the learned representations are captured through the best model attains SOTA on the CoCo dataset. The proposed NAS (Neural Architecture Search) [87] implements a reinforcement strategy to optimize the configurations to design a good neural architecture. This method implies 2 different cells with a similar structure and separate weights. These cells are normal and reduction which is shown in Fig. 14. The normal cell input and output are of the same dimensions whereas, the reduction cell reduces the shape of input dimensions to half the previous input (i.e. stride 2 is applied). These cells provide faster and efficient search with appropriate generalization. The NAS which is mentioned in Fig. 14, has a controller block is a recurrent neural network that predicts multiple architectures with multiple probabilities. Then a small network (child) is trained to reach convergence with a certain accuracy score. The gradients of multiple probabilities attained are scaled in such a way to attain new accuracy scores and are updated to the controller.



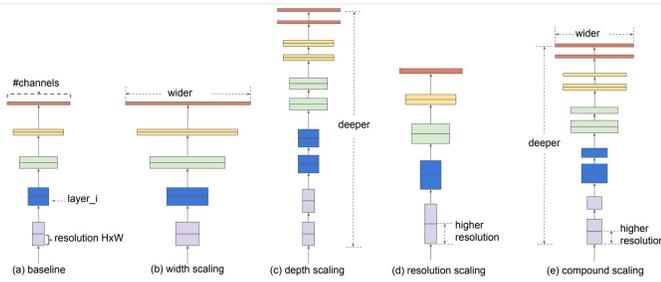


Fig. 18. The above Figure Illustrates the Scaling of Variant Components Involved in Convnets.

more block with the precise model.

The model is trained on ImageNet with RMSProp as an optimizer, an initial learning rate of 0.04 and decayed after 2.2 epochs with a batch size of 32. The architecture consists of 86.1M parameters which are smaller than NASNet. The model has achieved a state of the art results with T-1 and T-5 accuracy of 82.9% and 96.2% respectively.

#### L. EfficientNet

M. Tan and Quoc V. Le proposed a model by scaling the depth of the network, width of the network and resolution of the image [90]. The model is developed by using a combination of MobileNets and ResNets. By scaling those parameters, the model led to better performance with less computation cost. The scaling of the network is done in such a way they maintained a constant ratio throughout the network this scaling method is known as effective compound scaling. The scaling of the model is done as shown in Fig. 18. Due to various resources, they face a problem while scaling the convnet. So, they increased the depth, width and resolution of the image by a factor of  $P^k$ ,  $Q^k$  and  $R^k$  respectively where P, Q, R are small grid constant coefficients. By increasing the depth of the network, a convnet can apprehend more complicated features. Here, a problem of vanishing gradients arises and it is very complicated to train the network. By scaling the depth with a coefficient P, they maintained balance in the network. The next constraint is to balance the width of the network which is usually done in very small models. Increasing the width can capture more fine-grained features and takes less time for training. Their experimentations have shown, the wider the network, the more is the drop in accuracy. The resolution of the image is scaled by a factor R because of the higher resolution of the image takes more time for training. The proposed method enhances the accuracy and optimizes the FLOPS. By examining the depth, width and resolution values of the network to be 1.4, 1.2 and 1.3 respectively are found to be accurate with 2.3B FLOPS.

The model (EfficientNet-B7) achieved a T-1 and T-5 accuracy of 84.4% and 97.1% respectively with 66M parameters which are 8.4x smaller than the previous state-of-the-network.

#### M. FixResNeXt

Hugo et al. [91] performed augmentation trails for acquiring better generalization by choosing appropriate train and test size for a network. During experimentation, it is justified

that, lower training resolution for an image and higher testing resolution eventually improved the performance to a greater extent by reducing training computational cost. This procedure was implemented on ResNeXt-101 by outperforming the existing models and obtained state-of-the-art performance on 2019 ILSVRC. There was a good significant shift in the model when the training and the testing methods are fine-tuned separately. A joint optimization is done by scaling the train-test resolutions equivalently by maintaining individual RoC (region of classification) sampling. To overcome the distribution, shift the first two layers of the model are prioritized to fine-tune by varying the crop resolution. A detailed analysis is done to pre-process the model by increasing the crop resolution at the testing phase and during training, roc sampling is done appropriately. This eventually, acquired a good generalization by providing lower train resolutions and higher test resolutions. The computation is reduced by 3-fold by halving training resolution which in turn speed up the training procedure. Implying larger batches for training impacted a good performance with saving GPU memory. A further modification is done to the model by adjusting activation statistics of the layer which is preceding the global average pooling (GAP) layer. When these techniques are implemented on ResNet-50 by varying the test size the results obtained are mentioned (CR is equivalent to crop resolution). First, with 64 as CR, the model obtained an accuracy score of 29.4% on ImageNet. Further, with an increase in resolution by 128 the model obtained an accuracy score of 65.4%. A higher accuracy score of 78.4% was obtained for 288 as CR.

It is observed that increasing test resolution further (more than 288) the accuracy score was gradually decayed. Even after assigning appropriate test resolution a set of skewed activations were observed and they were addressed by two methods. First, a parametric adaption is chosen and the other is an adaption by tuning appropriately i.e., fine-tuning. Hence the parameters of the architecture are to be addressed in detail with experimental results. Instead of performing the train-test method for generalization 10-fold cross-validation is implied with mean and standard deviation for each execution. During the training process, extra training data was provided for most of the implementations. The best performing model (ResNeXt-101) acquired parameters of 829 M. While training ResNet-50 learning rate was initialized as 0.1 and is decayed by 10 for every 30 epochs. Initially, 512 samples were fed into the network as a batch with a horizontal flip, color jittering and random resize crop as augmentation parameters. The experimentation was performed on eight Tesla V100 GPUs. Subsequently, a set of 80 CPU clusters were inserted along with GPUs. The experimentation was carried out on standard pre-trained networks such as ResNet-50, ResNeXt-101 and PNASNet. Large network classification was done by complete fine-tuning PNASNet-5-Large with a train resolution of 331x331 which obtained the highest T-1 accuracy and T-5 accuracy of 83.7% and 98.0% on 480x480 test resolution respectively. Whereas, ResNeXt-101 was trained on 224x224 as a resolution to obtain a state-of-the-art accuracy of 86.4% with 320x320 as test image resolution. Further, this method was effective even on various transfer learning tasks and it obtained state-of-the-art performance for CUB-200-2011 and Birdsnap datasets.

TABLE I. IMPLEMENTATION DETAILS AND SOURCE CODE REGARDING STATE-OF-THE-ART MODELS

SOTA Works	Source Code with Implementation Details
AlexNet	<a href="https://worksheets.codalab.org/worksheets/0xfafcca55b584e6eb1cf71979ad8e778">https://worksheets.codalab.org/worksheets/0xfafcca55b584e6eb1cf71979ad8e778</a>
ZeNet	<a href="https://github.com/atriumlts/subpixel">https://github.com/atriumlts/subpixel</a>
VGGNet	<a href="https://github.com/tensorflow/models/blob/master/research/slim/nets/vgg.py">https://github.com/tensorflow/models/blob/master/research/slim/nets/vgg.py</a>
InceptionV2	<a href="https://github.com/tensorflow/models/blob/master/research/slim/nets/inception_v2.py">https://github.com/tensorflow/models/blob/master/research/slim/nets/inception_v2.py</a>
InceptionV3	<a href="https://github.com/tensorflow/models/blob/master/research/slim/nets/inception_v3.py">https://github.com/tensorflow/models/blob/master/research/slim/nets/inception_v3.py</a>
InceptionV4	<a href="https://github.com/tensorflow/models/blob/master/research/slim/nets/inception_v4.py">https://github.com/tensorflow/models/blob/master/research/slim/nets/inception_v4.py</a>
ResNeXt	<a href="https://github.com/facebookresearch/ResNeXt">https://github.com/facebookresearch/ResNeXt</a>
DPN	<a href="https://github.com/rwightman/pytorch-image-models">https://github.com/rwightman/pytorch-image-models</a>
PNAS*	<a href="https://github.com/chenxi116/PNASNet_pytorch">https://github.com/chenxi116/PNASNet_pytorch</a>
NASNet	<a href="https://github.com/tensorflow/models/blob/master/research/slim/nets/nasnet/nasnet.py">https://github.com/tensorflow/models/blob/master/research/slim/nets/nasnet/nasnet.py</a>
NoisyStudent	<a href="https://github.com/google-research/noisystudent">https://github.com/google-research/noisystudent</a>
EfficientNet*	<a href="https://github.com/tensorflow/tpu/tree/master/models/official/amoeba_net">https://github.com/tensorflow/tpu/tree/master/models/official/amoeba_net</a>
FixResNext	<a href="https://github.com/facebookresearch/FixRes">https://github.com/facebookresearch/FixRes</a>
BiT	<a href="https://github.com/google-research/big_transfer">https://github.com/google-research/big_transfer</a>
ViT	<a href="https://github.com/google-research/vision_transformer">https://github.com/google-research/vision_transformer</a>

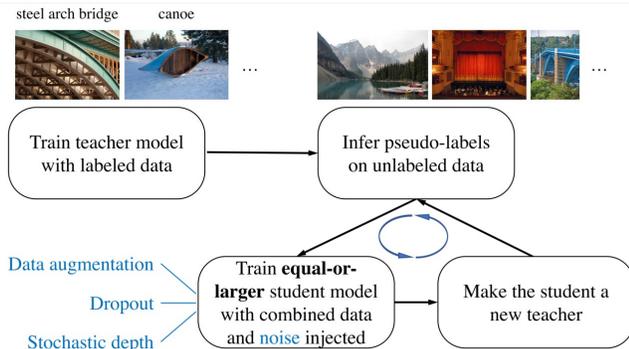


Fig. 19. The Working Principle behind the NoisyStudent Procedure.

#### N. NoiseStudent

Q. Xie et al. [92] implied self-supervised for training large scale images. This approach is based on a student-teacher learning paradigm. First, EfficientNet is trained on a set of labelled images(as a teacher model) of ImageNet and then produced pseudo labels by evaluating on a different data set which consists of 300 Images. Second, the larger EfficientNet model is considered as a student model and this is trained on the grouped labels i.e., pseudo labelled and labelled images. Next, the student model is replaced with the teacher and this process is iterated to attain significant performance. It is observed that the teacher model does not contain noisy labels as they were trained through a supervised approach. In the student model, a noise component such as dropout, stochastic depth, and random augmentations are implied. These implementations helped the student model to have greater generalization to that of the teacher model.

There are certain hyperparameters involved in tuning the model. The batch size is assigned as 2048 as default. A varying batch was implied i.e. 512, 1024, and 2048 to the EfficientNet model and all the batches turned out to have the same performance. The student model was trained for

350 epochs and smaller student models were trained for 700 epochs. The noise implied to student model with a dropout of 50%. Further, the random augmentation [18 for STNS] provided a magnitude of 27 for two operations. Finally, the probability of survival is set to 0.8 for the stochastic depth. The Noisy Student model beats the current state-of-the-art BiT Large with a 0.9% increment in accuracy i.e., the best performing NoisyStudent acquired an accuracy score of 88.4% T-1 accuracy and 98.7% T-5 accuracy respectively. This model consumed 480 Million parameters and which is approximately half the computational resource of the previous state-of-the-art by training the model with 300 unlabelled samples considered from the JFT dataset. The best performing model considered EfficientNet-L2 as the backbone to imply the NoisyStudent approach as mentioned in the Fig. 19. Further, the importance of adding a noise component in training the student model is discussed and evaluated. The training signal tends to vanish if the student samples were trained in a similar approach to that of a teacher by attaining zero cross-entropy loss. The T-1 accuracy obtained on ImageNet is 83.9%. This indeed shows large variation from the proposed method i.e., high variance from the current state-of-the-art. The co-training helps in segregating the two disjoint segments and training two models in a student-teacher self-supervised fashion helped in improving the performance to a greater extent.

#### O. BiT (Big Transfer)

Kolesnikov et al [93], performed transfer learning on large scale image recognition to improve tuning of hyperparameters and sample efficiency. The parameters are tuned cautiously by focusing on certain components for various vision tasks to improve performance with feature reproducibility. To provide greater performance transferability is provided on large scale vision tasks and performed transfer learning to produce three variant models BiT-Small, BiT-Medium and BiT-Large. The models were trained by fixing the architecture and varying the size of the data. Where small is performed on ILSVRC-2012 consisting of 1.2 million samples with 1000 classes. The medium is trained on full ImageNet with 14.2 million samples

with 21 thousand labels. Finally, the large utilized JFT dataset consisting of around 300 million samples and approximately 1.2 labels per sample. A set of tricks are considered by understanding certain components to attain higher performance for a neural network. They addressed two necessary components to build an effective neural architecture which is upstream and downstream components.

**Upstream Components:** Upstream components are implied for pre-training definite task. The components considered during up-stream pre-training are scale, Group normalization, and Weight standardization. Properly adjusting these components led to having a lower computational budget and greater efficiency. Further, group normalization and weight standardization obliged faster training over large batch structures.

**Downstream Components:** Whereas, Downstream components are applied for fine-tuning a similar visual task. In this, a heuristic rule is applied by discarding computationally expensive hyperparameters. Simple image pre-processing techniques such as resizing input to squared shape, cropping a short square randomly, and performing horizontal flip at training time. The parameters tuned while pre-training the model, at upstream and downstream are discussed independently. Most of the BiT models utilize ResNetV2 as backbone architecture to imply transferability. The upstream models utilize SGD as an optimizer and initializing the learning rate by  $3 \times 10^{-2}$ . Additionally, a momentum of 0.9 was induced for faster convergence. The input samples were isotopically resized to  $224 \times 224$  shape. Next, the small and medium models were trained with 90 epochs. But the training procedure was different as the learning rate was reduced by 10 after 30, 60 and 80 epochs. Subsequently, the large model was trained by decaying learning rate after 25%, 57.5%, 75% and 92.5% of the training progress. Similarly, for the downstream task, the SGD was implied as an optimizer with a learning initializer of 0.03 and to progress convergence, a momentum of 0.9 is added. The input shapes were reshaped appropriately to the context of the dataset. In a large scale visual classification challenge, the T1 accuracy obtained by the BiT-Large model on ImageNet-1K is 87.54% (with a standard deviation of 0.02). It remained a state-of-the-art model not only for ImageNet but also, for multiple standard data sets such as CIFAR-10, CIFAR-100, Pets, Flowers, VTAB. Further, the BiT was analysed on object detection, which implied RetinaNet as the backbone. This attained a state-of-the-art average precision of 43.8. With the BiT transferability, the object detection model attained an improvement of around 7.3%.

P. ViT (Visual Transformer)

Dosovitskiy et al. [94] utilized a transformer, the standard neural architecture for natural language processing onto computer vision task to drive self-attention for large scale visual recognition. This visual transformer was able to drive present state-of-the-art with lower computational cost to that of Convnets. The transformer is implied invariant fields depicting its performance. A Visual Transformer (ViT) is trained by appropriately setting the input embedding to the transformer to extract visual representations. The patch embeddings are obtained by resizing the image of a 2D image into sequential 2D patches. These embeddings are inserted into the transformer

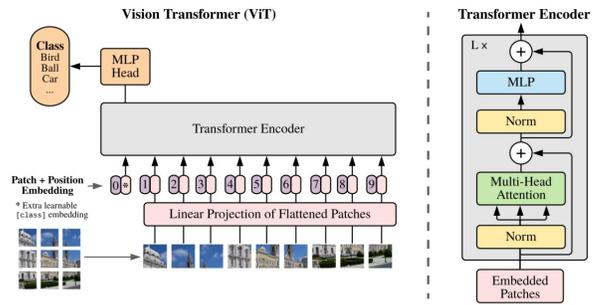


Fig. 20. The above Figure Illustrates the Architecture and the Patch Embedding of the Vision Transformer.

TABLE II. IT GIVES DETAILS ABOUT THE ACCURACY SCORES OBTAINED BY SOTA MODELS.

SOTA Methods	Top-1 accuracy	Top-5 accuracy
AlexNet	62.5	83
ZeNet	64.0	85.3
Overfeat	66.0	86.7
VGGNet	76.3	93.2
InceptionV2	79.9	95.1
InceptionV3	78.8	4.4
InceptionV4	80.1	95.1
ResNeXt	79.6	94.7
DPN	81.4	95.8
PNASNet	82.9	96.2
NASNet	82.7	96.2
NoisyStudent	88.4	98.7
EfficientNet	84.4	97.1
FixResNext	83.7	98.0
BiT	87.5	-
ViT	85.5	-

similar to that of BERT’s model class token. The architecture and patch embeddings are visually described in the Fig. 20.

The ViT model and the models considered for comparison were trained on certain parameters. The optimizer implied is adam with an initial learning rate set to default (0.001). Further, the  $\beta_1$  and  $\beta_2$  were set as 0.9 and 0.999 respectively. A weight decay of 0.1 was applied and it helped to construct good performance. Further, to fine-tune the model was initiated with a batch size of 512 and the optimizer as SGD. A small momentum was applied to improve the training speed. A maximum dropout of 0.1 was used for the ViT model trained on a large ImageNet dataset. Self-attention is provided by the transformer helped to combine the features extraction at the lower layer on focusing on the definite set of entities residing in the image.

VI. SUGGESTIONS FOR ARCHITECTURE CONSTRUCTION

Observing the state-of-the-art literature in the convnets there are certain factors observed in the construction of a novel architecture with greater performance and lower computational cost. These certain factors are constructed by analysing the minute parameters providing a better model. The performance

of various SOTA models is produced in Table II.

### A. Architecture Tips

The architecture tips fairly include all the factors influencing to develop a resilient architecture that extracts invariant features. Larger kernel size in the beginning layers of the convolution provides loss of information which degrades performance but, speeds the training process. Similarly, the higher the stride faster the model is trained but the accuracy degrades successively. Without adding residual connections developing a model just by increasing the depth can lead to the problem of degradation. A network architecture without bottleneck activations can explode in terms of computational cost hence, a set of bottleneck activations are to be implanted into the networks. The varying dimensionality of the receptive field can provide invariant features. An architecture trained on very small data cannot perform well on most of the unseen samples. Hence, solutions for these problems are explicitly provided for building a resilient convnet.

- A small receptive field provides a set of variant abstract features which carry detailed invariances.
- A smaller stride can eventually provide good representation by reducing the loss of the information through excessive pooling.
- To skip the problem of degradation, residual connections can be implied accordingly. Further, this improves the performance and also reduces the computational cost for deeper architectures
- A set of bottleneck connections can provide a generic feature representation and reduce computational effort while developing a convent width-wise.
- The asymmetric receptive fields with an appropriate bottleneck layer provide a greater representation of features.
- Finally, a model trained on multiple tasks with an appropriate set of samples can eventually improve in terms of performance acquiring state-of-the-art without much effort in parametric tuning.

### B. Optimization Tips

The optimization tips include developing representation in convnets by altering the hyperparameters and indicating their right implementation. The hyperparameters which are widely implied in the deep learning paradigm to observe a conventional change in the model behaviour during stochastic optimization are described in detail.

- **Dropout:** Dropout helps in generalizing the model by halting a set of neurons during training and releasing them during the validation or testing time. Hence, selecting the percentage of dropout is crucial. According to the present implementations, most of the research implies 50%. But it can be varied from 30-50% and choosing it in this interval provides good generalisation is densely connected networks.
- **Normalization:** Local response normalization implemented in AlexNet did not perform well in most of the

instances. As it has a huge number of hyperparameters it is a complicated task to imply such a normalization technique. Further, the Batch normalization technique was implied and it provided a great deal of succession in convnets by solving the problem of covariate shift. It is mostly utilized in the present research as it does not include very few parameters to tune and it works globally for variant architectures. Next, some problems were addressed in batch normalization and overridden by group normalization. It shows very minute performance variation when incurred on a smaller task but has a good variety when applied on large scale. Hence, group normalization can be used while developing a deeper model and for a small architecture batch normalization and group normalization works equivariantly.

- To skip the problem of degradation, residual connections can be implied accordingly. Further, this improves the performance and also reduces the computational cost for deeper architectures
- Lastly selecting optimizer and scheduling the learning rates is still tedious. Hence, most of the research imply SGD with varying learning rate based on the problem and varying momentum by observing the convergence. Hence, for building a small scale convnets Adam optimizer with small learning rates and high batch size is provided for good performance. Whereas, training a large-scale model the parameters might vary from the architecture and choice of dataset.

## VII. CONCLUSION

A detailed survey regarding the previous state-of-the-art is conducted. Additionally, a section explicitly gives an intuition of developing a good model with high performance and less computational power. This illustrates developing resilient architecture by tuning specific hyperparameters which as insightful in developing deep models.

Further, a set of details are not mentioned in this survey are to be described and held as our future direction. There a variant model which is developed in between these high-performance models which are not mentioned in this work. A set of small-scale models which resolve the problems in convolutions (i.e. Capsule Networks) does not describe explicitly. A detailed set of implementation framework which can reduce the effort of the implicit utility of architectures is not provided. These are taken as a challenge for the successive research and designing a framework overhauling these problems is chosen as future scope of work.

## ACKNOWLEDGMENT

We kindly thank the Department of IT for providing extensive support during the research. Further, we thank GITAM University for support and appropriate guidance.

## REFERENCES

- [1] O'Mahony N. et al. (2020) Deep Learning vs. Traditional Computer Vision. In: Arai K., Kapoor S. (eds) Advances in Computer Vision. CVC 2019. Advances in Intelligent Systems and Computing, vol 943. Springer, Cham. [https://doi.org/10.1007/978-3-030-17795-9\\_10](https://doi.org/10.1007/978-3-030-17795-9_10).

- [2] T. Kohonen, "The self-organizing map," *Proceedings of the IEEE*, vol. 78, no. 9, pp. 1464–1480, 1990.
- [3] G. Hinton, L. Deng, D. Yu, G. Dahl, A. Mohamed, N. Jaitly, A. Senior, V. Vanhoucke, P. Nguyen, T. Sainath, and B. Kingsbury, "Deep Neural Networks for Acoustic Modeling in Speech Recognition: The Shared Views of Four Research Groups," *IEEE Signal Processing Magazine*, vol. 29, no. 6, pp. 82–97, Nov. 2012.
- [4] Rabiner, Lawrence. "Fundamentals of speech recognition." *Fundamentals of speech recognition* (1993).
- [5] Collobert, R., Weston, J., Bottou, L., Karlen, M., Kavukcuoglu, K. and Kuksa, P., 2011. Natural language processing (almost) from scratch. *Journal of machine learning research*, 12(ARTICLE), pp.2493-2537.
- [6] A. Graves, A. Mohamed, and G. Hinton, "Speech recognition with deep recurrent neural networks," 2013 IEEE International Conference on Acoustics, Speech and Signal Processing, May 2013.
- [7] Stearns, S.D., 1985. of Aldapfive *Signal Processing*.
- [8] Stanley, W.D., Dougherty, G.R., Dougherty, R. and Saunders, H., 1988. *Digital signal processing*.
- [9] Bruderlin, A. and Williams, L., 1995, September. Motion signal processing. In *Proceedings of the 22nd annual conference on Computer graphics and interactive techniques* (pp. 97-104).
- [10] Ye, Jong Chul, Yoseob Han, and Eunju Cha. "Deep convolutional framelets: A general deep learning framework for inverse problems." *SIAM Journal on Imaging Sciences* 11.2 (2018): 991-1048.
- [11] He, Miao, and David He. "Deep learning based approach for bearing fault diagnosis." *IEEE Transactions on Industry Applications* 53.3 (2017): 3057-3065.
- [12] He, M. and He, D., 2020. A new hybrid deep signal processing approach for bearing fault diagnosis using vibration signals. *Neurocomputing*, 396, pp.542-555.
- [13] J. Pennington, R. Socher, and C. Manning, "Glove: Global Vectors for Word Representation," *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, 2014.
- [14] G. A. Miller, "WordNet," *Communications of the ACM*, vol. 38, no. 11, pp. 39–41, Nov. 1995.
- [15] Manning, C. and Schütze, H., 1999. *Foundations of statistical natural language processing*. MIT press.
- [16] L. A. Zadeh, "Outline of a New Approach to the Analysis of Complex Systems and Decision Processes," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. SMC-3, no. 1, pp. 28–44, 1973.
- [17] Vaswani, A., Shazeer, N., Parmar, N., Uszkoreit, J., Jones, L., Gomez, A.N., Kaiser, L. and Polosukhin, I., 2017. Attention is all, in "Advances in neural information processing systems 2017".
- [18] Manning, C.D., Surdeanu, M., Bauer, J., Finkel, J.R., Bethard, S. and McClosky, D., 2014, June. The Stanford CoreNLP natural language processing toolkit. In *Proceedings of 52nd annual meeting of the association for computational linguistics: system demonstrations* (pp. 55-60).
- [19] S. BOCCALETTI, V. LATORA, Y. MORENO, M. CHAVEZ, and D. HWANG, "Complex networks: Structure and dynamics," *Physics Reports*, vol. 424, no. 4–5, pp. 175–308, Feb. 2006.
- [20] Xu, K., Hu, W., Leskovec, J. and Jegelka, S., 2018. How powerful are graph neural networks? *arXiv preprint arXiv:1810.00826*.
- [21] Wu, Z., Pan, S., Chen, F., Long, G., Zhang, C. and Philip, S.Y., 2020. A comprehensive survey on graph neural networks. *IEEE transactions on neural networks and learning systems*.
- [22] Scarselli, F., Gori, M., Tsoi, A.C., Hagenbuchner, M. and Monfardini, G., 2008. The graph neural network model. *IEEE transactions on neural networks*, 20(1), pp.61-80.
- [23] Qu, M., Bengio, Y. and Tang, J., 2019, May. Gmn: Graph markov neural networks. In *International conference on machine learning* (pp. 5241-5250). PMLR.
- [24] Dwivedi, V.P., Joshi, C.K., Laurent, T., Bengio, Y. and Bresson, X., 2020. Benchmarking graph neural networks. *arXiv preprint arXiv:2003.00982*.
- [25] R. M. Haralick, K. Shanmugam, and I. Dinstein, "Textural Features for Image Classification," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. SMC-3, no. 6, pp. 610–621, Nov. 1973.
- [26] T. Ojala, M. Pietikainen, and T. Maenpää, "Multiresolution gray-scale and rotation invariant texture classification with local binary patterns," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 24, no. 7, pp. 971–987, Jul. 2002.
- [27] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A Fast Learning Algorithm for Deep Belief Nets," *Neural Computation*, vol. 18, no. 7, pp. 1527–1554, Jul. 2006.
- [28] Lu, D. and Weng, Q., 2007. A survey of image classification methods and techniques for improving classification performance. *International journal of Remote sensing*, 28(5), pp.823-870.
- [29] Wang, F., Jiang, M., Qian, C., Yang, S., Li, C., Zhang, H., Wang, X. and Tang, X., 2017. Residual attention network for image classification. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 3156-3164).
- [30] Chappelle, O., Haffner, P. and Vapnik, V.N., 1999. Support vector machines for histogram-based image classification. *IEEE transactions on Neural Networks*, 10(5), pp.1055-1064.
- [31] Dalal, N., & Triggs, B. (n.d.). Histograms of Oriented Gradients for Human Detection. 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR '05). doi:10.1109/cvpr.2005.177
- [32] Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., ... Fei-Fei, L. (2015). ImageNet Large Scale Visual Recognition Challenge. *International Journal of Computer Vision*, 115(3), 211–252. doi:10.1007/s11263-015-0816-y.
- [33] Viola, P., & Jones, M. (n.d.). Rapid object detection using a boosted cascade of simple features. *Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition*.
- [34] Girshick, Ross. "Fast r-cnn." *Proceedings of the IEEE international conference on computer vision*. 2015.
- [35] He, Kaiming, et al. "Mask r-cnn." *Proceedings of the IEEE international conference on computer vision*. 2017.
- [36] S. Ren, K. He, R. Girshick and J. Sun, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 39, no. 6, pp. 1137-1149, 1 June 2017.
- [37] H. Bay, A. Ess, T. Tuytelaars, and L. Van Gool, "Speeded-Up Robust Features (SURF)," *Computer Vision and Image Understanding*, vol. 110, no. 3, pp. 346–359, Jun. 2008.
- [38] T.-Y. Lin, M. Maire, S. Belongie, J. Hays, P. Perona, D. Ramanan, P. Dollár, and C. L. Zitnick, "Microsoft COCO: Common Objects in Context," *Lecture Notes in Computer Science*, pp. 740–755, 2014.
- [39] M. Everingham, L. Van Gool, C. K. I. Williams, J. Winn, and A. Zisserman, "The Pascal Visual Object Classes (VOC) Challenge," *International Journal of Computer Vision*, vol. 88, no. 2, pp. 303–338, Sep. 2009.
- [40] P. F. Felzenszwalb, R. B. Girshick, D. McAllester, and D. Ramanan, "Object Detection with Discriminatively Trained Part-Based Models," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 32, no. 9, pp. 1627–1645, Sep. 2010.
- [41] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Jun. 2016.
- [42] V. Caselles, R. Kimmel, and G. Sapiro, *International Journal of Computer Vision*, vol. 22, no. 1, pp. 61–79, 1997.
- [43] A. Geiger, P. Lenz, and R. Urtasun, "Are we ready for autonomous driving? The KITTI vision benchmark suite," 2012 IEEE Conference on Computer Vision and Pattern Recognition, Jun. 2012.
- [44] Toshev, A. and Szegedy, C., 2014. Deeppose: Human pose estimation via deep neural networks. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1653-1660).
- [45] Murphy-Chutorian, E. and Trivedi, M.M., 2008. Head pose estimation in computer vision: A survey. *IEEE transactions on pattern analysis and machine intelligence*, 31(4), pp.607-626.
- [46] Cao, Z., Simon, T., Wei, S.E. and Sheikh, Y., 2017. Realltime multi-person 2d pose estimation using part affinity fields. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 7291-7299).
- [47] J. Shotton, A. Fitzgibbon, M. Cook, T. Sharp, M. Finocchio, R. Moore, A. Kipman, and A. Blake, "Real-time human pose recognition in parts from single depth images," *CVPR 2011*, Jun. 2011.

- [48] T. B. Moeslund, A. Hilton, and V. Krüger, "A survey of advances in vision-based human motion capture and analysis," *Computer Vision and Image Understanding*, vol. 104, no. 2–3, pp. 90–126, Nov. 2006.
- [49] O. Ronneberger, P. Fischer, and T. Brox, "U-Net: Convolutional Networks for Biomedical Image Segmentation," *Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015*, pp. 234–241, 2015.
- [50] J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation," *2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Jun. 2015.
- [51] Jianbo Shi and J. Malik, "Normalized cuts and image segmentation," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 22, no. 8, pp. 888–905, 2000.
- [52] R. Girshick, J. Donahue, T. Darrell, and J. Malik, "Rich Feature Hierarchies for Accurate Object Detection and Semantic Segmentation," *2014 IEEE Conference on Computer Vision and Pattern Recognition*, Jun. 2014.
- [53] Haralick, R.M. and Shapiro, L.G., 1985. Image segmentation techniques. *Computer vision, graphics, and image processing*, 29(1), pp.100-132.
- [54] Zhang, Y.J., 1996. A survey on evaluation methods for image segmentation. *Pattern recognition*, 29(8), pp.1335-1346.
- [55] Antol, S., Agrawal, A., Lu, J., Mitchell, M., Batra, D., Zitnick, C.L. and Parikh, D., 2015. Vqa: Visual question answering. In *Proceedings of the IEEE international conference on computer vision* (pp. 2425-2433).
- [56] R. R. Selvaraju, M. Cogswell, A. Das, R. Vedantam, D. Parikh, and D. Batra, "Grad-CAM: Visual Explanations from Deep Networks via Gradient-Based Localization," *2017 IEEE International Conference on Computer Vision (ICCV)*, Oct. 2017.
- [57] D. Kahneman and D. T. Miller, "Norm theory: Comparing reality to its alternatives.," *Psychological Review*, vol. 93, no. 2, pp. 136–153, Apr. 1986.
- [58] V. D. Calhoun, T. Adali, G. D. Pearson, and J. J. Pekar, "A method for making group inferences from functional MRI data using independent component analysis," *Human Brain Mapping*, vol. 14, no. 3, pp. 140–151, 2001.
- [59] R. Krishna, Y. Zhu, O. Groth, J. Johnson, K. Hata, J. Kravitz, S. Chen, Y. Kalantidis, L.-J. Li, D. A. Shamma, M. S. Bernstein, and L. Fei-Fei, "Visual Genome: Connecting Language and Vision Using Crowdsourced Dense Image Annotations," *International Journal of Computer Vision*, vol. 123, no. 1, pp. 32–73, Feb. 2017.
- [60] P. Anderson, X. He, C. Buehler, D. Teney, M. Johnson, S. Gould, and L. Zhang, "Bottom-Up and Top-Down Attention for Image Captioning and Visual Question Answering," *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, Jun. 2018.
- [61] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, 521(7553), 436–444. doi:10.1038/nature14539.
- [62] Goodfellow, Ian, Yoshua Bengio, Aaron Courville, and Yoshua Bengio. *Deep learning*. Vol. 1, no. 2. Cambridge: MIT press, 2016.
- [63] LeCun, Y., Boser, B., Denker, J.S., Henderson, D., Howard, R.E., Hubbard, W. and Jackel, L.D., 1989. Backpropagation applied to handwritten zip code recognition. *Neural computation*, 1(4), pp.541-551.
- [64] LeCun, Yann, Y. Bengio et al. "Gradient-based learning applied to document recognition." *Proceedings of the IEEE* 86.11 (1998): 2278-2324.
- [65] Dumoulin, V. and Visin, F., 2016. A guide to convolution arithmetic for deep learning. *arXiv preprint arXiv:1603.07285*.
- [66] Krizhevsky, Alex, Ilya Sutskever, and Geoffrey E. Hinton. "Imagenet classification with deep convolutional neural networks." *Advances in neural information processing systems* 25 (2012): 1097-1105.
- [67] Nair, V. and Hinton, G.E., 2010, January. Rectified linear units improve restricted boltzmann machines. In *ICML*.
- [68] Jarrett, Kevin, Koray Kavukcuoglu, Marc' Aurelio Ranzato, and Yann LeCun. "What is the best multi-stage architecture for object recognition?." In *2009 IEEE 12th international conference on computer vision*, pp. 2146-2153. IEEE, 2009.
- [69] Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I. and Salakhutdinov, R., 2014. Dropout: a simple way to prevent neural networks from overfitting. *The journal of machine learning research*, 15(1), pp.1929-1958.
- [70] Zeiler M.D., Fergus R. (2014) Visualizing and Understanding Convolutional Networks. In: Fleet D., Pajdla T., Schiele B., Tuytelaars T. (eds) *Computer Vision – ECCV 2014*. ECCV 2014. *Lecture Notes in Computer Science*, vol 8689. Springer, Cham.
- [71] K. He, X. Zhang, S. Ren and J. Sun, "Deep Residual Learning for Image Recognition." *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Las Vegas, NV, USA, 2016, pp. 770-778, doi: 10.1109/CVPR.2016.90.
- [72] He, K., Zhang, X., Ren, S. and Sun, J., 2016, October. Identity mappings in deep residual networks. In *European conference on computer vision* (pp. 630-645). Springer, Cham.
- [73] G. Huang, Z. Liu, L. Van Der Maaten and K. Q. Weinberger, "Densely Connected Convolutional Networks," *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Honolulu, HI, USA, 2017, pp. 2261-2269, doi: 10.1109/CVPR.2017.243.
- [74] G. Huang, Z. Liu, G. Pleiss, L. Van Der Maaten and K. Weinberger, "Convolutional Networks with Dense Connectivity," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, doi: 10.1109/TPAMI.2019.2918284.
- [75] Sermanet, Pierre, et al. "Overfeat: Integrated recognition, localization and detection using convolutional networks. 2nd international conference on learning representations, iclr 2014." *2nd International Conference on Learning Representations, ICLR 2014* (2014).
- [76] Simonyan, Karen, and Andrew Zisserman. "Very deep convolutional networks for large-scale image recognition." In *ICLR 2015*.
- [77] Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S., Anguelov, D., Erhan, D., Vanhoucke, V. and Rabinovich, A., 2015. Going deeper with convolutions. In *Proceedings of the IEEE conference on computer vision and pattern recognition* (pp. 1-9).
- [78] Sergey Ioffe. 2017. Batch renormalization: towards reducing minibatch dependence in batch-normalized models. In *Proceedings of the 31st International Conference on Neural Information Processing Systems (NIPS'17)*. Curran Associates Inc., Red Hook, NY, USA, 1942–1950.
- [79] Huang, L., Yang, D., Lang, B. and Deng, J., 2018. Decorrelated batch normalization. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 791-800).
- [80] Ioffe, Sergey, and Christian Szegedy. "Batch normalization: Accelerating deep network training by reducing internal covariate shift." *International conference on machine learning*. PMLR, 2015.
- [81] Szegedy, Christian, Vincent Vanhoucke, Sergey Ioffe, Jon Shlens, and Zbigniew Wojna. "Rethinking the inception architecture for computer vision." In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 2818-2826. 2016.
- [82] Szegedy, Christian, Sergey Ioffe, Vincent Vanhoucke, and Alexander Alemi. "Inception-v4, inception-resnet and the impact of residual connections on learning." In *Proceedings of the AAAI Conference on Artificial Intelligence*, vol. 31, no. 1. 2017.
- [83] Ruder, S., 2016. An overview of gradient descent optimization algorithms. *arXiv preprint arXiv:1609.04747*.
- [84] Xie, Saining, Ross Girshick, Piotr Dollár, Zhuowen Tu, and Kaiming He. "Aggregated residual transformations for deep neural networks." In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 1492-1500. 2017.
- [85] Chen, Yunpeng, Jianan Li, Huaxin Xiao, Xiaojie Jin, Shuicheng Yan, and Jiashi Feng. "Dual path networks." *arXiv preprint arXiv:1707.01629* (2017).
- [86] Zoph, Barret, Vijay Vasudevan, Jonathon Shlens, and Quoc V. Le. "Learning transferable architectures for scalable image recognition." In *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 8697-8710. 2018.
- [87] Bello, I., Zoph, B., Vasudevan, V. and Le, Q.V., 2017, July. Neural optimizer search with reinforcement learning. In *International Conference on Machine Learning* (pp. 459-468). PMLR.
- [88] Bergstra, J. and Bengio, Y., 2012. Random search for hyper-parameter optimization. *Journal of machine learning research*, 13(2).
- [89] Liu, Chenxi, Barret Zoph, Maxim Neumann, Jonathon Shlens, Wei Hua, Li-Jia Li, Li Fei-Fei, Alan Yuille, Jonathan Huang, and Kevin Murphy. "Progressive neural architecture search." In *Proceedings of the European conference on computer vision (ECCV)*, pp. 19-34. 2018.

- [90] Tan, M. and Le, Q., 2019, May. Efficientnet: Rethinking model scaling for convolutional neural networks. In *International Conference on Machine Learning* (pp. 6105-6114). PMLR.
- [91] Touvron, Hugo, Andrea Vedaldi, Matthijs Douze, and Hervé Jégou. "Fixing the train-test resolution discrepancy." In *NeurIPS 2019*.
- [92] Xie, Qizhe, Minh-Thang Luong, Eduard Hovy, and Quoc V. Le. "Self-training with noisy student improves imagenet classification." In *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, pp. 10687-10698. 2020.
- [93] Kolesnikov A. et al. (2020) Big Transfer (BiT): General Visual Representation Learning. In: Vedaldi A., Bischof H., Brox T., Frahm JM. (eds) *Computer Vision – ECCV 2020*. ECCV 2020. *Lecture Notes in Computer Science*, vol 12350. Springer, Cham.
- [94] Alexey Dosovitskiy, Lucas Beyer, Alexander Kolesnikov, Dirk Weissenborn et al., "An image is worth 16X16 words: Transformers for image recognition at scale.", In *ICLR*, 2021.

# University Course Timetabling Model in Joint Courses Program to Minimize the Number of Unserved Requests

Purba Daru Kusuma<sup>1</sup>  
Computer Engineering  
Telkom University, Bandung, Indonesia

Abduh Sayid Albana<sup>2</sup>  
Industrial Engineering  
Institut Teknologi Telkom Surabaya, Surabaya, Indonesia

**Abstract**—This work proposes a novel course timetable model for the national joint courses program. In this model, the participants, both students and lecturers, come from different universities. It is different from most existing university course timetabling models where the environment is physical, and the system can dictate the timeslots and classrooms for the students and lecturers. The courses are delivered online in this model, so physical classrooms are no longer required, as was the case in most previous course timetabling studies. In this model, the matching process is conducted based on the assigned timeslots and the requested courses. The courses are elective rather than mandatory. Three metaheuristic methods are used to optimize this model: artificial bee colonies, cloud theory-based simulated annealing, and genetic algorithms. Due to the simulation process, the cloud theory-based simulated annealing performs best in minimizing the number of unserved requests. This method outperforms the two other metaheuristic methods, the genetic algorithm, and the artificial bee colony algorithm. According to the simulation results, when the number of students is low, the cloud theory-based simulated annealing has 91 percent fewer unserved requests than the genetic algorithm. When the number of students is large, this figure drops to 62%.

**Keywords**—Course timetabling; joint course program; artificial bee colony; simulated annealing; genetic algorithm; online course

## I. INTRODUCTION

In January 2020, the Ministry of Education and Culture of Indonesia launched a national program called Merdeka Belajar Kampus Merdeka (MBKM). This program is conducted for undergraduate students in Indonesia. Through this program, students can take courses or earn credits outside of their study program. For example, these students can take several courses from other universities. Besides, students can also take courses which are not related to their study program. For example, a computer engineering student can take management or accounting courses from outside his university. This general program is then followed by several joint programs. In this joint program, several universities provide several courses together. Each university provides several courses so that external students can attend these courses. In some programs, students can select universities and the related courses (lecturers) explicitly. In other programs, students just select the courses without knowing the lecturers who provide the selected courses so that the students cannot choose the lecturers. As a national program, the provided courses are conducted online so

that geographic barriers do not matter, for example, in rural and remote areas [1]. It also minimizes the cost due to providing the physical classrooms [1].

Despite the fact that this program gives benefits to students, especially in the flexibility, affordability, and accessibility aspects [1], there is a problem in arranging the courses. Students who follow this national program still need to attend the physical courses conducted at their own universities. The lecturers who participate in this program also teach at their own universities. Both students and lecturers have their own schedule. Based on that, schedule matching between lecturers and students in this national program becomes a critical issue.

Unfortunately, existing course timetabling models in many studies cannot be implemented directly to solve this problem. The main reason is that, in general, the existing course timetabling models were conducted for single department [2] or university [3,4]. The system has full authority to allocate the resources (lecturers, physical rooms, and timeslots) and manage the students. The system can dictate the timeslots for both students and lecturers. Besides, most course timetabling studies were conducted in a physical environment where the courses were conducted in physical rooms, so that the limited number of rooms became a constraint [5,6]. In this national joint course program, the courses are conducted online so that the physical rooms are not needed anymore. On the other hand, the system cannot dictate timeslots for both students and lecturers.

Based on this problem, this work aims to develop a course timetabling model that suits the circumstances of this national joint course program where the participants are students and lecturers from different universities. Both students and lecturers choose their available timeslots. A lecturer handles one specific course only. A student can take or request several courses provided by the program. The objective of this model is to minimize the number of unserved requests. In the context of a timetabling study, the number of unserved requests becomes the soft constraint.

Like the existing course timetabling studies where the models were optimized by using metaheuristic techniques, for example: genetic algorithm [7,8], simulated annealing [9,10], tabu search [2], and so on, this model is also optimized by using three metaheuristic methods: artificial bee colony algorithm, cloud theory based simulated annealing, and genetic

algorithm. The artificial bee colony and simulated annealing are chosen due to their advantage in finding global optimization by avoiding local optimal traps [11]. The cloud theory-based simulated annealing is a derivative of the basic simulated annealing that gives a faster process [12].

The contributions to this work are as followed:

- This work proposes a novel course timetabling for a joint online course program where the students and the lecturers come from many universities.
- The proposed model arranges course timetables based on the available timeslots and requested courses.
- Its objective is to minimize unserved requests, which is rare in many existing course timetabling studies.

This proposed model can be used practically in many joint courses program. It can be applied not only in national scale program, as it is stated in the opening paragraph, but in smaller scale. For example, universities with same foundation or same area (district or province) can make a joint courses program. Besides, the joint courses program can be conducted for universities with same subjects, such as computer science, finance, law, and so on. The key is that the joint program is conducted in voluntary and online based approach so that this proposed model can be applied.

This paper is organized as follows. The background, research purpose, and the contribution are explained in section one. The theoretical aspects of course timetabling and several recent studies in course timetabling are reviewed in Section two. The proposed model is described in Section three. The simulation and result are presented in Section four. The findings are discussed in Section five. The conclusion of this work and the future research potential are explained in Section six.

## II. RELATED WORK

A timetable can be defined in several ways. Aziz and Aizam [13] defined a timetable as a table with all the data of events and the information about these events, such as time and place. Alghamdi, Alhakami, Alsubait, and Baz [14] defined a timetable as a table of various events or activities with their schedule. Zhu, Li, and Li [7] defined timetabling as a process of distributing activities among limited resources (place and time). The timetabling problem can be categorized as an NP-complete problem, so it is difficult to find the general optimal solution [7].

The educational timetable problem has become the most well-known among the timetable studies. An educational timetable problem is a combinatorial problem with the objective of assigning a certain number of didactic activities to a certain room within certain timeslots [3]. The entities are courses, instructors, rooms, and registered students [5]. Educational timetabling can be divided into three categories: course timetabling, school timetabling, and examination timetabling [7]. Course timetabling is assigning lecturers and courses to timeslots, rooms, and other facilities [7]. School timetabling involves assigning teachers or instructors to courses based on their specialization [7]. School timetabling

can also be called curriculum-based course timetabling [7]. Examination timetabling is assigning exams into rooms and timeslots [7]. Several factors that affect the educational timetable design are the number of courses, the average number of lectures per day, the targeted free timeslots per day, and targeted off-days in a week [14].

There are two types of constraints in the timetabling problem: hard constraints and soft constraints. Hard constraints are constraints or rules that cannot be violated [15]. Soft constraints are constraints that can improve the performance of the timetable if they are not violated [15]. Several common hard constraints are as follows:

- A lecturer can only teach a course at a certain time [3,16].
- A student cannot attend more than one lecture at one time [5].
- The attendants cannot surpass the room's capacity [3,5].
- The timeslot must be conducted within a certain time window [3].

Meanwhile, there are several soft constraints used in several educational timetabling studies. These soft constraints are as follows:

- There is a minimum number of courses in a day for the students [5].
- There is a maximum number of courses in a day for the lecturers [5,6].
- Lecturers may have preferred teaching timeslots [16].
- Lecturers may have minimum working days [17].
- Lecturers may have preferred classrooms [6].
- The last timeslots of the day should be avoided [2].

There are many studies conducted on this educational timetabling problem. Each study is developed based on its specific circumstances, objectives, and methods. Most studies use computational methods, especially metaheuristic methods, to find the optimal solution. Table I shows the recent studies on the educational timetable problem with their objectives and methods. These studies were conducted from 2016 to 2021. They are presented chronologically.

There are several notes on this presented literature. First, most studies on the course timetabling problem were conducted in face-to-face interaction between students and lecturers, so the number of limited physical rooms becomes a constraint. Second, all these studies were conducted in a department or university so that the system could dictate the timeslot allocation.

Based on these notes, this work proposes a novel course timetabling model due to specific circumstances in the national joint courses program. These circumstances are not found in the existing course timetabling studies. First, this joint program is conducted online. Second, the system cannot dictate the timeslots for both students and lecturers. The matching process is conducted based on the available timeslots that are allocated

by the students and lecturers. Third, the courses are open elective so that students can choose any course provided in the system and they can choose more than one course. Like the existing studies, this work will use several metaheuristic techniques to optimize the solution. These techniques will be compared to each other.

TABLE I. RECENT STUDIES IN EDUCATIONAL TIMETABLING PROBLEM

Authors	Objectives	Methods
[4]	improve resources utilization	genetic algorithm
[5]	minimize conflicts	genetic algorithm
[8]	minimize penalty	multi-objective genetic algorithm, hill climbing, simulated annealing
[17]	minimize total sum of penalty points	mixed integer linear programming (MILP), large neighborhood search
[10]	minimize clashes	genetic algorithm, simulated annealing
[6]	optimize resources	genetic algorithm
[19]	minimize the number of classrooms	linear programming
[2]	minimize students' maximum number of events per day, avoid the usage of the last timeslot of the day	tabu search, variable neighborhood search
[20]	improve accuracy	genetic algorithm, supervised learning (regression and classification)
[22]	maximize lecturers' presence time and education quality	three-stage heuristic algorithm
[3]	minimize idle time	genetic algorithm
[18]	reduce redundant workload, improve classroom seat utilization	genetic algorithm, fuzzy pattern algorithm
[21]	minimize soft constraints	integer linear programming (ILP), branch-and-bound algorithm

### III. PROPOSED MODEL

This model consists of several entities. A student is a person who takes a course or several courses. A lecturer is a person who delivers courses to students. A course is a unit of teaching that is delivered by a lecturer, for example: artificial intelligence, machine learning, mobile programming, and so on. A class is a group of students that take the same course and are taught by the same lecturer with the same timeslot. A Request is a course requested by a student.

The system consists of a certain number of students and lecturers. The students come from any universities, and so do the lecturers. The relationships between students and lecturers are many to many. It means a student can be taught by more than one lecturer depending on the number of courses that this student takes. The number of students is greater than the number of lecturers. Meanwhile, a lecturer can teach many students. This relation is shown in Fig. 1.

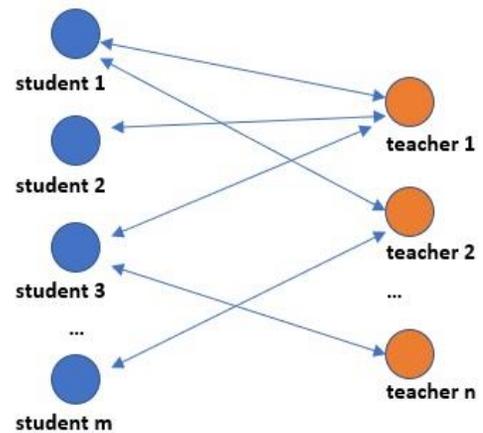


Fig. 1. Student-Lecturer Relationship.

In this system, a lecturer can only teach a course due to the expertise factor. Meanwhile, a student can take several courses. Both lecturers and students assign several available timeslots. These timeslots are week-based timeslots. It means there are a certain fixed number of timeslots in a week. The number of timeslots that are booked by a lecturer represents the number of classes that are taught by him or her. A student can take a course that is delivered by a lecturer as long as the course in this class is the same as the course that is taken by this student and the class timeslot is the same as the student's timeslot. The illustration of this relationship is shown in Fig. 2.

The explanation of Fig. 2 is as follows. There is a lecturer who teaches a course, for example, course A. He assigns two timeslots for this course so that he handles two classes, class 1 and class 2. Meanwhile, there are five students who want to take course A. Based on the matched timeslot, three students (student 1, student 2, and student 3) are assigned to class 1 and two students (student 4 and student 5) are assigned to class 2.

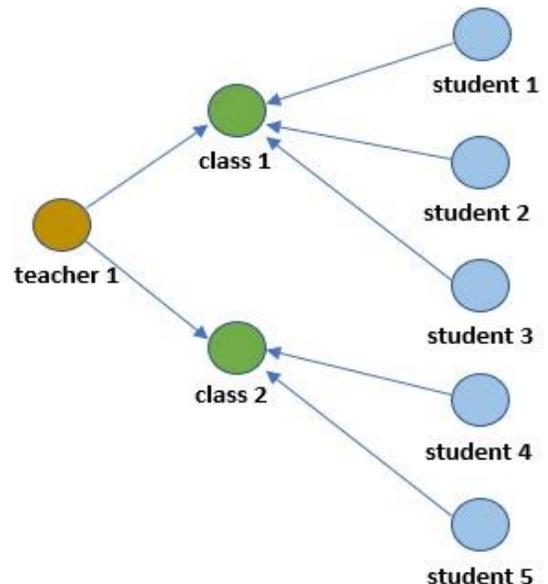


Fig. 2. Illustration of Classes.

This model is developed based on several hard constraints as follows:

- Students are not permitted to attend more than one class at a time [3].
- A lecturer is not permitted to teach more than one class at a time [5].
- A student cannot be assigned to a class where its timeslot is outside of his available timeslots [3].
- A student cannot be assigned to a class where the course is not his requested course.
- Students cannot request a course outside of the provided courses.
- A lecturer cannot teach a class where the timeslot is outside of his available timeslots [3].
- The number of class attendants cannot exceed the maximum capacity of the class [5].
- A class cannot be plotted outside of the available timeslots in a week.

This model is also developed by using several annotations as follows:

$c$	class
$c_{sel}$	selected class
$C$	set of classes
$C_{pos}$	set of possible classes
$s$	student
$S$	set of students
$l$	lecturer
$L$	set of lecturers
$n$	number of entities
$o$	course
$O$	set of courses
$q$	quantity (number of attendants)
$q_{max}$	maximum quantity
$r$	request
$R$	set of requests
$v$	status
$t$	timeslots
$T$	set of timeslots
$T_{pos}$	set of possible timeslots
$u$	unserved request
$U$	set of unserved requests
$v_q$	class availability status based on capacity
$v_t$	class availability status based on timeslot
$v_o$	class availability status based on course
$v_{at}$	student's availability status at certain timeslot

The objective of this model is to minimize the number of unserved requests. This objective is formalized by using (1) and (2). Equation (2) shows that the unserved request is a request where its status is 0. Meanwhile, if this request is served, its status will be 1. In this system, a request can be unserved because of several problems. First, there is a mismatch between the timeslot of the request and the timeslot of the available classes for the same course. Second, there is a

class or several classes whose course is the same as the course of the request, and the timeslot of the class is also matched, but the number of attendants has reached the maximum capacity of this class.

$$\min(n(U)) \quad (1)$$

$$u = r | v_r(r) = 0 \quad (2)$$

At the beginning, both the lecturers and the students make preparations. The lecturers assign their own timeslots or classes. Meanwhile, the students choose courses that they want to take and their available timeslots in a week. This lecturer's set up is formalized by using (3) and (7). Meanwhile, the student's set up is formalized by using (8) and (10).

$$C(l) = \{c | o(l) = o(c) \wedge c \in C\} \quad (3)$$

$$n(C(l)) = n(T(l)) \quad (4)$$

$$T(l) = \{t | t \in T\} \quad (5)$$

$$t(c_i) \neq \forall t(c) | c \in C(l) \wedge c_i \in C(l) \wedge c \neq c_i \quad (6)$$

$$n(C) = \sum_{v_l} n(C(l)) \quad (7)$$

The explanations for (3) to (7) are as follows. Equation (3) declares that all classes that are handled by a lecturer must have the same course as the lecturer. Equation (4) shows that the number of classes handled by a lecturer is equal to this lecturer's number of timeslots. Equation (5) shows that the lecturer's timeslots must be within the allocated timeslots in a week. The hard constraint where a lecturer can only visit one class in a timeslot is formalized in (6). Equation (7) shows that the number of classes is equal to the accumulation of the number of classes of all lecturers.

$$R(s) = \{r | o(r) \in O\} \quad (8)$$

$$T(s) = \{t | t \in T\} \quad (9)$$

$$n(R) = \sum_{v_s} n(R(s)) \quad (10)$$

The explanation of (8) to (10) is as follows. Equation (8) states that student can request courses within the provided courses. Equation (9) states that the students' timeslots must be within the provided timeslots in a week. Equation (10) shows that the total number of requests is the accumulation of all students' requests.

After setup, the next process is the matching process. This process is conducted iteratively from the first request to the last request. The matching order is shuffled so that the first request is not prioritized rather than the last process. Each request consists of two attributes: the student and the course. This matching process is formalized by using (11) to (17).

$$c_{sel}(r) = rand(C_{pos}(r)) \quad (11)$$

$$C_{pos}(r) = \{c | v_q(c) = 1 \wedge v_t(r, c) = 1 \wedge v_o(r, c) = 1\} \quad (12)$$

$$v_q(c) = \begin{cases} 1, & q_c(c) < q_{max} \\ 0, & else \end{cases} \quad (13)$$

$$v_t(r, c) = \begin{cases} 1, & \exists t_{pos}(s(r)) = t(c) \\ 0, & else \end{cases} \quad (14)$$

$$T_{pos}(s(r)) = \{t | t \in T(s) \wedge v_{at}(t, s) = 1\} \quad (15)$$

$$v_{at}(t, s) = \begin{cases} 1, \forall t(s), \exists t(r(s)) = t \\ 0, else \end{cases} \quad (16)$$

$$v_o(r, c) = \begin{cases} 1, o(r) = o(c) \\ 0, else \end{cases} \quad (17)$$

The explanation of (11) to (17) is as follows. Equation (11) shows that the class is selected randomly among the possible classes for the request. Equation (12) states that the possible class must meet three aspects: capacity, time, and course. Equation (13) shows that the class is available if its current number of attendants is still less than its maximum capacity. Equation (14) shows that the class meets the time aspect if there exists a possible student's timeslot that is the same as the timeslot of this class. Equation (15) shows that the set of possible timeslots of the student consists of the student's timeslots that are still available. Equation (16) shows that the student's timeslot is available if it has not been occupied by any other student's request. Equation (17) shows that the class meets the course aspect if the course of the class is the same as the course of the request.

In this work, we compare three metaheuristic algorithms: the genetic algorithm (GA) [18], cloud theory-based simulated annealing algorithm (CSA) [12], and artificial bee colony algorithm (ABC) [23]. As metaheuristic algorithms, they consist of a stochastic approach, especially during the initialization process and the improvement process. In the genetic algorithm method, the half best solution becomes the new generations during the reproduction process.

All these algorithms are population-based algorithms. A population consists of individuals or solutions. An individual consists of an array of requests. Each element consists of attributes: request, student, and class.

During the improvement process, the pairwise interchange is conducted by selecting a served request, finding a new class, assigning this request to the new class, and then allocating the abandoned seat to another unserved request. This pairwise interchange process is formalized by the use of algorithm 1.

---

**Algorithm 1: pairwise interchange**

---

```
1   $r_{sel1} = \text{rand}(R, v_r(r) = 1)$ 
2   $c_{sel1} = \text{rand}(C, r_{sel1})$ 
3  if found ( $c_{sel1}$ ) then
4    assign ( $r_{sel1}, c_{sel1}$ )
5   $r_{sel2} = \text{rand}(U)$ 
6  if found ( $r_{sel2}$ ) then
7     $c_{sel2} = \text{rand}(C, r_{sel2})$ 
8  if found ( $c_{sel2}$ ) then
9    assign ( $r_{sel2}, c_{sel2}$ )
10 end if
11 end if
12 end if
```

---

#### IV. SIMULATION AND RESULT

This proposed model is then implemented into the course timetabling simulation. As mentioned before, there are three metaheuristic techniques that are used to optimize the model:

the genetic algorithm (GA), cloud theory-based simulated annealing algorithm (CSA), and artificial bee colony algorithm (ABC). The objective function applied in these algorithms is to minimize the number of unserved requests. The reason is that this objective function is related to the objective of this work and proposed model.

The technical parameters used in these metaheuristic algorithms are as follows. In the GA, the population size is 10 individuals and the maximum number iterations is 100 iterations. In the CSA, the population size is 5 solutions, the initial temperature is 100, the termination temperature 50, and the number of iterations is 10. In the ABC, the population size is 10 bees, the maximum number of iterations is 50 iterations, and the limit is 30.

The scenario used in this simulation is as follows. In the beginning, a certain number of students and lecturers are generated. A lecturer teaches only one course. A student can request several courses. Both students and lecturers select their available timeslots. The number of timeslots that are chosen by the lecturer represents the number of classes that he will handle. The students will be allocated based on the timeslots that they have chosen. The simulation then runs based on this initial setting. During the simulation process, students will be matched with the available classes based on their selected course timeslots. At the end of the simulation, certain requests may be unserved due to a mismatch.

There are two simulations conducted in this work. The observed parameter is the number of unserved requests. This parameter also becomes the fitness function of these three metaheuristic techniques (minimizing the number of unserved requests). There are several adjusted parameters that are set as default. There are five courses in the system. The number of lecturers is 20. The maximum capacity of each class is 40 attendants. There are 20 timeslots that can be chosen by both students and lecturers. The number of courses that are requested by a student is generated randomly and follows a normal distribution. The average number of requests is 3 courses. The number of timeslots that are chosen by both lecturers and students is also generated randomly and it follows normal distribution.

The first simulation is conducted to observe the relation between the number of students with the number of unserved requests. The number of students ranges from 400 to 600 students, with a step size of 20 students. The average number of chosen timeslots is 3 timeslots. The result is shown in Fig. 3.

In Fig. 3, it is shown that the number of unserved requests increases due to the increase in the number of students. This trend occurs in all methods. The rationale for this condition is that demand is increasing, whereas supply is still the same, so the scarcity is also increasing. Compared among methods, cloud theory-based simulated annealing performs as the best model in creating the lowest number of unserved requests. On the other hand, the genetic algorithm performs as the worst method. The artificial bee colony performs moderately. When the number of students is low (400), the simulated annealing algorithm generates 91% fewer unserved requests than the genetic algorithm. When the number of students is large (i.e., 600), the gap narrows to 62 percent.

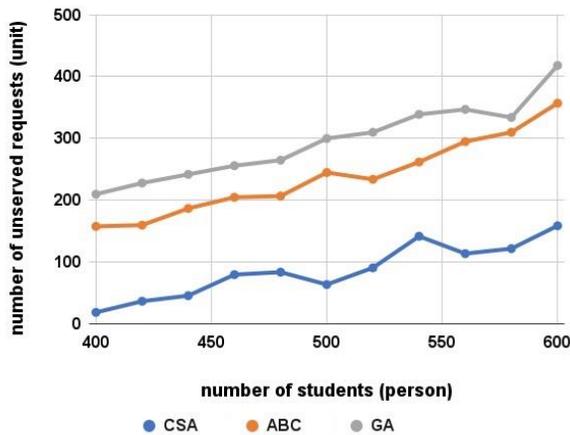


Fig. 3. Relation between the Number of Students and the Number of unserved Requests.

The second simulation is conducted to observe the relation between the average number of timeslots and the number of unserved requests. The average number of timeslots ranges from 3 to 5 timeslots. The number of students is 500 students. The result is shown in Fig. 4.

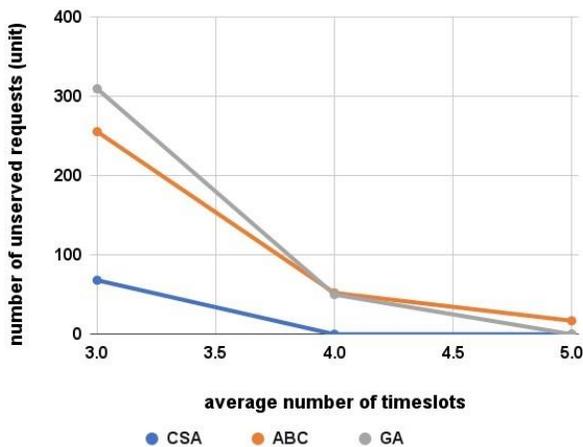


Fig. 4. Relation between the Average Number of Timeslots and the Number of unserved Requests.

In Fig. 4, it is shown that the number of unserved requests decreases due to the increase in the average number of timeslots. This condition occurs in all metaheuristic methods. The rationale is as follows. The increasing of the lecturers' timeslots means the increasing of the supply (number of classes). On the other hand, the increasing of the students' timeslots means the matching possibility increases too. When comparing among methods, the cloud theory-based simulated annealing performs as the best model. In the beginning, simulated annealing created the lowest number of unserved customers. Starting with four timeslots, the simulated annealing performs zero unserved requests. When the average number of timeslots is 3 timeslots, the artificial bee colony performs better than the genetic algorithm. The artificial bee colony has 17% fewer unsatisfied requests than the genetic algorithm. Meanwhile, when the average number of timeslots

is 4 timeslots, their number of unserved requests is almost equal. Starting from 6 average timeslots, the genetic algorithm performs zero unserved requests. On the other hand, the artificial bee colony still creates a positive number of unserved requests, although its value is low (17 unserved requests).

## V. DISCUSSION

In general, these three metaheuristic models can be used to optimize the proposed course timetabling model. In the first simulation, the number of unsatisfied requests remains less than 50%. When the supply is fixed, the number of unserved requests is proportional to the demand (the number of students), as is shown in Fig. 3. On the other hand, when the demand is fixed, the increase in the supply (lecturers' number of timeslots) makes the number of unserved requests decrease. After the zero unserved requests are achieved, the increase in supply does not change the condition.

Compared among the metaheuristic techniques, the cloud theory-based simulated annealing outperforms the two other methods, the genetic algorithm, and the artificial bee colony. This performance comes from two aspects. First, in its basic form, simulated annealing is designed to achieve global optimization by avoiding local optimal traps [11]. This process is conducted by tolerating current worse solutions with a certain degree of probability during the iteration process, especially at the beginning of temperature declination [11]. Second, cloud theory based simulated annealing improves the basic simulated annealing by conducting multiple individuals (solutions) that act independently [12]. The final best solution can be selected among the population after the iteration process ends [12].

The artificial bee colony performs the second-best method. Like simulated annealing, the artificial bee colony can also avoid the local optimal trap. In an artificial bee colony, the local optimal trap avoidance is conducted during the scout-bee phase by finding new alternative solutions, i.e., diversifying the search process [24]. This phase is taken after the onlooker-bee phase and the employed-bee phase, whose objective is to intensify the solution around the current solution [24]. Unfortunately, the process of finding an absolute new solution is not conducted in every iteration. As previously stated, this concept differs from simulated annealing in that the local optimal trap avoidance can be performed with a high degree of probability in every iteration [11].

The genetic algorithm performs as the worst solution in creating a low number of unserved requests. This performance occurs because, in its basic form, the genetic algorithm cannot avoid the local optimal trap, despite the fact that it has been widely used to optimize the course timetabling problem in [4-6]. In genetic algorithms, new offspring are generated based on the best individuals as the improvement mechanism [11].

## VI. CONCLUSION

This work has demonstrated that the proposed course timetabling model can be used in the national joint courses program that is attended by students and lecturers from different universities. This model also meets the requirements that are stated as the hard constraints. Due to the simulation process, the cloud theory-based simulated annealing performs

best in minimizing the number of unserved requests. This method outperforms the two other metaheuristic methods, the genetic algorithm, and the artificial bee colony algorithm. Due to the simulation results, when the number of students is low, the number of unserved requests for the cloud theory-based simulated annealing is 91 percent lower than the genetic algorithm. When the number of students is large, this figure falls to 62 percent. This performance is achieved because of the characteristics of cloud theory-based simulated annealing in achieving global optimization by avoiding local optimal traps.

This model is developed based on several limitations. First, there is not any prioritization in the lecturers and courses selection. In certain conditions, a student prefers certain lecturers rather than other lecturers. It is because in the same course, some lecturers are more favorite or popular rather than other lecturers. For example, lecturers from higher-ranked universities may be more popular than lecturers from lower-ranked universities. A student may also prefer certain courses to other courses. It means a student may tolerate losing less preferred courses or lecturers. Based on this circumstance, the proposed model of this current work can be extended or improved by concerning this preference factor.

#### ACKNOWLEDGMENT

This work was funded and supported by Telkom University, Indonesia.

#### REFERENCES

- [1] S. Dhawan, "Online learning: a panacea in the time of COVID-19 crisis", *Journal of Educational Technology Systems*, vol. 49, no. 1, pp. 5-22, 2020.
- [2] A. Muklason, R. G. Irianti, and A. Marom, "Automated course timetabling using tabu-variable neighbourhood search based hyperheuristic algorithm", *Procedia Computer Science*, vol. 161, pp. 656-664, 2019.
- [3] I. Balan, "A new genetic approach for course timetabling problem", *Journal of Applied Computer Science & Mathematics*, vol. 15, no. 1, pp. 9-14, 2021.
- [4] A. Al-Majmar and T. H. Al-Shfaq, "Solving of lectures timetabling problem and automatic timetable generation using genetic algorithm", *International Journal of Advanced Research in Computer and Communication Engineering*, vol. 5, no. 9, pp. 505-512, 2016.
- [5] M. Assi, B. Halawi, and R. A. Haraty, "Genetic algorithm analysis using the graph coloring method for solving the university timetable problem", *Procedia Computer Science*, vol. 126, pp. 899-906, 2018.
- [6] D. M. Premasiril, "University timetable scheduling using genetic algorithm approach case study: Rajarata University of Sri Lanka", *Journal of Engineering Research and Application*, vol. 8, no. 12, pp. 30-35, 2018.
- [7] K. Zhu, L. D. Li, and M. Li, "A survey of computational intelligence in educational timetabling", *International Journal of Machine Learning and Computing*, vol. 11, no. 1, pp. 40-47, 2021.
- [8] C. Akkan and A. Gulcu, "A bi-criteria hybrid genetic algorithm with robustness objective for the course timetabling problem", *Computers and Operations Research*, vol. 90, pp. 23-32, 2018.
- [9] R. A. O. Vrieling, E. A. Jansen, E. W. Hans, and J. van Hillegersberg, "Practices in timetabling in higher education institutions: a systematic review", *Annals of Operations Research*, vol. 275, no. 1, pp. 145-160, 2019.
- [10] S. Susan and A. Bhutani, "Data mining with association rules for scheduling open elective courses using optimization algorithms", *Proceeding of International Conference on Intelligent Systems Design and Application*, Cham, 2018.
- [11] A. P. Engelbrecht, *Computational Intelligence: An Introduction*, 2nd ed., Wiley: West Sussex, 2007.
- [12] C. L. Hsu, W. C. Lin, L. Duan, J. R. Liao, C. C. Wu, and J. H. Chen, "A robust two-machine flow-shop scheduling model with scenario-dependent processing times", *Discrete Dynamics in Nature and Society*, article ID: 3530701, pp. 1-16, 2020.
- [13] N. L. A. Aziz and N. A. H. Aizam, "A brief review on the features of university course timetabling problem", *AIP Conference Proceedings*, vol. 2016, no. 1, pp. 1-7, 2016.
- [14] S. L. M. Sainte, R. Jan, A. Al-Matouq, and S. Alabduhadi, "The impact of timetable on student's absences and performance", *PloS ONE*, vol. 16, no. 6, pp. 1-22, 2021.
- [15] H. Alghamdi, H. Alhakami, T. Alsubait, and A. Baz, "A review of optimization algorithms for university timetable scheduling", *Engineering, Technology, & Applied Science Research*, vol. 10, no. 6, pp. 6410-6417, 2020.
- [16] R. Ansari and N. Saubari, "Application of genetic algorithm concept on course scheduling", *IOP Conference Series: Material Science Engineering*, vol. 821, pp. 1-6, 2020.
- [17] M. Lindahl, M. Sorensen, and T. R. Stidsen, "A fix and optimize matheuristic for university timetabling", *Journal of Heuristics*, vol. 24, pp. 645-665, 2018.
- [18] J. Xu, "Improved genetic algorithm to solve the scheduling problem of college English course", *Complexity*, article ID: 7252719, pp. 1-11, 2021.
- [19] N. K. Oladejo, A. Abolarinwa, S. A. Salawu, M. O. Bamiro, and A. F. Lukman, "Application of optimization principles in classroom allocation using linear programming", *International Journal of Mechanical Engineering and Technology*, vol. 10, no. 1, pp. 874-885, 2019.
- [20] P. Kenekayoro, "Incorporating machine learning to evaluate solutions to the university course timetabling problem", *Covenant Journal of Informatics & Communication Technology*, vol. 7, no. 2, pp. 18-35, 2019.
- [21] N. M. Arratia-Martinez, C. Maya-Padron, and P. A. Avila-Torres, "University course timetabling problem with professor assignment", *Mathematical Problems in Engineering*, article ID: 6617177, pp. 1-9, 2021.
- [22] M. M. Tavakoli, H. Shirouyehzad, F. H. Lotfi, and S. E. Najafi, "Proposing a novel heuristic algorithm for university course timetabling problem with the quality of courses rendered approach: a case study", *Alexandria Engineering Journal*, vol. 59, pp. 3355-3367, 2020.
- [23] H. Xuan, H. Zhang, and B. Li, "An improved discrete artificial bee colony algorithm for flexible flowshop scheduling with step deteriorating jobs and sequence-dependent setup times", *Mathematical Problems in Engineering*, article ID: 8520503, pp. 1-13, 2019.
- [24] B. Peng, L. Wu, Y. Wang, and Q. Wu, "Solving maximum quasi-clique problem by a hybrid artificial bee colony approach", *Information Sciences*, vol. 578, pp. 214-235, 2021.

# Symbolic Representation-based Melody Extraction using Multiclass Classification for Traditional Javanese Compositions

Arry Maulana Syarif<sup>1</sup>, Khafiizh Hastuti<sup>4</sup>  
Faculty of Computer Science  
Universitas Dian Nuswantoro  
Semarang, Indonesia

Azhari Azhari<sup>2</sup>, Suprpto Suprpto<sup>3</sup>  
Department of Computer Science and Electronics  
Universitas Gadjah Mada  
Yogyakarta, Indonesia

**Abstract**—Traditional Javanese compositions contain melodies and skeletal melodies. Skeletal melodies are an extraction form of melodies. The melody extraction problem is similar to the chord detection in Western music, where chords are extracted from a melody. This research aims to develop a melody extraction system for traditional Javanese compositions. Melodies which have a time series data structure were designed as a part of the supervised learning problem to be solved using the pattern recognition technique and the Feed-Forward Neural Networks method. The melody data source uses a symbolic format in the form of sheet music. The beats in melodies data are used as the input and notes in skeletal melodies are used as the target. An FFNN multi-class classifier was built with six classes as the targets, where the class represents notes of the musical scale system. The network evaluation was conducted using accuracy, precision, recall, specificity and F-1 score measurements.

**Keywords**—Melody extraction; symbolic representation-based; multiclass classification; feed-forward neural network; Gamelan

## I. INTRODUCTION

This research is part of a program to preserve traditional Javanese music using artificial intelligence methods with the expectation of preserving the authenticity of the compositions throughout the ages. Traditional Javanese compositions known as Gamelan music consist of melodies and balungan (Javanese: skeletal melodies). The Gamelan composers create compositions by first composing a melody and then extracting it into a skeletal melody, or constructing a skeletal melody first which is then filled with harmonization into a melody. The melody extraction to form skeletal melodies is chosen as the background problems in this research. Skeletal melodies can be analogous to chords in Western music, and the challenge in this research is similar to the problem of determining chords to accompany the melody.

Chord detection uses time series data, and such data structures can be designed as part of a supervised learning problem to be solved using pattern recognition techniques. Chords are detected by extracting features from audio sources, filtering and matching the patterns [1], and this method has been used in various works [2-7]. Instead of using audio sources and performing feature extraction, a symbolic representation approach is proposed using sheet music as the

dataset source. Learning directly from sheet music is to get original and complete information of the musical elements that is difficult to obtain through feature extraction from audio sources. Hence, a new method for a symbolic representation-based melody extraction was proposed by recognizing the note sequence pattern based on musical theory, which is carried out by calculating the duration of the notes. The proposed method in this research is in line with what [8] stated, the music theory approach without audio can be used as a complementary technique in the field of music information retrieval. In a different context, musical theory is disproved by using chord sequences found in the dataset so that theoretically unusual chord sequences are possible to learn [9]. The proposed method is also similar to that stated by [9] in the context of using all the sequences of notes or chords found in the dataset but the metrical structure in musical theory is still used as a reference to avoid metrical structure errors in composition. Further, a multi-class classifier using the Feed-Forward Neural Networks (FFNN) method was used to build a melody extraction system for traditional Javanese compositions. The FFNN network was trained using melodies as input and skeletal melodies as the output.

The availability of datasets is a challenge in building a melody extraction system for traditional Javanese compositions. Unlike western music, which has a well-organized composition documentation system that supports easy data access, traditional Javanese composition data in sheet music format is not well documented and difficult to access online. This causes a limited number of datasets. Data augmentation is a challenge in itself, and proper data mapping techniques are needed to increase the cardinality of the data.

This paper is structured as follows. Section II introduces traditional Javanese compositions. Section III describes the related work of chord detection which has in principle a similar task to melody extraction, as well as research on traditional Javanese compositions utilizing an AI approach. Section IV describes the methodology used in developing a melody extraction system for traditional Javanese compositions which consists of data preparation, beat detection, vector length adjustment, data mapping and feature selection, and binary representation. Section V discusses training and evaluation. Finally, Section VI discusses conclusions and future works.

## II. THE TRADITIONAL JAVANESE COMPOSITION

Traditional Javanese music called karawitan consists of a set of music instruments called Gamelan and compositions with or without vocal called gendhing. Gamelan consists of two musical scale systems, which are pelog and slendro. The pelog scale system consists of seven notes: 1, 2, 3, 4, 5, 6, 7. The slendro scale system consists of five notes: 1, 2, 3, 5 and 6. The pelog and slendro scale systems are different in their tuning. Moreover, there are dotted notes as addition that represent moments of silence. Based on their function in performing the composition, a set of Gamelan instruments is divided into three groups, which are ricikan garap, ricikan balungan and structural ricikan. The group of ricikan garap contains instruments to play the melody parts, such as gender, rebab, suling and gambang. The group of ricikan balungan contains instruments to play the skeletal melody parts, such as saron, demung, peking and slenthem. The group of structural ricikan contains instruments to play notes that form the type of compositions, such as kethuk, kempyang, kenong, kempul and gong.

There is a musical mode system called pathet on both the pelog and slendro scale systems. This system controls the dominant notes at certain positions in the sequence. The slendro mode system consists of manyura, nem and sanga, while the pelog mode system consists of barang, lima and nem. There are types of compositions, such as ladrang, lancaran and ketawang. The type of compositions is determined based on the number of beats in the skeletal melody, and it can be identified based on the play of the instruments of the group of structural ricikan. Fig. 1 shows illustration of the traditional Javanese compositions and Gamelan known as Gamelan music.

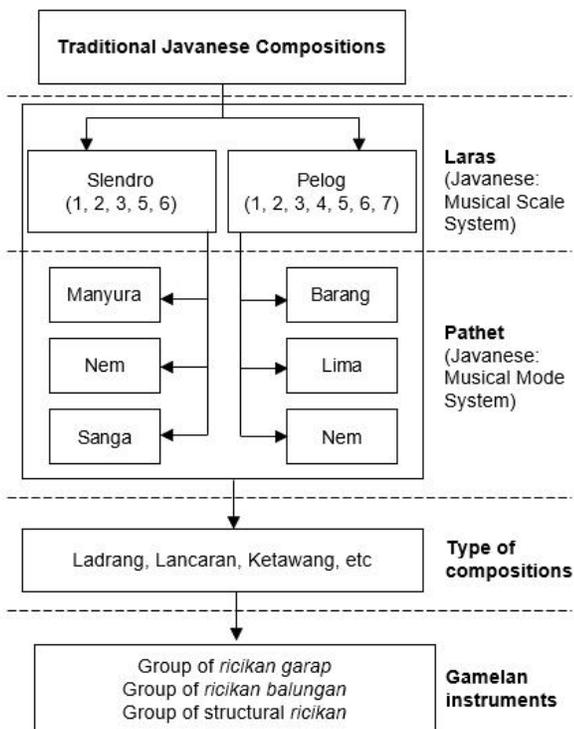


Fig. 1. Illustration Traditional Javanese Compositions and Gamelan Instruments.

Ladrang Wilujeng, Laras Slendro Pathet Manyura

(a)	•	•	6	•	ī	5	ī	6								
(b)	•	•	•	•	6	6	•6ī	5	•	6	ī	2̣	•3̣	ī2̣	ī	6
(a)	3	5	5	•	ī	6	5	3	2							
(b)	•	•	•	•	3̣	3̣	3̣5̣2̣	1	•	2̣	ī2̣6	3	•5	2̣5	3	2
(a)	6	6	•	•	ī	5	ī	6								
(b)	•	•	•	•	6	6	•6ī	5	•	6	ī	2̣	•3̣	ī2̣	ī	6
(a)	ī	ī	3	2	•	1	2	6								
(b)	•	•	ī	2̣	ī6	35	3	2	•	•	35	3	•	ī2̣	1	6

Fig. 2. A Traditional Javanese Sheet Music Example of a Composition Entitled Ladrang Wilujeng.

Time signature in Gamelan music is known as tempo, and it is divided into 1/1, 1/2, 1/4, 1/8 and so on. Tempo represents the note duration of beats of melodies and skeletal melodies. Tempo of 1/1 means that each beat in the melody and skeletal melody has note duration of 1, tempo of 1/2 means that each beat in the skeletal melody has note duration of 1 and each beat in the melody has note duration of 2. The note duration consists of 1, 0.5 or 0.25, and in the sheet music it is indicated by a single or double horizontal lines above the notes. The notes without any horizontal line have a note duration of 1, a single horizontal line represents a note duration of 0.5 and a double horizontal line represents a note duration of 0.25.

Musical element symbols, such as circular symbols and curves symbols above the notes of the skeletal melody, represent the type of the composition. Curve symbols below the notes in the melody represent the legato sign which is similar to those in Western music, horizontal line symbols above the notes in the melody represent the note duration, dotted notes above and below the notes in the melody represent the notes register (low, middle and high notes). Fig. 2 shows an example of a traditional Javanese music sheet of a composition played with a tempo of 1/2. The composition consists of four lines of the skeletal melody marked with (a) and the melody marked with (b).

## III. RELATED WORK

Pattern recognition are common for chord detection problems in which chords are detected by extracting features from audio source, giving filter and matching the pattern [1]. This approach was implemented in various works by [2-7], and the method usually uses audio signal as the input source, and a features extraction is conducted to set an input by selecting relevant features from the audio source. Features for chord detection are called pitch class profile (PCP), or known with chroma features, which consists of 12 semi-tones values attributes. Chroma features are still proven as the main features

in chord detection [10]. These 12 semi-tones were used to set 12 bin vectors for faster processing [4], while 178 bin vectors [3] and 180 bin vectors [7] were set from variations of 12 semi-tones to set a frequency range. Feature extraction for random variables data can be conducted using the  $\chi^2$  statistics method in which the target and features are discrete finite values [11].

The decomposition of each chord label into a meaningful set of musical components was used to overcome the problem of insufficient sample size for model training in chord data quality [12]. Meanwhile, target and features can be determined based on data segmentation technique then followed by supervised learning implementation [13], and this technique can also increase the number of corpuses. Sequence mapping technique is used to calculate weighted moving average based on previous data of a time ordered sequence, such as works to predict stock index that implemented sliding window technique to map sequence data [14]. So, features for chord detection or melody extraction that uses a dataset collected from symbolic data can be determined by data segmentation and followed by data mapping using sliding window technique as proposed in this research. Sequence padding and sequence truncation are common techniques to solve a vector length problem in a time series prediction. Sequence padding adds a number of zeroes in the beginning (pre-sequence padding) or in the ending (post-sequence padding) of vectors as much as the maximum number of the vector's length. While sequence truncation chops a number of elements of vector in the beginning (pre-sequence truncation) or in the ending (post-sequence truncation) of vector to obtain a defined number of vector length. Sequence padding is better to find pattern in given data than to predict based on previous data [15]. This is also proven in a pre-experiment conducted in this research in which the use of sequence truncation achieves higher prediction on accuracy than sequence padding.

Several computer and music researches have been conducted to generate a note sequence of skeletal melodies. The grammar approach was used to formalize note sequence patterns of bars of the skeletal melody [16]. Meanwhile, the

grammar based on a bar structure was analyzed to define note sequence patterns of bars of the skeletal melodies [17]. The rule-based method used for the solutions of the same problem, but the formulation includes note sequence patterns between bars, and then the note sequence rules were determined by segmenting data using the sliding window technique [18]. Further, the rules were implemented as constraints to generate note sequences of skeletal melodies using Genetic algorithm [19]. Different from existing researches, this research aims to extract note sequences of skeletal melodies from note sequences of melodies.

#### IV. METHODOLOGY

A feed-forward neural networks classifier with supervised learning approach and pattern recognition technique was proposed to build a melody extraction system for traditional Javanese compositions. The task of the classifier is to extract melodies into skeletal melodies, where the class is determined based on the notes of the musical scale system. Data of compositions are segmented into beats to reveal the patterns of the notes correlation between melodies and skeletal melodies as illustrated in Fig. 3. This technique can increase the number of corpuses, as more corpus results in better accuracy in the FFNN method. For example, a composition containing six lines contributes 12 bars and 48 beats if the beats are used as the corpus.

A collection of music sheet used as the data source was manually converted into a text-based format for computation process. Each composition data consists of melodies used as input, and skeletal melodies used as target. The difference in the number of notes in a melody beat determined by the note duration has an impact on the difference in vector length. The vector length adjustment was performed so that all vectors have the same element length as the FFNN input requirements. Further, the beats are mapped to restructure the data into time series format data and to determine features and to increase the cardinality of corpuses. Finally, the results of data mapping were converted into the binary format before being sent to train the network.

Tempo illustration for a composition played with a tempo of 1/2

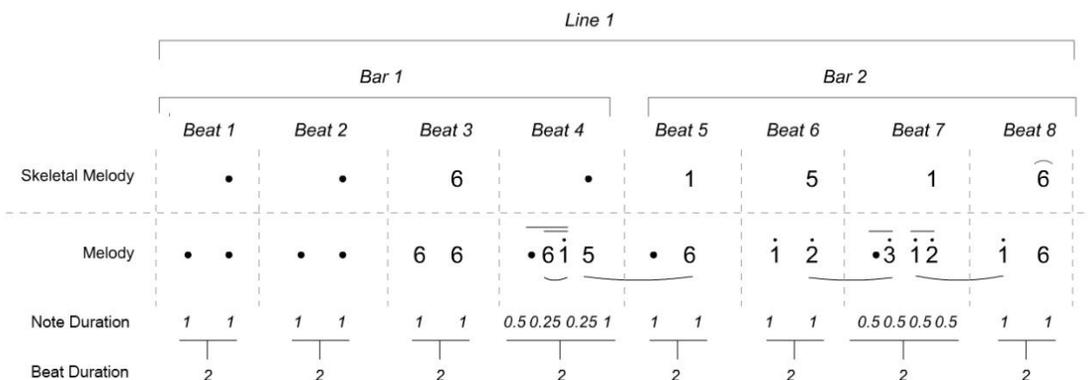


Fig. 3. Data Segmentation based on the Beats.

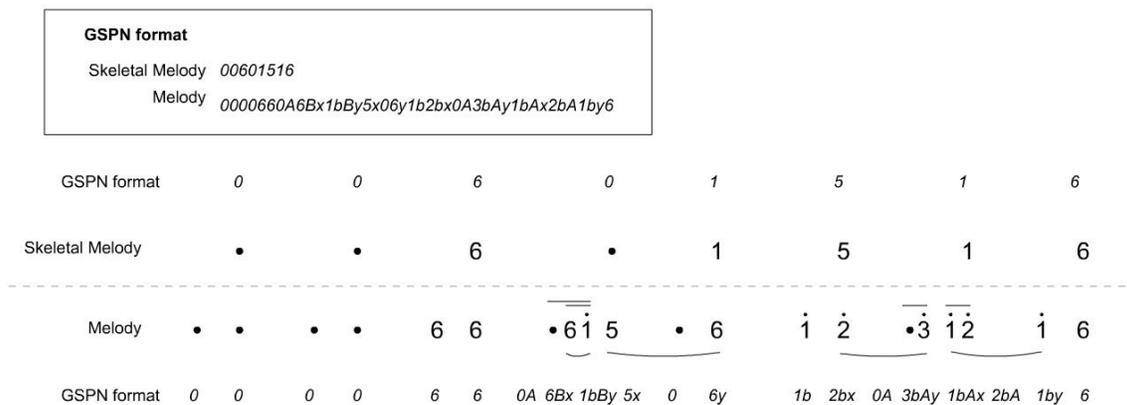


Fig. 4. Illustration of Text-based Format in the GSPN Model.

### A. Data Preparation

The experiment was limited to the compositions of the *slendro* scale system played with a tempo of 1/2. The *slendro* scale system of *slendro* contains five notes, which are 1, 2, 3, 5 and 6, and also the dotted notes as an addition. The source of data which was 55 traditional Javanese music sheets was collected from [www.gamelanbvg.com](http://www.gamelanbvg.com). Data were converted to a text-based format using a model of a text-based note writing for traditional Javanese compositions called *Ghending Scientific Pitch Notation* (GSPN). The model was developed to represent sheet music containing data of notes, note duration, note register and legato signs in a text-based format that can be read by human and computer [20]. The text-based conversion was manually conducted using a text editor program. Data of melodies and skeletal melodies were separately typed in two text files. To store information of the melody and its skeletal melody, each line in two text files was filled with one melody and one skeletal melody from each composition. Human errors are possible during conversion but the GSPN model supports a computational process that can detect typing errors. Note duration information can be calculated to detect the duration value of each beat so that typing errors can be detected if there are beats with different duration values in a composition. Once sheet music is converted to GSPN format, the data can be explored and calculated for information.

The code to represent the musical elements in GSPN format is case sensitive. Notes in *slendro* scale system, including the dotted note, are written in the numbers 0, 1, 2, 3, 5 and 6. Note duration is coded with no code, A and B where code A represents the note duration of 0.5, code B represents the note duration of 0.25, and no code represents the note duration of 1. Note register is coded with no code, a and b where code a represents the low notes, code b represents the high notes, and no code represents the middle notes. The legato sign is coded with no code, x and y where code x represents the beginning of the legato sign, code y represents the end of the legato sign, and no code represents notes that are between the beginning and end of a legato sign or notes that are not part of any legato sign. The code is written in order of note, note duration, note value and legato sign. Fig. 4 shows an illustration of a text-based format in the GSPN model converted from a music sheet.

TABLE I. GSPN IN TABULAR DATA FORMAT

	Note Sequence of Melody												
	0	0	0	0	6	6	0	6	1	5	...	6	
NT													
NR									b		...	a	
ND							A	B	B		...		
LS								x	y	x	...		

The following is an GSPN format example of a melody and its skeletal melody of a composition entitled *Ladrang Wilujeng* shown in Fig. 2.

Skeletal Melody:

00601516356165326600151611320126

Melody:

0000660A6Bx1bBy5x06y1b2bx0A3bAy1bAx2bA1by6000  
03b3b3bBx5bB2bAy1x02by1bBx2bB6Ay3x0A5Ay2Ax5A3y  
20000660A6Bx1bBy5x06y1b2bx0A3bAy1bAx2bA1by6001b  
2bx1bA6Ay3Ax5A3y2003Ax5Ay301Ax2A1y6a

Table I shows illustration of GSPN in a tabular data format using melody data example above with NT stands for notes, ND stands for the notes duration, NR stands for the notes register and LS stands for the legato signs.

### B. Beat Detection

In traditional Javanese sheet music, the melody part contains the musical elements of notes, note durations, note registers and legato signs, while the skeletal melody part usually contains only notes. The legato signs also do not used in the skeletal melody. The beats in the skeletal melody contains one note so every note in the skeletal melody has a duration note value of 1.

Beat detection was performed by converting letter codes in GSPN format into numbers. The note register encoded with a for low notes, and b for high notes, and no code for middle notes, was converted to 1, 0 and 2, respectively. The note duration encoded with A for the note of duration 0.5, and B for the note of duration 0.25, and no code for the note of duration 1 was converted to 0.5, 0.25 and 1, respectively. The legato sign

encoded with x for the beginning of legato, and y for the end of legato, and no code for notes that fall between the legato signs and notes that are not part of the legato signs, was converted to 1, 2 and 0, respectively.

Next, beat detection was done by calculating the notes duration value. The dataset uses compositions with a tempo of 1/2 which means each beat has a duration value of 2. The following is the pseudocode for detecting beats using data of a composition entitled Ladrang Wilujeng. The first pseudocode is to detect the number of notes duration (ND) in the sequence by adding up the note duration values, then dividing by the beat duration values based on the tempo (TP). Given NB as the number of beats then the pseudocode is:

```
TP = 2
NB = 0
ND = (1, 1, 1, 1, 1, 1, 0.5, 0.25, 0.25, 1, ..., 1)
for (i = 0; i < ND.length; i++) {
    NB += ND [i]
}
```

```
NB = NB/TP
```

Next is to group the sequence of notes (NT), notes register (NR), note duration (ND), legato signs (LS) into beats. This grouping is performed using the following pseudocode:

```
NT = (0, 0, 0, 0, 6, 6, 0, 6, 1, 5, ..., 6)
NR = (0, 0, 0, 0, 0, 0, 0, 2, 0, ..., 1)
LS = (0, 0, 0, 0, 0, 0, 1, 2, 1, ..., 0)
```

```
for (i = 0; i < NB; i++) {
    BT [i] = []
    BR [i] = []
    BD [i] = []
    BL [i] = []
}
k = 0
m = 0
for (i = 0; i <= ND.length; i++) {
    if (m < 2) {
        BT[k].push(NT[i])
        BR[k].push(NR[i])
        BD[k].push(ND[i])
        BL[k].push(LS[i])
    }
```

```
m += ND [i]
if (m > 2) {
    m = 0
```

```
k += 1
}
}
```

Based on the pseudocode above, the sequence breakdown of NT, NR, ND, and LS into beats is stored in notes per beat (BT), notes register per beat (BR), notes duration per beat (BD) and legato signs per beat (BL) respectively. Furthermore, each beat that has been defined is correlated with each note in the skeletal melody (SM) as follows:

```
BT = ((0, 0), (0, 0), (6, 6), (0, 6, 1, 5), ..., (... , 6))
BR = ((0, 0), (0, 0), (0, 0), (0, 0, 2, 0), ..., (... , 1))
BD = ((1, 1), (1, 1), (1, 1), (0.5, 0.25, 0.25, 1), ..., (... , 1))
BL = ((0, 0), (0, 0), (0, 0), (0, 1, 2, 1), ..., (... , 0))
SM = (0, 0, 6, 0, ..., 6)
```

Table II shows illustration of the beat detection using the pseudocodes above.

TABLE II. BEAT DETECTION RESULTS

	Melody											
NT	0	0	0	0	6	6	0	6	1	5	...	6
NR	0	0	0	0	0	0	0	0	2	0	...	1
ND	1	1	1	1	1	1	0.5	0.25	0.25	1	...	1
LS	0	0	0	0	0	0	0	1	2	1	...	0
	Skeletal Melody											
SM	0	0	6	0	...	6						

### C. Vector Length Adjustment

The length of the beat element of melody data varies whereas the FFNN requires the same element length for the vector. Sequence padding and sequence truncation techniques are commonly used to solve element length problems. Truncation techniques that cut data elements can lose important information, while padding techniques that add elements in the data are computationally expensive.

Pre-experiments were conducted to compare the use of sequence padding and sequence truncation techniques based on prediction accuracy. By using the same dataset, the results show that the data managed by the sequence truncation technique achieves higher prediction accuracy results. The risk of losing important information due to truncation seems to be reduced by mapping the data using a sliding window technique after the data is truncated. So, sequence truncation technique was chosen to solve the beat element length problem.

The post-sequence truncation technique was implemented to notes per beat (BT), notes register per beat (BR), notes duration per beat (BD) and legato signs per beat (BL). Table III shows an example of the implementation of the post-sequence truncation technique to set the vector length of the notes per beat (BT) data, and the elements that are retained are two bits.

TABLE III. BEAT SEQUENCE TRUNCATION

ID	Beat Sequence	Truncation
1	(0, 0)	(0, 0)
2	(0, 0)	(0, 0)
3	(6, 6)	(6, 6)
4	(0, 6, 1, 5)	(0, 6)
...	...	...
32	(1, 6)	(1, 6)

D. Data Mapping & Feature Selection

Data mapping was performed based on the beats using the sliding window technique, a technique for data mapping by restructuring time series data to be used in a classification problem. This technique produces data segmentation based on the previous or the following sequences. The previous beat, selected beat and next beat are selected as the features. So, the sliding window implementation defines a pattern of  $(B_{n-1}, B_n, B_{n+1})$  for the data mapping, where B stands for beat and n stands for sequence index. Melody has repetitive pattern; after reaching the last pitch, melody continues to restart from the first pitch. This solves the problem in indexing a sequence. The data mapping for the first beat is set to  $(B_{last}, B_1, B_2)$ , and for the last beat is set to  $(B_{last-1}, B_{last}, B_1)$ . The sliding window technique was implemented to BT, BR, BD and BL. Table IV shows an example of the implementation of the sliding window technique to set the data mapping of the notes per beat (BT).

Features are selected based on the data mapping implemented to BT, BR, and BD. Meanwhile, BL was not used as a feature to reduce the computation cost. Beat per bar index was also used as a feature because the position of the beat order per bar affects the musical mode system so it is important to use it as a feature. Each bar consists of four beats so that the sequence of beats per bar is a repeating pattern of 1, 2, 3, 4 and back to 1. Table V shows illustration of the feature selection based on BT, BR, BD, LS and beats ID per bar.

TABLE IV. DATA MAPPING\_BT

BT (Input)			SM (Output)
ID	Beats	Data Mapping	
1	(0, 0)	(1, 6, 0, 0, 0, 0)	0
2	(0, 0)	(0, 0, 0, 0, 6, 6)	0
3	(6, 6)	(0, 0, 6, 6, 0, 6)	6
4	(0, 6)	(6, 6, 0, 6, 1, 2)	0
...	...	...	...
32	(1, 6)	(0, 1, 1, 6, 0, 0)	6

TABLE V. DATA MAPPING\_BEATS

Beats (Input)				SM (Output)
ID	BT	BR	BD	
1	(1, 6, 0, 0, 0, 0)	(0, 1, 0, 0, 0, 0)	(1, 1, 1, 1, 1, 1)	0
2	(0, 0, 0, 0, 6, 6)	(0, 0, 0, 0, 0, 0)	(1, 1, 1, 1, 1, 1)	0
3	(0, 0, 6, 6, 0, 6)	(0, 0, 0, 0, 0, 0)	(1, 1, 1, 1, 0.5, 0.25)	6
4	(6, 6, 0, 6, 1, 2)	(0, 0, 0, 0, 0, 0)	(1, 1, 0.5, 0.25, 1, 1)	0
...	...	...	...	...
4	(0, 1, 1, 6, 0, 0)	(0, 0, 0, 1, 0, 0)	(1, 0.5, 1, 1, 1, 1)	6

E. Binary Representation

Binary representation was implemented using the localist representation technique. The localist representation uses values of 0 and 1 to control an activation of variables. The *slendro* scale system consists of five notes: 1, 2, 3, 5 and 6, and the dot notation is converted into the number 0. Thus, the localist representation for each note consists of six bits, which is: 0 = 100000, 1 = 010000, 2 = 001000, 3 = 000100, 5 = 000010, and 6 = 000001. The notes register consists of three values: 1 represents the low notes, 2 represents the high notes and 0 represents the middle notes. Thus, the localist representation for each note register consists of three bits, which is: 1 = 100, 2 = 010, and 0 = 001. The notes duration consists of three values: 1 represents the value of 0.25, 2 represents value of 0.5 and 0 represents value of 1. Thus, the localist representation for each note duration consists of three bits, which is: 2 = 100, 1 = 010, and 0 = 001. The beat ID consists of four values: 1 represents the first beat in a bar, 2 represents the second beat in a bar, 3 represents the third beat in a bar, and 4 represents the fourth beat in a bar. Thus, the localist representation for each beat ID consists of four bits, which is: 1 = 1000, 2 = 0100, 3 = 0010, and 4 = 0001. Thus, the localist representation of the input data yields the length of each input:  $(6 \times 6) + (6 \times 3) + (6 \times 3) + (1 \times 4) = 36 + 18 + 18 + 4 = 76$  bits, and the length output is  $6 \times 1 = 6$  bits which is the notes elements of the *slendro* scale system.

V. TRAINING AND EVALUATION

An FFNN classifier was developed using the supervised learning approach and scaled conjugate gradient backpropagation algorithm to extract melodies into skeletal melodies. There are six classes for the melody extraction classification, where the output of each class is notes of the skeletal melodies. The length of the input vector is 76 bits and the length of the output vector is 6 bits.

The networks architecture consists of input, hidden and output layers. The best network performance was determined using an epoch with a parameter of six consecutive incorrect predictions. The number of hidden layer units was determined experimentally in multiples of 10 units and starts from 10 to 100 units. Each training was limited by 100 retrains. The training can be stopped before reaching the 100<sup>th</sup> training repetition if the results of the training meet the best prediction parameters. Later, experiments showed that the configuration of the number of hidden layer units of 40 units gives the best prediction results. Less than 40 units, the prediction error by the FFNN network is more than 40%, and more than that number the predictions are trapped in the local minima.

The best prediction parameters are determined based on the balance of the number of prediction errors between training, validation and test data in the FFNN network training with the maximum value of prediction error is 40%. The experiments used 55 music sheets, each of which contains a melody and its skeletal melody. The dataset mapped based on beats produced 2,808 beats for the corpus. Fig. 5 shows the FFNN architecture for the melody extraction.

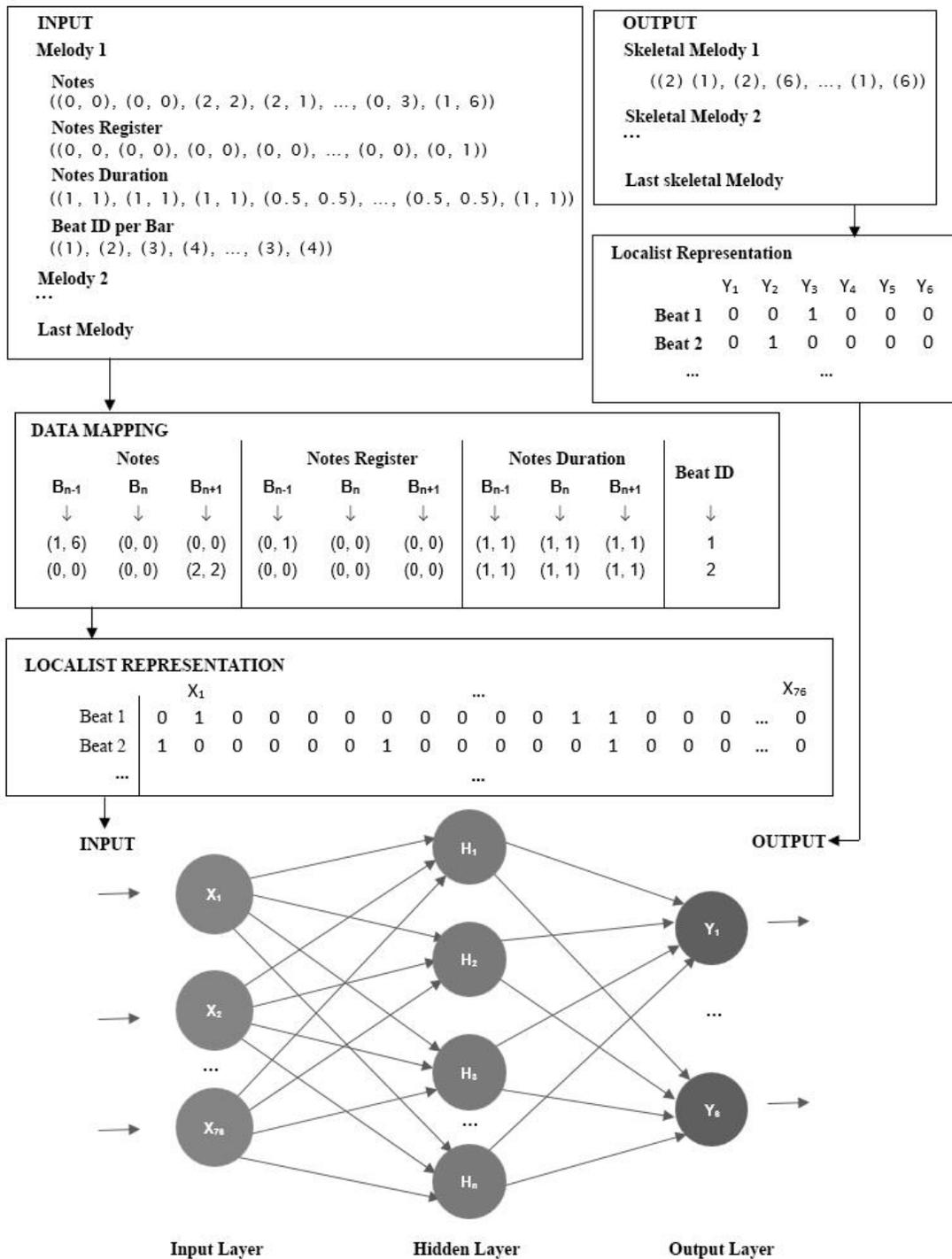


Fig. 5. The FFNN Architecture.

Of the 55 compositions used as datasets, 50 compositions were used for training data, while the remaining 5 compositions were used for test data. Of the 50 compositions used as training data, the input matrix is  $76 \times 2,568$  bits and the output matrix is  $6 \times 2,568$  bits. The distributed corpus in class 1, 2, 3, 4, 5, and 6 is 424, 387, 486, 525, 324, and 422 samples, respectively. Furthermore, the data is divided randomly into

training, validation and test data with a proportion of 80:10:10 and resulted 2,054, 257 and 257 samples, respectively. Table VI shows the dimensions of the matrix, after applying the data transpose, the results of dividing the dataset into training data, and test data consisting of five compositions for testing the composition separately.

TABLE VI. VECTOR MATRIX DIMENSIONS

Data		Input	Output
Training	Training	76 × 2054	6 × 2054
	Validation	76 × 257	6 × 257
	Test	76 × 257	6 × 257
Evaluation	Composition 1	76 × 48	6 × 48
	Composition 2	76 × 48	6 × 48
	Composition 3	76 × 48	6 × 48
	Composition 4	76 × 48	6 × 48
	Composition 5	76 × 48	6 × 48

The FFNN network with the number of hidden layer units of 40 units meets the best prediction criteria with the number of prediction errors in each training, validation and test data of 34,81012e-0%, 35,79766e-0% and 35,79766e-0%. The best validation performance was obtained with a cross-entropy value of 0.17844 at epoch 34 as shown in Fig. 6, while Fig. 7 shows the graph of the receiver operating characteristic (ROC) performance and Fig. 8 shows the results of calculating the confusion matrix.

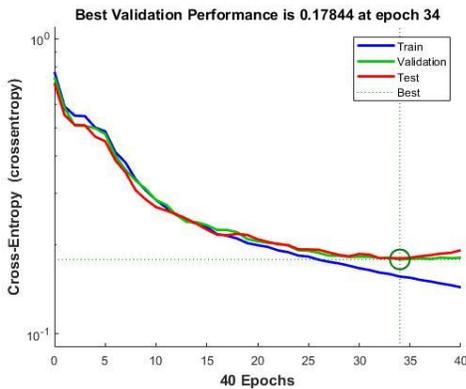


Fig. 6. The Best Validation Performance Graph.

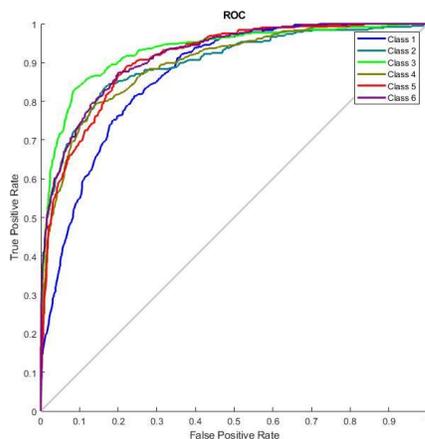


Fig. 7. The ROC Graph.

Confusion Matrix							
Output Class	Target Class						
	1	2	3	4	5	6	
1	216 8.4%	44 1.7%	35 1.4%	72 2.8%	19 0.7%	30 1.2%	51.9% 48.1%
2	37 1.4%	258 10.0%	26 1.0%	32 1.2%	23 0.9%	22 0.9%	64.8% 35.2%
3	45 1.8%	23 0.9%	378 14.7%	27 1.1%	23 0.9%	24 0.9%	72.7% 27.3%
4	47 1.8%	27 1.1%	15 0.6%	335 13.0%	41 1.6%	24 0.9%	68.5% 31.5%
5	22 0.9%	9 0.4%	14 0.5%	27 1.1%	187 7.3%	27 1.1%	65.4% 34.6%
6	57 2.2%	26 1.0%	18 0.7%	32 1.2%	31 1.2%	295 11.5%	64.3% 35.7%
	50.9% 49.1%	66.7% 33.3%	77.8% 22.2%	63.8% 36.2%	57.7% 42.3%	69.9% 30.1%	65.0% 35.0%

Fig. 8. The Confusion Matrix Results.

The ROC graph shows that the curve for class 1 initially moves along the curves of other classes before finally moving away. This condition is also shown by the results of the confusion matrix calculation, the prediction accuracy reaches 50.9%, or 216 of 424 class 1 data can be predicted correctly. In more detail, the calculation of the values of accuracy, precision, recall, specificity and F1-score of the FFNN network is shown in Table VII.

The experiment was continued by testing the networks using a hold-out test data which consisted of five compositions (abbreviated as C1, C2, C3, C4, C5). All of compositions, except C4, consist of 48 corpus, while C4 which consists of 64 corpus. The evaluation results show that, all measurements have improved performance in all compositions except C4, in which there was a decrease of 3.1% in the recall measure and 0.3% in the F1 measurement. Table VIII shows the comparison of evaluation results on training data and evaluation data which are divided into data of five compositions which are measured separately and combined, with C1 to C5 representing the first composition to the fifth composition.

TABLE VII. VECTOR MATRIX DIMENSIONS

Measurement	Training (%)	Evaluation (%)				
		C1	C2	C3	C4	C5
Accuracy	65.0	70.8	85.4	68.8	67.2	68.8
Precision	64.5	71.3	85.1	71.7	64.8	68.3
Recall	64.6	72.3	84.3	71.3	63.7	72.2
Specificity	65.0	70.8	85.5	68.8	67.1	68.7
F1 score	64.5	71.8	84.7	71.5	64.2	70.2

## VI. CONCLUSION AND FUTURE WORK

Overall, the proposed method successfully combines musical theory in notes sequence pattern recognition by extracting melodies using a multi-class classification based on notation duration and beat rules. Based on the evaluation of the measurement of accuracy, precision, recall, specificity and F1 score on the melody extraction per composition, the performance of the networks in correctly classifying the notes of skeletal melodies from the beats of melodies, including distinguishing extracted notes from targets that are not in their class, has increased compared to the results obtained in training.

Table VIII shows the results of the accuracy test per class per composition. On the melody extraction with target class 3 (note 2), the performance of the FFNN network looks good with the lowest accuracy of the five compositions being 83.3%, which are at C1 and C3, even at C2 and C5, the accuracy reaches 100%. Good performance is also shown in the class 6 (note 6) where the lowest accuracy is 70% at C4, and overall C4 does contribute to a decrease in accuracy. Similar conditions also occur in class 2 (note 1) with 100% accuracy results in C2 and C5, but there is a decrease in accuracy in C3 even though it can still be categorized as a good achievement, which is 87.5%. Meanwhile in C1 and C4, there was a decrease to 66.7% and 60%, respectively. Class 1 (note 0), 4 (note 3) and 5 (note 5) gave a poor contribution to the accuracy of the melody extraction.

TABLE VIII. ACCURACY TEST RESULTS PER NOTE CLASS

Target	Output (%)				
	C1	C2	C3	C4	C5
1 (note 0)	71.4	50	83.3	62.5	40.0
2 (note 1)	66.7	100	87.5	60.0	100
3 (note 2)	83.3	100	83.3	84.6	100
4 (note 3)	45.5	100	33.3	80.0	50.0
5 (note 5)	77.8	66.7	50.0	25.0	55.6
6 (note 6)	88.9	88.9	90	70.0	87.5

The accuracy of the melody extraction in notes 2 and 6 is directly proportional to the fact that the dominant notes or note strength in the *manyura* musical mode system in the *slendro* scale system used as a dataset is in both notes. Thus, it can be concluded that the networks can recognize the musical mode system and the musical scale system using the melody extraction approach. On the other hand, the conditions of the other four notes, which are 0, 1, 3 and 5, and some of which are still not well predicted. It still cannot be used to conclude that the networks failed in extracting melodies. The unique characteristics of *Gamelan* music allow differences in notes in the same condition not to be a mistake as long as all the different tones do not change the meaning of the composition and can still be accepted by the *Gamelan* music community (Hastuti et al., 2017).

The performance of the networks in extracting melodies into skeletal melodies can be said to be quite successful and promising. However, there are still several factors that need to be explored further to improve networks performance, such as

the need to apply artificial intelligence methods for feature selection and data mapping to increase the cardinality of the corpus to overcome the problems of limited number of datasets and confusion faced by the networks.

## REFERENCES

- [1] T. Cho, R.J. Weiss, and J.P. Bello, "Exploring Common Variations in State of the art Chord Recognition Systems", in Proceedings of the 7<sup>th</sup> Sound and Music Computing Conference (SMC), Barcelona, Spain, 2010, pp. 1-8.
- [2] T. Carsault, J. Nika, and P. Esling, "Using Musical Relationships between Chords Label in Automatic Chord Extraction Task", in 19<sup>th</sup> International Society for Music Information Retrieval Conference, Paris, France, 2018, pp. 18-25.
- [3] F. Korzeniowski, and G. Widmer, "Improved Chord Recognition by Combining Duration and Harmonic Language Model", in 19<sup>th</sup> International Society for Music Information Retrieval Conference, Malaga, Spain, 2016, pp. 10-17.
- [4] J. Osmalskyj, J.J. Embrechts, S. Piérard, and M. Van Droogenbroeck, "Neural Networks for Musical Chord Recognition". In Actes des Journées d'Informatique Musicale (JIM 2012), Belgique, 2012, pp. 39-46.
- [5] J. Park, K. Choi, S. Jeon, D. Kim, and J. Park, "A Bi-directional Transformer for Musical Chord Recognition", in 20<sup>th</sup> International Society for Music Information Retrieval Conference, Delft, Netherlands, 2019, pp. 620-627.
- [6] Z. Rao, X. Guan, and J. Teng, "Chord Recognition Based on Temporal Correlation Support Vector Machine". Applied Science, Vol. 6, No. 5, 2016, pp. 1-14.
- [7] X. Zhou, and A. Lerch, "Chord Detection using Deep Learning", in 16<sup>th</sup> International Society for Music Information Retrieval Conference, Malaga, Spain, 2015, pp. 52-58.
- [8] L. Marques, "A chord distance metric based on the Tonal Pitch Space and a key-finding method for chord annotation sequences", in 17<sup>th</sup> Brazilian Symposium on Computer Music - SBCM 2019, São João del-Rei, 2019, pp. 136-140.
- [9] H.V. Koops, W. Bas de Haas, J. Bransen, and A. Volk, "Automatic chord label personalization through deep learning of shared harmonic interval profiles", Neural Computing and Applications (2020) 32:929-939, DOI: <https://doi.org/10.1007/s00521-018-3703-y>.
- [10] J. Pauwels, K. O'Hanlon, E. Gómez, and M.B. Sandler, "20 Years of Automatic Chord Recognition from Audio", in 20<sup>th</sup> International Society for Music Information Retrieval Conference, Delft, Netherlands, 2019, pp. 54-63.
- [11] B. Ghogh, M.N. Samad, S.A. Mashhadi, T. Kapoor, W. Ali, F. Karray and M. Crowley, "Feature Selection and Feature Extraction in Pattern Analysis: A Literature Review", arXiv:1905.02845 [cs.LG], 2019.
- [12] J. Jiang, K. Chen, W. Li, G. Xia, "Large-Vocabulary Chord Transcription via Chord Structure Decomposition", in 20<sup>th</sup> International Society for Music Information Retrieval Conference, Delft, The Netherlands, 2019, pp. 644-651.
- [13] D. Efrosinin, and V. Sturm, "Time Series Segmentation of Linear Stochastic Processes for Anomaly Detection Problem using Supervised Methods", in Proceedings of the 56<sup>th</sup> ESReDA Seminar, Linz, Austria, 2019, pp. 1-11.
- [14] H.S. Hota, R. Handa, and A.K. Shrivastava, "Time Series Data Prediction using Sliding Window based RBF Neural Network", International Journal of Computational Intelligence Research, Vol. 13, No. 5, 2017, pp. 1145-1156.
- [15] M. Dwarampudi, and N.V.S. Reddy, "Effects of Padding on LSTMS and CNNs", arXiv:1903.07288 [cs.LG], 2019.
- [16] J. Becker, and A. Becker, "A Grammar of the Musical Genre Srepegan", Asian Music, Vol. 14, No. 1, 1982, pp. 30-73.
- [17] D.W. Hughes, "Deep Structure and Surface Structure in Javanese Music: A Grammar of Gendhing Lampah", Ethnomusicology, Vol. 32, No. 1, 1988, pp. 23-74.
- [18] K. Hastuti, A. Azhari, A. Musdholifah, and R. Supanggah, "Building Melodic Feature Knowledge of Gamelan Music using Apriori based on

- Functions in Sequence (AFiS) Algorithm”, *International Review on Computers and Software*, Vol. 11, No. 12, 2016, pp. 1127-1137.
- [19] K. Hastuti, A. Azhari, A. Musdholifah, and R. Supanggih, “Rule-based and Genetic Algorithm for Automatic Gamelan Music Composition”, *International Review on Modelling and Simulations*, Vol 10, No. 3, 2017, pp. 202-212.
- [20] A.M. Syarif, A. Azhari, S. Suprpto, and K. Hastuti, “A Model of Computation-based Naming System for Musical Elements of Java Traditional Song”, *IOP Conference Series: Materials Science and Engineering*, Vol. 803 (012031), 2020.

# LightGBM-based Ransomware Detection using API Call Sequences

Duc Thang Nguyen, Soojin Lee\*

Department of Computer Science and Engineering  
Korea National Defense University, Nonsan, Republic of Korea

**Abstract**—Along with the development of technology as well as the explosion in digital data in the era of fourth industrial revolution, cyberattacks using ransomware are emerging as a serious threat to many agencies and organizations. The harm of ransomware is not limited to the areas of information technology and finance but also affects areas related to people's lives, such as the medical field. Therefore, research to identify and detect these types of malicious code is urgent. This paper presents a novel approach of identifying and classifying ransomware based on dynamic analysis techniques combined with the use of machine learning algorithms. First, this research focused on the Application programming interface (API) call functions that are extracted during a dynamic analysis of executable samples using the Cuckoo sandbox. Second, research used LightGBM, a gradient boosting decision tree algorithm, for training and then detecting and classifying normal software and eight different types of ransomware. Experimental results showed that the proposed approach achieves an overall accuracy rate of 98.7% when performing multiclass classification. In particular, the detection rates of ransomware and normalware were both 99.9%. At the same time, the accuracy in identifying two specific types of ransomware, WannaCry and Win32:FileCoder, reached 100%.

**Keywords**—Ransomware; machine learning; API call; dynamic analysis technique; gradient boosting decision tree; GBDT; lightGBM

## I. INTRODUCTION

Ransomware is a form of malicious code which, upon infecting a victim's device, encrypts and then steals the victim's data and prevents legitimate access to it until the victim pays a ransom. In early versions of ransomware, the code mainly performed the trick of locking the victim's system, aimed at non-computer savvy users. However, today's ransomware mainly uses crypto-viral extortion techniques. These methods take advantage of the most modern encryption techniques to encrypt almost all of the victim's personal data (e.g., photos, documents, texts). Even the most knowledgeable users or experts also face considerable difficulties. It is almost impossible to recover the data until receiving the decryption key. In a properly executed crypto-viral ransomware attack, recovering data without a decryption key is a problem that is difficult to solve. The attack also requires digital currencies that are difficult to track, such as Bitcoin, for ransom, making it even more difficult to investigate and track down the culprit.

The use of ransomware is accelerated and becoming increasingly dangerous compared to levels seen in the past. Ransomware is now a national security issue for all countries

around the world, and it will only become worse. In particular, during the recent Covid-19 pandemic, attacks on many hospitals and medical facilities indicate a new risk of ransomware, considering that its influence caused the death of a patient (Fireeye's 2021 report). Ransomware at present is a real threat to humans' lives. Threat actors will increasingly target the most critical assets, such as sensitive data and architectures, held by organizations, leading to much higher ransom amounts. Ransoms have already reached the tens of millions of dollars and are expected to grow. While many organizations pay ransoms and do regain access to their data. And they often forget that the attackers still have their data and can allow anyone to buy the data right from their websites (SophosLab's Threat Report 2021). Data theft creates a secondary extortion market.

The continued success of ransomware poses a serious cyber security threat. According to the statistics of reputable security firms, ransomware can spread maliciously in many types of ways, via sophisticated techniques used to avoid detection by antivirus software. Therefore, the need to analyze these types of malware is urgent given the explosion of data in the fourth industrial revolution with millions of Internet of Things devices connected to the Internet every day.

Attackers are increasingly turning to ransomware as a service (RaaS) with more customization capabilities that rapidly increase the number of ransomware variants and types. Therefore, traditional signature-based detection techniques are not effective. Current techniques often build on complex models that combine many features extracted through static analysis or dynamic analysis, along with various transformations to distinguish between ransomware and normal software. They are based on certain features extracted from a dynamic analysis or static analysis, such as API sequences, opcode strings of files, file entropy levels, and/or change in system files. The use of the API function call sequence to detect and classify ransomware types had been applied in many practical studies, such as in [1], [2], [3], [4], showing promising results. However, the fundamental problem of detection methods based on static analysis is weak detection when attackers use code obfuscation methods or zero-day attacks. Furthermore, the malicious code classification methods based on API functions extracted from static analysis lead to one drawback. These methods are easily evaded when an attacker inserts normal API calls or declares unused API functions during a ransomware execution.

Among various features, this research focuses on the Windows API call frequency, which is extracted via a dynamic analysis technique. The proposed method uses it as the primary

\*Corresponding Author

factor in conjunction with certain transformations that improve the speed and accuracy in identifying instances of malicious code extortion. Proposal method also applies LightGBM, a gradient boosting decision tree (GBDT) algorithm, to increase the accuracy and speed of detecting and classifying ransomware.

The next sections of the paper are organized as follows: Section 2 presents ransomware detection techniques that are currently being studied. Section 3 describes the proposed approach and algorithms used, and Section 4 explains the collected dataset and the experimental method. Section 5 analyzes the experimental results and Section 6 concludes the paper.

## II. RELATED RESEARCH

There are two main approaches when analyzing and detecting ransomware: static analysis and dynamic analysis [5]. While the static analysis technique mainly focuses on analyzing and checking the file structure and executable file formats without running the file, a dynamic analysis allows malware to run to observe its behavior in the system ultimately to eliminate the infection.

This Section reviews several ransomware analysis methods which are on the basis of the above two techniques in terms of the extracted information. Then, current multiclass classification methods will be reviewed.

In terms of API sequences, to achieve malicious purposes especially when implementing ransomware, attackers must use and execute a specific API sequence. So there are big differences between malicious codes and normal software in API call sequences. There have been several studies focusing on an analysis of API call sequences to detect general malware as well as ransomware. For example, in [1] Sgandurra et al. presented a ransomware detection method based on dynamic analysis and applied a type of machine learning known as EldeRan. They collected several features extracted from their dynamical analysis, such as API calls, registry and file system change logs, dropped files, and crypto-function patterns in binary files. EldeRan studied a dataset with 1524 samples consisting of 582 ransomware and 942 benign samples. By using a regularized logistic regression method for classification, they could achieve 96.3% detection rate in binary classification.

In [3] Hwang et al. combined a Markov model with random forest model to build two-stage mixed ransomware detection model. The Markov model is used to capture the characteristics of ransomware with the Windows API call sequence pattern that obtained by a dynamic analysis. During the second stage, the random forest machine learning model's mission is to control misclassified samples in the remaining data. The accuracy of this two-stage mixed detection method is 97.3%. In binary classification, False positive (FP) and False negative (FN) rate are relatively high, 4.8% and 1.5% respectively. In [6], Bae et al. used the Intel PIN tool to extract Windows API call sequences and then generated n-gram sets from these API sequences. These n-gram sets were used to classify ransomware, malware and benign files. The authors concluded

that their method could detect ransomware with a detection accuracy up to 98.65%.

Several file-based techniques can identify the presence or existence of ransomware based on the transformation in files of system or in files of a particular format. In [7], after studying a dataset including 1359 ransomware samples from 2006 to 2014, Kharraz et al. concluded that it is not complicated to design an advanced technique to block several types of ransomware by monitoring file system anomaly activities. This method can be effective even against those using sophisticated cryptographic malware or some types of zero-day ransomware attacks. In [8], Lee et al. measured the entropy of six different file formats and then used machine learning to detect infected files to protect the original file in a backup system while synchronizing the time. By identifying files infected with ransomware, this method allows the recovery of those files from system storage when the user's system is infected. Khammas [4] proposed a method that detects ransomware based on a static analysis. The method used frequent pattern mining and the gain ratio technique to extract 1000 features directly from raw binary files. A random forest technique is applied to the classification process. The dataset consists of 1680 executable files made up of 840 ransomware and 840 normal files. The accuracy rate was 97.7%.

In network-based studies, Cabaj et al. [9] proposed a solution to identify ransomware based on HTTP traffic communication when the ransomware connects to the attacker's C&C server. The experimental results obtained detection rates of 97–98%. However, the authors only monitored and observed the network traffic communication of two types of ransomware, CryptoWall and Locky. The author in [10] presented an advanced ransomware identification method based on an analysis of network traffic activities. The study observed TCP, HTTP, DNS, and NBNS traffic and extracted 18 different features. They prototyped a multi-classifier network-based ransomware detection method that combines of two different levels: the packet level and the flow level. The highest detection accuracy rates for the two corresponding levels were 97.92% and 97.08%. However, this research only focused and analyzed on the Locky ransomware's network activities and is thus not suitable for other types of ransomware.

Other researchers also used a hybrid method that integrates dynamic and static analysis techniques to distinguish between ransomware and normalware. For instance, Shaukat et al. [11] presented a method called RansomwareWall. The set of features collected by static analysis and dynamic analysis is fed to the machine learning engine for binary classification of samples as ransomware or benign. Using a dataset of 574 samples from 12 ransomware families, the experimental result presented detection rates ranging from 85.7% (using logistic regression) to 98.25% (using a gradient tree boosting algorithm).

For multiclass classification, some researchers are not only working to distinguish between ransomware files and normal files but also looking for ways to distinguish between different types of ransomware. For example, Zhang et al. proposed an approach for multiple classifications of seven ransomware

families based on a static analysis [12]. They built N-gram sequences by extracting opcode sequences from Portable executable (PE) file samples and then calculated the term frequency - inverse document frequency (TF-IDF) to identify the feature N-gram vectors. The feature vectors were then subjected to five machine-learning methods to classify ransomware. The dataset included 1,787 ransomware samples of seven ransomware families crawled from VirusTotal that broke out from 2012 to 2017. In the experiments, the best accuracy achieved was 91.43% for the multiclass classification method when using a random forest algorithm and 99.3% for the binary classification of ransomware and 'goodware'.

In [13], Baldwin et al. presented a WEKA toolset for ransomware multiclass classification based on a static analysis. They extracted 443 opcodes from binary files and used them to calculate the percentage of each opcode occurrence relative to the overall opcode. The support vector machine (SMV) learning technique was used for binary classification between benign and ransomware, while the PUK kernel was used for multiclass classification. The best accuracy gained from the results was approximately 96.5% when differentiating a dataset consisting of 443 samples of six classes (one benign and five ransomware families). Vinayakumar et al. studied a dataset of 974 samples (219 benign files and 755 ransomware files from seven ransomware families) and focused on the API call sequence for ransomware detection [2]. Their method gathered 131 API sequences with a dynamic analysis technique and used a multi-layer perceptron (MLP) model for classification. The experimental results showed that the best accuracy rate was 98% for multiclass classification; however, the true positive rates (TPR) of crypto-locker and cryptowall ransomware were only 88.9% and 83.3%.

Current studies mainly focus on binary classification between ransomware and normalware. However, with the rapid growth of blackmail attacks as well as the variety of types of ransomware, the detection and detailed classification of each ransomware family type are necessary at present. There have been a few studies related to multiclass classification, but those studies mainly focused on classifying categories together. Moreover, the accuracy when identifying each type of ransomware is not very high, leading to the ineffective prevention of malicious code, placing user data in danger. In order to overcome the drawbacks of previous multiclass classification techniques, this paper present a novel approach based on a dynamic analysis and the LightGBM algorithm to detect multiple types of ransomware and to distinguish between ransomware and benign files.

### III. PROPOSED METHOD AND ALGORITHM

#### A. LightGBM Algorithm

Decision trees “learn” by breaking down observations based on feature values. In the decision tree learning process, finding the best split is the most time-consuming stage. Two algorithms which use different gradient boosting decision tree (GBDT) implementations to find the best splits are as follows:

- Pre-sort: Object values are pre-sorted and all split points can be evaluated.

- Histogram-based: Continuous features are divided into separate bins used to create histograms for features.

Histogram-based algorithms are more efficient in terms of memory consumption and training speeds. However, for every feature, all data instances must be scanned to find all possible split points. So that both pre-sorted and histogram-based methods become slower as the number of instances or features increases. The LightGBM algorithm aims to address the training speed and memory consumption issues associated with typical implementations of GBDT when working with large datasets.

First, LightGBM grows the tree in a leaf-wise manner using a vertical growth strategy. This is different from the horizontal growth strategy (level-wise growth) tactics of the other decision tree algorithms. When growing leaf-wise, the gradient-based method can help the errors minimize and effectively reduce the loss. The balance of the tree is maintained via a level-wise growth strategy, whereas the leaf-wise strategy helps to reduce the loss the most. With the same number of leaves, a leaf-wise-based tree will be deeper than other trees. In particular, when necessary leaf-wise growth can be used to grow a tree into a more balanced tree. Compared to horizontal growth, vertical planting can provide converge much more rapidly [14].

Secondly, LightGBM developed two techniques to reduce memory consumption and speed up the training time [15]. These are gradient-based one-side sampling (GOSS) and exclusive feature bundling (EFB). With GOSS, LightGBM reduces the number of instances by keeping all large instance gradients and random sampling instances with small gradient instances. The complexity of constructing the histogram for all features is  $O(\#data * \#features)$  and the complexity of subsequently finding the optimal split points is proportional to  $O(\#bins * \#features)$ . Generally,  $\#bins \ll \#data$ . Therefore, this approach is computationally much more efficient than earlier approaches.

---

#### Algorithm 1. Gradient-based One-Side Sampling (GOSS) Technique

---

**Input:**  $I$ : training data,  $d$ : iterations

**Input:**  $a$ : sampling ratio of large gradient data

**Input:**  $b$ : sampling ratio of small gradient data

**Input:**  $loss$ : loss function,  $L$ : weak learner

models  $\leftarrow \{\}$ , fact  $\leftarrow (1-b)/a$

topN  $\leftarrow a \times \text{len}(I)$ , randN  $\leftarrow b \times \text{len}(I)$

**for**  $i = 1$  **to**  $d$  **do**

    preds  $\leftarrow$  models.predict( $I$ )

$g \leftarrow loss(I, \text{preds})$ ,  $w \leftarrow \{1, 1, \dots\}$

    sorted  $\leftarrow$  GetSortedIndices(abs( $g$ ))

    topSet  $\leftarrow$  sorted[1:topN]

    randSet  $\leftarrow$  RandomPick(sorted[topN:len( $I$ )], randN)

    usedSet  $\leftarrow$  topSet + randSet

$w[\text{randSet}] \times = \text{fact}$  : Assign weight  $fact$  to the small gradient data.

    newModel  $\leftarrow L(I[\text{usedSet}], -g[\text{usedSet}], w[\text{usedSet}])$

    models.append(newModel)

---

Step 1: Based on the list sorted according to the data instance gradient values, GOSS selects the top  $a \times 100\%$  largest gradient instances.

Step 2: Perform random sampling  $b \times 100\%$  on the remaining instances with small gradients.

Step 3: Recalculate the information gained by amplifying the sampled data of small gradients with  $(1-a)/b$ .

In this way, LightGBM can focus more on larger gradient (under-trained) instances without altering the original data distribution much.

EFB is a technique that uses a greedy algorithm to combine (or bundle) these mutually exclusive features into a single object (bundle of exclusive objects) and thus reduce the size. The complexity of feature histogram building is now proportional to the number of bundles  $O(\#data * \#bundle)$  rather than the number of features  $O(\#data * \#feature)$ . With EFB, LightGBM can reduce the GBDT training time without having a great impact on the accuracy.

---

Algorithm 2. Exclusive Feature Bundling (EFB) Technique

---

**Input:** *numData*: number of data  
**Input:** *F*: One bundle of exclusive features  
 $binRanges \leftarrow \{0\}$ ,  $totalBin \leftarrow 0$   
**for** *f* **in** *F* **do**  
     $totalBin += f.numBin$   
     $binRanges.append(totalBin)$   
     $newBin \leftarrow new\ Bin(numData)$   
**for** *i* = 1 **to** *numData* **do**  
     $newBin[i] \leftarrow 0$   
    **for** *j* = 1 **to**  $len(F)$  **do**  
        **if**  $F[j].bin[i] \neq 0$  **then**  
             $newBin[i] \leftarrow F[j].bin[i] + binRanges[j]$

**Output:** *newBin*, *binRanges*

---

By experimenting on several public datasets, the results demonstrated that using the LightGBM algorithm increased the training speed by more than 20 times while maintaining the same level of accuracy.

In conclusion, LightGBM offers many advantages when used to address current practical issues:

- Higher efficiency as well as faster training speeds.
- Lower memory consumption.
- Better accuracy.
- Can handle large-scale data well.
- Supports GPU and parallel learning.

### B. Proposed Ransomware Detection Method

This approach fully utilizes the advantages of LightGBM algorithm described above and presented in some previous studies [16] and [17]. Because the API functions that used in the each sample (ransomware and benign) are very different, so that the dataset based on this features is spare. To fill the gap in current ransomware multiclass classification and to overcome the disadvantages of previous methods, this research present an

approach based on a dynamic analysis and apply the LightGBM algorithm to process highly sparse data. By only using the API call sequence as the primary factor, this approach is more simple than others.

To recognize a portable executable (PE) file as good software or ransomware and further to categorize ransomware into their respective categories, we utilize a machine learning architecture, as shown in Fig. 1.

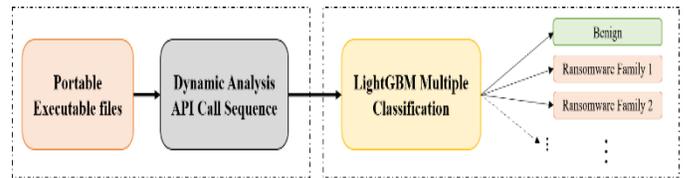


Fig. 1. Ransomware Multiple-Classification Proposed Method.

In the first step, “tagged” PE files are analyzed by means of a dynamic analysis. After which information extraction of the API call sequence functions of each individual file were performed and consider them as key features in this proposal. For the second step, samples with corresponding features and assigned labels are passed as input to the LightGBM multiclass classifier to generate learning trees that help to distinguish between good software and ransomware.

## IV. DATASET AND EXPERIMENTAL METHOD

### A. Database Gathering and Analysis

Currently, no complete dataset of ransomware on Windows platforms has been made public in cyberspace. Many authors have collected ransomware samples from multiple sources and built datasets for their own research. On the other hand, samples of ransomware often exist only sporadically in some test datasets. These dataset all malware marked ransomware, regardless of ransomware types. Previous researchers have also actively grouped ransomware types, but in experimental studies, they still mainly stop at distinguishing ransomware from normalware. Currently, there are very few researchers delving into the simultaneous identification and discernment of benign software and ransomware of various categories.

Towards the above goal, this research attempt to build a ransomware dataset for research that not only helps to distinguish between ransomware and benign software but also improves the accuracy when classifying each type of ransomware. The dataset was constructed based on a number of scientific guidelines and best practices suggested by Rossow [18]. Ransomware samples were collected from two of the most popular data-sharing sources, VirusTotal<sup>1</sup> and Virusshare<sup>2</sup>, under academic license and with the administrator's consent. Research focused on collecting both recent and earlier ransomware samples (from 2014 to early 2021) and worked to gather as much of each type of ransomware as possible. Because malicious samples were collected from two different sources, this research used a distinctive SHA hash to avoid duplications in the sample dataset. To be cautious when choosing the ransomware, we confirmed that an instance of

<sup>1</sup> <https://www.virustotal.com/>

<sup>2</sup> <https://virusshare.com/>

malware is ransomware if at least five antivirus engines marked it belonging to this category. Research rely on the naming policy of the Avast engine to determine the family of each sample before starting the process of analyzing and collecting data about the behavior of ransomware.

For benign samples, the executable files in the Windows system directory (...\Windows\System32) with a variety of functions and features of the files were selected. This could help to assess and classify malware in a more objective manner.

While Table I shows information about the benign files and ransomware samples that were taken from the two main sources, Table II details the types of ransomware along with the number of samples collected in each case.

After a dynamic analysis of 5,811 samples, we can realize that the number of API functions used by a sample ranges from 01 to 172 with approximately 286 different API functions. Ransomware and benign files both use the same API functions, but for separate purposes. Moreover, the number of API function calls in each executable file differs significantly. There are functions that are only called and used one to two times in one PE file but are used many times in other executables. During the dynamic analysis, it was noted that there are API functions invoked and used by a file during its execution up to hundreds of thousands of times. At the same time, the number of APIs used by the each sample also differs across ransomware and benign files. While 'goodware' files mostly use 10-20 different API functions, the number of API functions used by ransoms typically exceed 100. Therefore, the dataset is extremely sparse. This is highly suitable when applying the LightGBM algorithm given its many advantages when experimenting on this sparse dataset.

**B. Experiment**

The experimental process is depicted in Fig. 2 and is divided into five main steps, as follows:

**Step 1: Dynamic Analysis**

After being collected, the executable files were divided into categories, in this case benign files and ransomware files of different types (eight types of malicious codes).

TABLE I. THE NUMBER OF FILE COLLECTED FROM EACH SOURCE

Sample	Source	Number of sample
Benign	Windows system files	4,008
Ransomware	Virusshare.com	1,373
	Virusotal.com	430
Total		5,811

TABLE II. RANSOMWARE FAMILIES

No.	Ransomware Family	Number of sample
1	Reveton	522
2	TeslaCrypt	167
3	Win32:Ransom	204
4	Win32:Cryptor	123
5	Win32:Crypt	146
6	LockScreen	123
7	WannaCry	491
8	Win32:FileCoder	27
Total (Ransomware)		1,803

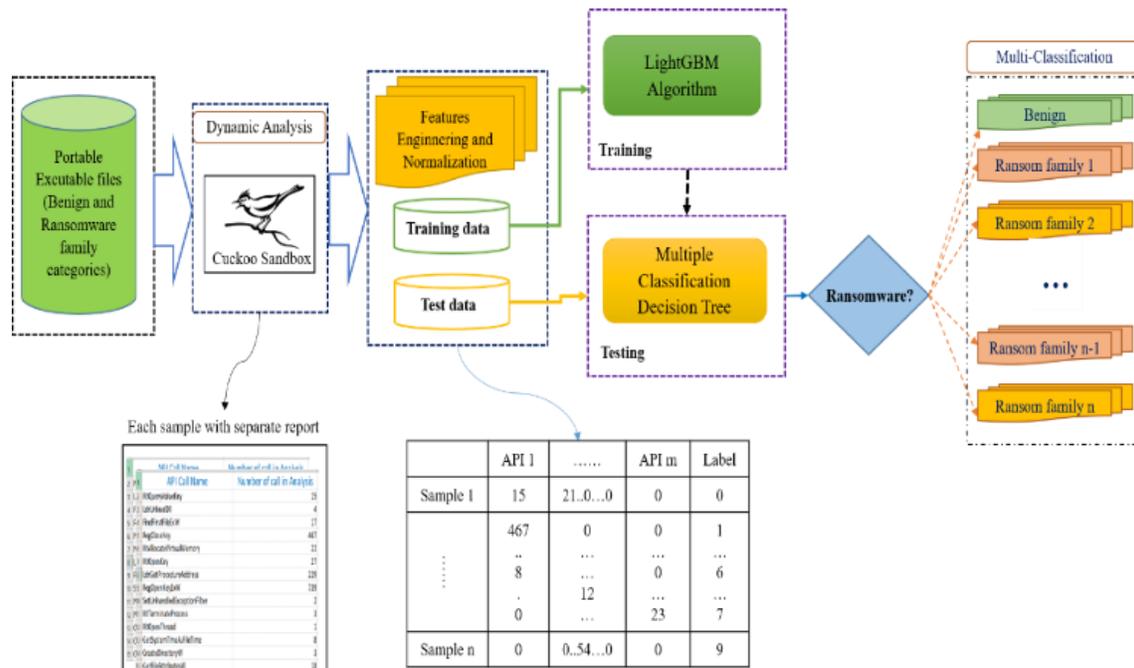


Fig. 2. Experimental Process.

The PE files are then put into the Cuckoo sandbox environment for a dynamic analysis. This is necessary and ensures safety and convenience during the dynamic analysis. The ransomware is executed in a simulated environment, during which all behaviors of every sample are collected in sandbox logs. Fig. 3 explains the Cuckoo architecture.

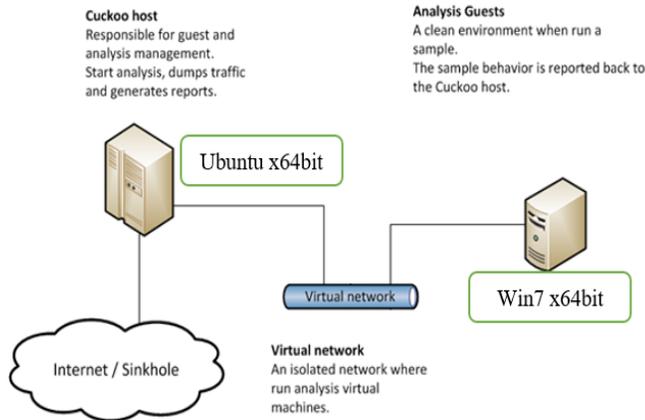


Fig. 3. The Cuckoo Sandbox's Architecture.

### Step 2: Extract API call sequence

Then information regarding the API calls that were executed during the dynamic analysis is extracted, including information about the API functions list in the order of execution and the number of times each function was executed for each individual PE file, as displayed in Fig. 4.

### Step 3: Feature Engineering and Normalization

The extracted data is then compiled into a summary of information for the entire sample. The information in the resulting table includes a list of all sample PE files along with information regarding the API calls that each file used and the number of times each function was used. With regard to API functions that are not called, the corresponding value for that function for the sample file is set to 0. At the same time, each executable file pattern is labeled corresponding to the type of ransomware or benign file, as in Table III. Because LightGBM works effectively with a sparse dataset, all features will be used in the training and testing phases.

TABLE III. LIST OF CLASS LABELS

No.	Class name	Label
1.	Benign	0
2.	Reveton	1
3.	TeslaCrypt	2
4.	Win32:Ransom	3
5.	Win32:Cryptor	4
6.	Win32:Crypt	5
7.	LockScreen	6
8.	WannaCry	7
9.	Win32:FileCoder	8

Data Normalization: Research used the MinMaxScaler of scikit-learn for data normalization. Given that the scope of the raw data is very wide, for some machine learning algorithms their objective functions will not work properly and may produce bias when the data is not normalized. MinMaxScaler normalization scales the range of all features to the range of [0, 1].

The transformation is given by Alg.3:

Algorithm 3. The MinMaxScaler normalization

$$X_{std} = \frac{X - X_{\min(\text{axis}=0)}}{X_{\max(\text{axis}=0)} - X_{\min(\text{axis}=0)}}$$

$$X_{scaled} = X_{std} * (\max - \min) + \min$$

Where: Xmin, Xmax: min, max of one feature

min, max: min, max of overall data.

The following Fig. 4 shows the data normalization process from after extracting sandbox log file to before feeding them to LightGBM algorithm.

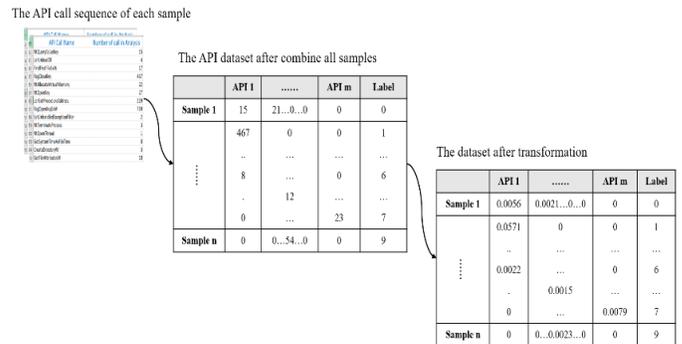


Fig. 4. The Transformation of the Data.

All data is divided as follows: training set: 80%, test set: 20%. Each dataset is then used for the subsequent training and test phases.

### Step 4: Training phase

In [17], Dongzi et al. illustrated the LightGBM training process with the model consists M trees in Algorithm 4.

Algorithm 4. The training of LightGBM

Require: Input: Training set  $\{(x_i, y_i)\}_{i=1}^M$

Ensure: Output: LightGBM model  $\hat{y}_i^{(t)}$

1. Initialize the first tree as a constant:  $\hat{y}_i^{(0)} = f_0 = 0$

2. Train the next tree by minimizing the loss function:

$$f_t(x_i) = \underset{f_t}{\operatorname{argmin}} L_{(t)} = \underset{f_t}{\operatorname{argmin}} L(y_i, \hat{y}_i^{(t-1)} + f_t(x_i))$$

3. Get the next model in an additive manner:

$$\hat{y}_i^{(t)} = \hat{y}_i^{(t-1)} + f_t(x_i)$$

4. Repeat the Step 2 and Step 3 until the model reaches the stop condition.

5. Obtain and return the final model:

$$\hat{y}_i^{(t)} = \sum_{t=0}^{M-1} f_t(x_i)$$

Here:  $f_t(x_i)$  and  $\hat{y}_i^{(t)}$ : are correspondingly the learned function and predictive value of sample i at iteration t.

$L_{(t)}$ : The loss function represents the error between the prediction  $\hat{y}$  and the true value  $y$ .

The stop condition of the training process occurs when the process reaches the M-th iteration or when the loss value of the model is lower than the predefined loss value.

Step 5: Testing phase

The test dataset is classified based on GBDT trees that have been created during training phase.

V. EXPERIMENTAL RESULT

A. Evaluation Criteria

To evaluate the detection performance of the proposed method, this paper employed the following metrics: the accuracy of the entire model, precision, recall, the F1 measure of each class, and a confusion matrix.

When evaluating each class, the class being evaluated is the positive class and the remaining eight classes are the negative class. True positive (TP) refers to the number of positive class samples that are correctly classified. False positive (FP) refers to the number of negative class samples that are misclassified into the class under evaluation. True negative (TN) represents samples in the negative class are correctly classified into the negative class. False negative (FN) represents samples in the consideration class that are misclassified.

Precision is defined as the ratio of true positive scores among those classified as positive.

$$Precision = \frac{TP}{TF + FP}$$

Recall is the fraction of the relevant samples that are successfully classified.

$$Recall = \frac{TP}{TF + FN}$$

The F1 score is used to evaluate the quality of the model.

$$F1 - score = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

Accuracy is determined simply by calculating the ratio between the number of correctly classified samples and the total in the test dataset.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN}$$

For multiclass classification, the overall accuracy is the ratio of the sum of the true positives of all families divided by the total sample. It is determined according to the following formula.

$$Overall - accuracy = \frac{correctly\ classified\ instances}{total\ number\ of\ instances}$$

The confusion matrix (CM),  $M = [m_{x,y}]_{n \times n}$ , is used to evaluate the quality of the classifier's output on the dataset. The values of the diagonal elements represent the number of samples and the percentage of correct predictions, while the other elements represent the samples that have been classified incorrectly. A confusion matrix with higher diagonal values represents a higher percentage of correct predictions.

B. Experimental Results

As shown in Table IV, the classification accuracy is very high, with overall accuracy of about 98.7%. However, the correct identification rate for all ransomware is close to 96%, while the lowest rate of identification for TeslaCrypt is 89.5%.

TABLE IV. CLASSIFICATION EVALUATION RESULTS

No.	Classes	Size	Precision	Recall	F1-Score
1	Reveton	102	0.961	0.961	0.961
2	TeslaCrypt	38	0.971	0.895	0.932
3	Win32:Ransom	38	1.000	0.921	0.959
4	Win32:Cryptor	25	0.885	0.920	0.902
5	Win32:Crypt	21	0.800	0.952	0.870
6	LockScreen	22	1.000	1.000	1.000
7	WannaCry	100	0.980	1.000	0.990
8	Win32:FileCoder	3	1.000	1.000	1.000
9	Benign	814	1.000	0.999	0.999
Total		1163	Overall accuracy = 0.987		

Fig. 5 presents the CM of the eight ransomware classes, in this case Reveton, TeslaCrypt, Win32:Ransom, Win32:Cryptor, Win32:Crypt, LockScreen, WannaCry, and Win32:FileCoder, along with the benign files in the experiments. The CM shows that the proposed method provides the best classification for three ransomware families, LockScreen, WannaCry and Win32:FileCoder, in which not a single sample is misclassified. This is followed by Reveton, with accuracy of approximately 96.1%.

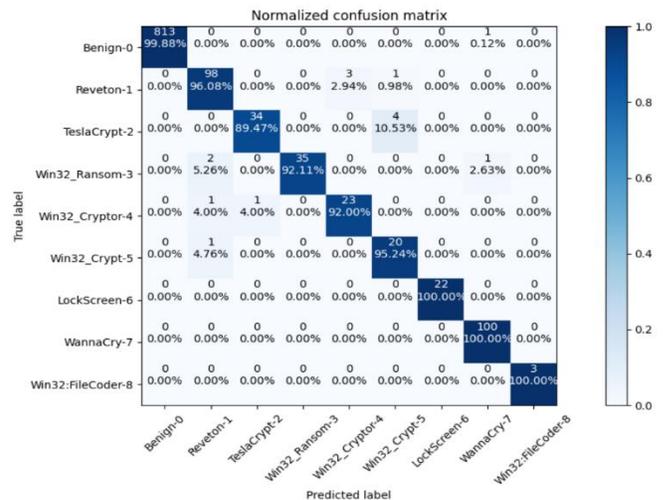


Fig. 5. Confusion Matrix.

Fig. 6 shows feature importance based on the number of times that a feature is used as split points in all learned trees. The most important API call function for detection and classification of the ransomware in this case is “NtOpenKey,” used more than 1000 times as a split point in a learned tree. This is followed by the two other API call functions of “NtAllocateVirtualMemory” and “NtTerminateProcess,” called 995 and 866 times, respectively. The three API call functions above are also among the API call functions most commonly used by samples (ranks: “NtTerminateProcess:” 1st, “NtOpenKey:” 4th, and “NtAllocateVirtualMemory:” 21st). However, while the “NtAllocateVirtualMemory” and “NtTerminateProcess” functions were used many times by all PE files (19,564,674 and 5,182,284 times) and are correspondingly ranked 3rd and 12th, the “NtOpenKey” function was only called 86,487 times and is ranked 111th of 286 (as showed in Table V). This shows that the importance of features in determining split points does not depend much on the number of times they are called or the number of file that used them.

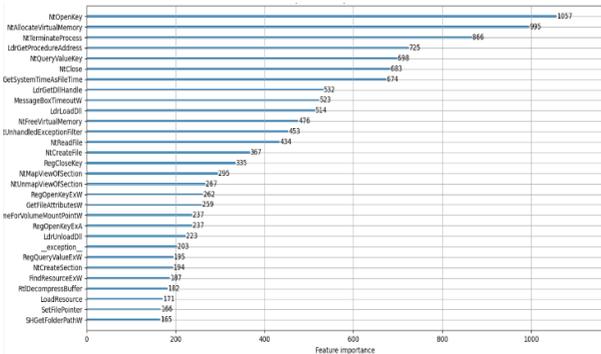


Fig. 6. The Top 30 Important Features in the Experiment.

## VI. ANALYSIS AND DISCUSSION

The experimental results have shown that the method proposed here to identify and classify malicious codes based on API call functions obtained from dynamic analysis results combined with the GBDT LightGBM algorithm can achieve high performance.

TABLE V. THE USE OF API CALL BY PE FILES

No.	API name	Times used
1	RegSetValueExA	26,547,071
2	ShellExecuteExW	26,135,049
3	<b>NtAllocateVirtualMemory</b>	<b>19,564,674</b>
4	NtOpenFile	14,268,859
5	OpenServiceW	9,484,238
...	...	...
12	<b>NtTerminateProcess</b>	<b>5,182,284</b>
...	...	...
111	<b>NtOpenKey</b>	<b>86,487</b>
...	...	...
286	NtShutdownSystem	1

The proposed method identified ransomware samples with very high accuracy, reaching 100%. When evaluating the effectiveness of distinguishing between malicious code and normal software, the experimental results show that the system did not miss or miscategorized any ransomware sample as normal software. This promises to bring about a positive effect with regard to protecting system and user data. At the same time, the rate of misidentification of benign software was low, as less than 0.01% of benign samples were misidentified as malicious samples. Therefore, the proposed method will not affect system availability and allows the user experience to be retained.

When evaluating the effectiveness of classifying ransomware types, out of eight types of malware conducted experimentally, the proposed method has the ability to identify sensitively three types of extortion malware. In this case LockScreen, WannaCry, and Win32:FileCoder, with absolute precision of 100%. In addition, there were a few small mistakes between different types of malware, such as TeslaCrypt, Win32:Ransom, and Win32:Crypt.

The test results here also demonstrated the advantages of the dynamic analysis in support of ransomware detection. The method based on dynamic analysis greatly reduced the number of features in the sample database. According to this study of the collected dataset, the number of features (API call functions) that must be analyzed and processed during the static analysis method is very large at approximately 6,684 different features with ransomware and nearly 28,500 different features in the benign case. Meanwhile, using the dynamic method, the number of API call functions to be processed for all ransomware and benign samples was only 282. This enhances the efficiency of the data analysis, classification and processing steps while also minimizing the time required for the training and detection phases, which are very time-consuming steps given numerous features. The proposed method also minimizes interference from an attacker to bypass static-analysis-based methods, such as by adding normal API call patterns or by attempting to use an obfuscation technique.

## VII. CONCLUSION

This chapter discusses the results of the proposed method, the advantages of the dynamic analysis technique in supporting ransomware detection and classification.

In fact, proposal method achieves a 98.7% classification accuracy rate, with excellent ransomware recognition and a low error rate during benign software classification. Compared to previous studies, the experimental results not only dominate in terms of detection between ransomware samples and goodware (99.9% accuracy versus 98.65%, 97.74%, and 97.3% as in [6], [4] and [3]) but is also more efficient when classifying ransom types of malware (between proposal method at 96% and corresponding rates of 88.9%, 94.2%, and 91.4% as in [2], [13], [12]). This helps to increase the efficiency of the identification process of malicious code, thereby accelerating the response and implementing countermeasures to protect the system when necessary. In particular, using LightGBM algorithm significantly shortens the time compared to other machine learning or GBDT algorithms.

The study also demonstrated the role of each API function in identifying and classifying ransomware by assessing the importance of each API function by determining the split points during the construction of the learning trees used here. This makes it possible for us to engage in more research and evaluations to reducing the number of attributes further when the number of file samples increases in the future. This helps to reduce the computational pressure while maintaining the accuracy of the method, thus enhancing the efficiency of the system.

The proposed plan has shown very positive results. Experiments also highlighted the importance of each API function in the detection and classification process. Therefore, work to reduce the number of API functions when the numbers of ransomware samples and types increase in order to reduce the computational burden while ensuring high accuracy also represents a promising research direction for future studies.

#### REFERENCES

- [1] Sgandurra D., Muñoz-González L., Mohsen R., Lupu E.C., 2016. Automated dynamic analysis of ransomware: benefits, limitations and use for detection. *Cryptography and security*, arXiv:1609.03020.
- [2] Vinayakumar R., Soman K.P., Senthil Velan K.K., Ganorkar S., 2017, Evaluating shallow and deep networks for ransomware detection and classification. *International conference on advances in computing, communications and informatics*, pp259-265, doi:10.1109/ICACCI.2017.8125850.
- [3] Hwang J., Kim Y., Lee S., Kim K., 2020. Two-stage ransomware detection using dynamic analysis and machine learning techniques. *Wireless personal communications volume 112*, 2597–2609. doi:10.1007/s11277-020-07166-9.
- [4] Khammas B.M., 2020, Ransomware detection using random forest technique, *ICT Express*, Volume 6, Issue 4, pp325-331. doi:10.1016/j.icte.2020.11.001.
- [5] Sikorski M. and Honig A., 2012. *Practical malware analysis: The hands-on guide to dissecting malicious software*, William Pollock Publisher, 38 Ringold Street, San Francisco, CA, 802pp.
- [6] Bae S.I., Lee G.B., Im E.G., 2020. Ransomware detection using machine learning algorithms. *Concurrency computat pract exper*. doi:10.1002/cpe.5422.
- [7] Kharraz A., William R., Davide B., Leyla B., Engin K., 2015. Cutting the gordian knot: A look under the hood of ransomware attacks. *12th International conference: Detection of intrusions and malware, and vulnerability assessment*, Milan, Italy, pp3-24. doi:10.1007/978-3-319-20550-2 1.
- [8] Lee K., Lee S.Y., Yim K.B., 2019. Machine learning based file entropy analysis for ransomware detection in backup systems. *IEEE Access*, vol. 7, pp110205-110215. doi:10.1109/ACCESS.2019.2931136.
- [9] Cabaj K., Gregorczyk M., Mazurczyk W., 2018. Software-defined networking-based crypto ransomware detection using HTTP traffic characteristics. *Computers & electrical engineering*, vol66, pp353-368. doi:10.1016/j.compeleceng.2017.10.012.
- [10] Almashhadani A.O., Kaiiali M., Sezer S., O’Kane P., 2019. A multi-classifier network-based crypto ransomware detection system: a case study of locky ransomware. *IEEE Access*, vol. 7, pp47053-47067, doi:10.1109/ACCESS.2019.2907485.
- [11] Shaukat S.K., Ribeiro V.J., 2018. RansomWall: A layered defense system against cryptographic ransomware attacks using machine learning. *10th International conference on communication systems & networks (COMSNETS)*, pp. 356-363. doi:10.1109/COMSNETS.2018.8328219.
- [12] Zhang H., Xiao X., Mercaldo F., Ni S., Martinelli F., Sangaiah A.K., 2019. Classification of ransomware families with machine learning based onN-gram of opcodes. *Future generation computer systems*, vol90, pp211-221. doi: 10.1016/j.future.2018.07.052.
- [13] Baldwin J., Dehghantanha A., 2018. Leveraging support vector machine for opcode density based detection of crypto-ransomware. In: *Dehghantanha A., Conti M., Dargahi T. Cyber threat intelligence. advances in information security*, vol70. Springer, Cham. doi:10.1007/978-3-319-73951-9\_6.
- [14] Haijian Shi, 2007. *Best-first decision tree learning*. PhD thesis, The University of Waikato, pp120.
- [15] G. Ke, Q. Meng, T. Finley, T. Wang, W. Chen, W. Ma, Q. Ye, T.-Y. Liu, 2017. LightGBM: A highly efficient gradient boosting decision tree. *Microsoft*, <https://www.microsoft.com/en-us/research/publication/lightgbm-a-highly-efficient-gradient-boosting-decision-tree/> [accessed 15 January, 2021].
- [16] Mohammad A.A., Ahmed M.A., Mouhammad A., 2020. Robust intelligent malware detection using light gbm algorithm. *International journal of innovative technology and exploring engineering (IJITEE)*, doi:10.35940/ijitee.F4043.049620.
- [17] Dongzi J., Yiqin L., Jiancheng Q., Zhe C., Zhongshu M., 2020. SwiftIDS: Real-time intrusion detection system based on LightGBM and parallel intrusion detection mechanism. *Computers & security*. doi:10.1016/j.cose.2020.101984.
- [18] C. Rossow , 2012. Prudent practices for designing malware experiments: status quo and outlook. *IEEE symposium on security and privacy*, pp65-79, doi:10.1109/SP.2012.14.

# Integrated Document-based Electronic Health Records Persistence Framework

Aya Gamal<sup>1\*</sup>

Faculty of Computers and Artificial Intelligence  
South Valley University, Hurghada, Egypt

Sherif Barakat<sup>2</sup>, Amira Rezk<sup>3</sup>

Information System Department, Faculty of Computers and  
Information, Mansoura University, Egypt

**Abstract**—Electronic health record systems work beyond just recording patients' health data. They have multiple secondary functionalities, such as data reporting and clinical decision support. As each of these systems' workloads has contradictory different needs, managing a multipurpose electronic health record is a challenge. This paper proposes a unified healthcare data framework that can simplify health information system infrastructure. It investigates the suitability of the document-based NoSQL persistence mechanism, storing electronic health records data as a design choice for managing varied complexity ad hoc queries used in operational business intelligence. The performance of the most popular two document-based NoSQL back-ends, Couchbase Server and MongoDB, is compared according to the size of the database and query execution time. Results showed that while MongoDB can execute simple single-document queries nearly in milliseconds. It does not provide satisfactory response time for unplanned complex queries spanning multiple documents. By utilizing its analytics services and multi-dimensional scaling architecture, Couchbase Server multi-node cluster outperforms the response times of MongoDB for both simple and complex healthcare data access patterns. The primary advantage of the proposed tightly coupled EHRs processing framework is its flexibility to manage workload according to changing requirements.

**Keywords**—Electronic health records; operational business intelligence; document data model; NoSQL; health information system; persistence framework; Couchbase server

## I. INTRODUCTION

Electronic health records (EHRs) system is a quintessential part of healthcare information system (HIS). It is an ecosystem for maintaining a long-term patient's health record. This system usually has multiple core functionalities. Primarily, it is used for storing and retrieving individual patient records for healthcare purposes. These EHRs data could be used in clinical decision support (CDS) to suggest the next steps for treatment or predict future conditions trends by analyzing transactional data [1]. EHRs data are not possessed by any particular healthcare provider. To interconnect these different healthcare practitioners, EHRs need to be interoperable through following certain standards to facilitate health information exchange (HIE) and sharing [2]. HIS workload usually encompasses two main practices: clinical use, which is regarded as a transactional workload, and research use which is dedicated to analytical workload.

As each of these workloads has a different access pattern, they have seemingly contradictory solutions. There is also the

operational business intelligence (BI) workload, including ad hoc queries, which are in the middle between primary and secondary uses. This data access pattern tends to be unpredictable; it typically involves reading an extensive amount of data at one time and can include various complex joins [3]. There are various architectural methodologies [4,5] to manage those conflicting workloads. Traditional HISs could use transactional systems for providing answers to analytical queries in one engine, but the system performance may degrade dependent on the number and the complexity of queries submitted to the database. Therefore, following the "one size does not fit all" rule [6], a clinical data warehouse (CDW) [7,8] a specialized storage structure, is used for data analysis to segregate tasks and maintain the performance at an acceptable level. It utilizes extract, transform, and load (ETL) to integrate patient-level data from separate silos inside or across healthcare organizations, facilitating analysis and reporting. Thus, various healthcare application frameworks [9] have been introduced to offer diversified EHRs data analytical capabilities.

Earlier healthcare data persistence systems [10] were built depending on the relational schema approach. However, these traditional relational database management systems RDBMS are built for strong consistency level and data control [11]. With the rise of the "no one size fits all" concept [12], several alternative NoSQL stores have been developed [13] to address the shortcomings of RDBMS. NoSQL databases refer to a category of flexible data storage systems that manage data using a key-value structure. They are clustered into four main classes [14,15] based on their data model: (1) key-value data stores, (2) document data stores, (3) column-family stores, and (4) graph data stores. This categorization is necessary since each data storage architecture provides different solutions depending on the application's needs.

Healthcare data is complex, dynamic, intermittent, and diverse in nature. Furthermore, HIS applications' access patterns usually need their scale, performance, and flexibility requirements to surpass their transactional needs [16,17]. Thus, NoSQL data stores are more suitable to meet the specifications of distributed EHRs systems [18]. There are several criteria, such as data model, performance, data persistence, and CAP support [19], which must be considered when choosing which NoSQL store to be used. Various data modeling approaches [3,20–27] have been introduced for medical data persistence according to use case scenarios. These works investigate not only the type of NoSQL store that has to be chosen but which NoSQL products in that type will be used [19].

\*Corresponding Author

Managing a fully functional EHRs system with the involvement of all healthcare participants is not a simple task because of the rapid development and growth of medical knowledge. To fulfill a variety of use cases, organizations nowadays commonly end up deploying different databases, leading to a “database sprawl” that causes delayed analytics. This layered architecture approach was challenged by the white paper [28] which argued that advances in memory technology enable data to be stored just once without compromising either transactions or analytical workloads. Massive parallel processing (MPP) database platform is considered as another architectural alternate to CDWs that could support medical data analytics [29]. It could be used for ad hoc population queries, which may not be quickly obtained from the CDW.

The capability to store data quickly is not a problem. But the challenge is the capability to do meaningful and quick insights with that data. Recently, Analytical application characteristics diverged from the typical characteristics of the online analytical processing (OLAP) system and become more real-time, operational, and proactive. Modern applications frameworks require blurring borders between operational and analytical workload [4]. Several terms, such as Hybrid Transactional and Analytical (HTAP) databases [30,31], are being used to describe this general trend in databases that supports hybrid workload processing requirements within a single logical database. Couchbase Server recently introduces multi-dimensional scaling (MDS) architecture [33] to support scaling workload independently according to the changing needs. It aims to offer a single, integrated platform that can be used for almost all varied complexity operational workloads as well as operational analytics. The motivation for this paper is that nevertheless, these hybrid data processing and management techniques [16,32] could provide solutions to a wide range of healthcare data problems, such as data silos. Few researchers evaluate their performance in the healthcare sector.

The main contribution of this paper is it proposes a unified multipurpose HIS framework that could improve healthcare services provision. This flexible Couchbase-based healthcare architectural framework provides different levels of services that could be efficiently adapted according to varied application workload requirements. As both database selection and its related schema architecture are aspects that affect the effective management of healthcare data, particularly in real-time usage systems [10]. This paper first discusses the suitability of the document data model as storage persistence for managing EHRs data. After that Couchbase Server and MongoDB which are the most popular document-oriented database management systems (DODBMSs) are evaluated for BI workload. These two storage back-ends storing EHRs are compared on the subject of their execution time and storage space requirements for handling varied queries complexities.

The rest of this paper is organized as follows: Section 2 reviews document-based data modeling techniques and their suitability for the healthcare domain. Section 3 describes the experimental environment, including datasets, workload specifications, and query implementation. Section 5 reports the experimental results for the two different size datasets. Section 4 briefly discusses the obtained results.

## II. DOCUMENT DATA MODELING

A document database is a set of key-value in which each key corresponds to a complex data structure value known as a document. Each document holds a unique automatically generated key which not only enables gathering related documents. But also enables an application to perform keys-based document lookup, which is extremely fast. A document’s structure in the document model database is made up of the arrangement of its internal attribute-value pairs [34]. In document-oriented databases, stored values are arranged, in a self-descriptive document that can be examined easily. There are several advantages of using document-oriented modeling, unlike relational databases that force applications to fit data into predefined models, regardless of their needs [35]. First, there is no impedance mismatch between application objects models and documents data models [36]. Second, they do not impose standard document structures, even across several documents. It allows a schema to gradually evolve by adding properties and structures to the document as required without the need to update other documents in the same way. Thus, the schema is explicit but variable, since attributes may vary among instances [37]. This allows applications to change their behavior without having to overhaul all the source data or take applications offline to make a basic change. Therefore, they offer faster write performance than the conventional relational model, besides efficient indexing features. In relational databases, [38] children use foreign keys to refer to their parents. On the other hand, parents refer to their children in document databases. This is because, unlike a field in a row, a field within a document can have several values.

Embedding and referencing are two techniques that could be used to link documents. Document embedding concerns nesting documents into another. It entails merging subclass entities into superclass entities and denormalizing relationships without the need for a reference table. On the other side, document refereeing is based on two separate documents, and one is refereeing into another. It involves adding a key to the object [34,39] and it is good when the referenced objects and relationships are static. Usually, deciding how to model related data documents normalized, denormalized or a hybrid is based on the type of relationship and the access pattern.

In today’s market, there are a variety of document-oriented NoSQL databases; Couchbase [40] and MongoDB [41] are the most popular. Couchbase is a scalable in-memory NoSQL database, which was designed particularly for distributed processing and has native support for JSON documents[42,43]. It was created through merging two complementary technologies: Membase Server, a distributed key-value database based on Memcached, and CouchDB, a single-node document database supporting JSON. It has N1QL, a declarative query language that can manipulate JSON documents. A Couchbase node usually comprises of cluster manager and, optionally, data, query, index, analytics, search, and eventing services. Couchbase Server introduces MDS architecture, which is independent scaling architecture, for minimizing interference between services [33]. MongoDB uses a slightly modified version of JSON called BSON (Binary JSON). It has its own DBMS, including the full set of CRUD (create, read, update and delete) operations.

### A. Document-based EHRs Data Modeling

Because of the special persistence policies of EHRs data. NoSQL systems fit better [20,21], as they allow healthcare data to be stored in a structure that is much closer to its real representation. NoSQL databases are aggregate-oriented data stores [36], as the aggregate is the unit of operation and consistency. They can be more scalable and faster where data volumes are extremely large, or when there are no internal document references that might degrade the performance or data consistency. On the other hand, healthcare applications could be an obvious example of an application type, where the presence of connections between various documents and their subcomponents has no impact on the application's basic functionality and consistency. This is because, if part of these data is updated during such medical treatment, a new extract with new information and their appropriate connections should be created, rather than overwriting any previously stored data elements [18]. This is a rigorous medical information constraint since it may be used to make medical decisions. When using a document-based store instead of a relational system, information about a particular patient is easily isolated from other patients' information.

So, healthcare tasks could be considered document-based tasks. Retrieving all patients' demographic data and linked hospital admissions. These flexible modeling approaches could efficiently adapt to the nature of healthcare data. Thus, several studies have been initiated along this path [3,20,24,44-47]. According to related work [20] result, MongoDB is best for handling single patient queries because of their concurrency. While Couchbase in [3,24] achieved better query response

times and throughput. Thus, it is the best for handling the analytical workload of scalable, large data size.

### III. PROPOSED DOCUMENT-BASED ELECTRONIC HEALTH RECORDS FRAMEWORK

In multi-node cluster topology, the Couchbase Server services are distributed across several nodes within the cluster, rather than a single node cluster. The main aim of this microservices architecture is deploying both query and analytics services, which are complementary services with contradicting workload needs, into two independent nodes within the cluster. Query service is used to support many users in making inexpensive operational queries. While analytics service is used to support complex and expensive analytical queries made by a much smaller number of users [43]. Data and query services provide user-facing applications with low-latency key-value and/or query-based access to their data. For analytics service, operational EHRs data is pushed into shadow buckets of the same data for immediate analysis by a dedicated massively parallel processing (MPP) analytics engine. These shadowed buckets are copies of data that are linked directly to the operational data in real-time. So, these analytical queries do not affect the performance of operational data queries. Cross data-center replication (XDCR) is used to replicate EHRs data per bucket basis between two data nodes in different clusters depending on application requirements. These replicated vBuckets can support read requests as they are kept constantly up to date by receiving a continuous stream of mutations from the active vBucket through database change protocol (DCP). Fig. 1 shows a high-level illustration of the deployed EHRs multi-node topology for varied access patterns.

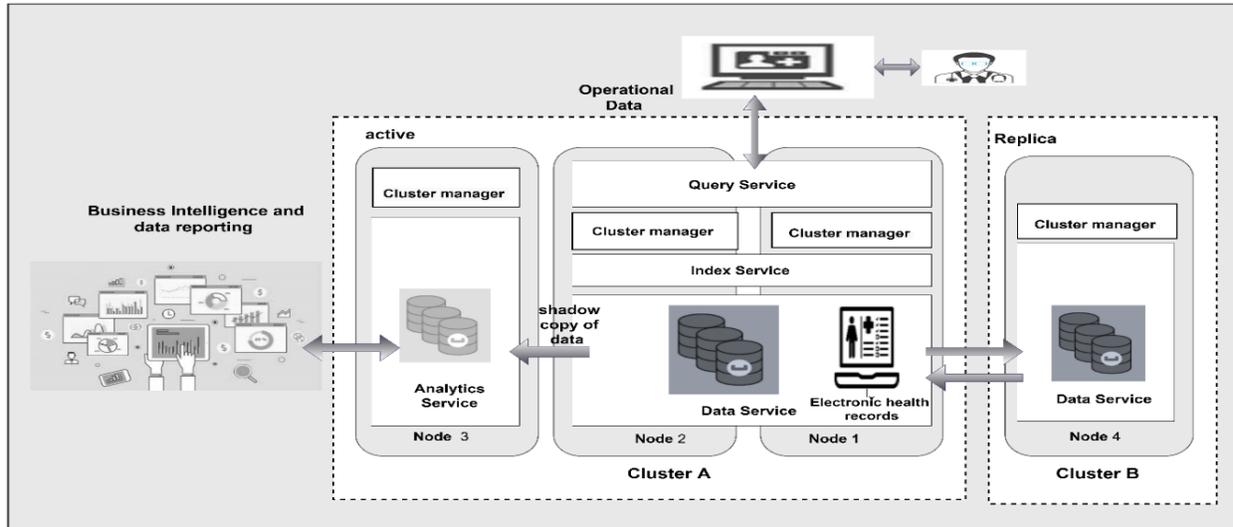


Fig. 1. Proposed Document-based Multifunctional EHRs Persistence Framework.

#### IV. EXPERIMENTAL SETUP

Two NoSQL database management systems: Couchbase 6.6.2 and MongoDB 4.4.3 are used to assess the suitability of document-based persistence to store and retrieve EHRs objects. The two NoSQL products were deployed in a single machine with the following specifications: Intel core i7 -10750h CPU @ 2.60GHz, with 16GB of memory and an SSD storage system of 256GB, running windows 10 \_64 bits.

The workloads were tested under the following conditions: data fit the memory, and replication is set to “1” signifying that just a single replica is available for each dataset. All executions are warm runs, so either caching techniques must be disabled, or each query must be performed individually to fill the cache. Queries must be prepared according to the native scripting language of the target database and run directly from the command line interpreter within the chosen system.

##### A. Dataset

Our experiment investigates the performance of the document-oriented database to store Fast Healthcare Interoperability Resources (FHIR) [48] compliant EHRs data. The used EHRs data is two different size synthetic patient datasets with COVID-19 [49,50]. These synthetic datasets have been generated by SyntheaTM [51], an open-source patient population simulation available from the MITRE Corporation.

SyntheaTM is a synthetic patient generator [52] that simulates the medical history of synthetic patients. Patient data and related health records covering several aspects of healthcare are realistic but not genuine. Every record in this EHRs dataset contains administrative, demographic, and healthcare information concerning a patient. These records are subdivided into different data sources or categories that encompass all the different aspects of healthcare. They also span practitioner, care team, device, organization, location, healthcare service, diagnostic, medications, as well as the financial tasks, such as insurance coverage. Core data elements are presented in Table I.

FHIR specification is a next-generation standard framework developed by HL7 to facilitate faster and more efficient integration, exchange, and retrieval of EHRs data. It bases on the concept of “resources”. One of the key objectives of FHIR is that it does not enforce the exchange of whole documents, but it allows the exchange of specific pieces of information. Hence, enabling interoperability across various functional applications and ultimately reducing the cost of the implementation. FHIR data model is relational in nature. It centers around the ‘patient’ object or resource. Each object has a unique identifier ‘id’ field. This id is used to reference most resources to the ‘patient’ object. As a result, the patient resource collection has been normalized into individual resource-type documents in which the objects that are associated with a patient are linked by the patient’s id in the subject field.

##### B. Workload

HIS workload usually involves clinical practice queries which are used to get single patient data and research queries that are dedicated analytical workloads.

TABLE I. DATASETS SIZE AND THEIR ATTRIBUTE NUMBER

Objects	10k patient	100k patient
Allergies	5,417	51,592
Careplans	37,715	377,726
Conditions	114,544	1,143,900
Devices	2,360	23,694
Encounters	321,528	3,188,675
Imaging_Studies	4,504	45,609
Immunizations	16,481	168,160
Medications	431,262	4,227,723
Observations	1,659,750	16,219,969
Organizations	5,499	9,175
Patients	12,352	124,150
Payer_Transitions	41,392	409,553
Payers	10	10
Procedures	100,427	979,564
Providers	31,764	60,534
Supplies	143,110	1,389,858
<b>Total Item Number</b>	2928115	28419892
<b>MongoDB Size</b>	878.732 MB	8.17 GB
<b>Couchbase Size</b>	1.37GB	14.2GB
<b>CSV Data File Size</b>	504 MB	4.78 GB

Operational BI workload is read-intensive, with writes that do not conflict with reading queries. It resembles the workload of an OLTP application, where quick response times are desired. This workload includes a type of ad hoc query that is used for real-time reporting.

The motivation behind this paper was the belief that ad hoc queries are not planned before, thus having any query indexing. It investigates two back-ends behaviors for ad hoc queries that are examples of real-time analytical queries with different levels of complexity and may have joins and aggregations. The performance of each database was evaluated under queries range in complexity, from simple ad hoc read queries to complex join queries. Simple read workload usually includes filtering constraints and sorting operations and aggregate lookups. While join workload involves join operations with grouping and aggregation functions. These queries declared in Table II and Table III were identified and written according to each database query language. Specific queries whose behavior could differ widely from the others are chosen to differentiate the performance of the databases and avoid bias.

##### C. Query Implementation

Two database architectural topologies for the two storage back-ends storing EHRs were deployed to investigate for handling different queries complexities. MongoDB experiments were deployed to single unsharded data cluster architecture. While Couchbase Server investigates two database topologies, which are single node cluster and multi-node cluster.

TABLE II. SIMPLE AD HOC READ QUERIES

Q1	Retrieve patients' names and their age
Q2	Rank the encounter count of hospitals
Q3	Find all dead patients' data.
Q4	The number of inpatients.
Q5	Arrange conditions according to their co-occurring
Q6	Arrange encounters according to the number of conducted encounter class
Q7	Count of non-survivor
Q8	The age of dead patients
Q9	The average age of non-survivor
Q10	Max-age of non-survivors
Q11	Mortality by sex
Q12	Mortality by age
Q13	Total count of supplies
Q14	Medications dispensed to patients with COVID-19 since January 20, 2020
Q15	Total cost for every medication dispensed to patients with COVID-19
Q16	Number of patients required ventilator
Q17	All the conditions starting after January 20, 2020
Q18	Cumulative case count of covid over time
Q19	Number of patients with COVID-19 conditions
Q20	The max duration length of any COVID-19 patients
Q21	Care plans for all COVID-19 patient
Q22	Allergies ordered according to co-occurrence
Q23	Maximum observed temperature
Q24	The total number of patients who take influenza immunizations
Q25	The max cost of procedures

TABLE III. COMPLEX JOIN QUERIES

Q1	Retrieve patients' names and their current unresolved conditions
Q2	All patients who were at Beverley hospital on 2011-08-18
Q3	Patients' names with their insurance claim cost
Q4	Merge patients' names with their COVID-19 conditions
Q5	Period time every covid patient connected to a ventilator
Q6	Total cost for every covid patient
Q7	The total cost of medication for every covid patient
Q8	The number and total cost of immunization for every patient
Q9	Period time for every covid patient
Q10	Number of female and male patients with covid
Q11	Number of providers in every organization
Q12	All observations for patients with covid
Q13	All observations for patients who are not diagnosed

For Single node topology in MongoDB, the aggregation pipeline framework is used to implement queries using the concepts of multi-stage data processing pipelines. It uses the \$lookup operator to apply left outer JOIN queries over an unshared collection in the same database [53].

For Couchbase Server single node cluster topology, all database services (query, index, and data) are contained in a single zone. In such architecture, the query service is used to handle all different complexity workload types. While for multi-node cluster topology, the Couchbase Server services are distributed across several nodes across several nodes rather than a single node.

## V. EXPERIMENTAL RESULTS

### A. Evaluation Criteria

The majority of the healthcare system's tasks usually entail searching the databases. An EHRs system's execution time is an essential performance parameter, and storage space efficiency could decrease future maintainability costs. Thus, reducing database query response time significantly improves the EHR system's performance and functionality [54]. This paper evaluates how DODBMSs store and retrieve EHRs in the context of storage space and response time.

### B. Database Size

Both 10k and 100k patients' datasets files [55] are initially available in the SCV format with approximately 500 megabyte and 5-gigabyte sizes. Table I shows the two data sets' sizes when stored in each backend. To upload data into the Couchbase server, a command-line utility, \$cimport, is used to import synthase COVID-19 CSV files into JSON Couchbase format. While for uploading data into MongoDB, the mongoimport tool is used. Couchbase and MongoDB demand 2.9 and 1.7 times more space correspondingly than CSV storage space for both datasets of different sizes.

## VI. RESPONSE TIME

Database performance is defined by the speed at which a database process workload. In our evaluation, the primary factors related to the performance of the database are the query complexity level and the size of the dataset. To investigate the scaling capability of the two back-ends, the same queries were applied to both 10k patients and 100 k patients' datasets, respectively. All queries' response time and the number of examined documents grouped by the database are represented in the following tables. Queries are mainly divided into two types. Simple ad hoc read queries that retrieve data from a single collection or bucket and complex join queries that span multiple collections to get data.

Table IV and Table V respectively show simple retrieval queries' execution times for the two datasets. There is a linear complexity increase in query response time as the database size grows. This is because the database execution time increases with the same queries, by scaling the dataset from 10k patients to 100k patients. However, query optimization techniques like indexing are not likely to be used for that type of ad hoc analytical query. Execution time was reported with and without documents indexing for the small dataset to declare the benefit of indexing to enhance query performance. Even Q23 scanned the observation document, which has the largest size. It achieved the smallest execution time value because the two attributes of the query are indexed to make a covering query. Covered queries usually retrieve results directly from the index without the need to access datasets documents. Without

indexing, Q23 achieved the highest execution time for both databases. The same explanation is for Q7, Q8, Q9, and Q10 execution time. These queries utilized indexing deathdate and birthdate attributes as a covering index. Q24 achieved the lowest execution time because the number of scanned attributes is quite smaller than many other queries besides that it used the covering index. Even with indexing, Q6 reported high response time values. This is because of the low selectivity of the encounter class's attribute values. MongoDB reported observable better execution time than Couchbase in the case of simple queries scanning the small 10k patient dataset.

For the larger 100k patient dataset, MongoDB still reports better execution time than Couchbase except for Q4, Q6, and Q13. This is because of the large number of the queries' scanned attributes and usually, Couchbase is reported to be better for large-scale data. By utilizing Couchbase analytical services in multi-node architecture, database performance was enhanced significantly.

TABLE IV. SIMPLE QUERIES EXECUTION TIME FOR 10K PATIENT DATASET

	Execution time (ms) with index		Execution time (ms) without index		Number of examined documents
	<i>Couchbase</i>	<i>MongoDB</i>	<i>Couchbase</i>	<i>MongoDB</i>	
Q1	711	39	731.6	64	12352
Q2	411.4	12	419.1	42	5499
Q3	413.9	9	812.1	19	12352
Q4	22700	319	50200	871	321528
Q5	7300	288	5800	453	114544
Q6	20500	505	48900	806	321528
Q7	266.3	2	691.5	53	12352
Q8	158.6	14	721.5	22	12352
Q9	169.5	12	778.6	56	12352
Q10	241.4	17	840.8	26	12352
Q11	240.4	10	690.4	66	12352
Q12	173.5	18	670.4	77	12352
Q13	12900	276	7000	452	143110
Q14	25800	328	1m0.8s	631	431262
Q15	23800	393	1m11.1s	1073	431262
Q16	88.9	10	235	20	2360
Q17	7200	125	6200	246	114544
Q18	468.7	32	5800	102	114544
Q19	200.5	20	6200	142	114544
Q20	1300	91	5900	123	114544
Q21	2300	78	2400	328	37715
Q22	328.1	21	352.5	35	5417
Q23	3800	90	4m28s	3498	1659750
Q24	50	6	821.1	36	16481
Q25	6800	111	5400	200	100427

TABLE V. SIMPLE QUERIES EXECUTION TIME FOR 100K PATIENT DATASET

	Execution time (ms) with a primary index		Execution time (ms) without index	Number of examined documents
	<i>Couchbase</i>	<i>MongoDB</i>	<i>Couchbase analytics</i>	
Q1	4600	1169	1500	124150
Q2	377	129	111.90	3188675
Q3	3900	899	323.55	124150
Q4	4700	12137	1990	3188675
Q5	6600	3142	1830	1143900
Q6	7.900	15136	3720	3188675
Q7	5200	447	111.76	124150
Q8	4400	694	86.31	124150
Q9	4400	579	95.64	124150
Q10	4300	864	98.67	124150
Q11	4600	420	78.66	124150
Q12	4700	344	122.34	124150
Q13	1400	5136	867.99	1389858
Q14	24800	13236	4800	4227723
Q15	49200	8974	5.24s	4227723
Q16	919.1	46	128.67	23694
Q17	2800	1796	2210	1143900
Q18	17800	1400	673.41	1143900
Q19	8100	1876	557.71	1143900
Q20	7200	1678	757.81	1143900
Q21	13500	1211	607.60	377726
Q22	1700	439	146.02	51592
Q23	10m0s	31427	19510	16219969
Q24	5100	766	370.29	168160
Q25	21700	3039	781.44	979564

For complex join queries, Table VI and Table VII show execution time for the two datasets correspondingly. For the 10k dataset, Couchbase achieved better response time than MongoDB except for Q2 and Q7, which scanned few attributes. Q12 achieved the highest response time for both back-ends. As it both examined and retrieved many documents. Conversely, Q2 achieved the lowest response time for both back-ends besides Q6 for Couchbase. The number of scanned attributes results from the total number of joined documents attributes. MongoDB was considerably slower than Couchbase for join queries. It was not investigated against join queries for the 100k patient dataset, as it reported a very long response time for the small dataset. Even there is no indexing and there are many examined documents. Couchbase Analytics service enhances the execution time of ad hoc join workload dramatically. Q11 and Q12 reported the lowest and the highest execution time, respectively. This is because the Couchbase Analytics service is usually based on parallel join and those two queries examine the largest and the smallest number of scanned attributes. For two different queries with the same complexity and attribute number, the execution time is approximately the same.

TABLE VI. JOIN QUERIES RESPONSE TIME FOR 10K PATIENT DATASET

Join query	Couchbase execution Time	MongoDB execution Time	Number of examined documents
Q1	26500	6205489	321528
Q2	1800	691	5499
Q3	32800	562485	12,352
Q4	16400	192263	114544
Q5	2700	6725	2360
Q6	1100	31164	321528
Q7	19800	744	431262
Q8	6000	373802	16481
Q9	1600	195980	114544
Q10	1700	67823	321528
Q11	5000	322827	31764
Q12	51900	3085553	1659750
Q13	6900	3002136	1659750

TABLE VII. JOIN QUERIES RESPONSE TIME FOR 100K PATIENT DATASET WITH ANALYTICS SERVICE

Join query	Execution Time Couchbase analytical service	num. of docs scanned
Q1	10800	3312825
Q2	2400	3322000
Q3	15570	3312825
Q4	1920	1268050
Q5	13730	3212369
Q6	3030	3312825
Q7	3320	1050668
Q8	876.43	292310
Q9	2510	3312825
Q10	2210	3312825
Q11	350.12	69709
Q12	39300	19408644
Q13	37980	19408644

## VII. DISCUSSION

This research investigates the appropriateness of two DODBMS storing EHRs data for BI workload. For single-node topology, MongoDB performed better for simple look-up queries, but their performance decreased with JOIN queries spanning multiple collections and involving aggregation. It was considerably slower than Couchbase for join queries of larger datasets. Conversely, Couchbase single node cluster reported better performance for complex join queries, but their performance decreased for simple lookup queries.

These results motivated us to utilize Couchbase server MDS architecture to distribute services across several nodes rather than a single node. An interesting result of the Couchbase multi-node cluster performance analysis is that, by using an analytics service with no index, the Couchbase server reported better response times than MongoDB for both types of ad hoc queries. This multi-service architecture decreased the query latency dramatically.

MongoDB uses the \$lookup operator to apply JOIN operations, which traverse several collections. According to the result, this costly operation significantly increases latency and overall strain on the database. An alternative solution to handle these costly join operations in MongoDB is to denormalize the data model by embedding elements into their parent objects and performing a regular query. The major disadvantage of this denormalization approach, especially in a distributed system, is that it leads to data redundancy, which causes a significant write-performance downgrade to maintain consistency across multiple copies through multiple write operations. Furthermore, this modeling approach brings additional storage costs. It could be considered as an optimal response scenario with only one user submitting a single query at a time. Besides that, MongoDB provides a native connector for BI, which could provide support for real-time analytics by integrating with a leading BI and analytics tool.

The proposed converged Couchbase EHRs system infrastructure has significant advantages compared to the other loosely coupled alternatives. It supports using a common flexible document data model for both operational and analytical data with no transformation required for analysis. So, it could offer fast reporting and decision-making capabilities based on real-time and advanced analytics for large volumes of data without needing to move data around. Instead of managing and synchronizing many systems with several connections points [31].

The analytical workload is usually read and compute-intensive because it entails more massive costly calculations over data. So, it is typically ideal to perform analytical workload in isolation. Couchbase Server separates the competing workloads into independent services and isolates them from each other. Consequently, interference among them is minimized. Operational workload latency and throughput are isolated from analytical query workload slowdowns but without the complexity of operating a separate analytical database. It allows running analytics in extremely current data with no ETL process that delays data.

An important principle in medical systems is that when any data element is modified, it will not be overwritten. Rather, a new element with a suitable link is added. On the other hand, large-scale healthcare applications scenarios usually do not strictly enforce ACID properties. They deploy optimistic locking, as they desire isolation, but not at the rate of a significant performance penalty. For such scenarios, Couchbase Server, which is an append-only store that enforces the BASE (Basically Available, Soft State, Eventually Consistent) philosophy, seems to be a promising solution covering many EHRs systems use-cases. Their flexible MDS framework enables users to scale or shrink their cluster, involving data management resources as requirements change.

## VIII. CONCLUSION

This paper investigates the appropriateness of DODBMS for handling operational BI workload. MongoDB does not provide satisfactory response time for unplanned join queries spanning multiple documents contrarywise Couchbase which reports better performance for these complex queries. By utilizing its analytics services and multi-dimensional scaling

architecture, Couchbase Server multi-node cluster outperforms the response times of MongoDB for both simple and complex healthcare data access patterns. Couchbase is the ideal solution for our needs as long as we need to store unstructured health data in various EHR systems. This paper proposes a tightly coupled Couchbase healthcare framework that can efficiently adapt to different workload needs. Along this path, using complementary Couchbase services for architecting a monolithic framework enables new technical capabilities which serve as the foundation for a new class of intelligent applications such as machine learning, real-time operational reporting. Finally, the emergence of HTAP DBMSs does not imply the end of the massive, monolithic OLAP warehouse. But such systems will be required to serve as a universal back-end database for all an organization's front-end OLTP silos.

#### REFERENCES

- [1] F. Winter, A. Haux, R. Ammenwerth, E. Brigl, B. Hellrung, N. Jahn, *Health Information Systems: Architectures and Strategies*, Springer-Verlag London, 2011. <https://doi.org/DOI 10.1007/978-1-84996-441-8>.
- [2] G. Pradeep K. Sinha, A.D. Sunder, Prashant Bendale, Manisha Mantri, *Electronic Health Record Standards, Coding Systems, Frameworks, and Infrastructures*, Wiley, 2013. <https://doi.org/10.1055/s-0038-1638463>.
- [3] S.M. Freire, D. Teodoro, F. Wei-Kleiner, E. Sundvall, D. Karlsson, P. Lambrix, Comparing the performance of NoSQL approaches for managing archetype-based electronic health record data, *PLoS One*. 11 (2016) 1–20. <https://doi.org/10.1371/journal.pone.0150069>.
- [4] R. Jain, In Search of Database Nirvana: The Challenges of Delivering Hybrid Transaction/Analytical Processing, (2016).
- [5] F. Özcan, Hybrid Transactional Analytical Processing: A Survey, (2017) 1771–1775. <https://doi.org/https://dl.acm.org/doi/10.1145/3035918.3054784>.
- [6] M. Stonebraker, U. Çetintemel, 'One size fits all': An idea whose time has come and gone, *Proc. - Int. Conf. Data Eng.* (2005) 2–11. <https://doi.org/10.1109/ICDE.2005.1>.
- [7] M.J.S. Benjamin M. Davis, Glen F. Rall, Using Electronic Health Records for Population Health Research: A Review of Methods and Applications, *Physiol. Behav.* 176 (2017) 139–148. <https://doi.org/10.1016/j.physbeh.2017.03.040>.
- [8] L. Marco-Ruiz, D. Moner, J.A. Maldonado, N. Kolstrup, J.G. Bellika, Archetype-based data warehouse environment to enable the reuse of electronic health record data, *Int. J. Med. Inform.* 84 (2015) 702–714. <https://doi.org/10.1016/j.ijmedinf.2015.05.016>.
- [9] V. Palanisamy, R. Thirunavukarasu, Implications of big data analytics in developing healthcare frameworks – A review, *J. King Saud Univ. - Comput. Inf. Sci.* 31 (2019) 415–425. <https://doi.org/10.1016/j.jksuci.2017.12.007>.
- [10] K.K.Y. Lee, W.C. Tang, K.S. Choi, Alternatives to relational database: Comparison of NoSQL and XML approaches for clinical data storage, *Comput. Methods Programs Biomed.* 110 (2013) 99–109. <https://doi.org/10.1016/j.cmpb.2012.10.018>.
- [11] S. Navathe, R. Elmasri, *Fundamentals of Database Systems*, 7th ed., Addison-Wesley, USA, 2016.
- [12] M. Stonebraker, S. Madden, D.J. Abadi, S. Harizopoulos, N. Hachem, P. Helland, The end of an architectural Era (It's time for a complete rewrite), 33rd Int. Conf. Very Large Data Bases, VLDB. (2007) 1150–1160. <https://doi.org/10.1145/3226595.3226637>.
- [13] N. Leavitt, Will NoSQL Databases Live Up to Their Promise?, *Computer (Long Beach, Calif.)*. 43 (2010) 12–14. <https://doi.org/10.1109/mc.2010.58>.
- [14] R. Cattell, Scalable SQL and NoSQL data stores, *SIGMOD Rec.* 39 (2010) 12–27. <https://doi.org/10.1145/1978915.1978919>.
- [15] A. Davoudian, L. Chen, M. Liu, A survey on NoSQL stores, *ACM Comput. Surv.* 51 (2018). <https://doi.org/10.1145/3158661>.
- [16] C.S. Kruse, C. Kristof, B. Jones, E. Mitchell, A. Martinez, Barriers to Electronic Health Record Adoption: a Systematic Literature Review, *J. Med. Syst.* 40 (2016). <https://doi.org/10.1007/s10916-016-0628-9>.
- [17] T. Nguyen, Big data system for health care records, *J. Sci. Policy Manag. Stud.* 33 (2017) 146–156. <https://doi.org/10.25073/2588-1116/vnupam.4101>.
- [18] M.Z. Ercan, M. Lane, Evaluation of NoSQL databases for EHR systems, *Proc. 25th Australas. Conf. Inf. Syst. ACIS.* (2014).
- [19] P.P. Khine, Z. Wang, A review of polyglot persistence in the big data world, *Information*. 10 (2019). <https://doi.org/10.3390/info10040141>.
- [20] R. Sánchez-De-Madariaga, A. Muñoz, R. Lozano-Rubí, P. Serrano-Balazote, A.L. Castro, O. Moreno, M. Pascual, Examining database persistence of ISO/EN 13606 standardized electronic health record extracts: Relational vs. NoSQL approaches, *BMC Med. Inform. Decis. Mak.* 17 (2017) 1–14. <https://doi.org/10.1186/s12911-017-0515-4>.
- [21] K. Kaur, R. Rani, Managing Data in Healthcare Information Systems: Many Models, One Solution, *Computer (Long Beach, Calif.)*. 48 (2015) 52–59. <https://doi.org/10.1109/MC.2015.77>.
- [22] H.M. Kruse, A. Helhorn, L.A. Phan-vogtmann, E. Thomas, A.J. Heidel, K. Saleh, A. Scherag, Modeling a Graph Data Model for FHIR Resources, (2019) 398355.
- [23] S. Kalogiannis, K. Deltouzos, E.I. Zacharaki, A. Vasilakis, K. Moustakas, J. Ellul, V. Megalooikonomou, Integrating an openEHR-based personalized virtual model for the ageing population within HBase, *BMC Med. Inform. Decis. Mak.* 19 (2019) 1–15. <https://doi.org/10.1186/s12911-019-0745-8>.
- [24] D. Teodoro, E. Sundvall, M.J. Junior, P. Ruch, S.M. Freire, ORBDA: An openEHR benchmark dataset for performance assessment of electronic health record servers, *PLoS One*. 13 (2018) 1–22. <https://doi.org/10.1371/journal.pone.0190028>.
- [25] S. El Helou, S. Kobayashi, G. Yamamoto, N. Kume, E. Kondoh, S. Hiragi, K. Okamoto, H. Tamura, T. Kuroda, Graph databases for openEHR clinical repositories, *Int. J. Comput. Sci. Eng.* 20 (2019) 281–298. <https://doi.org/10.1504/IJCSE.2019.103955>.
- [26] H.Y. Yip, N.A. Taib, H.A. Khan, S.K. Dhillon, Electronic health record integration, *Encycl. Bioinforma. Comput. Biol.* 1–3 (2018) 1063–1076. <https://doi.org/10.1016/B978-0-12-809633-8.20306-3>.
- [27] E. Choi, M.W. Dusenberry, G. Flores, Z. Xu, Y. Li, Y. Xue, A.M. Dai, Learning Graphical Structure of Electronic Health Records with Transformer for Predictive Healthcare, *ICML 2019 Work. Learn. Reason. with Graph-Structured Data.* (2019). <https://graphreason.github.io/papers/38.pdf>.
- [28] H. Plattner, A common database approach for OLTP and OLAP using an in-memory column database, *SIGMOD-PODS'09 - Proc. Int. Conf. Manag. Data 28th Symp. Princ. Database Syst.* (2009) 1–2. <https://doi.org/10.1145/1559845.1559846>.
- [29] E. Begoli, D. Kistler, J. Bates, Towards a heterogeneous, polystore-like data architecture for the US Department of Veteran Affairs (VA) enterprise analytics, *IEEE Int. Conf. Big Data.* (2016) 2550–2554. <https://doi.org/10.1109/BigData.2016.7840896>.
- [30] N. Yuhanna, M. Gualtieri, Emerging Technology: Translytical Databases Deliver Analytics At The Speed Of Transactions Next-Generation Databases Seamlessly Support Both Transactions And Analytics, (2015). <http://www.odbms.org/wp-content/uploads/2017/10/Forrester-report-Translytical-Databases.pdf>.
- [31] F. Biscotti, M. Pezzini, N. Rayner, J. Unsworth, R. Edjlali, S. Tan, E. Rasit, A. Norwood, A. Butler, W. Roy Schulte, Real-time Insights and Decision Making using Hybrid Streaming, (2015). [http://www.gartner.com/technology/about/ombudsman/omb\\_guide2.jsp](http://www.gartner.com/technology/about/ombudsman/omb_guide2.jsp).
- [32] K. Jee, G.H. Kim, Potentiality of big data in the medical sector: Focus on how to reshape the healthcare system, *Healthc. Inform. Res.* 19 (2013) 79–85. <https://doi.org/10.4258/hir.2013.19.2.79>.
- [33] M. Al Hubail, A. Alsuliman, M. Blow, M. Careyl, D. Lychagin, I. Maxon, T. Westmann, Couchbase analytics: NoETL for scalable NoSQL data analysis, *Proc. VLDB Endow.* 12 (2018) 2275–2286. <https://doi.org/10.14778/3352063.3352143>.

- [35] C.P. Services, data modeling guide, *Ann. Oncol.* 32 (2021) iii. [https://doi.org/10.1016/s0923-7534\(21\)01110-8](https://doi.org/10.1016/s0923-7534(21)01110-8).
- [36] M. Sandeep Kumar, J. Prabhu, Comparison of nosql database and traditional database-an emphatic analysis, *Int. J. Informatics Vis.* 2 (2018) 51–55. <https://doi.org/10.30630/joiv.2.2.58>.
- [37] P. Sadalage, M. Fowler, *NoSQL Distilled: A Brief Guide to the Emerging World of Polyglot Persistence*, 1st ed., Addison-Wesley Professional, 2012. <https://doi.org/0321826620>.
- [38] V. Herrero, A. Abelló, O. Romero, NOSQL design for analytical workloads: Variability matters, *Lect. Notes Comput. Sci. (Including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*. 9974 LNCS (2016) 50–64. [https://doi.org/10.1007/978-3-319-46397-1\\_4](https://doi.org/10.1007/978-3-319-46397-1_4).
- [39] Couchbase, *Moving from Relational to NoSQL: How to Get Started*, (2020).
- [40] R.A.S.N. Soransso, M.C. Cavalcanti, Data modeling for analytical queries on document-oriented DBMS, in: *Proc. ACM Symp. Appl. Comput.*, 2018: pp. 541–548. <https://doi.org/10.1145/3167132.3167191>.
- [41] Apache, *Apache CouchDB*, (2018) 495. <http://couchdb.apache.org/>.
- [42] MongoDB, (2020). <https://www.mongodb.com/>.
- [43] D. Borkar, R. Mayuram, G. Sangudi, M. Carey, Have your data and query it too: From key-value caching to big data management, *Proc. ACM SIGMOD Int. Conf. Manag. Data.* 26-June-20 (2016) 239–251. <https://doi.org/10.1145/2882903.2904443>.
- [44] Couchbase, *Couchbase Under the Hood - An Architectural Overview*, (2019) 1–32.
- [45] A.M.C. de Araújo, V.C. Times, M.U. da Silva, PolyEHR: A Framework for Polyglot Persistence of the Electronic Health Record, *He 17th Int. Conf. Internet Comput. Internet Things.* (2016) 71–78. <http://worldcomp-proceedings.com/proc/p2016/ICM3836.pdf>.
- [46] R. Sreekanth, G. Rao, S. Nanduri, Big Data Electronic Health Records Data Management and Analysis on Cloud with MongoDB: A NoSQL Database, *Ijaegt.Com.* (2015). <http://ijaegt.com/wp-content/uploads/2015/05/409533-pp-946-949-venu.pdf>.
- [47] F. Khennou, Y.I. Khamlichi, N.E.H. Chaoui, Improving the use of big data analytics within electronic health records: A case study based OpenEHR, *Procedia Comput. Sci.* 127 (2018) 60–68. <https://doi.org/10.1016/j.procs.2018.01.098>.
- [48] O. Schmitt, T.A. Majchrzak, Using document-based databases for medical information systems in unreliable environments, *9th Int. Conf. Inf. Syst. Cris. Response Manag.* (2012) 1–10. [https://www.researchgate.net/profile/Oliver\\_Wannenwetsch/publication/272885088\\_Using\\_Document-Based\\_Databases\\_for\\_Medical\\_Information\\_Systems\\_in\\_Unreliable\\_Environments/links/5825780908ae61258e456ad3/Using-Document-Based-Databases-for-Medical-Information-](https://www.researchgate.net/profile/Oliver_Wannenwetsch/publication/272885088_Using_Document-Based_Databases_for_Medical_Information_Systems_in_Unreliable_Environments/links/5825780908ae61258e456ad3/Using-Document-Based-Databases-for-Medical-Information-).
- [49] FHIR, *Fast Healthcare Interoperability Resources*, <https://fhir.org/>.
- [50] J. Walonoski, S. Klaus, E. Granger, D. Hall, A. Gregorowicz, G. Neyarapally, A. Watson, J. Eastman, Synthea™ Novel coronavirus (COVID-19) model and synthetic data set, *Intell. Med.* 1–2 (2020) 100007. <https://doi.org/10.1016/j.ibmed.2020.100007>.
- [51] Synthea, (n.d.). <https://synthea.mitre.org/downloads>.
- [52] The MITRE Corporation, *Synthea by the Standard Health Record Collaborative*, (2017). <https://synthetichealth.github.io/synthea/>.
- [53] J. Walonoski, M. Kramer, J. Nichols, A. Quina, C. Moesel, D. Hall, C. Duffett, K. Dube, T. Gallagher, S. McLachlan, Synthea: An approach, method, and software mechanism for generating synthetic patients and the synthetic electronic health care record, *J. Am. Med. Informatics Assoc.* 25 (2018) 230–238. <https://doi.org/10.1093/jamia/ocx079>.
- [54] MongoDB, *MongoDB: Delivering Real-Time Insight with Business Intelligence & Analytics*, *MongoDB White Pap.* (2017). [http://s3.amazonaws.com/info-mongodb-com/MongoDB\\_BI\\_Analytics.pdf](http://s3.amazonaws.com/info-mongodb-com/MongoDB_BI_Analytics.pdf).
- [55] S. Balsamo, A. Di Marco, P. Inverardi, M. Simeoni, Model-based performance prediction in software development: A survey, *IEEE Trans. Softw. Eng.* 30 (2004) 295–310. <https://doi.org/10.1109/TSE.2004.9>.
- [56] CSV File Data Dictionary • synthetichealth/synthea Wiki • GitHub, (n.d.). <https://github.com/synthetichealth/synthea/wiki/CSV-File-Data-Dictionary>.

# Cyber Threat Intelligence in Risk Management

## A Survey of the Impact of Cyber Threat Intelligence on Saudi Higher Education Risk Management

Amira M. Aljuhami, Doaa M. Bamasoud  
Dept. of IS  
College of Computing and Information Technology  
University of Bisha, Bisha  
Saudi Arabia

**Abstract**—Cyber Threat Information (CTI) has emerged to help cybersecurity professionals keep abreast of and respond to rising cyber threats (CT) in real-time. This paper aims to study the impact of cyber threat intelligence on risk management in Saudi universities in mitigating cyber risks. In this survey, a comprehensive review of CTI concepts and challenges, as well as risk management and practices in higher education, is presented. Previous literature was reviewed from theses, reviews, and books on the factors influencing the increase of cyber threats and CTI as well as risk management in higher education. A brief discussion of previous studies and their contribution to the current paper and the impact of CTI on risk management to reduce risk. An extensive search of more than 65 research papers was conducted and 28 were cited in this survey. Cyber threats are changing in addition to the huge flow of information about them and dealing with these threats on time requires advance and deep information about the nature of these threats and how to take appropriate defensive measures, and this is what defines the concept of CTI. The use of cyber threat information in risk management enhances the ability of defenders to mitigate growing cyber threats.

**Keywords**—Cyber threat intelligence; risk management; cyberthreat; cyber security

### I. INTRODUCTION

In the twenty-first century, the world is witnessing a technological revolution and a qualitative shift in the field of cybersecurity significantly. From here emerged the awareness of the Kingdom of Saudi Arabia and its interaction with these changes and developments with what appears in this era. Therefore, the royal order was issued to establish the National Cybersecurity Authority and its relationship with the King, may God protect him, in line with Vision 2030, to be specialized in cybersecurity and its affairs, and it is considered the main reference for the Kingdom [1]. Rania in [2] assumed that despite this development in the Kingdom, the Kingdom is considered more vulnerable to cyber threats in the Middle East as organization face a new generation of cyber threats. It is distinguished by its ability to easily bypass traditional defenses, such as intrusion prevention systems or firewalls, etc. It has been considered effective for the previous generation of threats. The authors in [3] hypothesize that the old approach renders traditional defenses vulnerable to complex threats because they exploit unknown vulnerabilities. This requires the

need to prepare for these threats through cyber threat intelligence. With this technological revolution, systems have become more complex, resulting in lower levels of security. Because of the changing forms and functions of cyber threats targeting individuals, businesses, and government agencies, cyber threats are not limited to online attackers and hackers. Instead, the authors add in [3] it has grown into threats and funds that are financed and organized for financial gain or political ends.

The authors define in [4] CTI as a means of gathering knowledge to understand what the attacker wants and predict future attacks. CTI is used to achieve appropriate awareness of conditions and cyber threats can be countered by including CTI in defense systems. Threats are analyzed based on historical information about actual incidents in the past, and as one of the advantages of information about security threats, operations are improved effectiveness and efficiency in terms of preventative capabilities and investigations. The authors argue in [5] that the purpose of the CTI is to obtain evidence to aid decision-making because what determine the ability of the security team to produce accurate and actionable threat information is the maturity, skills, and resources of the CTI.

Although technology and information continue to grow in cyberspace, it becomes difficult to identify and respond to threats on time. Therefore, CTI management is needed to reduce cybersecurity risks. This paper aims to identify the role of CTI applications in risk management in the Kingdom of Saudi Arabia.

This paper is organized into six sections. Section 2 provides a deep explanation of the concept of CTI, where its types, main challenges, and characteristics are mentioned. Section 3 explains the concept of risk and its types. It also discusses the concept of risk management, its processes, and the most prominent practices of risk management in higher education. In section 4, the most prominent previous literature that discussed the reasons for the increase of cyber threats in addition to the importance of CTI and risk management in higher education was highlighted. In Section 5 discusses the relationship of previous studies to the current paper and the extent of its support and disagreement with it is. Section 6 provides concluding observations with suggestions for some future directions.

## II. CYBER THREAT INTELLIGENCE

### A. Threat Intelligence (TI)

The author in [6] defines TI as the process of understanding enterprise threats based on available data points that go beyond just collecting data points. The data must also be relevant to the organization as a whole [6]. In [7] the authors define TI as any evidence-based knowledge about threats, intending to prevent an attack or shorten the period between penetration and detection. The author explained in [6] that TI can also refer to evidence-based information, such as context, mechanisms, indicators, implications, and actionable advice for a topic regarding an existing or emerging risk or risk on an asset that can be used to make informed decisions about the response to risk or risk. TI can be information collected from a variety of technical sources (for example, local sensors) or human sources (for example, observed discussions in secret forums, communication with peers). Thus, the authors stated in [3] that threat information includes technical indicators, context, mechanisms, implications, and actionable advice about current or emerging threats.

SysAdmin Audit, Network, and Security (SANS) defines a CTI as the collection, classification, and eventual use of information about adversaries, specific information about their tactics, to discover or block them. As mentioned by one of the authors, CTI is used to determine opponent intent [8].

The study in [9] provided several definitions of CTI that are based on processes, analysis, and domain. Hence, in [9] CTIs are defined by the authors as actions taken in cyberspace to compromise and defend protected information and capabilities in the field.

The researchers proposed in [10] the definition of CTI: as “the process and product resulting from the interpretation of raw data into information that satisfies a requirement as it relates to adversaries who have the intent, opportunity, and ability to cause harm.” The research conducted in [10] claimed that Threat Intelligence (TI) involved the process of converting data into information about the adversary.

CTI can easily become an uncontrollable alert stream. The context allows the security analyst to understand the type of threat or actor they are dealing with so that they can formulate an appropriate response plan. The three main components of a CTI are relevant, timely, and actionable. A complete CTI definition needs to cover these three elements to ensure that relevant threat data is collected, analyzed, and processed on time, and the outcome can produce actionable intelligence to aid decision-making [11].

### B. Cyber Threat Intelligence Challenges

In [12] the authors discuss that cybercriminals use a variety of methods to attack their victims to:

- Steal their sensitive personal information (such as financial information).
- Accessing and controlling the victim’s device to commit other malicious acts such as ransomware which can provide malware (in case of Botnet) and lock/encrypt the victim’s device (in case of Botnet).

The authors argue in [12] that although different types of cyber-attacks use a variety of infection methods, in essence, they follow a similar life cycle: beginning with victim reconnaissance and ending with malicious activities on the victim’s device/network.

1) *Vector reconnaissance attack*: Identifying the attack point and system vulnerabilities that cybercriminals can exploit is a challenge in defending against cyberattacks. In addition to the common methods that have always been used to deceive victims (for example, phishing) into performing the actions desired by the attackers, the attackers have used more intelligent and innovative methods in recent years [12]. The authors hypothesize in [12] that methods range from delivering malicious software (malware) in an unexpected format (e.g. Word documents or PDF files) to one-day exploits of vulnerabilities, to infringing anonymous communications to contact threat actors. New families of ransomware, which have worm-like behaviors, have infected tens of hundreds of individuals, organizations, and important systems with such advanced attacks. These advances in attack techniques make it very difficult to determine the point of origin of the attack as well as to identify the attacker.

2) *Attack indicator poll*: The authors report in [12] that cybercriminals also use sophisticated methods to combat forensics and evasion in their malicious code, making standard security assessment methods, for example, CVSS (Common Vulnerability Scoring System), or persistent malware and traffic analysis, less efficient. Models, such as Software Defined Networking (SDN), Internet of Things (IoT), and cloud computing, and their widespread adoption by organizations (e.g. using cloud resources to process and store big data) require modern forensic techniques such as Well [12].

### C. Types of Cyber Threat Intelligence

In [13] the authors discussed that CTI can be classified into four types based on their features and the role of the consumer in the organization as shown in Fig. 1:

- Strategic Threat Intelligence.
- Operational Threat Intelligence.
- Tactical Threat Intelligence.
- Technical Threat Intelligence.



Fig. 1. Types of CTI.

The author hypothesizes in [13] that the purpose of strategic intelligence is to provide management personnel with high-quality information about attack trends and threats that can influence high-level business decisions. TI's operational information provides information about specialized and technically focused intelligence (mostly from campaigns, malware, forensic reports, and/or tools) of an organization's specific security incident and is consumed by security managers and the organization; Tactical TI deals with the tactics, techniques, and procedures (TTPS) used by various threat actors, IOCS (Indicators of Settlement) to advocate for signature-based settlements. The author mentioned in [13] that threat intelligence is consumed by incident response teams, and technical threat intelligence is consumed through information feeds, which are often automatically consumed by enforcement or monitoring and analysis systems such as firewalls.

#### D. Cyber Threat Intelligence Characteristics

The ability to perceive and capture the enemy's attention during the reconnaissance, armament and transmission phases of the cyberattack lifecycle provides the opportunity to take appropriate action to protect the network and prevent attacks. Effective recovery and response strategies can also be created in this way. In [14] the authors claimed that conditioning the following characteristics would result in greater efficacy in TI:

- **Timely:** For effective threat intelligence, time plays a critical role. Intelligence must be conveyed quickly with petty frivolity.
- **Relevant:** Threat information must be applied to the relevant environment.
- **Accurate:** To be able to take more reasonable and effective action against attacks, it is necessary to have more accurate intelligence. Therefore, the information provided through Threat Information must be true, complete, and frank.
- **Specific:** More detailed and more specific threat information can allow defenders to choose appropriate countermeasures.
- **Actionability:** Actions need to be defined by threat information to ensure the data necessary to respond to threats.
- The author mentioned in [14] that understanding these four aspects of the model, finding the data that corresponds to each of them, and knowing where the attacker's killing chain occurs, gives insight to the attackers and facilitates the production of threat intelligence. Both fuel the active cyber defense cycle.

### III. RISK MANAGEMENT

#### A. Classification of Risks

In [15] the authors discussed the classifications that determine the nature of the operations generated by the types of risks that have an impact on achieving goals at the level of the economic organization, as shown in Fig. 2, which are:



Fig. 2. Classification of Risks.

- Strategic risk relates directly to the development strategy of the organization and is associated with its strategic goals.
- Organizational risks are related to organizational processes, operational activities, and procedures.
- Financing risks are caused by interest rates, inflation, insurance, taxes, protectionist policy, regional policy, and the necessity to minimize losses.
- Risks of change are caused by legislative changes, professional ethics, levels of culture and training, the diversity of needs and requirements, staff fluctuations, and the issues of turnover.
- Operational risks have a direct relationship to the functional compartments within an organization and are linked to the specific objectives defined at the level of functional groups.

#### B. Types of Risks

The author stated in [15] that the identification of risks to which the organization is exposed may be divided into two categories, namely, inherent risks, and residual risks as shown in Fig. 3, and the risks inherent in any business are those that usually exist before applying internal control measures to reduce risks, or the overall The risks that lie with the entity or organization, whether internal or external, measurable or not. In this way, the inherent risk is the possibility that the administrative and financial statements contain errors or inconsistencies before the implementation of internal control measures.

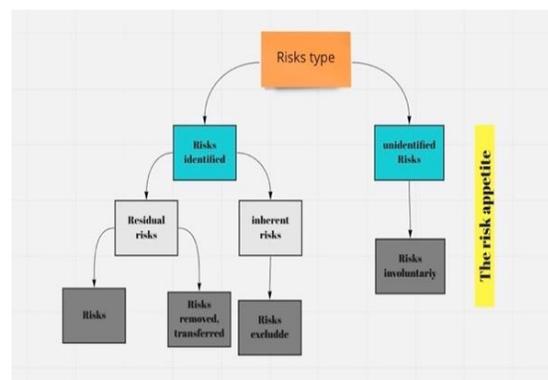


Fig. 3. The Risks Type.

- The author assumed in [15] that the residual risk is the risk that remains after taking measures to mitigate it, the risk-mitigating measure is part of the internal control, and the residual risk is a measure of the effectiveness of the internal control, which is why some countries have replaced the term residual risk with the term “residual risk.” Control, therefore, the residual risk is the residual risk after the implementation of internal control measures, the internal control measures must have the effect of reducing the inherent risks at reasonable levels for the organization, and the inherent and residual risks can be considered as illusions of the same risks. As a result, there were inherent risks before the internal controls were introduced, and residual risks emerged after they were introduced.
- Besides inherent and residual risks, there are also control risks and undetected risks that occur at the enterprise level, and there are control risks when the internal control system of the enterprise fails to prevent or detect errors, irregularities, or fraud on time, there may be individual risks associated with the account balance or a class of transactions or both, and risks can be aggregated [15]. In other words, undetectable is the risk that a particular threat cannot be identified and managed, experts in this field believe that economic organizations should focus on assessing risks and keeping them within the limits that they can accept and tolerate because risks cannot be avoided or eliminated.

### C. Risk Management

The author defined in [15] the risk management process as a plan developed by the leaders of economic organizations and implemented by all employees, and the process includes risk assessment, identification of risk tolerance, and treatment of uncontrollable risks.

Risk management at the level has become necessary due to the uncertainty like threats that may affect the achievement of organizational goals and the environment in which the organization operates, as part of risk management, and the goal is to manage risks in such a way that it can ensure the protection of resources and the protection of employees.

The author argued in [15] that risk management is continuous, and the results arise from decisions made regarding accepting, reducing, or eliminating risks that affect the achievement of objectives, and to prevent losses, avoid threats and take advantage of opportunities, exposure to risks must be optimal.

### D. The Risk Management Process

The author mentioned in [16] that it is the manager and project team members at different levels who identify and manage risks in several ways, but without a unified framework for risk assessment, this is ineffective, as there will be no full impact assessment.

Risk management is an iterative process, and every aspect of risk management must be planned and implemented at every stage [16]. The risk management process consists of four steps

as shown in Fig. 4: Identifying, analyzing, evaluating, and controlling risks.

1) *Risks management plan*: Risk management frameworks are reviewed and adapted to define project risk management plans at project initiation. The author assumes in [16] that risk management plans include the following guidelines:

- List of possible sources and categories of risk.
- Impact and probability matrix.
- Risk reduction and action plan.
- Intervention plan.
- Threshold and risk values.

2) *Identification of risks*: The author stated in [16] that risks should be identified and addressed as early in the project as possible. Risks are identified throughout the project life cycle, focusing on key stages. Risk identification is an important topic in the project landscape and the reporting sessions. Some risks emerge easily to the team (known risks), while others may take longer to identify. Risks are identified in a disciplined and systematic way, ensuring that no significant threats are overlooked:

- Risk log: list of risks from history (other projects)
  - List of potential risks
- Expert judgment, using brainstorming.
  - Project status, which includes progress reports.
  - Classification of risks by categories.

3) *Risk analyses*: Risk analysis or risk assessment involves examining how project outcomes and objectives may change because of the risk event [16]. The risks are identified and then analyzed to determine the qualitative and quantitative impact of the risks on the project so that appropriate mitigation measures can be taken. In general, the author advises in [16] a risk analysis based on these guidelines: the likelihood of occurrence, the extent to which the risk will occur, the exposure to the risk, and the period during which the risk will occur.

4) *Risk management*: The author mentioned in [16] that risk management includes planning the response to risks, identifying risk drivers, and identifying the person responsible for solving the risks.

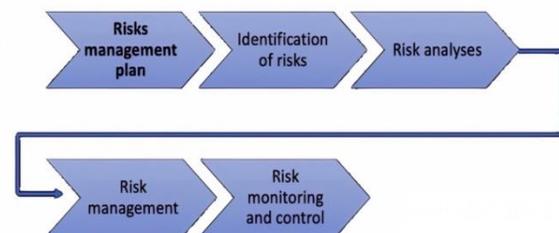


Fig. 4. Risk Management Process.

- Planning the risk response

It may not be possible to eliminate or reduce all the risks associated with a project seamlessly. Managing some risks over longer periods may be necessary and strategically beneficial. To reduce these risks, action plans should be developed [16].

- Risk triggers

In the risk log, the trigger must be recorded for each risk.

The author mentioned in [16] that the triggers are symptoms or warning signs that indicate danger. Risk triggers also indicate when a particular risk is expected to occur, after the implementation of response plans, the degree of risk will be reduced once stakeholder consultation has taken place.

- Risk responsibility

As a basic principle, it is the responsibility of the project manager to manage all risks. The risk owner (who does not necessarily have to be the project manager) must be identified and named in the risk register [16]. The risk owner may be best suited to monitor the risk catalyst but may also be the best suited to implementing and managing the metrics identified, the author assumes in [16] that it is the responsibility of the risk owner to promptly report any change in the risk release status, as well as implement countermeasures specified.

#### 5) Risk monitoring and control

In [16] the authors note that risk monitoring and control include:

- Identifying new risks and planning for them.
- Track existing risks to verify that:
  - Reassessment of risks is necessary.
  - Any risk conditions have been triggered.
- Monitor any risks that may become more critical over time.
- Addressing other risks that require a long-term, planned, and managed approach with risk action plans.

#### E. Risk Management Principles in Higher Education Institutions

It is very important for higher education institutions that they prevent events that could lead to risk in their processes, projects, and other activities, thereby preventing harm from occurring. As well as the above principles, there are other factors to consider [17]:

- Institutions of higher education should integrate risk management into their process maps with defined process features that work in tandem with their main, ancillary, and management processes.
- They must be a key part of decision-making at all levels of management and raise awareness of their importance to the training and business processes among all stakeholders.

- Risk management is the systematic, structured, and timely activity of all institutions' leaders and processes.
- Risk management always adapts to specific situations.
- Risk management is dynamic, repeatable, and sensitive to change.
- Risk management explicitly addresses all types of uncertainty in training processes.
- Risk management is beneficial to the improvement of quality education, processes, and the whole institution.

## IV. LITERATURE REVIEW

### A. Influencing Factors of Cyber Threats

The study of [18] discussed that risk management has emerged and evolved since the emergence of human societies and has improved greatly over time, including identifying, accepting, evaluating, and controlling undesirable events, and preventing the exploitation of opportunities and threats through risk management actions. The primary function of cybersecurity research is to focus efforts on those circumstances and metrics in which the people involved gain an understanding of how to perceive and respond to specific cybersecurity challenges, bearing in mind that cybersecurity is rapidly evolving from technical specialization into a strategic concept, concluding that most security incidents Caused by inadequate management and regulation with the unpredictability of attacks and insecurity, a lack of attention to security concerns may threaten the future of the organization, so it is important to categorize and prioritize risks [18]. The study of [18] is based on the identification of necessary measures to be taken to protect the information, resources, and resources based on an assessment of threats and vulnerabilities and aim to assist governments and organizations in making decisions about security measures against threats.

The study of [19] discusses the growing popularity of information and communication technology that has led to the rapid increase in cybercrime. In addition, many countries around the world are making the necessary interventions to ensure cybersecurity. It also reported that Saudi Arabia was the worst victim of cybercrime in the Gulf region. The study [19] deals with the extent of Saudi Arabia's readiness to confront and defend cyber threats. The carried work in [19] concluded that despite the existence of an anti-cybercrime law that covers the basic areas of combating cybercrime, it is flawed in the protection against identity theft in addition to the violation of privacy and cyberbullying. Therefore, the Kingdom of Saudi Arabia needs to strengthen the cybercrime law, cybersecurity systems, and the National Cyber Security Authority, and it also needs to develop a strategy and standards for cybersecurity [19].

The study of [20] indicates that the twenty-first century has witnessed a new dimension of security known as cybersecurity. With this development, there has been an exploitation of vulnerabilities in cybersecurity, especially between countries to compete. Over time, malware has become a security threat that cannot be underestimated in cybersecurity. And the Kingdom of Saudi Arabia is a prime target for cyber-attacks due to its

economic activity and the high rate of technology use with digital transformation. The study [20] also presented a case study on attacks against Saudi Arabia and focused on two types of malwares: ransomware and Shamoon. The study of [20] suggested some best practices that can be followed to curb attacks, including restricting access, following correct password policies, developing a strong team to respond to incidents in real-time, and providing them with appropriate tools and procedures. The study of [20] showed a lack of scientific studies and investigations dealing with attacks in the Kingdom of Saudi Arabia.

The study of [21] discusses that the technological development of cyber security and the increasing dependence of individuals, societies, and states on it was the reason for the emergence of new and constantly changing threats, where the rapidly developing threats are much more than what can be assessed. The study of [21] showed that defense organizations against attacks in nation-states are considered lagging behind the rapid development of these threats, and this calls for the need to respond to threats in real-time. The study of [21] aims to provide an overview of the most prominent cyber threats and their trends. The study of [21] concluded that it is necessary to increase the capabilities of cyber-threat intelligence in addition to training because it is late and limited compared to the threats.

Cyber security is witnessing the growth and spread of data in information communication technologies, it will be difficult to obtain valid and actionable data from big data to detect and respond to an attack in real-time [22]. The study of [22] suggests a way to organize a large amount of data from different sources, they adopted a pilot approach and reviewed the methodologies for an extensive study on platforms for exchanging information about CTI, implement an online CTI platform, it works to exchange intelligence to reduce the risks of cyber security [22].

### *B. Leveraging the Cyber Threat Intelligence in Risk Management*

Real-time risk assessment is very important, given the nature of the evolving threats that arise from attackers and electronic criminal groups. The study of [23] describes the Polish national platform for cyber security for analyzing cyber risks using CTI. The approach presented came to meet the needs for numerical risk assessment at the national level, to assess risks in real-time, they aim to provide a broad and comprehensive view of cyber threats at the country level And monitor the current situation of the various technical services, Where the proposed approach on the platform is to achieve several goals: From monitoring the cyber security space, detecting threats early, and preparing for measures against hazards in advance, This is the first approach at the national level that uses smart threats, as one of its results is that it leads to building awareness and avoiding the situation.

In [3] the authors discuss that given today's cyber threats and attacks, this requires a new approach to security defenses, since traditional defenses are incompatible with the new generation of more complex threats, any organization needs to collect and share information about cyber threats and turn it into intelligence about Threats and thus contribute to

preventing attacks or at least implementing timely disaster recovery. A study by [3] found a classification of types of CTI, providing reliable strategies for sharing information about CTI and some research and criteria to mitigate threat intelligence problems Technical (TTI) and evaluation of most-sourced tools were surveyed [3].

The rapid development of information technology has been associated with an increased risk of cyber-attacks by malicious hackers [24]. The study of [24] argues that organizations aim to develop CTI to enable effective cybersecurity decisions, and many have been interested in Major cybersecurity companies such as Anomal, FireEye, and many others are developing CTI platforms due to their many benefits, including a high ability to identify key threat actors and prioritize threats, as well as an understanding of their technologies, tools, and procedures, and identification of appropriate security controls. The study of [24] aims to provide a systematic review of the CTI platforms that exist today within the industry. This has led to potential future directions that CTI startups can explore, integrate with improved data mining capabilities, and move from CTI platforms to open-source intelligence platforms (OSINT).

The study of [25] discusses the global increase in attacks and cyber threats, and the trend of many organizations at present to CTI. The main function of CTI is to help organizations better understand and know their enemies by pre-detecting threats and responding to them on time [25]. The study of [25] clarified that prior knowledge of the nature of threats is not considered a major direction for risk management and therefore success in risk management with the massive spread of threats and their changing nature is considered low. The study of [25] proposes the work of a CTI-CM model that describes the main capabilities necessary for CTI practitioners to participate effectively in CTI activities. The study of [25] found that at present, threats spread tremendously and faster than prevention information, although this spread makes it more difficult to keep up with these threats, CTI helps to reduce these threats.

In [5] the authors claim that the success of CTI in cybersecurity requires a base that contains an error in knowledge about CTI, and in addition to a good way of representing this knowledge, classifications and sharing criteria are used to serve this purpose. The study of [5] aims to introduce the CTI model. It enables defenders to learn about their CTI capabilities and understand their behavior against changing cyber threats.

The study of [26] discussed that cyberattacks cost the global economy about \$445 billion annually. To reduce attacks, many companies have relied on Cyber Threat Information (CTI). The [26] study contributed to the creation of a new framework for CTI by utilizing a web, data, and text approach. Using this framework, many freely available malicious assets, such as encryption programs and keyloggers, have been identified.

### *C. Risk Management in Higher Education*

Higher education institutions have been exposed in recent years to an increasing number of reported security violations, which embody the importance of confidentiality, integrity, and

availability of information in universities. The study of [27] aims to systematically review the literature by examining papers that have been published in the past thirteen years in the field of information security management in higher education. The study of [27] found several theoretical contributions, including highlighting the complexity of universities in the practices they apply concerning confidentiality, safety, and access to information. The study of [27] concluded that the field of research is still emerging and that there is an urgent need to increase research efforts in the field of risk management in higher education due to the increasing interest in this field.

Information is one of the most important assets of universities and must be protected from security breaches. Whereas the study of [28] aims to analyze the security threats that develop particularly in the university network environment and recommend an information security framework for the university network environment. The study of [28], evaluation addressed issues at Vikram University, such as enforcing password policies, managing remote access, and restricting mandatory account permissions. The study of [28] when applying the proposed framework to the campus network of Vikram University concluded that the current methods of securing the network are ineffective concerning the university environment and that there is a need to apply for frameworks information protection in the university network, as the proposed framework contributed to Enhancing the level of security in the campus network.

## V. DISCUSSION

Risk management has evolved and improved significantly over time and includes identifying, accepting, evaluating, and controlling undesirable events and preventing the exploitation of opportunities and threats through risk management procedures. A study [18] concluded that one of the main reasons that led to the failure to address threats on time is the insufficient management and organization with the inability to anticipate attacks and insecurity, and thus threatens the future of the organization. This confirms the position of the current study in the importance of CTI in enhancing the role of risk management to respond to attacks on time. A study [19] also discussed that one of the reasons for the increase in threats and electronic attacks is the increasing reliance on information and communication technology. Also, many countries around the world have taken the necessary measures to ensure that cybersecurity is so important at present. A study [19] also mentioned that the Kingdom of Saudi Arabia is the worst victim of cybercrime in the Gulf. This reinforces the need to prepare in advance for these threats and to govern the vast amount of information about threats to address them. A study [20] confirmed that, despite the paradigm shift in cyber security in the twenty-first century, there is an increase in cyber threats and their degree of complexity and has even become a subject of competition between countries, and this is something that cannot be underestimated. In addition, the study [21] discussed the increasing adoption of technology by individuals, societies, and countries, which led to the emergence of new and constantly changing threats. This underlines the need to keep pace with these changes by using CTI and training risk response teams on it to reduce risks. In addition, the study [22]

discussed a way to organize a large amount of data from various sources, in addition to it focused on the importance of information exchange platforms about cyberthreat intelligence, as it works to reduce cybersecurity risks by exchanging information. A study [23] was based on the work of a Polish national platform for cybersecurity. This platform analyzes cyber risks using CTI. One of the most important and most prominent results of this platform was to achieve awareness and avoid risks, in addition to the fact that there was early detection of threats, and this is one of the most prominent benefits of the intelligence of cyber threats. Moreover, in [3] it is also found that organizations with the new generation of cyber threats need to strengthen defenses through the exchange of CTI information, which effectively contributes to preventing attacks or at least recovering from disasters on time. In [24], the study emphasized that many major companies in the field of cyber security have tended to develop CTI platforms due to their multiple benefits. This illustrates the current awareness of the importance of the CTI and its ability to identify the main actors of the threat and the priority of threats, as well as the ability through the CTI to determine the measures necessary to confront the threats. The study [25] concluded that prior knowledge of the nature of threats is not a major trend for risk management, and this makes managing risks at present with the massive spread of threats considered difficult. Therefore, to enhance risk management and keep it up to date with this development in cyber threats, the capabilities of CTI must be used. The study [5] aimed to present a CTI model characterized by this model in working on the capabilities of defenders in CTI and knowing their behavior against cyber threats. Strengthening the capabilities of defenders through CTI is one of the most important reasons that help reduce risks and make maximum use of CTI capabilities. A study [26] benefiting from the web, data, and text approach contributed to the creation of a new framework for CTI. This framework helped identify malicious assets free of charge. This indicates the multiplicity of ways to take advantage of CTI. A study [27] focuses on the increase in threats with the development in cybersecurity, including higher education, and in recent years it has had an increasing number of security violations. Maintaining the confidentiality of information in the university network is a very important matter that cannot be underestimated. Therefore, it is necessary to increase the security of the university network and to highlight the importance of protecting information and reducing the risks to which higher education institutions are exposed. In addition, the study [28] also discussed the importance of information, as it is one of the most important assets of universities that must be protected from security violations. Due to the great dependence of universities on technology, especially with the digital transformation that we are witnessing in the 21st century, and despite the importance of protecting information on the university network, there is not enough focus on this topic by another research.

Previous studies that were mentioned earlier discussed the reasons for the increase in cyber threats, in addition to the role of CTI in reducing risks, as well as the need for risk management to address threats on time and discussed the need for higher education to focus on protecting information and raising the level of security in the university network. The

REFERENCES

applications of previous studies for CTI and ways to benefit from it differed. However, previous studies did not discuss the idea of using CTI to improve the ability of risk management to address threats promptly; although she discussed the inability to manage risks to deter threats. In addition to the lack of studies that discuss the need for higher education to enhance security despite its importance. The present paper highlights the utilization of CTI's capabilities in enhancing risk management to reduce threats in higher education.

VI. CONCLUSION AND FUTURE WORK

Today, with the increasing adoption of information technology and the emergence of new opportunities and possibilities, but the rapid and continuous progress and development of information technology have increased the complexity of digital systems, which makes these systems less secure and thus leads to the complexity and change of forms and functions of cyber threats. Despite the current development in cybersecurity, there is a new generation of advanced threats that can easily bypass traditional defenses as these defenses were designed to combat a previous generation of attacks. In addition, risk management currently lacks in addressing these threats, which has resulted in them not being addressed on time. Higher education is hard without these threats. In recent years, a high rate of threats has been recorded, due to the reason that computers are an integral part of the university environment, in addition to increasing dependence on technology. Therefore, there is a need to improve these defenses using CTI, as CTI represents information about the nature of threats and a deep understanding of the attacker's objectives and thus the ability to respond to threats and take appropriate defensive measures. CTI aims to clarify the information an organization needs to know to increase awareness about threats to identify and address risks on time, as well as increase the capabilities of defenders to detect and respond. Threat information must be accurate and actionable to take full advantage of CTI. This survey focused on the impact of CTI in enhancing risk management for real-time response and discussed the main challenges and advantages of CTI as well as risk management processes and practices in higher education. CTI enables defenders to increase the ability to make decisions quickly in addition to addressing current and future attacks. The field of cyber security is an evolving field that is constantly changing, where it is possible to increase the strength and development of threats on a continuous and almost daily basis. This topic requires in-depth research on ways to take advantage of CTI, as well as a practical application that demonstrates CTI's ability to combat and reduce threats and raise the level of security in the university's network. Despite previous research efforts, studies discussing the use of CTI in risk management in higher education are almost non-existent despite the importance of the topic. One of the future directions of this survey is to propose a unified platform for Saudi universities to exchange CTI information. Training CTI specialists to raise their awareness and increase their capabilities in dealing with risks. However, gathering actionable information about threats is a significant challenge.

- [1] The National Cybersecurity Authority Website. Retrieved from <https://nca.gov.sa/pages/about.html>.
- [2] Rania, (2017 oct 20). Saudi Arabia is more than Middle Eastern countries vulnerable to cyber-attacks. Retrieved from [https://www.aleqt.com/2017/10/19/article\\_1269641.html](https://www.aleqt.com/2017/10/19/article_1269641.html).
- [3] Tounsi, W., & Rais, H. (2018). A survey on technical threat intelligence in the age of sophisticated cyber-attacks. *Computers & security*, 72, 212-233. K. Elissa, "Title of paper if known," unpublished.
- [4] Kim, Daegeon, and Huy Kang Kim. "Automated Dataset Generation System for Collaborative Research of Cyber Threat Analysis." *Security and Communication Networks* 2019 (2019).
- [5] Mavroeidis, Vasileios, and Siri Bromander. "Cyber threat intelligence model: An evaluation of taxonomies, sharing standards, and ontologies within cyber threat intelligence." 2017 European Intelligence and Security Informatics Conference (EISIC). IEEE, 2017.
- [6] Bromiley, M. (2016). Threat intelligence: What it is, and how to use it effectively. SANS Institute InfoSec Reading Room, 15, 172.
- [7] Chismon, D., & Ruks, M. (2015). Threat intelligence: Collecting, analysing, evaluating. MWR InfoSecurity Ltd.
- [8] Shackelford, D. (2017). Cyber threat intelligence uses, successes and failures: The sans 2017 cti survey. SANS Institute.
- [9] Boeke, S., & van de BDP, J. (2017). Cyber threat intelligence—from confusion to clarity; an investigation into cyber threat intelligence.
- [10] Qiang, L., Zeming, Y., Baoxu, L., Zhengwei, J., & Jian, Y. (2016). Framework of cyber attack attribution based on threat intelligence. In *Interoperability, Safety and Security in IoT* (pp. 92-103). Springer, Cham.
- [11] Abu, M. S., Selamat, S. R., Ariffin, A., & Yusof, R. (2018). Cyber threat intelligence—issue and challenges. *Indonesian Journal of Electrical Engineering and Computer Science*, 10(1), 371-379.
- [12] Conti, M., Dargahi, T., & Dehghantanha, A. (2018). Cyber threat intelligence: challenges and opportunities. In *Cyber Threat Intelligence* (pp. 1-6). Springer, Cham.
- [13] Sukhabogi, S. (2021). A Theoretical review on the importance of Threat Intelligence Sharing & The challenges intricated. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(3), 3950-3956.
- [14] Seker, E. (2020). Cyber threat intelligence understanding fundamentals & Technological Research Council of Turkey, 12(3).
- [15] Croitoru, I. (2019). RISK MANAGEMENT-BETWEEN NECESSITY AND OBLIGATION. *Internal Auditing & Risk Management*, 14(1).
- [16] DOVAL, E. (2019). RISK MANAGEMENT PROCESS IN PROJECTS. *Review of General Management*, 29(2).
- [17] Knok, Ž., Kondić, V., & Brekalo, S. (2020). Risk Management in the Higher Education Quality Insurance System. *Tehnički glasnik*, 14(1), 46-54.
- [18] Riza, I. (2017). Risk management from the information security perspective. *Junior Scientific Researcher*, 3(2), 1-8.
- [19] Alshammari, T. S., & Singh, H. P. (2018). Preparedness of Saudi Arabia to Defend Against Cyber Crimes: An Assessment with Reference to Anti-Cyber Crime Law and GCI Index. *Archives of Business Research*, 6(12).
- [20] Alelyani, S., & Kumar, H. (2018). Overview of cyberattack on saudi organizations.
- [21] Kettani, H., & Wainwright, P. (2019, March). On the top threats to cyber systems. In 2019 IEEE 2nd International Conference on Information and Computer Technologies (ICICT) (pp. 175-179). IEEE.
- [22] Mtsweni, J., Muyowa Mutemwa, and Njabulo Mkhonto. "Development of a cyber-threat intelligence-sharing model from big data sources." *Journal of Information Warfare* 15.3 (2016): 56-68.

- [23] Janiszewski, Marek, Anna Felkner, and Piotr Lewandowski. "A Novel Approach to National-level Cyber Risk Assessment Based on Vulnerability Management and Threat Intelligence." *Journal of Telecommunications and Information Technology* (2019).
- [24] Samtani, S., Abate, M., Benjamin, V., & Li, W. (2020). Cybersecurity as an industry: A cyber threat intelligence perspective. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 135-154.
- [25] Shin, B., & Lowry, P. B. (2020). A review and theoretical explanation of the 'Cyberthreat-Intelligence (CTI) capability' that needs to be fostered in information security practitioners and how this can be accomplished. *Computers & Security*, 92, 101761.
- [26] Samtani, S., Chinn, R., Chen, H., & Nunamaker Jr, J. F. (2017). Exploring emerging hacker assets and key hackers for proactive cyber threat intelligence. *Journal of Management Information Systems*, 34(4), 1023-1053.
- [27] Bongiovanni, I. (2019). The least secure places in the universe? A systematic literature review on information security management in higher education. *Computers & Security*, 86, 350-357.
- [28] Joshi, C., & Singh, U. K. (2017). Information security risks management framework—A step towards mitigating security risks in university network. *Journal of Information Security and Applications*, 35, 128-137.

# Expert's Usability Evaluation of the Pelvic Floor Muscle Training mHealth App for Pregnant Women

Aida Jaffar<sup>1</sup>, Sherina Mohd Sidik<sup>2\*</sup>, Novia Admodisastro<sup>3</sup>, Evi Indriasari Mansor<sup>4</sup>, Lau Chia Fong<sup>5</sup>

Faculty of Medicine and Health Sciences, Universiti Putra Malaysia, Serdang, Selangor, Malaysia<sup>1,2</sup>

Faculty of Medicine and Defence Health, Universiti Pertahanan Nasional Malaysia, Kuala Lumpur, Malaysia<sup>1</sup>

Faculty of Computer Science and Information Technology, Universiti Putra Malaysia, Serdang, Selangor, Malaysia<sup>3</sup>

Abu Dhabi School of Management, Abu Dhabi, United Arab Emirates<sup>4</sup>

Faculty of Science, Universiti Malaya, UM, Kuala Lumpur, Malaysia<sup>5</sup>

PeonTech Solutions, Petaling Jaya, Selangor, Malaysia<sup>5</sup>

**Abstract**—Pelvic floor muscle training (PFMT) is the first line in managing urinary incontinence. Unfortunately, personal, and social barriers involvement hinder pregnant women to perform PFMT. Therefore, a Kegel Exercise Pregnancy Training (KEPT) app was developed to bridge the accessibility barriers among incontinent pregnant women. This study aimed to evaluate the usability properties of the KEPT app developed for pregnant women to improve their pelvic floor muscle training. A purposive sampling method of the experts was conducted from a sample of experts in informatics and a physician with a special interest in informatics. The design activities were planned in the following sequence: cognitive walkthrough for learnability of the app, heuristic evaluation for the interface of the app and usability questionnaire to evaluate the usability properties (quantitative assessment) of the app. The mHealth application usability questionnaire (MAUQ) was used as its assessment tool to assess the application usability. A total of four experts were involved in this study. Cognitive walkthrough revealed that the KEPT app has several major learnability issues especially the training interface and language consistency to ensure its learnability. Heuristic evaluation showed that the training interface must provide additional information regarding the displayed icon. KEPT app was rated by MAUQ being as ease-of-use, the interface and satisfaction with the usefulness by all the experts which scored 5.80/7.0, 5.57/7.0, and 5.83/7.0, respectively. The suggestions were shared to assist future researchers and developers in developing PFMT mHealth app.

**Keywords**—Pregnant women; pelvic floor muscle training; mHealth app; usability evaluation; cognitive walkthrough; heuristic evaluation

## I. INTRODUCTION

Urinary incontinence (UI) is an involuntary urine leakage [1]. UI commonly occurs about 40% among pregnant women and negatively affects their quality of life [2–4]. Unfortunately, despite UI affecting their daily activities, only one-tenth of pregnant women seek help due to the misperception that UI would resolve by itself [5]. Therefore, correct information on UI and its management by performing regular pelvic floor muscle training (PFMT) should be available for pregnant women.

However, there were barriers in delivering the PFMT health information to pregnant women. The issues such as healthcare providers focusing on a higher priority medical illnesses in pregnancy or antenatal services midwives have busy workloads in a service structure hindrance the health education to pregnant women [6]. Additionally, pregnant women tend to normalize and perceived that the incontinence is normal during pregnancy and will disappear after the delivery of their baby [7]. An alternative method in delivering health education is needed to educate pregnant women effectively according to their time and their availability.

Recently, smartphones gaining its popularity and has become a daily used items the most popular mobile technology. People tend to multitask using their smartphones seeking the information through smartphone applications conveniently. Additionally, they were able to search and confirm information while they use various other media or smartphone applications simultaneously [8]. The multitasking element enable the mobile health app becomes trending nowadays. Mobile health (mHealth) apps have been shown to be one of the rising in literature in sharing health information and education across several diseases. Unfortunately, mHealth apps demonstrated weak evidence in its effectiveness which may be improved in the evaluative approaches to the development and assessment of the health care improvement apps [9].

Motivation of this research is to conduct a rigor evaluation on the development of the app to ensure the usability and its effectiveness. This study aims to evaluate a newly developed mHealth application (Kegel Exercise Pregnancy Training or KEPT app) which was designed and developed to improve the delivering pelvic floor muscle strength health education to pregnant women. The specific objectives of the study are:

- 1) To understand the heuristic evaluation, cognitive walkthrough, and usability evaluation of the KEPT app from the experts' evaluation.
- 2) To suggest the improvement for the KEPT app for better usability.

\*Corresponding Author

## II. RELATED WORK

### A. PFMT and Pregnant Women

PFMT or Kegel exercise is an important exercise among pregnant women to strengthen their pelvic floor muscles [10], which enables them to prevent UI during their advance trimester and early postpartum period [11]. Despite having good knowledge of PFMT, the practices are still low [4]. This finding suggests that incontinent pregnant women with good PFMT knowledge are not practicing PFMT or those practicing PFMT may be less likely to perform it correctly. Pregnant women need to tailor the PFMT according to their schedules to improve its adherence.

There are a few hiccups in delivering PFMT to the pregnant women at the primary care clinics in this country. There was a dedicated physiotherapist scheduled monthly in certain clinics and for some clinics, the selected pregnant women met in a group session once or twice per year. Unfortunately, these sessions could be troublesome for some pregnant women who are busy managing their family and work at the same time. Furthermore, with the current COVID-19 pandemic, the number of daily attendances has been reduced to avoid the crowdedness in the clinic and abide with the social distancing protocol. Therefore, a carefully designed digital health intervention (mHealth app) has the potential to disseminate PFMT and improve the adherence of these women to manage their UI especially among primigravida with stress UI [12].

### B. Expert Evaluation

To ensure the quality of mHealth app, usability concept or assessment need to be assessed [13,14]. Usability evaluation or inspection is the generic name for a set of cost-effective ways of evaluating user interfaces to find usability problems [15]. Usability is defined when an app can be well understood, easily operated and has its unique attraction to the users in order to accomplish certain tasks in specific environments [16,17]. Hence, usability is also mentioned as being feasible and acceptable to be effective in changing mHealth lifestyle [18].

Nielsen explained that there are four basic ways in evaluating user interface such as via automatically (usability measures computed by running a user interface specification through some program), via empirically (usability assessed by testing the interface with real users), via formally (using exact models and formulas to calculate usability measures), and informally (based on rules of thumb and the general skill and experience of the evaluators) [15].

Additionally, the recruitment sampling of the experts is crucial whereby the experts can be either the academicians with software design (mobile application) or clinician with a special interest in mobile apps who are not from the researcher's team as the usability evaluators. Three to five experts are recommended for the usability testing for heuristic evaluation (user interface) in major issues detection [19]. In this study, we will focus on three types of usability evaluations: cognitive walkthrough, heuristic evaluation, and usability testing.

### C. Cognitive Walkthrough (CW)

Cognitive walkthrough (CW) by the experts were evaluated on the difficult task to add more depth for critical assessments [20]. CW utilizes accurate detailed procedures to simulate a user's problem-solving process at each step through the dialogue or user interface, to study whether the simulated user's goals and memory content can be assumed to direct the users to perform the next correct action [15].

To assist the experts, a persona is used for them to understand the user's characteristics and literacy in using the mobile application. Persona is defined as, "memorable representations of users that remain conspicuous in the minds of those who design and build products" [21]. Persona consists of specific facts, has a concrete representations of target users, which in this study is pregnant women. Persona is constructed in an engaging, and actionable image which provides as a design target. Persona's main role is to assist the experts to be more user focused.

The users, being complicated and varied took great effort to be understood with their health conditions, needs, and behaviors. The experts who were not from the users' socio-economic background faced difficulties to imagine and understand the users' behavior and challenges using the app. Without preliminary informative such as persona, it is more likely the experts imposed their assessment based on their own perspective and not from the users'. If the researcher and developer proceed with these findings, it will be a non-user centered app which may affect the users' involvement and jeopardize their targeted behavior changes.

### D. Heuristic Evaluation (HE)

There are challenges in creating mobile learning applications since smartphones or mobile devices built-in with small screen size, small memory, lack of input capability, and limited processing power [22]. Nielsen (1994) proposed ten heuristic evaluations to detect user interface problems cost-effectively: a) visibility system status; b) system matched with real world; c) user control; d) consistency; e) error prevention; f) recognition than recall; g) flexibility; h) aesthetic and minimalist; i) learning retention; and j) documentation.

Additionally, Kumar and Goundar (2019) added three new heuristics assessment for mobile learning applications. This is because, smartphone has limited function such as the small screen, despite its almost always accessible. The assessments included were: a) selection driven commands; b) content organization; and c) visual representation [23].

Furthermore, the mobile applications included health intervention. Hence, to further assess the heuristic element in this study, Khowaja and Al-Thani (2020) suggested a questionnaire which is called "Heuristic Evaluation of mHealth Apps (HE4EH)" to be used. HE4EH consisted of 25 checklist items, where the most relevant to this study were the self-monitoring and behavioral change items to evaluate the interface according to its objective [24].

### E. Usability Questionnaire (UQ)

There were a few validated questionnaires which can be used to evaluate the usability of an app, for example, the System Usability Scale (SUS) [25], and Post-Study System Usability Questionnaire (PSSUQ) [26]. However, a recent usability questionnaire has been developed and validated to assess usability of an mHealth app which is called the “mHealth App Usability Questionnaire (MAUQ)” [27] which has three domains focusing on the ease of use, interface and satisfaction, and usefulness of the mHealth app [27].

SUS is a ten-item questionnaire using a Likert scale, which assess a global view of usability assessments. The aim was to obtain a quantitative assessment, which was conducted based on general agreement that the evaluated system was “really easy to use”. The user must be given a chance to use the “system” in the first place. After that, the user must assess the “system” using SUS before any debriefing session. The user is required to record their immediate response to each item without any hesitancy [25].

PSSUQ indicated a 3-factor structure consistent with usability that initially described factors for System Usefulness, Information Quality, and Interface Quality. This questionnaire was used to assess the user satisfaction after participation in a scenario-based usability [28]. The 18 questions-assessment was based on a seven-point Likert scale from “Strongly agree” for 1 and “Strongly disagree” for point 7. However, these two usability questionnaires were not specifically designed for the mobile health app usability.

Hence, recently, a usability questionnaire has been developed and validated to assess 18-usability properties for the mobile Health app which is called as mHealth App Usability Questionnaire (MAUQ) [27].

### III. KEGEL EXERCISE PREGNANCY TRAINING APP

Kegel Exercise Pregnancy Training (KEPT) app was developed from a combination of Persuasive Techniques and Capability, Opportunity, Motivation-Behaviour model. It was developed using Interviewing Mapping which embedded in a user-centered design using UCD-11 framework [29]. KEPT app runs on Android platform only.

This KEPT app encouraged pregnant women to train their pelvic floor muscle according to their daily schedule and individual capability. It has five user interfaces; (1) educational video - to deliver the PFMT training sessions (Fig. 1), (2) calendar charting for user interface UI symptoms, (3) training mode stopwatch assistance, (4) progress chart to self-monitor progress, and (5) Frequently Asked Question (FAQ) for information sharing regarding correct method in PFMT.

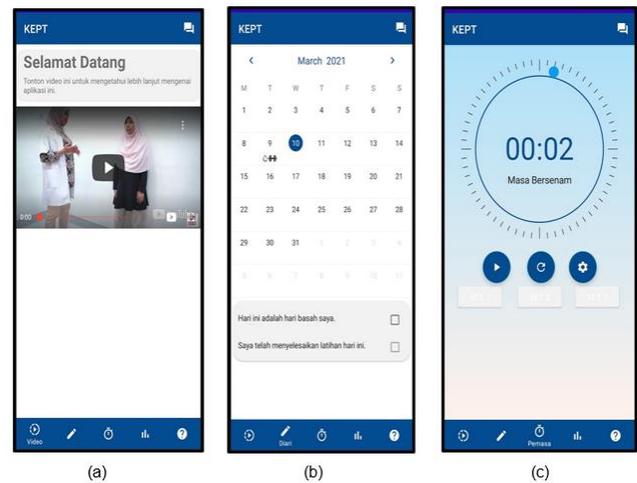


Fig. 1. Some of the KEPT App user Interfaces (a) Educational Video; (b) Calendar Charting; (c) Timer Exercise.

### IV. METHODS

The ethical approval was obtained from Ethics Committee for Research Involving Human Subjects, Universiti Putra Malaysia (JKEUPM-2019-368) and Medical Research and Ethics Committee (MREC), Ministry of Health Malaysia (NMRR-19-412-45606) before the commencement of the study.

#### A. Expert Evaluation

A total of six academics and one from the industry were invited as experts of the study. However, only four academics were agreed to become the experts in this study as listed in Table I. The study was conducted at their own time allocated and their own place.

The experts were required to evaluate the application in three sections; (a) cognitive walkthrough; (b) heuristic evaluation; and (c) usability questionnaire (Fig. 2).

TABLE I. EXPERT’S LIST

ID	Age and Gender	Ethnicity	Experts
E1	44/ Female	Malay	Senior Lecturer, Centre for Software Technology and Management, Public University
E2	41/ Male	Malay	Associate Professor, Science and Technology System, Public University
E3	42/ Female	Chinese	Associate Professor, Department of Family Medicine, Public University
E4	44/ Female	Malay	Associate Professor, School of Multimedia Technology and Communication Educational Multimedia, Public University

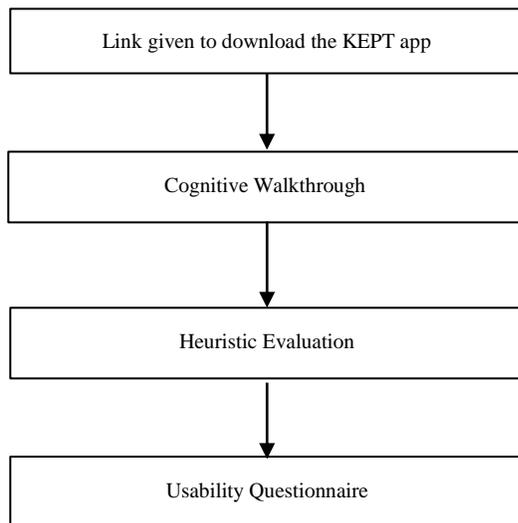


Fig. 2. Expert Evaluation Tasks.

### B. Cognitive Walkthrough (CW)

At the beginning of the session, a persona was introduced to the expert which was adopted from the previous study (Jaffar et al., 2020) to help the expert to understand the situation of a pregnant woman's experience of urinary incontinence as below.

- **Background.** Mrs Aida, a 38-year-old housewife, has a history of being unable to control her urination (urinary incontinence) for a month. She is currently pregnant (unplanned pregnancy but wanted), with her fifth pregnancy at 34 weeks.
- **Medical condition.** Mrs Aida has anaemia in all pregnancies, including this current pregnancy. She sometimes skipped her meals as she had no time to have lunch and suffered from gastritis.
- **Psychological.** Mrs Aida is stressed about her current pregnancy as she is having incontinence and busy managing her family. She felt tired quickly and suffered poor sleep. In the morning, Mrs Aida needs to prepare breakfast and rush to send her kids to school and manage house chores. She has to take care of her 12-year-old son, 10-year-old girl, 9-year-old son and 8-year-old-son.
- **Level of health literacy.** Mrs Aida does not know about urinary incontinence, and she thought it is “normal” during the pregnancy period and during post-natal.
- **Social.** Her husband is a technician and is seldom at home as he has another job (Grab-food delivery) to support the family.
- **Technological literacy.** Mrs Aida used her handphone to make phone calls, WhatsApp, and recently online meeting platform for her children's online schooling using her mobile data. She does not have any social media apps. She claims she has no time to use her phone and only uses her phone to make a call only or for her children's school activities.

- **Relationship with healthcare providers.** She has a good relationship with them and will try her best to follow their advice. She received a food basket from the clinic for her children as they have been diagnosed with malnourishment.
- **Information preferences.** Mrs Aida prefers watching videos, especially when it involves an expert. Unfortunately, her educational status was until secondary school, and she could not absorb too much information at one time.
- **Current issue.** Mrs Aida just downloaded the “Kegel Exercise Pregnancy Training” app (KEPT app) as she seriously wants to control her urination. She is very busy managing her daily chores and does not have time to go for a physiotherapist appointment. She hopes that using this app can help her remind her of the exercise (despite her busy daily schedule) and manage her urinary incontinence.

After understanding the persona, experts were required to interact with the application and performed the following tasks: (a) to sign-up; (b) to watch the video; (c) to do charting (self-monitoring); (d) to perform PFMT; (e) to submit feedback; and (f) to log out the app.

Then, experts were asked to evaluate the application based on the following criteria: (a) major issues - important to fix with high priority; (b) minor issues - to fix the problem with low priority; and (c) no usability issues - may fix if time is available.

### C. Heuristic Evaluation (HE)

During the heuristic evaluation session, experts were asked to rate the interfaces of the application based on 15 items. The first ten questions were based on Nielsen (1994) and adopted by Kumar et al., (2019), the next three questions emphasized on the mobile learning by Kumar and the last two questions were adopted from mobile health apps evaluation by Khowaja et al., (2020) which focus on the behavioral changes and self-monitoring [15,23,24]. The experts assessed the interface using the given rating-scale: [1] to denote a usability disaster; [2] a major problem; [3] a minor problem; [4] a superficial problem; and [5] not a problem at all [23].

#### 1) Ten-Heuristic [15]:

- **Visibility of the system status** whereby the user was given the appropriate feedback.
- **Match between the system and real world** which enable users to identify the elements of the application.
- **User control and freedom** that allowing the users to go different menus easily.
- **Consistency and standards** to ensure the consistency of the application.
- **Error prevention** whereby the users can recover from their errors.
- **Recognition rather than recalls** minimizing the user' s memory load while using the apps.

- Flexibility and efficiency of use whereby the app can be adjusted by anyone.
- Aesthetic and minimalist design by removing the unnecessary information.
- Help users recognize, diagnose, and recover from errors to allow user’s learning retention.

2) Mobile learning (Kumar & Goundar, 2019):

- Help and documentation whereby the app can assist the users in learning.
- Selection driven commands whereby the users engage with the apps.
- Content organization as the app can highlight the key objectives.
- Visual representation on the usage of the icons to assist the users understanding.

3) Mobile health app (Khowaja & Al-Thani, 2020):

- Behaviour changes included the app's design that gradually starts with easy tasks, until target behavior is performed.
- Self-monitoring with several specific steps to self-monitor their expected outcomes.

D. Usability Questionnaire

Finally, all experts were instructed to answer a set of questions which covered three main domains such as, the ease of use, interface and satisfaction, and the usefulness of mHealth apps using the mHealth App Usability Questionnaire [27]. The experts rated each of the items using a 7-point Likert scale ranging from 1 (strongly disagree) to 7 (strongly agree).

Zhou et al (2019) listed three main domains for usability assessment in mHealth app which are ease of use (5 questions), interface and satisfaction (7 questions), and usefulness (6 questions). The overall Cronbach alpha was 0.932, which scored 0.895, 0.829, and 0.900, for ease of use, interface and satisfaction, and usefulness, respectively.

All participants' names were replaced with an identification code. The CW reports were extracted from the word documents. The feedback from the experts was analyzed based on the severity of the issues. The suggestions were then reported, and the clarification was made directly to the experts for better understanding.

HE and UQ data were analyzed descriptively using the SPSS 26.0 to report the mean, median and standard deviation. Similarly, the suggestions from the experts have been recorded.

V. RESULTS

A. Cognitive Walkthrough (CW)

The experts listed a few major issues from the cognitive walkthrough method with the most major issue being the training interface. Training PFMT had four major issues which signified the lack of clarity and self-explanation of the training

section. However, there was heterogeneity of the assessments by the experts whereby E4 detected more major issues compared to others while E2 detected the least issues. The compilation of the reports as listed in Table II.

TABLE II. COGNITIVE WALKTHROUGH

Task	Issues and recommendation
To sign-up	<p>E1: Major Issue: Font on registration text boxes (active boxes) faded. Difficult to read. Recommendation: Change active text box font colour.</p> <p>E2: Cosmetic: Good and clear instruction</p> <p>E3: Minor issue: The (!) mark at the end of the email address said invalid email address. Recommendation: 1. The comment should read “Awaiting admin approval” instead of “invalid email address”. If the app is in Malay, the comments should be in Malay as well. 2. Add a checkbox for the app to remember login details for users who have problems with remembering passwords. 3. Guided tutorial for new users on identifying the main sections of the app.</p> <p>E4: Major issues: (a) Create account, The instruction was not functioning/ clickable Recommendation: Need to fix or omit the function as it will not mainly affects the registration form (b) Patient Information Sheet Instruction was not given on how to use the KEPT apps. Recommendation: Need to give a user manual via video demo on how to use/operate the KEPT apps. The given video was about to educate the Kegel Exercise demo but not on the KEPT apps itself.</p>
The video	<p>E1, E2 and E3: Cosmetic problem only</p> <p>E4 Major issue: (a) The physiotherapist was mentioned about “imagine the muscle contraction as eating the spaghetti” in the video but the FAQ did not mention this. Recommendation: To consistently use terminology with the physiotherapist in the FAQ. (b) The name of the app was provided in the English acronym as KEPT (Kegel Exercise Pregnancy Training) but the main language used in the apps is in Bahasa Malaysia. Recommendation: It is recommended to standardize in using only one language -Bahasa Malaysia due to the main language used in this apps is in Bahasa Malaysia</p>
The charting (self-monitoring)	<p>E1, E2 and E3: Cosmetic problem only</p> <p>E4 Major Issues: (a) The language used was in English and reflects the inconsistency issue. Recommendation: Need to consistently use Bahasa Malaysia instead of using mixed languages. (b) The statement of “I have done the exercise today” was not clickable. Recommendation: Need to fix or omit the function based on the functional requirement of the apps. (c) The status of “total wet day” and “Total Day Completed exercise” were confusing as not showing any status. Recommendation: Need to omit the status based on its confusion.</p>

The Training	<p>E1 and E2: Minor issue: Difficult to understand</p> <p>E3: Minor Issue: The cogwheel icon is placed last in the row of buttons. There is no description for its function, which is to set the difficulty level. Recommendation: Place the cogwheel icon first before the play button. Label it as difficulty level.</p> <p>E3 Major Issues: (a) There is no explanation on the timer. Users may not know that they are supposed to do the exercise while the timer runs. Users cannot see how many times they have done the exercise for each set. Recommendation: Need to have instruction before start, that this page is for the exercise. 2 second timer for ready, 6 second timer for contracting muscles. Should have a counter to show completion of each set. Example: 1/6, 2/6 (b) User does not know whether the exercise was done correctly or not. Recommendation: Tips or Cues on knowing whether done correctly. Prompts to say you need to complete ... number of sets to complete today's exercise. (c) I am not sure of the function of the reset button. Recommendation: Explanation on what the reset button is for.</p> <p>E4: Major issue (a) Set 1, Set 2 and set 3 menus were not functioning, and also got typo error. Recommendation: Need to fix or omit the function based on the functional requirement of the apps.</p>
The Feedback	<p>E1- no issue E2: Cosmetic problem only Recommendation: More infographics to make interesting</p> <p>E3: Cosmetic problem: A question mark icon usually represents the help button in most apps. Here it is representing the questionnaire. Recommendation: Use the pen or notepad icon for questionnaire instead of question mark.</p> <p>E3 Minor issues: (a) Users may not know when to fill in the questionnaire. No reminder for the user of which timing to choose. (b) If the user chooses the wrong timing, not sure of how to get back to the main questionnaire screen. Recommendation: 1. Built in calendar tracking for the day of first use. Reminder to fill in a questionnaire at time points from new user registration. 2. Add instructions to the user: To go back, tap on the questionnaire icon again.</p> <p>E4 Major Issue: There was no instruction given on that page. The use of 'app' in the labelling was not suitable. Recommendation: Need assistance or cue on what to do on that page Replace the 'app' with the name of the app</p>
The Logout	<p>E1, E3 and E4 Major Issue: I cannot find the logout button. Recommendation: Logout button, account profile should be visible somewhere. Need to provide an exit/log in back widget in the app.</p>

**B. Heuristic Evaluation**

Similarly, as the CW, there was heterogeneity of the HE among the experts as illustrated in Fig. 3. The lowest score of user interface was the “visibility-provide feedback” which has been expected as this app is a standalone app without any direct communication to the healthcare providers. The highest

user interface score was the behavior change element which highlights that the KEPT app was able to encourage the users to change their behavior in a real-world situation with the user’s compliance. Therefore, the HE results may conclude that the KEPT app interfaces have been designed in an acceptable manner to assist the users’ PFMT adherence as listed in Table III.

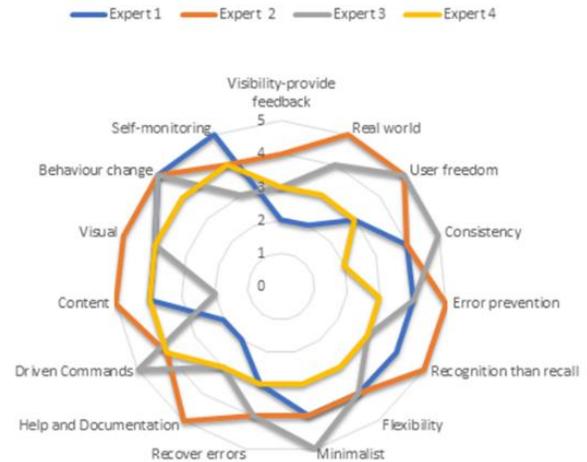


Fig. 3. Heuristic Evaluation Expert’s overview.

TABLE III. HEURISTIC EVALUATION

Heuristic assessment	Mean (SD)	Heuristic assessment	Mean (SD)
1. Visibility of system status	3.00 (0.82)	9. Help users recognize diagnose and recover from errors	3.50 (0.58)
2. Match between system and real world	3.50 (1.29)	10. Help and documentation	3.25 (1.26)
3. User control and freedom	4.00 (1.15)	11. Selection driven commands	3.75 (1.26)
4. Consistency and standards	3.75 (1.26)	12. Content organization	3.75 (1.26)
5. Error prevention	4.00 (0.82)	13. Visual representation	4.25 (0.50)
6. Recognition rather than recall	3.75 (0.96)	14. Behaviour change	4.75 (0.50)
7. Flexibility and efficiency of use	3.75 (0.50)	15. Self-monitoring	4.00 (0.82)
8. Aesthetic and minimalist design	4.00 (0.82)		

**C. Usability Questionnaire (UQ)**

The usability questionnaire assessment was scored with “somewhat agree” to “agree” across all three components. (Tables IV, V, and VI). The average for “Ease of use”, “Interface and satisfaction”, and “Usefulness” scored 5.80/7.0, 5.57/7.0, and 5.83/7.0, respectively.

The “Ease of Use” scored highest among the three domains denotes that the app has simplicity in its design (Table IV). These results concluded that the KEPT app was easy and useful among pregnant women with several modifications needed to specific interfaces, especially the organization of the

information and acknowledgement from the app when the users completed their tasks (Table V). The experts agreed that KEPT app was a useful app in behavioral changes and healthcare services as listed in Table VI.

The least scores were: (1) The information in the app was well organized, so I could easily find the information I needed; (2) Whenever I made a mistake using the app, I could recover easily and quickly; and (3) I could use the app even when the Internet connection was poor or not available.

TABLE IV. EASE OF USE

	MAUQ: Ease of Use	Mean (SD)
1.	The app was easy to use.	5.75 (0.96)
2.	It was easy for me to learn to use the app.	5.50 (1.29)
3.	The navigation was consistent when moving between screens.	6.00 (0.82)
4.	The interface of the app allowed me to use all the functions (such as entering information, responding to reminders, viewing information) offered by the app.	6.25 (0.96)
5.	Whenever I made a mistake using the app, I could recover easily and quickly.	5.50 (1.29)

1 - strongly disagree, 2 - disagree, 3 - somewhat disagree, 4 - neither agree nor disagree, 5 - somewhat agree, 6 - agree, 7 - strongly agree

TABLE V. INTERFACE AND SATISFACTION

	MAUQ: Interface and satisfaction	Mean (SD)
1	I like the interface of the app	6.25 (0.50)
2	The information in the app was well organized, so I could easily find the information I needed	5.00 (1.41)
3	The app adequately acknowledged and provided information to let me know the progress of my action.	5.25 (1.50)
4	I feel comfortable using this app in social settings.	5.50 (1.29)
5	The amount of time involved in using this app has been fitting for me.	5.50 (0.58)
6	I would use this app again.	5.75 (0.50)
7	Overall, I am satisfied with this app.	5.75 (1.26)

1 - strongly disagree, 2 - disagree, 3 - somewhat disagree, 4 - neither agree nor disagree, 5 - somewhat agree, 6 - agree, 7 - strongly agree

TABLE VI. USEFULNESS

	MAUQ: Usefulness	Mean (SD)
1	The app would be useful for my health and well-being.	6.25 (0.96)
2	The app improved my access to healthcare services.	5.75 (0.96)
3	The app helped me manage my health effectively.	6.00 (0.82)
4	This app has all the functions and capabilities I expected it to have.	6.00 (0.82)
5	I could use the app even when the Internet connection was poor or not available.	5.00 (2.71)
6	This mHealth app provides an acceptable way to receive healthcare services, such as accessing educational materials, tracking my own activities, and performing self-assessment.	6.00 (1.41)

1 - strongly disagree, 2 - disagree, 3 - somewhat disagree, 4 - neither agree nor disagree, 5 - somewhat agree, 6 - agree, 7 - strongly agree

From these assessments, the team suggested with list of improvements such as, (1) to arrange the interface according to the user’s daily PFMT activities and monitoring steps; (2) to explain the “undo” icon; and (3) to inform to the users that the app can functioned without the internet access. They need the internet connection only when submitting the questionnaires.

## VI. DISCUSSION

This study investigated the usability of a newly user-centered PFMT app designed and developed for pregnant women with urinary incontinence. Three types of usability assessment used were the cognitive walkthrough, heuristic evaluation, and usability questionnaire. There were a few difficulties in learning of the KEPT app for example, the organization of the information, and the PFMT interface whereby the users are expected to perform three times daily. This usability evaluation was able to assist the researchers to improve the app’s design for better acceptability and usability in the KEPT app prototype for its pilot study [30].

The main objective for the KEPT app was to provide opportunities to pregnant women with UI to perform PFMT at their own convenience. It was crucial to ensure pregnant women have the confidence and understanding of the importance of PFMT especially so when they are experiencing UI. Studies reported that pregnant women face few barriers from either their own misunderstanding, lack of knowledge, lack of support from their partners and from the healthcare providers [6,7,31].

There were several key findings which could be divided into the learnability using the app, the elements of its user interface, and the usability issues of the app.

1) *Learnability of the app:* Most of the assessors were concerned about the organization of the apps and its training mode function. Poor organization of the app with lack of user manual to inform what the function of the icon and how the app works interfered with the understandability of using the app.

User manual was important to provide an overview of the app and the guidance using the app. Similarly, a mHealth app related with self-managing chronic heart failure among elderly reported that they appreciated having an instruction user manual prior to using the apps [32]. However, not all users used the instruction manual to understand the apps as some of them preferred to try a few times and be able to understand the functionality of the app [33]. Nevertheless, by having a manual it provided advantages to the users an option to read for better understanding of the app even to the professional users [34]. Hence, to improve the understanding of KEPT apps, a user’s manual will be added at the top right corner for the users’ better accessibility.

Another major concern by the experts was the lack of clarity in the training mode. The poor visibility of each icon and its function disrupt the understanding of the PFMT process. Clarity is crucial in understanding the functionality of the app especially when it involves behavioral change, for example apps for exercise or physical training. Lack of clarity will affect the user's understanding and further perceive it to be

difficult. Perceived ease of use has been highlighted by the Technology Acceptance Model (TAM) as the main domain to contribute to the actual use of the app [35,36]. Therefore, to ensure the daily use of the apps, the training mode needed to be re-designed for better clarity.

2) *User interface of the app*: Using heuristic evaluations, the experts who were providing their evaluation on the issues of the problematic user interface, were also supplementing their suggestions in their report. The insightful feedback was gathered, and further discussion will be made to improve the user interface system design for better clarity and ease of use by the users.

Another finding was the consistency using the Malay language in the KEPT app to better be understood by the users was highlighted. Consistency is one of the ten heuristic elements by Nielsen [15]. Without consistency, the flow of the app was disturbed and causing frustration to the users. Being difficult in understanding about the app leading to perceived lack of usefulness and affecting the user's attitude and behavior to use the app (TAM). Hence, the future KEPT app must have a consistency using Malay language throughout the apps.

The user interface for training was lack of clarification. There was no indicator to signal to the users on their current repetition out of ten for each set of PFMT. The expert suggests making it visible by proportion of the total set. Another major issue, they faced difficulty in understanding the training interface to be setting according to the user's PFMT ability. Therefore, their suggestions were to ensure the training mode interface is easy to understand, with the indicator showing the user's current exercise. The design needs to be simple, zero interruption, and able to record the data to the backend system without any disruption.

3) *Usability of the app*: The KEPT app was evaluated with "somewhat agree" in terms of its easy to use, good interface and satisfactory and useful as the overall overview. This signified that KEPT app development has proved its importance and could possibly improve the user's PFMT after its actual use in future. The usability questionnaire results confirmed the finding from CW and HE. Positive feedback from the result was that it scored high in its usefulness. This signals that the app might be able to improve the PFMT adherence among pregnant women through daily usage.

Therefore, the key findings when developing a mobile health (mHealth) app for pregnant women with an incontinence can be listed as the manual instruction for the users is crucial, the training interface should be designed with simplicity, and Malay language to be used throughout all the UI. Additionally, the arrangement of the icon interface should be arranged according to the users' daily activities for better systematic organization.

This usability assessment has limitation such as the session was conducted individually and not face to face with the researcher. The session was due to the restriction movement order that hinder the researcher to meet the experts. Hence, there could be issues due to technical problem such as incompatibility of the application with Android devices.

## VII. CONCLUSION

The KEPT app was developed to educate incontinent pregnant women to perform PFMT. This paper aimed to evaluate the usability properties of the app from the experts' point of view. KEPT app should be design with an efficiency, effective, and provides the users with the required information. Firstly, by conducting the cognitive walkthrough to understand and analyze the ability of the app to make the users complete their task. Next, heuristic evaluation which assessing the user interfaces available in the KEPT app conform with certain important guidelines for better usability properties.

Finally, the usability questionnaire evaluation conducted with the experts showed encouraging findings of its ease of use, interface and satisfaction, and usefulness. Nevertheless, the usability assessment indicated that a few interfaces of the KEPT app need to be improved. The organization of the interfaces, consistent Malay language usage, and system design for the training interface need to be improved according to the recommendations.

Few necessary iterations will be conducted to re-design the application prior to this usability evaluation. This study was the first usability evaluation PFMT mHealth app for pregnant women found in the literature and to the best of our knowledge such a study has not been conducted. The next step is to develop the KEPT app by improving the usability problems which were highlighted and suggested from the experts.

We hope that the findings in this study will be of assistance to other researchers in their future studies in developing the PFMT mHealth app.

## ACKNOWLEDGMENT

The authors thanked the team of experts for their contributions in evaluating the KEPT app comprehensively. This research was supported and funded by the Geran Putra Berimpak Universiti Putra Malaysia (UPM/800—3/3/1/GPB/2018/9668500).

## REFERENCES

- [1] Abrams P, Andersson K, Apostolidis A, Birder L, Bliss D, Brubaker L, et al. 6th International Consultation on Incontinence. Recommendations of the International Scientific Committee: evaluation and treatment of urinary incontinence, pelvic organ prolapse and faecal incontinence. *Neurourol Urodyn.* 2018;37(7):2271–2272.
- [2] Moosdorff-Steinhaus HFA, Berghmans BCM, Spaanderman MEA, Bols EMJ. Prevalence, incidence and bothersomeness of urinary incontinence in pregnancy: a systematic review and meta-analysis. *Int Urogynecol J.* 2021;32(7):1633–1652. PMID: 31229999.
- [3] Jaffar A, Mohd-Sidik S, Abd Manaf R, Foo CN, Gan QF, Saad H. Quality of life among pregnant women with urinary incontinence: A cross-sectional study in a Malaysian primary care clinic. *Rosier PFWM, editor. PLoS One. Public Library of Science;* 2021;16(4):e0250714.
- [4] Jaffar A, Mohd-Sidik S, Nien FC, Fu GQ, Talib NH. Urinary incontinence and its association with pelvic floor muscle exercise among pregnant women attending a primary care clinic in Selangor, Malaysia. *Rosier PFWM, editor. PLoS One. Public Library of Science;* 2020;15(7):e0236140.
- [5] Moosdorff-Steinhaus HFA, Berghmans BCM, Spaanderman MEA, Bols EMJ. Urinary incontinence during pregnancy: prevalence, experience of bother, beliefs, and help-seeking behavior. *Int Urogynecol J.* 2021;32(3):695–701. PMID: 33078344.
- [6] Woodley SJ, Hay-Smith EJC. Narrative review of pelvic floor muscle training for childbearing women—why, when, what, and how. *Int*

- Urogynecol J. International Urogynecology Journal; 2021;7–10. PMID: 33950309.
- [7] Terry R, Jarvie R, Hay-Smith J, Salmon V, Pearson M, Boddy K, et al. “Are you doing your pelvic floor?” An ethnographic exploration of the interaction between women and midwives about pelvic floor muscle exercises (PFME) during pregnancy. *Midwifery*. 2020;83:102647. PMID: 32014618.
- [8] Chen X, Wang Y, Tao D, Jiang L, Li S. Antecedents of smartphone multitasking: roles of demographics, personalities and motivations. *Internet Res*. 2021;31(4):1405–1443.
- [9] Iribarren SJ, Akande TO, Kamp KJ, Barry D, Kader YG, Suelzer E. Effectiveness of Mobile Apps to Promote Health and Manage Disease: Systematic Review and Meta-analysis of Randomized Controlled Trials. *JMIR mHealth uHealth*. 2021;9(1):e21563. PMID: 33427672.
- [10] Woodley SJ, Lawrenson P, Boyle R, Cody JD, Mørkved S, Kernohan A, et al. Pelvic floor muscle training for preventing and treating urinary and faecal incontinence in antenatal and postnatal women. *Cochrane Database Syst Rev*. 2020;2020(5). PMID: 32378735.
- [11] Ren S, Gao Y, Yang Z, Li J, Xuan R, Liu J, et al. The effect of pelvic floor muscle training on pelvic floor dysfunction in pregnant and postpartum women. *Phys Act Heal*. Ubiquity Press; 2020;4(1).
- [12] Wang X, Xu X, Luo J, Chen Z, Feng S. Effect of app-based audio guidance pelvic floor muscle training on treatment of stress urinary incontinence in primiparas: A randomized controlled trial. *Int J Nurs Stud*. England: Elsevier Ltd; 2020;104:103527. PMID: 32058140.
- [13] Peischl B, Ferk M, Holzinger A. The fine art of user-centered software development. *Softw Qual J*. 2015;23(3):509–536.
- [14] Holzinger A, Searle G, Kleinberger T, Seffah A, Javahery H. Investigating Usability Metrics for the Design and Development of Applications for the Elderly BT - Computers Helping People with Special Needs. In: Miesenberger K, Klaus J, Zagler W, Karshmer A, editors. Berlin, Heidelberg: Springer Berlin Heidelberg; 2008. p. 98–105.
- [15] Nielsen J. Usability inspection methods. *Conf companion Hum factors Comput Syst - CHI '94*. New York, New York, USA: ACM Press; 1994. p. 413–414.
- [16] Shareef S, Khan MNA. Evaluation of Usability Dimensions of Smartphone Applications. *Int J Adv Comput Sci Appl*. 2019;10(9):426–431.
- [17] Hornbæk K, Law EL-C. Meta-analysis of correlations among usability measures. *Proc SIGCHI Conf Hum factors Comput Syst*. 2007. p. 617–626.
- [18] Overdijkink SB, Velu A V., Rosman AN, van Beukering MDM, Kok M, Steegers-Theunissen RPM. The Usability and Effectiveness of Mobile Health Technology-Based Lifestyle and Medical Intervention Apps Supporting Health Care During Pregnancy: Systematic Review. *JMIR mHealth uHealth*. 2018;6(4):e109. PMID: 29691216.
- [19] Nielsen J, Molich R. Heuristic evaluation of user interfaces. *Conf Hum Factors Comput Syst - Proc*. 1990;(April):249–256.
- [20] Beauchemin M, Gradilla M, Baik D, Cho H, Schnell R. A Multi-step Usability Evaluation of a Self-Management App to Support Medication Adherence in Persons Living with Hiv. *Int J Med Inform*. Elsevier; 2019;122(August 2018):37–44. PMID: 30623782.
- [21] Pruitt J, Adlin T. The persona lifecycle: keeping people in mind throughout product design. Elsevier; 2006.
- [22] Kumar BA, Mohite P. Usability guideline for mobile learning apps: an empirical study. *Int J Mob Learn Organ*. Inderscience Publishers (IEL); 2016;10(4):223.
- [23] Kumar BA, Goundar MS. Usability heuristics for mobile learning applications. *Educ Inf Technol*. Education and Information Technologies; 2019;24(2):1819–1833.
- [24] Khowaja K, Al-Thani D. New Checklist for the Heuristic Evaluation of mHealth Apps (HE4EH): Development and Usability Study. *JMIR mHealth uHealth*. JMIR Publications; 2020;8(10):e20353.
- [25] Brooke J. Sus: a “quick and dirty” usability. *Usability Eval Ind*. 1996;189.
- [26] Lewis JR. Psychometric evaluation of the PSSUQ using data from five years of usability studies. *Int J Hum Comput Interact*. Taylor & Francis; 2002;14(3–4):463–488.
- [27] Zhou L, Bao J, Setiawan IMA, Saptono A, Parmanto B. The mHealth App Usability Questionnaire (MAUQ): Development and Validation Study. *JMIR mHealth uHealth*. 2019;7(4):e11500.
- [28] Lewis JR. Psychometric Evaluation of the Post-Study System Usability Questionnaire: The PSSUQ. *Proc Hum Factors Soc Annu Meet*. 1992;36(16):1259–1260.
- [29] Witteman HO, Vaissou G, Provencher T, Chipenda Dansokho S, Colquhoun H, Dugas M, et al. An 11-Item Measure of User- and Human-Centered Design for Personal Health Tools (UCD-11): Development and Validation. *J Med Internet Res*. 2021;23(3):e15032. PMID: 33724194.
- [30] Jaffar A, Mohd Sidik S, Foo CN, Muhammad NA, Abdul Manaf R, Fadhilah Ismail SI, et al. Protocol of a Single-Blind Two-Arm (Waitlist Control) Parallel-Group Randomised Controlled Pilot Feasibility Study for mHealth App among Incontinent Pregnant Women. *Int J Environ Res Public Health*. 2021;18(9):4792.
- [31] Perera J, Kirthinanda DS, Wijeratne S, Wickramarachchi TK. Descriptive cross sectional study on prevalence, perceptions, predisposing factors and health seeking behaviour of women with stress urinary incontinence. *BMC Womens Health*. 2014;14(1):78. PMID: 24985068.
- [32] Morey SA, Barg-Walkow LH, Rogers WA. Managing heart failure on the Go: Usability issues with mHealth apps for older adults. *Proc Hum Factors Ergon Soc*. 2017;2017-October:1–5.
- [33] Loh KP, Ramsdale E, Culakova E, Mendler JH, Liesveld JL, O’Dwyer KM, et al. Novel mHealth App to Deliver Geriatric Assessment-Driven Interventions for Older Adults With Cancer: Pilot Feasibility and Usability Study. *JMIR Cancer*. 2018;4(2):e10296. PMID: 30373733.
- [34] Saparamadu AADNS, Fernando P, Zeng P, Teo H, Goh A, Lee JMY, et al. User-Centered Design Process of an mHealth App for Health Professionals: Case Study. *JMIR mHealth uHealth*. 2021;9(3):e18079. PMID: 33769297.
- [35] Nadal C, Sas C, Doherty G. Technology acceptance in mobile health: Scoping review of definitions, models, and measurement. *J Med Internet Res*. 2020;22(7):1–17. PMID: 32628122.
- [36] Binyamin SS, Zafar BA. Proposing a mobile apps acceptance model for users in the health area: A systematic literature review and meta-analysis. *Health Informatics J*. SAGE Publications Ltd; 2021;27(1):1460458220976737.

# Aligning Software System Level with Business Process Level through Model-Driven Architecture

Maryam Habba<sup>1</sup>, Mounia Fredj<sup>3</sup>

AlQualsadi Research Team  
ENSIAS, Mohammed V University in Rabat  
Rabat, Morocco

Samia Benabdellah Chaoui<sup>2</sup>

Department of Mathematics and Computer Science  
Faculty of Sciences Ain Chock, Hassan II University  
Casablanca, Morocco

**Abstract**—Information systems are intended to provide organisations with a new way of sustaining themselves, by helping them manage their activities using innovative technologies. Information systems require aligned levels for maximum effectiveness. In this context, business and information technology (IT) alignment is an important issue for the success of organisations. This paper presents the first step of the proposed approach to align the software system level, modelled by a Unified Modeling Language (UML) class diagram, with the business process level, modelled by the Business Process Model and Notation (BPMN) model. A model-driven architecture approach is proposed as a means to transform a set of BPMN models into a UML class diagram. A set of transformation rules is proposed, followed by guidelines that help apply those rules.

**Keywords**—Information system alignment; business process; software system; Business Process Model and Notation (BPMN); Unified Modeling Language (UML); class diagram

## I. INTRODUCTION

The effective operation of organisations requires an approach that assesses and corrects ambiguities between its different entities. In fact, an alignment approach has become crucial for the continuity of organisations' information systems, as it provides solutions to problems associated with the diverse changes that may occur in these organisations' entities. Several previous studies have examined the subject of business/IT alignment [1]–[5]. The analysis and proposed approach described in this paper are based on the relevance of alignment in various situations. Indeed, in practice, an information system with aligned levels may undergo changes in one of these levels due to the improvement of goals or other factors. As a result, the levels will become misaligned. In another context, the levels of an organisation's information system may be modelled by different teams. Each team may then have a different perspective regarding the system, which can also result misaligned levels. Another example is the case of two organizations that merge in such a way that their levels may be of different natures. As a consequence, the resulting information system will contain levels that are not aligned. For all the mentioned situations, it seems to be a strong necessity to apply an alignment approach in order to have a successful information system.

In this context, approaches of related work based on business process and software system levels are analysed through this paper. Afterwards, an alignment approach is

proposed. The first step of this approach consists of providing a series of rules to transform a set of Business Process Model and Notation (BPMN) models into a Unified Modeling Language (UML) class diagram, based on model-driven architecture (MDA).

The proposed approach contributes to the existing literature by transforming a series of source-level models that contain a significant number of BPMN elements into a UML class diagram. Moreover, the proposed approach provides a method for preserving target level information.

This paper is organised as follows: Section II presents the background of the topic; it introduces the concept of alignment and transformation through MDA. Section III provides a brief overview of related work, while the proposed approach is presented in Section 0. Section V of this paper presents a case study. Finally, a conclusion describes the future work.

## II. BACKGROUND

### A. The Concept of Alignment

Alignment is an important topic that has been of interest for decades. Various expressions have been used to describe it in the existing literature. Chan [6] uses the terms fit and synergy. Henderson and Venkatraman [7] employ the terms fit, integration, and interrelationships. Reich and Benbasat [8] use the word linkage. Ciborra [9], defines alignment as a bridge. Smaczny [10] describes it as fusion. Luftman [11] uses the term harmony, and Nickels [12] names it congruence.

According to Ullah [5], alignment between business and IT concerns “the optimized synchronization between dynamic business objectives/processes and respective technological services provided by IT”. For Luftman [11], business-IT alignment consists on the application of IT in a timely and a suitable manner, in harmony with business strategies, goals and needs. This definition of alignment considers: the way that IT is aligned with the business, and the way the business should or might be aligned with IT.

In the current work, alignment of a target level with a source level is defined as a method that ensures the continued operation of the target level, while remaining suitable to the source level.

### B. Transformation and Model-Driven Architecture

Model-driven engineering considers models to have a very important role in software development. In this context, the

This work is sponsored by the Excellence Research Scholarships Program of CNRST (National Centre for Scientific and Technical Research) of Morocco (grant number 51UM52016).

Object Management Group (OMG) made their MDA initiative public [13]. Fig. 1 presents the model transformation concept [14] recommended by MDA. The model transformation takes a source model that conforms to its source metamodel and a target metamodel as input. It then uses a set of transformation rules to generate as output a target model that conforms to the target metamodel as output.

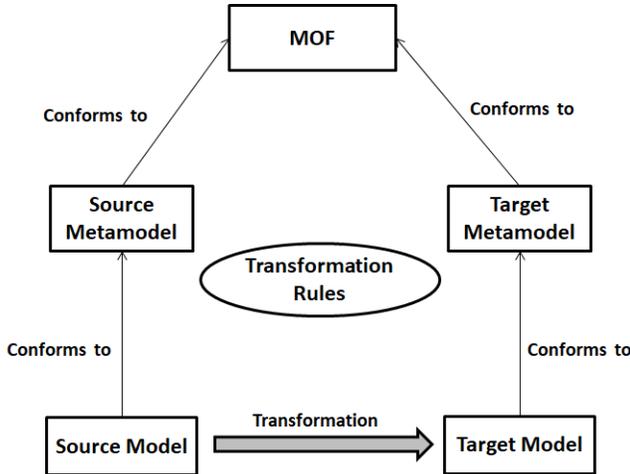


Fig. 1. Concept of Transformation in MDA [14].

### III. RELATED WORK

In the previous work [15], a pattern system was proposed as a guideline, to help organisations apply the alignment. The systematic literature review conducted by Habba et al. [16] identified various approaches of alignment of business requirement, business process and software system levels, that use different modeling languages.

We focus on UML and BPMN languages because they are standards defined by the Object Management Group (OMG). More precisely, in this paper, we focus on a business process level modelled by BPMN and a software system level modelled by a UML class diagram.

BPMN and class diagrams are subjects of interest in different approaches. Amr et al. [17] propose an MDA approach for transforming a BPMN source model into a UML class diagram, using a set of transformation rules. Brdjanin et al. [18] present an approach for the automated generation of a conceptual database model represented by a UML class diagram, from one BPMN model. Brdjanin et al. [19] take a set of business process models into account. Khelif et al. [20] describe an approach to transform a business process model into a class diagram, based on semantic and structural aspects. Rhazali et al. [21] suggest a set of transformation rules for transforming a BPMN model into a use case, state and class diagrams. Cruz et al. [22] propose an approach to obtain a data model from a business process model. Cruz et al. [23] present rules to transform a set of business process models into a data model. Kriouile et al. [24] describe an approach to transform a BPMN model into a domain class model. Bousetta et al. [25] propose an approach to building a domain class diagram, based on a BPMN model, using a set of business rules.

In organisations, models of both levels usually exist. The aim, therefore, is to align them. By analysing existing approaches, we notice that:

- Existing approaches propose transformation from the source level into the target level. However, an approach-based transformation is not always sufficient to apply alignment when business process and software system models exist. In fact, this approach causes a loss of information. Fig. 2 presents the result of applying one of the existing approaches when models exist in an organisation. M1 represents the business process level model and M2 is the software system level model. The existing approaches generate a new UML class diagram (M2') that is different from model M2. Therefore, information associated with the existing UML class diagram will be lost.

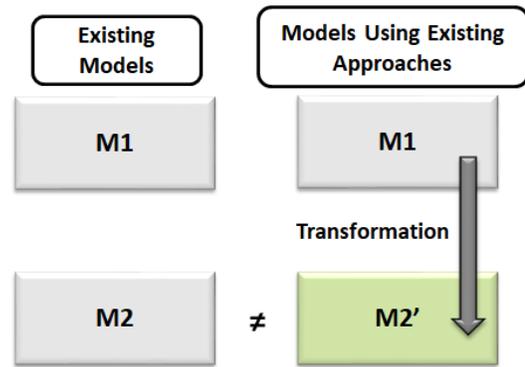


Fig. 2. Application of an Existing Approach.

- The majority of approaches take one model at the source level into consideration. Only two approaches ([19] and [23]) have achieved transformation using a set of BPMN models as a source. However, operations are not considered in the metamodel of the target model. (Table I, columns 3 and 6).
- The existing approaches do not consider all BPMN elements, such as all types of tasks and all types of data, in the source model (Table I, columns 4 and 5).

We synthesize the existing approaches in Table I, according to the criteria below:

- Preserving information: This column indicates if the proposed approach can be executed when the models of the two levels exist in the organisation.
- Considering a set of BPMN models: This column indicates if the proposed approach considers a set of BPMN models in business process level.
- Considering all types of tasks: This column indicates if the approach considers all types of tasks in the source model or not.
- Considering all types of data: This column indicates if the approach considers all types of data in the source model or not.

- Considering operations: This column indicates if the approach considers all types of data in the target model or not.

In Table I, Y shows that the criterion is considered.

TABLE I. SYNTHESIS OF APPROACH

Ref.	Preserving information	Considering a set of BPMN models	Considering all types of tasks	Considering all types of data	Considering operations
[17]	-	-	-	-	Y
[18]	-	-	-	-	-
[19]	-	Y	-	-	-
[20]	-	-	-	-	Y
[21]	-	-	-	-	Y
[22]	-	-	-	-	-
[23]	-	Y	-	-	-
[24]	-	-	-	-	Y
[25]	-	-	-	-	-

This analysis of existing approaches reveals the need for an alignment approach that preserves target level information, considers a large number of BPMN and UML elements, and uses a set of BPMN models as a source.

#### IV. PROPOSED APPROACH

##### A. Overview of the Proposed Approach

The aim of the proposed approach is to reduce the gap between the business process level and the software system level of an organisation, without losing information. The business process level is modelled using a set of BPMN models. It may be composed of a set of collaboration diagrams and expanded sub-processes, and it contains a high number of metamodel elements. The software system level is modelled by a UML class diagram. Fig. 3 illustrates a representation of the proposed approach. We assume that the organisation has two levels, composed of a set of BPMN models and one existing UML class diagram. The organisation needs to align the software system level with the business process level. The proposed alignment approach encompasses two steps:

1) *Step 1: Transformation.* This step consists of the application of rules to transform a set of BPMN models into a generated UML class diagram. It considers the important elements of the BPMN metamodel and the UML class diagram metamodel, including all types of tasks and all types of data.

2) *Step 2: Composition.* This step consists of creating a fusion between the UML class diagram generated in step 1 and the existing UML class diagram. The result is a final UML class diagram that will represent the software system level, which is aligned with the business process level.

By applying the two steps, the target level will be complete, as it contains the information related to the existing class diagram as well as the information related to the generated class diagram.

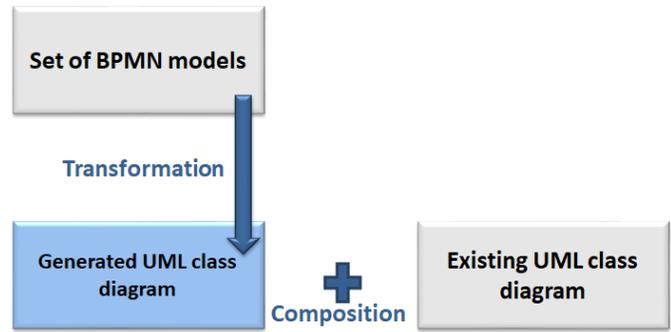


Fig. 3. Representation of the Approach.

In this paper, the first step of the approach is detailed: Transformation. This step uses a set of BPMN models as a source and applies transformation rules to derive a UML class diagram.

##### B. Example of a Set of BPMN Models

In this section, a set of BPMN models are presented. They represent the business process level of an organisation. Fig. 4 and Fig. 6 represent collaboration diagrams. Fig. 5, Fig. 7 and Fig. 8 depict expanded sub-processes, represented in collaboration diagrams as collapsed sub-processes.

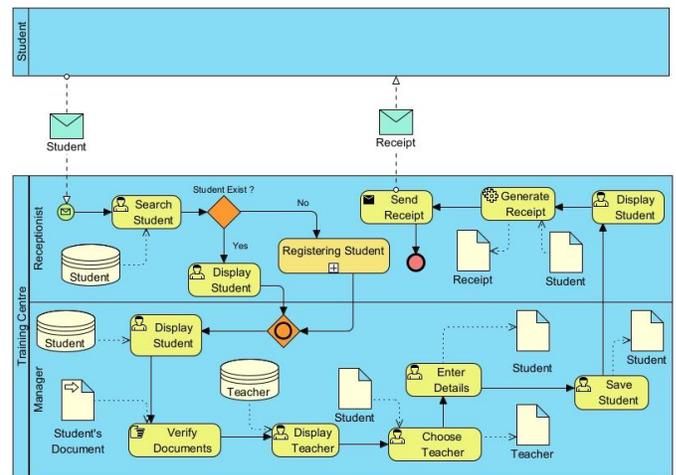


Fig. 4. Collaboration Diagram for Assigning a Professor to a Student.

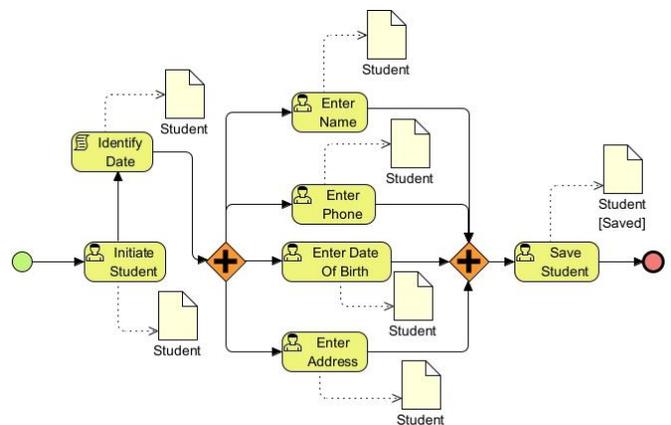


Fig. 5. Expanded Sub-process "Registering Student".

Fig. 4 illustrates the collaboration diagram for assigning a professor to a student. It is composed of two pools: “Student”, as a black box and “Training Centre”, which contains two lanes “Receptionist” and “Manager”. The diagram begins when a student arrives at the training centre for enrolment. The first activity is performed by the receptionist. It consists of searching for a student to see if they are registered or not. Two cases are possible: if the student is registered, the student’s file will be displayed. If not, the receptionist will proceed to the registration phase. Next, the manager will display the student file, verify documents, display teacher, choose teacher, enter details and then save the student file. Then, the receptionist will display the student file, generate a receipt and finally send the receipt. The second collaboration diagram (Fig. 6) contains two pools: “Supplier”, represented as a black box, and “Training Centre” which contains two lanes (“Receptionist” and “Teacher”). The teacher displays a student file, and then prepares a note that will be displayed by the receptionist to prepare a quote request that will be sent to a supplier. Finally, the receptionist will receive a quote.

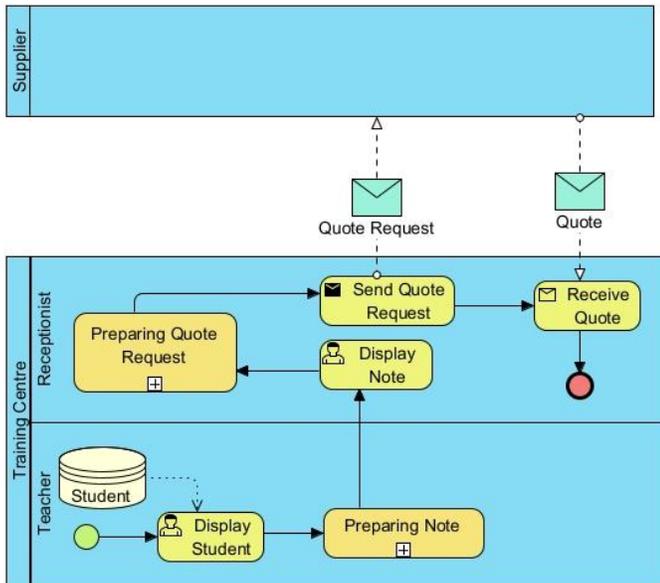


Fig. 6. Collaboration Diagram for Requesting a Quote.

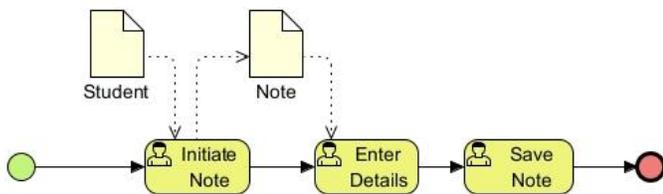


Fig. 7. Expanded Sub-process "Preparing Note".

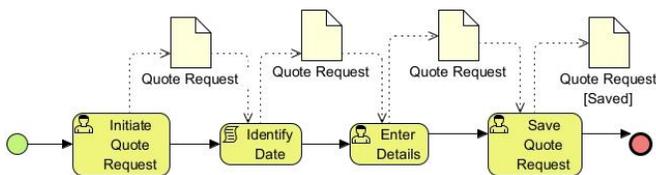


Fig. 8. Expanded Sub-process "Preparing Quote Request".

### C. Transformation Rules

In order to transform a set of BPMN models into a UML class diagram, a set of rules that take different elements of BPMN into consideration are proposed.

1) *Data* (data object, data input, data output and data store) related to send, receive, user, service, script or business rule tasks.

TR1: This rule transforms data that is related to send, receive, user, service, script or business rule tasks into a class with the same name, containing an attribute (id).

2) *Message*

TR2: This rule transforms a message into a class with the same name, containing an attribute (id).

3) *User task, service task, script task, business rule task*

a) *A task with input and output data*

TR3.1: Let TusvschrIO be a user, service, script or business rule task with data DIT (data object, data input or data store) as input, and data DOT (data object, data output or data store) as output.

TR3.1 transforms data DIT and DOT into classes, according to TR1. Then, it transforms the task TusvschrIO into an operation that will belong to the resulting class of DOT. The name of the operation is obtained by removing the spaces between words, making the first letter of the first word in the name of the task lowercase and the first letter of all other words uppercase. This name change is called "reduced form of the task name", RTusvschrIO. The DIT and DOT classes will be linked by an association (if the names of data DIT and data DOT are different). Fig. 9 presents an illustration of rule TR3.1. To identify multiplicities, the following guidelines are applied:

- If DIT is a singular data object, singular data input or data store, then the multiplicity on the side of the class corresponding to DIT is of value 1.
- If DIT is a collection data object or collection data input, then the value of the side of the class that corresponds to DIT is 1..\*.
- If DOT is a singular data object, singular data output or data store, then the multiplicity on the side of the class corresponding to DOT is of value 0..1.
- If DOT is a collection data object or collection data output, then the value of the side of the class that corresponds to DOT is 0..\*.

Fig. 10 presents an example of rule TR3.1. The user task “Initiate Note” has the data object “Student” in singular form as input, and the data object “Note” in singular form as output. Thus, in the class diagram, two classes DIT and DOT that contains an attribute (id) will be created. The class “Note” will contain the operation “initiateNote”. An association will be generated between the classes with multiplicities 1 on the side of the class “Student” and 0..1 on the side of the class “Note”.

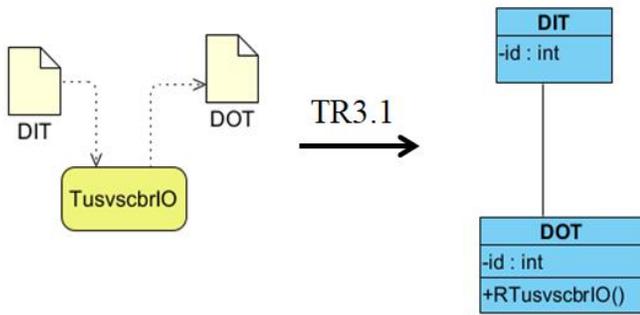


Fig. 9. Illustration of Rule TR3.1.

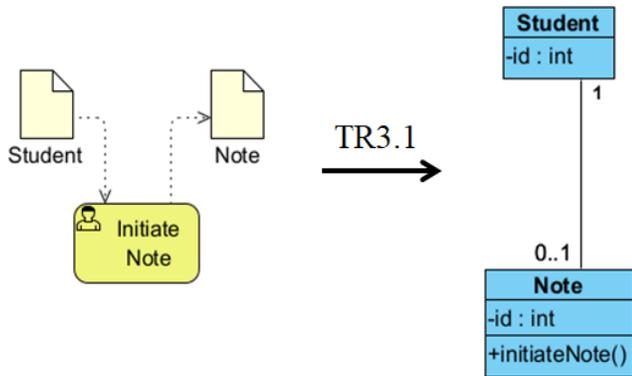


Fig. 10. Example of Rule TR3.1.

*b) A task with output data only*

TR3.2: Let TusvschrO be a user, service, script or business rule task with data JDOT (data object, data output or data store) as output, and no input data.

Rule TR3.2 transforms data JDOT into a class, according to TR1. Then, it transforms the task TusvschrO into an operation that will belong to the resulting JDOT class. The name of the operation will be the reduced form of the task name, RTusvschrO. Fig. 11 presents an illustration of rule TR3.2 while Fig. 12 presents an example.

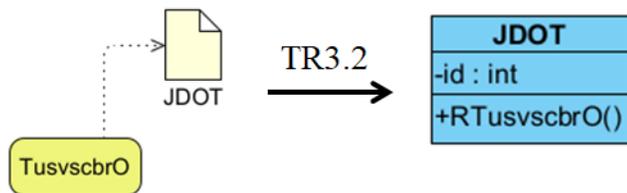


Fig. 11. Illustration of Rule TR3.2.

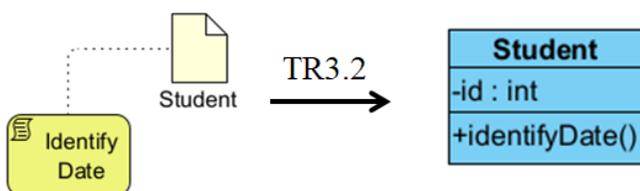


Fig. 12. Example of Rule TR3.2.

*c) A task with input data only*

TR3.3: Let TusvschrI be a user, service, script or business rule task linked to data JDIT (data object, data input or data store) as input.

Rule TR3.3 transforms data JDIT into a class, according to TR1. Then, it transforms task TusvschrI into an operation that will belong to the resulting JDIT class. The name of the operation will be the reduced form of the task name, RTusvschrI. Fig. 13 presents an illustration of rule TR3.3 while Fig. 14 presents an example.

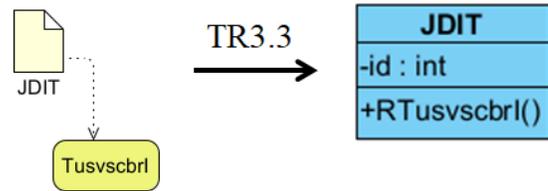


Fig. 13. Illustration of Rule TR3.3.

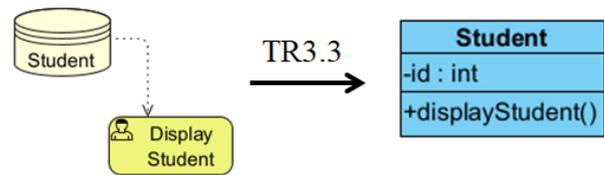


Fig. 14. Example of Rule TR3.3.

*d) A task without input or output data*

TR3.4: Let Tusvschr be a user, service, script or business rule task that is not linked to any data.

Rule TR3.4 transforms task Tusvschr into a class, named by using the singular form of the direct object of the task name. It's designated by SOTusvschr. The class will contain an attribute id and an operation. The name of the operation will be the reduced form of the task name, RTusvschr.

Fig. 15 presents an illustration of rule TR3.4 while Fig. 16 presents an example. The task Tusvschr, named "Display Note", is not related to any data. "Note" is a direct object of task Tusvschr and it is in a singular form. For this reason, the task named "Display Note" will be transformed into a class named "Note", containing an attribute id and an operation named "displayNote".

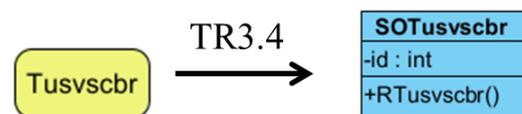


Fig. 15. Illustration of Rule TR3.4.

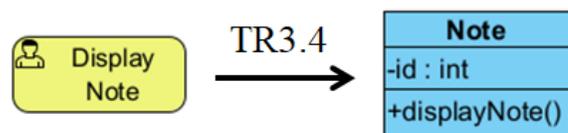


Fig. 16. Example of Rule TR3.4.

4) Send task

a) A send task with input and output data

TR4.1: Let TsdIO be a send task with data DIsdT (data object, data input or data store) as input and data DOsdT (data object, data output or data store) as output.

Rule TR4.1 transforms data DIsdT and DOsdT into classes, according to TR1. Then, it transforms task TsdIO into an operation that will belong to the resulting DOsdT class. The name of the operation will be the reduced form of the task name, RTsdIO. The DIsdT and DOsdT classes will be linked by an association (if the names of data DIsdT and data DOsdT are different). Fig. 17 presents an illustration of rule TR4.1. To identify multiplicities, the following guidelines are applied:

- If DIsdT is a singular data object, a singular data input or data store, then the multiplicity on the side of the class corresponding to DIsdT is of value 1.
- If DIsdT is a collection data object or collection data input, then the value of the side of the class that corresponds to DIsdT is 1..\*.
- If DOsdT is a singular data object, a singular data output or data store, then the multiplicity on the side of the class corresponding to DOsdT is of value 0..1.
- If DOsdT is a collection data object or a collection data output, then the value of the side of the class that corresponds to DOsdT is 0..\*.

b) A send task with output data

TR4.2: Let TsdO be a send task with data JDOsdT (data object, data output or data store) as output.

Rule TR4.2 transforms data JDOsdT into a class, according to TR1. Then, it transforms task TsdO into an operation that will belong to the resulting JDOsdT class. The name of the operation will be the reduced form of the task name, RTsdO. Fig. 18 presents an illustration of the rule TR4.2.

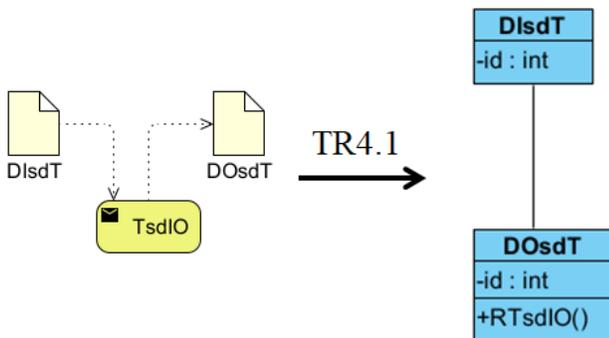


Fig. 17. Illustration of Rule TR4.1.

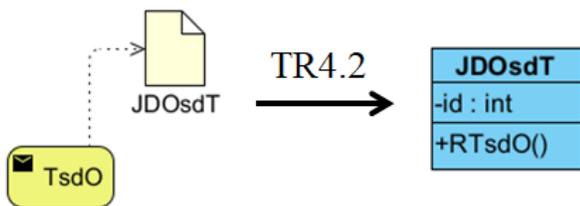


Fig. 18. Illustration of Rule TR4.2.

c) A send task with input data

TR4.3: Let TsdI be a send task with data JDIsdT (data object, data input or data store) as input.

Rule TR4.3 transforms data JDIsdT into a class, according to rule RT1. Then, it transforms task TsdI into a class, named using the singular form of the direct object (OTsdI) of the task name. It's designated by SOTsdI. The class will contain an attribute id and an operation. The name of the operation will be the reduced form of the task name, RTsdI. The JDIsdT and SOTsdI classes will be linked by an association (if the names of JDIsdT and SOTsdI are different). Fig. 19 presents an illustration of rule TR4.3. To identify multiplicities, the following guidelines are applied:

- If JDIsdT is a singular data object, a singular data input or a data store, then the multiplicity on the side of the class corresponding to JDIsdT is of value 1.
- If JDIsdT is a collection data object or collection data input, then the value of the side of the class that corresponds to JDIsdT is 1..\*.
- If OTsdI is in a singular form, then the multiplicity on the side of the class corresponding to SOTsdI is of value 0..1.
- If OTsdI is in plural, then the value of the side of the class that corresponds to SOTsdI is 0..\*.

d) A send task without input or output data

TR4.4: Let Tsd be a send task without data.

Rule TR4.4 transforms task Tsd into a class, named using the singular form of the direct object of the task name. It's designated by SOTsd. The class will contain an attribute id and an operation. The name of the operation will be the reduced form of the task name, RTsd. Fig. 20 presents an illustration of rule TR4.4, while Fig. 21 presents an example.

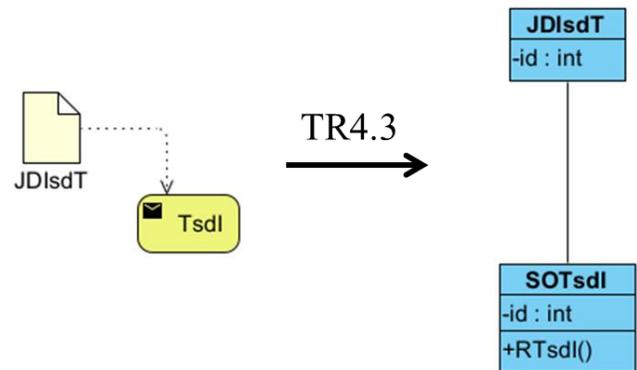


Fig. 19. Illustration of Rule TR4.3.

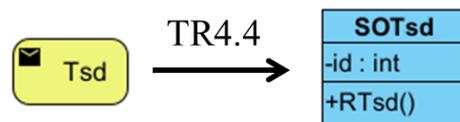


Fig. 20. TR4.4 Illustration.

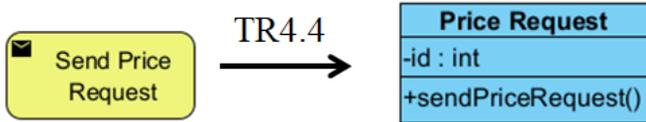


Fig. 21. Example of Rule TR4.4

5) Receive task

a) A receive task with input and output data

TR5.1: Let TrvIO be a receive task with data DIrvt (data object, data input or data store) as input and data DOrvt (data object, data output or data store) as output.

Rule TR5.1 transforms data DIrvt and DOrvt into classes, according to TR1. Then, it transforms task TrvIO into an operation that will belong to the resulting DIrvt class. The name of the operation will be the reduced form of the task name, RTrvIO. The DIrvt and DOrvt classes will be linked by an association (if the names of data DIrvt and data DOrvt are different). Fig 22 presents an illustration of the rule TR5.1.

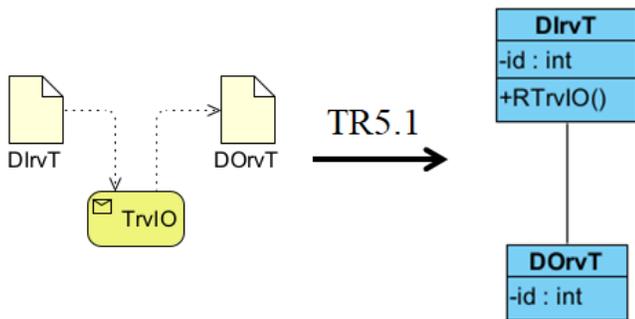


Fig. 22. Illustration of Rule TR5.1.

b) A receive task with input data

TR5.2: Let TrvI be a receive task with data JDIrvt (data object, data input or data store) as input. Rule TR5.2 transforms task TrvI into an operation in the class, corresponding to data TrvI. The name of the operation will be the reduced form of the task name, RTrvI. Fig. 23 presents an example of rule TR5.2.

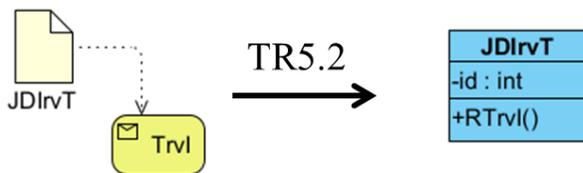


Fig. 23. Illustration of Rule TR5.2.

c) A receive task with output data

TR5.3: Let TrvO be a receive task with data JDOrvT (data object, data output or data store) as output.

Rule TR5.3 transforms data JDOrvT into a class, according to rule TR1. Then, it transforms task TrvO into a class, named using the singular form of the direct object (OTrvO) of the task name. It's designated by SOTrvO. The class will contain an

attribute id and an operation. The name of the operation will be the reduced form of the task name, RTrvO. Fig. 24 presents an illustration of rule TR5.3. The JDOrvT and SOTrvO classes will be linked by an association (if the names of JDOrvT and SOTrvO are different). To identify multiplicities, the following guidelines are applied:

- If OTrvO is in a singular form, then the multiplicity on the side of the class corresponding to SOTrvO is of value 1.
- If OTrvO is in a plural form, then the value of the side of the class that corresponds to SOTrvO is 1..\*.
- If JDOrvT is a singular data object, singular data output or a data store, then the multiplicity on the side of the class corresponding to JDOrvT is of value 0..1.
- If JDOrvT is a collection data object or collection data output, then the value of the side of the class that corresponds to JDOrvT is 0..\*.

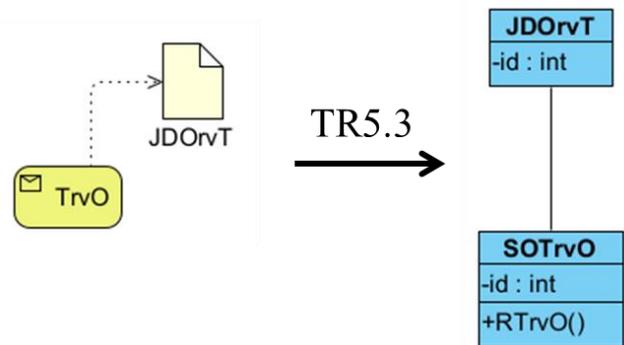


Fig. 24. Illustration of Rule TR5.3.

d) A receive task without input or output data

TR5.4: Let Trv be a receive task without data.

Rule TR5.4 transforms task Trv into a class, named using the singular form of the direct object of the task name. It's designated by SOTrv. The class will contain an attribute id and an operation. The name of the operation will be the reduced form of the task name, RTrv. Fig. 25 presents an illustration of rule TR5.4, while TR5.4 and Fig. 26 presents an example.

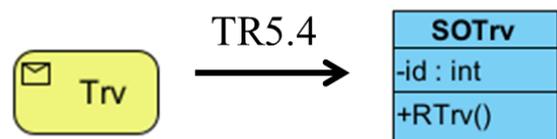


Fig. 25. Illustration of Rule TR5.4.

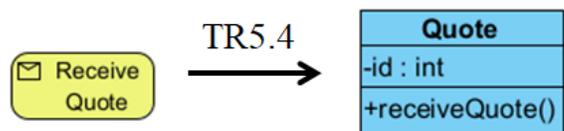


Fig. 26. Example of Rule TR5.4.

### 6) Pool

TR6: Rule TR6 transforms a pool into a class with the same name as the pool, containing five attributes (id, name, email, phone, address).

### 7) Lane within a pool

TR7: Rule TR7 transforms a lane within a pool into classes with the same names as the pool and the lane. Each class will contain five attributes (id, name, email, phone, address). Then, it adds aggregation between the class corresponding to the pool and the class corresponding to the lane (multiplicities 1 and 0..\* respectively).

### 8) Relationship between a pool/lane and a non-manual task belonging to it

TR8: Rule TR8 transforms a relationship between a pool/lane and a non-manual task belonging to it into an association between the class corresponding to the pool/lane and the class that contains the reduced form of the task's name (multiplicities 1 and 0 respectively).

### 9) Relationship between a message and an element that is the source or the target of the message flow (pool, event belonging to a pool/lane or task belonging to a pool/lane).

TR9: Rule TR9 transforms a relationship between a message and an element that is the source or the target of the message flow (pool, event belonging to a pool/lane or task belonging to a pool/lane) into an association between the class corresponding to the pool/lane and the class corresponding to the message (multiplicities 1 and 0..\* respectively).

## D. Isolated elements

In this section, the isolated elements are presented. An isolated element belongs to the BPMN metamodel and does not have an equivalent in the UML class diagram metamodel.

1) *Manual task*: A manual task is performed without the intervention of any application. Therefore, it will not be visualised by the software. For this reason, this type of task is considered an isolated element, and it has no equivalent in the class diagram.

2) *Data linked to a manual task*: Data that is linked to a manual task will not have traceability through the system.

Because the manual task has no visualisation, this data is considered an isolated element.

3) *Event*: Usually, an event is a fact that occurs during the process. Because the class diagram represents a static aspect, an event is considered an isolated element.

4) *Gateway*: The goal of a gateway is to control the convergence or divergence of flows in a process. It does not have an equivalent in the class diagram.

5) *Artifact*: An artifact (group or annotation) aims to provide more clarity to understand the process. It does not have an equivalent in the class diagram.

6) *Sequence flow*: A sequence flow can indicate the flow of activities through a process. It does not have an equivalent. In fact, the tasks linked by the sequence flows that have an equivalent in the class diagram.

7) *Association*: An association is a way to link the artifacts with different BPMN elements and does not have an equivalent in the class diagram.

## E. Steps for a Set of Models

In order to apply the rules presented in section C, a series of steps based on BPMN notation are presented in this section, to transform a set of BPMN models into a class diagram. Fig. 27 shows the process of this transformation. It constitutes five looped sub-processes.

### 1) Transformation of task: this sub-process can

- Identify non manual task.
- Identify task type.

According to the type of task, apply rule TR3.1, TR3.2, TR3.3, TR3.4, TR4.1, TR4.2, TR4.3, TR4.4, TR5.1, TR5.2, TR5.3 or TR5.4, which all call rule TR1. When applying a rule, a check is performed to determine whether an element (class, operation or association) has already been created by another rule. If it has:

- All the instructions associated with that rule are applied, except creation of the element.
- If an association already exists, such that the multiplicities are different, the existing association is kept, and the union of multiplicities is applied for each end of the association.

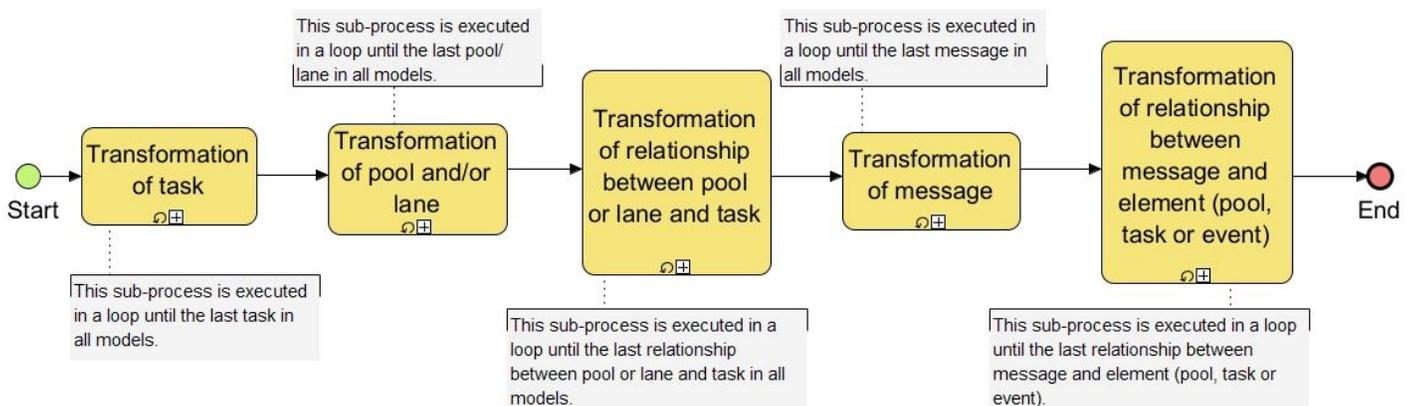


Fig. 27. The Transformation Process.

2) Transformation of pool and/or lane: for each pool that exists in the different models this sub-process can.

a) Identify the pool

b) According to the type of pool (with or without lanes), apply the rule TR6 or TR7. When applying a rule, a check is performed to determine whether an element (class, attribute or aggregation) has already been created by another rule. If this is the case, all instructions associated with that rule are applied, except creation of the element.

3) Transformation of relationship between pool or lane and task: for each relationship between a pool or a lane and a task this sub-process can.

a) Identify the relationship between the pool or lane and task.

b) According to the type of relationship, apply the rule TR8. When applying a rule, a check is performed to determine whether an association has already been created by another rule. If an association already exists such that the multiplicities are different, the existing association is kept, and the union of multiplicities is applied for each end of the association.

4) Transformation of message: for each message this sub-process can.

a) Identify a message.

b) Apply TR2.

5) Transformation of relationship between message and element (pool, task or event): for each relationship between a message and an element (pool, task or event) this sub-process can.

a) Identify the relationship between a message and an element (pool, task or event).

b) Apply TR9. When applying the rule, a check is performed to determine whether an association has already been created by another rule. If an association already exists such that the multiplicities are different, the existing association is kept, and the union of the multiplicities is applied for each end of the association.

## V. CASE STUDY

In order to illustrate the application of the proposed transformation rules, the set of BPMN models represented in section B are transformed into a UML class diagram. The example describes two collaboration diagrams and three expanded sub-processes. The first context is the training centre that receives students who want to have a teacher as a mentor. In the second context, the training centre communicates with suppliers to obtain a particular quote, related to student needs. Fig. 28 presents the class diagram obtained by the application of the transformation rules, according to the global process of transformation presented in Section EIVE.

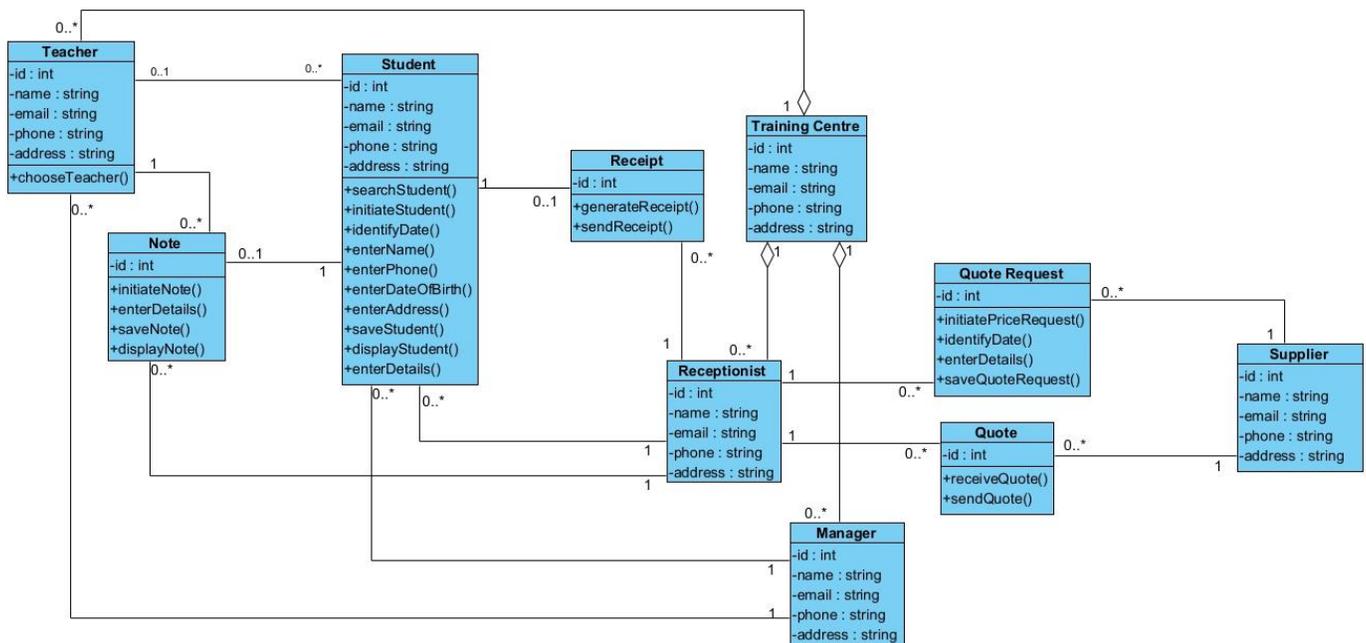


Fig. 28. Obtained Class Diagram.

## VI. CONCLUSION

In this paper, a method for aligning software system level using UML class diagram with business process level using BPMN notation is proposed. This proposal enables to contribute to the alignment process of an organization, by considering a set of models at the source level that contains a large number of BPMN metamodel elements. Furthermore, the method aims to preserve information, filling a crucial need for organisations' long-term success. The first phase was described here, detailing a series of rules for transforming a set of BPMN models into a UML class diagram. Moreover, a guideline is presented to help organisations apply rules properly. A set of isolated elements is also presented to explain the BPMN elements that are not considered by the transformation rules. The application of the proposed rules is demonstrated in a case study. In future work, we aim to use the ATLAS Transformation Language to automate the proposed transformation rules.

## ACKNOWLEDGMENT

We would like to thank the Excellence Research Scholarships Program of CNRST (National Centre for Scientific and Technical Research) of Morocco for supporting this research. This work is under research grant number 51UM52016.

## REFERENCES

- [1] T.Wasiuk, F.P.C.Lim, "Factors Influencing Business IT Alignment". International Journal of Smart Business and Technology, vol.9, no.1, pp.1-12, Mar. 2021.
- [2] H. Darii, J. Laval, V. Botta-Genoulaz, and V. Goepf, "Measurement of the business/IT alignment of information systems." In ILS 2020-8th International Conference on Information Systems, Logistics and Supply Chain, pp. 228-235. 2020.
- [3] P. Gajardo and L. P. Ariel, "The business-it alignment in the digital age." In The 13th Mediterranean Conference on Information Systems (ITAIS & MCIS), Naples, Italy. 2019.
- [4] M. Zhang, H. Chen, and A. Luo, "A systematic review of business-IT alignment research with enterprise architecture," IEEE Access, vol. 6, pp. 18933–18944, 2018.
- [5] A. Ullah and R. Lai, "A systematic review of business and information technology alignment," ACM Trans. Manag. Inf. Syst., vol. 4, no. 1, pp. 1–30, 2013.
- [6] Y. E. Chan, "Business Strategy, information system strategy, and strategic fit: Measurement and performance impacts," p. 362, 1992.
- [7] J. C. Henderson and H. Venkatraman, "Strategic alignment: Leveraging information technology for transforming organizations," IBM Syst. J., vol. 38, no. 2.3, pp. 472–484, 1999.
- [8] B. H. Reich and I. Benbasat, "Measuring the linkage between business and information technology objectives," MIS Q. Manag. Inf. Syst., vol. 20, no. 1, pp. 55–77, 1996, doi: 10.2307/249542.
- [9] C. U. Ciborra, "De profundis? Deconstructing the concept of strategic alignment," Scand. J. Inf. Syst., vol. 9, no. 1, p. 2, 1997.
- [10] T. Smaczny, "Is an alignment between business and information technology the appropriate paradigm to manage IT in today's organisations?," Manag. Decis., 2001.
- [11] J. Luftman, "Assessing business-IT alignment maturity," in Strategies for information technology governance, Igi Global, pp. 99–128, 2004.
- [12] D. W. Nickels, "Business and IT Alignment: What We Know That We Still Don't Know," Proc. 7th Annu. Conf. South. Assoc. Inf. Syst., pp. 79–84, 2004.
- [13] R. Soley, "Model driven architecture," OMG white Pap., vol. 308, no. 308, p. 5, 2000.
- [14] J. Bézin and O. Gerbé, "Towards a precise definition of the OMG/MDA framework," in Proceedings 16th Annual International Conference on Automated Software Engineering (ASE 2001), pp. 273–280, 2001.
- [15] M. Habba, M. Fredj, and S. B. Chaouni, "Towards an operational alignment approach for organizations," ACM Int. Conf. Proceeding Ser., pp. 29–34, 2017, doi: 10.1145/3149572.3149602.
- [16] M. Habba, M. Fredj, and S. Benabdellah Chaouni, "Alignment between Business Requirement, Business Process, and Software System: A Systematic Literature Review," J. Eng., vol. 2019, 2019.
- [17] M. F. Amr, N. Benmoussa, K. Mansouri, and M. Qbadou, "Transformation of the CIM Model into a PIM Model According to The MDA Approach for Application Interoperability: Case of the" COVID-19 Patient Management" Business Process," iJOE, vol. 17, no. 05, p. 49, 2021.
- [18] D. Brdjanin, G. Banjac, and S. Maric, "Automated synthesis of initial conceptual database model based on collaborative business process model," in International Conference on ICT Innovations, pp. 145–156, 2014.
- [19] D. Brdjanin, A. Vukotic, G. Banjac, D. Banjac, and S. Maric, "Automatic Derivation of Conceptual Database Model from a Set of Business Process Models," in 2020 International Conference on INnovations in Intelligent SysTems and Applications (INISTA), pp. 1–8, 2020.
- [20] W. Khlif, N. Elleuch, E. Alotabi, and H. Ben-Abdallah, "Designing BP-IS Aligned Models: An MDA-based Transformation Methodology," in Proceedings of the 13th International Conference on Evaluation of Novel Approaches to Software Engineering, pp. 258–266, 2018.
- [21] Y. Rhazali, Y. Hadi, and A. Mouloudi, "A methodology of model transformation in MDA: From CIM to PIM," Int. Rev. Comput. Softw., vol. 10, no. 12, pp. 1186–1201, 2015, doi: 10.15866/irecos.v10i12.8088.
- [22] E. F. Cruz, R. J. Machado, and M. Y. Santos, "From business process modeling to data model: A systematic approach," Proc. - 2012 8th Int. Conf. Qual. Inf. Commun. Technol. QUATIC 2012, pp. 205–210, 2012, doi: 10.1109/QUATIC.2012.31.
- [23] E. F. Cruz, R. J. Machado, and M. Y. Santos, "Deriving a Data Model from a Set of Interrelated Business Process Models.," in ICEIS (2), pp. 49–59, 2015.
- [24] A. Kriouile, N. Addamssiri, T. Gadi, and Y. Balouki, "Getting the static model of PIM from the CIM," in 2014 Third IEEE International Colloquium in Information Science and Technology (CIST), pp. 168–173, 2014.
- [25] B. Bousetta, O. El Beggar, and T. Gadi, "A methodology for CIM modelling and its transformation to PIM," J. Inf. Eng. Appl., vol. 3, no. 2, pp. 1–22, 2013.

# A Review of Modern DNA-based Steganography Approaches

Omar Haitham Alhabeeb<sup>1</sup>

Department of Software Engineering, Mosul University  
PhD. Candidate at Universiti Kebangsaan Malaysia  
Mosul, Iraq

Fariza Fauzi<sup>2</sup>, Rossilawati Sulaiman<sup>3</sup>

Faculty of Information Science and Technology  
Universiti Kebangsaan Malaysia  
Selangor, Malaysia

**Abstract**—In the last two decades, the field of DNA-based steganography has emerged as a promising domain to provide security for sensitive information transmitted over an untrusted channel. DNA is strongly nominated by researchers in this field to exceed other data covering mediums like video, image, and text due to its structural characteristics. Features like enormous hiding capacity, high computational power, and the randomness of its building contents, all sustained to prove DNA supremacy. There are mainly three types of DNA-based algorithms. These are insertion, substitution, and complementary rule-based algorithms. In the last few years, a new generation of DNA-based steganography approaches has been proposed by researchers. These modern algorithms overpass the performance of the old ones either by exploiting a biological factor that exists in the DNA itself or by using a suitable technique available in another field of computer science like artificial intelligence, data structure, networking, etc. The main goal of this paper is to thoroughly analyze these modern DNA-based steganography approaches. This will be achieved by explaining their working mechanisms, stating their pros and cons, and proposing suggestions to improve these methods. Additionally, a biological background about DNA structure, the main security parameters, and classical concealing approaches will be illustrated to give a comprehensive picture of the field.

**Keywords**—Information security in bioinformatics; deoxyribonucleic acid-based steganography; modern hiding approaches

## I. INTRODUCTION

Nowadays, the reliance on computer systems and the Internet has dramatically increased. The huge advancement in the technology of data storage and transmission has led to an increase in the information traffic between any two parties at an exponential rate. Many of these information are considered sensitive especially those belonging to the government, the army, or the big companies. It is quite risky to send such information over an untrusted channel [1]. The field of cybersecurity has the cumbersome task of protecting information from different types of threats and attacks. The attacks on shared information may cause it to be disrupted, corrupted, or stolen. Despite the availability of many information security techniques, cryptography and steganography seem to work perfectly together to achieve the mission of securely conveying information from source to destination. While cryptography aims to alter the message in such a way it becomes unreadable to a third party, steganography provides a concealing medium to the message

[2]. In cryptography, a key is usually used to perform the task of data encryption and decryption. There are mainly two types of cryptosystems, these are symmetric key encryption and asymmetric key encryption cryptosystems. The encryption and decryption processes are applied in the symmetric key method via a secret key shared between the sender and the receiver. The length of this key is relatively short which aids in completing the decryption stage quickly. Symmetric key encryption can be categorized into stream cipher or block cipher. In a stream cipher, every character in the message will be individually encrypted. While in block cipher, many bits are assembled in a single unit. Then, this unit will be encrypted. Some of the famous and dominant encryption algorithms that use symmetric key encryption are Digital Encryption Standard (DES), AES, RC4, and IDEA [3]. In the case of asymmetric key encryption, two keys are used to handle the encryption and the decryption processes. A public key is used to encrypt the message by the sender and a private key is used to decrypt the message by the receiver. This will eliminate the risk of losing a pre-shared key as in the previous technique. Although this technique provides high-security measures, a third party must be trusted as a key manager. An instance of asymmetric key encryption is the RSA encryption algorithm [4]. In the field of steganography, mediums like text [5], image [6], audio [7], and video [8,9] are used by researchers as containers to hide a message inside them. Concurrently, technologies of data storage and transmission withstand rapid development and improvements. Also, there are a noticeable diversity of threats and attacking methods that appear every year. All the covering mediums mentioned above struggle to cope with the increasing size of information as well as meet the demanded security measures [10]. An urgent need has arisen for a concealing medium capable of holding a large amount of data without corrupting or degrading the quality of this medium. Consequently, deoxyribonucleic acid (DNA) is proposed as the ultimate concealing medium that avoids or mitigates the drawbacks of other mediums [11]. DNA's most important feature is the huge capacity it has. Around 215 petabytes of data can be stored in one gram of DNA. Another useful feature is the randomness of the building blocks forming the DNA. Besides that, low power is required when dealing with DNA computing which leads to fast execution. For all the reasons mentioned above, many DNA steganography algorithms have been suggested since the beginning of the twenty-first century. As shown in Fig. 1, three components are combined to get the fake DNA sequence. These are the covering medium (which is the DNA sequence in our case), the message, and the secret

key [12]. An additional component can be added to the formula by firstly encrypting the message before hiding it. This will decrease the penetration probability and creates a complete crypto-stego system.

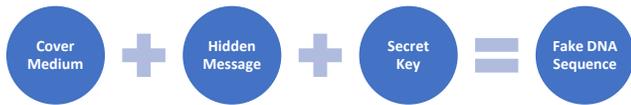


Fig. 1. DNA Steganography Process.

Generally, there are three classical techniques used in DNA-based steganography to embed the hidden message in the cover medium. These are insertion, substitution, and complementary rules-based algorithms. Each one of these techniques has its way of implementation, benefits, and limitations. Even hybrid algorithms of these techniques have been proposed to improve upon them [60]. In the attempt of improving the performance of currently used DNA steganography algorithms, a new trend has evolved. This trend relies on the concept of utilizing one of the DNA biological features and/or merging a technique existing in one of the fields of computer science with a DNA-based steganography algorithm. Doing so showed promising results in terms of overcoming or at least alleviating the issues and gaps that existed in the field of DNA computing. But with the advent of new solutions, new issues have also arisen. This motivates the authors of this manuscript to address these issues and suggest different methods to solve them. Therefore, the main purpose of this paper is to highlight the strong points and drawbacks of recently proposed DNA-base steganography algorithms. It also aims to be a reference for any researcher who wants to develop his/her novel hiding technique. This is accomplished by achieving four objectives. The first objective is exploring the field of genetics, dissecting the structure of the DNA sequence, and informing the reader on the constantly used biological terms in this area without delving into unnecessary clinical concepts. Secondly is enumerating and elaborating the security parameters in this field. Then, classical techniques used to hide a secret message in a DNA sequence are briefly explained. Last but not least is conducting an in-depth analysis of modern approaches.

The rest of the paper is organized as follows: section two includes a biological background about DNA. Section three enumerates the parameters of security measures. Section four contains a concise description of classical DNA-based steganography algorithms. Most importantly section five presents a critical analysis of some modern DNA-based steganography algorithms. Finally, section six discusses the primary open issues of DNA-based steganography, suggests some solutions, and concludes the paper.

## II. BIOLOGICAL BACKGROUND

To work in the field of DNA computing, prior knowledge of biology especially in the field of genetics is required. DNA preserves the genetic information that denotes the physical shape, behavior, and functions of all living organisms. DNA is

constructed from two lengthy strands twisted on each other. These two strands are attached via units called nucleotides to give DNA the shape of a helix ladder. Nucleotides are considered the building blocks of DNA and can be one of four main types. These types are adenine (A), guanine (G), cytosine (C), and thymine (T). The two strands are linked to each other by pairs of nucleotides. This linkage is not haphazardly formed. A is always paired with T via double hydrogen bonds, while C is always paired with G via triple hydrogen bonds [13]. Fig. 2 depicts the structure of the DNA.

Every three consecutive nucleotides represent a unit called a codon. Codons represent either one of the 20 possible amino acids or a stop signal. Since each nucleotide in the three locations of the codon has one of four possible values (A, C, G, and T), there are 43 or 64 different types of codons. Amino acids are represented with 61 types, and 3 dedicated for a stop signal. Every amino acid can be either represented with a single codon up to six types of codons. For example, tryptophan represented with (TGG), glutamic acid represented with (GAA, GAG), and threonine represented with (ACT, ACC, ACA, ACG). The case when an amino acid is represented with more than one codon is called ambiguity. Essential proteins for the human body are formulated from a long chain of amino acids [14]. A complete genetic code of DNA is presented in Table I. A distinctive biological feature in DNA is mutations. These mutations refer to changes that occur in the DNA sequence which modify the contents of one or more nucleotides. One of the reasons that cause this change is due to the errors in the DNA replication or recombination processes [13]. In general, there are three types of mutations:

1) *Base substitution*: occurs when the content of one or more bases is replaced with new content. The replacement process can be either transitional or transversional. Transitional replacement appears when a purine is replaced with another purine or when pyrimidine is replaced with another pyrimidine.

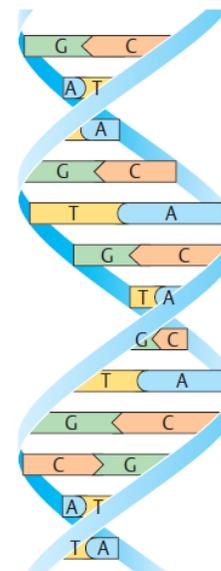


Fig. 2. DNA Double Helix.

TABLE I. THE GENETIC CODE [13]

		Second position									
		T		C		A		G			
		Code	Amino	Code	Amino	Code	Amino	Code	Amino		
First Position	T	TTT	phe	TCT	ser	TAT	tyr	TGT	cys	T	Third position
		TTC		TCC		TAC		TGC		C	
		TTA	TCA	TAA		STOP	TGA	STOP	A		
		TTG	TCG	TAG		STOP	TGG	trp	G		
	C	CTT	leu	CCT	pro	CAT	his	CGT	arg	T	
		CTC		CCC		CAC		CGC		C	
		CTA		CCA		CAA	CGA	A			
		CTG		CCG		CAG	CGG	G			
	A	ATT	ile	ACT	thr	AAT	asn	AGT	ser	T	
		ATC		ACC		AAC		AGC		C	
		ATA		ACA		AAA	lys	AGA	arg	A	
		ATG	ACG	AAG		AGG		G			
	G	GTT	val	GCT	ala	GAT	asp	GGT	gly	T	
		GTC		GCC		GAC		GGC		C	
		GTA		GCA		GAA	glu	GGA		A	
		GTG		GCG		GAG		GGG		G	

On the other hand, transversal replacement appears when a purine is replaced with a pyrimidine and vice versa. Base substitution mutations lead to different kinds of situations. For instance, when replacement occurs in the third location of a codon, there is a high probability that the amino acid is still the same. This kind of mutation is called a silent mutation. Another case arises when the replacement of bases converts an amino acid to a new one. This is called missense mutation and can be either conservative or non-conservative. In conservative mutation, the new amino acid has a similar structure and working mechanism compared to the old one. Consequently, the functionality of the protein is maintained regardless of the change in one of constructing amino acids. In non-conservative mutations, the new amino acid differs greatly compared with the old one. This will lead to altering the functionality of the whole protein. The last case of base substitution mutations appears when the replacement leads to one of the three-stop signals. This is called a nonsense mutation, which will terminate the sequence of amino acids building the protein and spoil its functionality.

2) *Base deletion*: occurs when one or more bases are omitted from the DNA sequence. Deleting one or more bases will cause a frameshift to the whole DNA sequence and make it non-functional. Deleting three or more bases may or may not affect the function of the protein.

3) *Base insertion*: occurs when one or more bases are added to the DNA sequence. Similar to the deletion case, this may have a negative effect on the biological function of the DNA sequence.

Studying and understanding the different types of mutations is essential to utilize them for data hiding purposes. Silent and conservative mutations types can be used to preserve functionality and produce a blind DNA-based steganography

algorithm. Finally, researchers in the field of DNA computing need DNA sequences for testing the performance of their proposed algorithms and comparing results. Fortunately, there are over 163 million DNA sequences that can be freely downloaded from different websites. Two of the most useful websites are the National Center for Biotechnology Information (NCBI) and the European Bioinformatics Institute (EBI) [15, 16].

### III. SECURITY ANALYSIS

This section illustrates some of the most important methods and crucial factors used in the development process of the DNA-based steganography algorithms. It also includes the parameters used to evaluate the performance of these algorithms.

1) *Data encoding*: to hide a secret message of any formatting type in a DNA sequence, elements of this message need to be encoded into genetic letters. One method to achieve this task is to use a lookup table to encode every character of the message to several genetic letters [17]. This technique suffers from two main defects. Firstly, the table is fairly static and fixed. Once it is revealed by an intruder, the whole steganography algorithm is compromised. The second issue is lookup tables used by many researchers to encode only alphabetic and numerical characters [18]. Special characters are ignored due to insufficient codons number. Another data encoding method is using a binary coding rule (BCR) table as shown in Table II.

In this case, the characters of the message are converted to binary form based on their ASCII code. Then, every two bits are assigned to a genetic letter [19]. An improved N-bits BCR has been suggested to increase characters encoding probability [20].

TABLE II. 2-BITS BINARY CODING RULE

DNA nucleotide	Binary form
A	00
C	01
G	10
T	11

2) *Hiding capacity*: denotes the total amount of data DNA sequence can tolerate. It is usually measured by the number of bits per nucleotide (BPN). A higher data capacity is obtained with a higher (BPN) value [23].

3) *Security key*: a very critical element in any crypto-stego system. Different factors have a direct effect on the used key or keys. For example, the purpose of using the key whether it is for encrypting or concealing the message, the type of the key whether it is a symmetric or asymmetric key, whether the key is randomly generated or created with a specific method, the size of the key, and the possibility of encrypting the key and merging it with the hidden data [22].

4) *Data encryption*: before concealing the secret message in the covering medium, it is preferred to encrypt it to add another layer of security to the algorithm. Many ciphering techniques have been used in the field of DNA-based steganography like DES, RSA, Vigenere, AES, and Playfair. Selecting and implementing the suitable encryption method is crucial since it has a direct effect on the other security parameters like the used key, hiding capacity, and cracking probability [21].

5) *Hiding method*: denotes the way characters of the secret message are embedded in the reference DNA sequence. Authors in [19] established three possible methods adopted by the majority of researchers afterward. Chunks of the secret message can be either inserted in different locations of the DNA sequence, added before the longest complimentary rule, or substituted with characters from the original sequence. These methods are vastly elaborated in the next section.

6) *Double layer embedding*: In many literature manuscripts, researchers suggest hiding the secret message in two mediums instead of one to offer higher security. Besides DNA sequence, a secret message can be concealed in an image [29], audio [30], or microdot [31].

7) *Cracking probability*: A measurement of the success probability of a brute force attack to break the proposed security algorithm. Some of the elements that have a direct effect on the cracking probability are the total number of possibly used DNA sequences, the number and the size of segments of the DNA reference sequence and the secret message, and the way of using a binary coding rule with a lookup table [2].

8) *Payload*: is the amount of extra data added to the DNA sequence due to the implementation of the DNA steganography algorithm. The best scenario occurs when the payload equals zero [24].

9) *Modification rate*: denotes the ratio of change in the fake DNA sequence compared to the original one. A high modification rate may spoil the protein's operations in the DNA sequence [24].

10) *Random variable*: In some of the developed steganography algorithms, researchers add one or more random variables in the data encryption and hiding processes. The reason behind that is making the task of cracking the algorithm even harder for an intruder. Some examples of random variables are using a random number of segments generation for insertion method [19, 25], random locations generation [26], random key generation [27], and random sequence generator [28].

11) *Blindness*: the algorithm is considered blind when there is no need to send the original DNA sequence used by the sender to the receiver. Generally, less amount of information used in the transmission process will improve the effectiveness of the applied method [32].

12) *Preserving functionality*: Codons are arranged in the DNA sequence in a specific order to form proteins. Every protein is generated to perform a unique biological function. One of the challenging goals in the field of DNA-based steganography is preserving this function after implementing the proposed data hiding algorithm [14].

#### IV. DNA-BASED STEGANOGRAPHY TECHNIQUES

From the beginning of the new millennium, many DNA-based steganography algorithms have been proposed. Each one of them follows a specific technique for data embedding in the DNA sequence. This section illustrates these classical approaches, describes their issues, and explains how these issues affect the development of recently proposed DNA-based steganography algorithms.

##### A. Insertion-Based Techniques

The Insertion-based technique is one of the first methods to hide a message in a DNA sequence. It is performed by inserting the data of the embedded message in one or more different locations of the DNA reference sequence. In [19], both the DNA sequence and the embedded message are divided into a random number of segments. Then, each segment of the message will be inserted before a segment of the medium. It is difficult for an intruder to deduce the number of segments or packets per message and the amount of data per packet [27]. An additional layer of protection can be added by encrypting the secret message with a solid encryption algorithm. For example, data encrypted with modified Playfair [25], AES-128 [31], RSA [33], or RC4 encryption algorithms [34] before data embedding stage. In [35], two images are concealed in another image without distortion based on grayscale and Least Significant Bit (LSB) insertion of the DNA form of the secret information. An improved insertion technique is proposed by [36] with the use of two keys. The first key is XORed with every 8 bits of the secret message, while the other key is responsible for dividing the DNA sequence into segments. The binary bits of the cipher are inserted at the beginning of each segment. This technique has a strong cracking probability and high security but the payload is

not zero. A powerful algorithm with complex data encryption and embedding techniques is presented in [32]. In the encryption phase, a Playfair cipher with a randomly shuffled 8\*8 matrix is used to gain an additional layer of security via codons replacement and circular rotation of rows and columns processes. In the embedding phase, both the message and the cover DNA sequence are spliced into a random number of segments. Then, these segments are concatenated to generate the fake DNA sequence. The main drawback of the insertion-based technique is the increasing size of the DNA reference sequence. This is a clear indication that data has been added to the carrier medium and will attract the attention of attackers. Also, algorithms adopt insertion technique are usually not blind. On the positive side, insertion algorithms have a low cracking probability. Furthermore, one or multiple random variables are used in the encryption or embedding stages. This will make breaking the algorithm even harder for intruders.

### B. Substitution-Based Techniques

In substitution-based technique, nucleotides from the DNA sequence are replaced with secret message characters. The replacement method can be applied using a lookup table [17] or at specific locations like the LSBs [37]. In [38], a histogram of frequently appeared values in the selected DNA reference is created. Then, the message is hidden in locations marks with zero. A novel technique based on Chebyshev chaotic maps is developed by [39]. The plain text is encoded into a DNA sequence and encrypted to another sequence via a Chebyshev map. The result is circularly shifted for a finite number of times and embedded through character by character substitution in a word document. Excessive random substitution of bases inside the DNA sequence will ruin the function of the protein. The approach in [40] took advantage of the ambiguity feature to solve this issue. Only the Least significant bases (LSB) locations of each codon are used as hiding locations of the secret message. This technique is blind and minimized the modification rate by a third. Enhanced algorithms are offered in [20] and [41] based on a 4-bits coding rule with data encryption using Playfair and AES. Another substitution-based technique is suggested by [42]. A codon dictionary table is manually generated. Then, every 6 bits of the message will be replaced with a codon. These codons are embedded in different intervals of the DNA reference. Several elements were used in [43] to provide dual cover steganography techniques based on an image and DNA. These elements are a 2D logistic map, three secret keys, and encrypt a secret message using RC4 and hiding it in LSB locations. Although offering high-security measures with double hiding layers, this technique demands much data for the hiding and extraction processes. Another double-layered steganography technique was proposed in [30]. After encrypting the message using RC4 and hiding it in the DNA sequence, a randomized LSB replacement method is used to embed the result in an audio file. Preserving the functionality of the DNA sequence can be achieved by embedding the secret message in non-coding regions of the sequence. This was accomplished in [44] by first encrypting the message using XOR and pseudo-random bit generator (PRBG) sequence. Then, the encoded message is segmented into pieces and replaced with nucleotides in sectors from non-coding regions. Another advantage of this technique is its ability to detect and recover deleted or changed nucleotides

affected by mutations. Also, it has a decent capacity ranged from 1.2 to 2 BPN. An enhanced 4\*4 Playfair cipher is developed in [21] instead of the 5\*5 usually used grid. After encrypting the plain text with it, the hiding technique developed in [45] is used to improve hiding capacity by 25%. A double-layered hiding algorithm based on a color image as a cover is presented in [29]. The secret data is divided into three parts using the XOR operator, and each one of them is concealed in the color of the cover image. This is a highly reliable approach though it is time-consuming during the extraction phase. Two DNA strands are used in [46] to increase hiding capacity. A substitution table is used for the embedding purpose and the message is sent to the receiver via a microdot. In [18], a combination of image and DNA-based steganography is applied. A secret image is embedded in another image – both with the same pixel size – by converting their pixel values to DNA triplet based on a lookup table. Then, these triplets are converted to binary form and XORed to get the stego image. This method offers a higher security level than other techniques like LSB but with a lower hiding capacity. The prominent benefit of the substitution-based technique is implementing the embedding process without any expansion in the size of the fake DNA sequence. On the other hand, a high modification rate applied to the DNA reference sequence will ruin its biological functionality. Besides that, by restricting the replacement locations to a limited number - as in the LSBs-based methods -, will highly decrease the data hiding capacity. Trying to increase hiding capacity may lead to lowering the performance of other parameters like modification rate or cracking probability [46].

### C. Complementary Rule-based Techniques

In this method, a complementary rule is initially considered and the data is inserted before the longest complementary substring in the reference DNA sequence. The complementary rule is set in such a way where  $x \neq c(x) \neq c(c(x)) \neq c(c(c(x)))$  and  $x$  is one of the four possible genetic letters [47]. For instance, if the following complementary rule is applied: ((AC) (CG) (GT) (TA)), the complementary string of AATGC will be CCATG [19]. In [48], each pair of encrypted secret message will be assigned to a matching index in the DNA reference sequence. Then, a list of these indices will be sent to the receiver. The hiding process can be implemented using a random generator function based on the size of the secret message [26]. Another method encoded text to DNA form and hide the result in grids of an image based on LSB and MSB [49]. A similar technique is suggested by [50] where the input message is encoded to DNA form and embedded in a randomly chosen frame of a video. A mathematical approach of data encryption and hiding is proposed in [28]. Two secret keys are generated using Elliptic Curve Cryptography (ECC) and Gaussian Kernel Function (GKF). The secret message is encrypted using these two keys, followed by DES. Characters of the encrypted message are embedded in locations from the new DNA sequence. While this technique is the simplest compared to other techniques, it is not blind and increases the message size. In some cases when a random DNA sequence is used, it is required to send the complementary rule to the receiver [51]. Security mainly depends on the selected DNA reference [52]. Also, it is not

always feasible to find the DNA sequence of all the matching elements with the secret message.

#### D. Hybrid Techniques

Many endeavors aimed to combine the advantages of the three techniques in the previous sections and nullify or at least mitigate their weaknesses by proposing hybridization between them. For example, authors in [45] used a substitution method with a complementary rule. A multi-level secured method that adopted a similar approach has been suggested in [53]. Data are firstly using Playfair and concealed in a randomly generated DNA sequence. Then, the DNA sequence is embedded in an audio file. An imperceptible double-layered algorithm based on image and DNA is proposed in [54]. Using the only component of the cover image – like blue color – to hide the DNA message is the main weakness in this algorithm. Generally, these algorithms hide the message with zero expansion and payload. Still, like their predecessors, they paid no attention to preserving the biological features of the reference DNA sequence. Also, they are un-blind algorithms. Authors in [19] employed a data hiding algorithm based on a combination of insertion and complementary rule methods. This algorithm is un-blind, expands the size of the DNA sequence, and ignores its biological functionality. In [55] the secret message is firstly encrypted with an improved Playfair cipher. After that, the encoded message is concealed via a novel substitution method in a cover DNA sequence and the result is inserted in another sequence. An improved version of this method with enhanced Generic complementary base substitution (GCBS) is recently presented in [61]. Using a DNA-based XOR cipher with a randomly generated key formulated from the cover medium is suggested. This proves to offer better results in terms of lower cracking probability and higher BPN.

### V. ANALYSIS OF MODERN APPROACHES

Classical or traditional methods of implementing DNA steganography discussed in the previous section used the traditional protection methods in the field of data security to achieve the desired task. In the last few years, a new generation of algorithms has been evolved. The new trend aims either to exploit the biological attributes of DNA or borrow a suitable technique from another field of computer science. The reason behind that is offering better solutions and performance compared to the old generation methods. In this section, a critical analysis will be initiated to the recently suggested techniques by describing their working mechanism, stating their pros and cons, and points to the possible ways to improve upon them.

#### A. Exploiting Biological Features

One of the most interesting features of DNA is the condition called single nucleotide polymorphism (SNP). In this case, a particular nucleotide in the genome sequence differs between members of the same species. As shown in Fig. 3, the two DNA sequences have different content in a specific position.

Researchers keenly noticed that regions including SNPs have the potential to hide a secret message. Attackers cannot distinguish between changes that occur because of data hiding and changes that occur because of SNPs. In [56], the author proposed a DNA steganography algorithm based on hiding a secret message in SNPs locations. Firstly, SNPs positions in the selected DNA sequence are assigned. Then, every character in the secret message is converted to three letters based on the DNA encoding table. For example, the letter (H) is encrypted to (TAC) and stored in three consecutive SNPs positions as shown in Fig. 4.

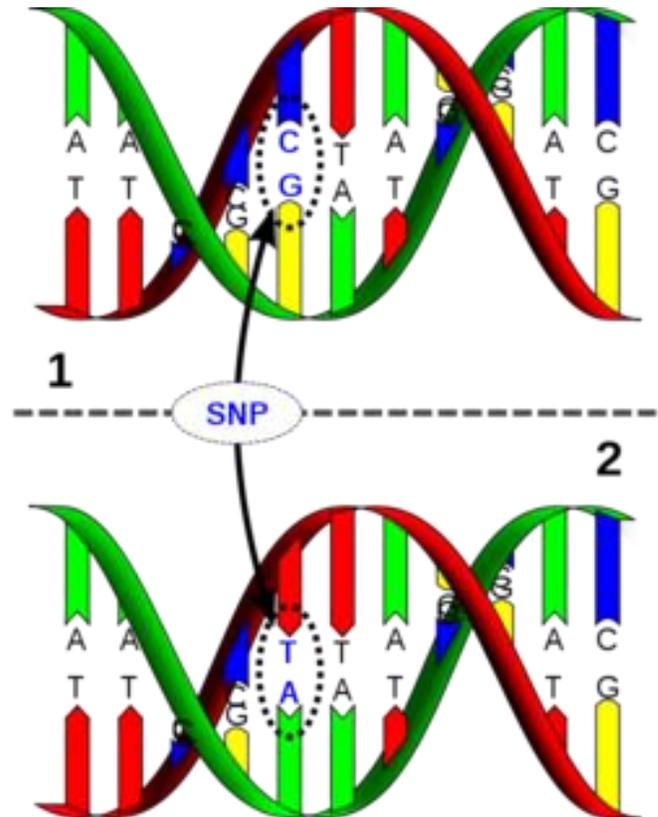


Fig. 3. Single Nucleotide Polymorphism [56].

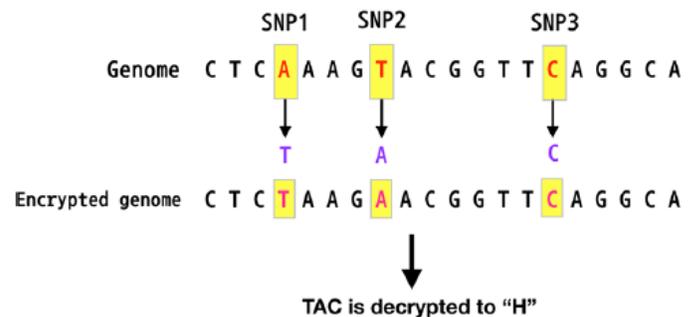


Fig. 4. Encrypting and Hiding a Character [56].

One of the limitations of the proposed algorithm noticed in the DNA encoding table, it has only alphabets and numbers. While SNPs offer good hiding locations in the encrypted message, they suffer from an obvious defect. The appearance probability of SNPs in a single DNA sequence is only 6%. Hence, the hiding capacity of the sequence is severely decreased. A suitable data compression technique can be used to increase the number of encrypted bits per location.

Another biological factor used in the process of data hiding is mutations. Although some types of mutations have negative effects like corrupting or terminating the protein, other types do not harm the protein. Silent and conservative mutations change nucleotides or amino acids in the protein and maintain its functionality. The approach in [23] took advantage of these types of mutations to develop a crypto-stego system with high hiding capacity and excellent security measures. This algorithm has two main stages on both sender and receiver sides. Firstly, the secret message is encrypted using an enhanced 8\*8 Playfair cipher. This new encryption technique overcomes the weakness that existed in the 5\*5 Playfair cipher where only alphabets are encrypted. Using Playfair cipher is justified since no extra information is required by the receiver in the decryption process besides lowering the cracking probability. In the second phase, LSBBase is used to hide bits of the secret message. The challenge is to hide two bits per nucleotide, where every amino acid will handle four possible substitutions. Via silent mutation, this is possible in all amino acids that can be represented with four codons or more. For instance, Alanine has four codons: GCA, GCC, GCG, and CGT. The LSBBase of these four codons can hide two bits – 00, 01, 10, and 11 – without issue. Unfortunately, not all amino acids can satisfy the rule of being represented with four codons or more. For example, Phenylalanine is an amino acid that can be represented with only two codons, TTT and TTC. These two codons can satisfy only half of the four possible values. To solve these issues, the authors suggested using the feature of conservative mutation. Here, an amino acid will replace another that shares a similar structure and functions. Amino acids that have less than four codons will be used interchangeably without disturbing the functionality of the protein. In the example mentioned above, Tyrosine will be used when Phenylalanine fails to satisfy the embedding requirements. One of the main contributions of the proposed algorithm is its ability to exploit concealing data in LSBBase locations efficiently with a high hiding capacity of 2 BPN. Another important contribution is hiding the message in a non-sequential and non-order pattern along the DNA sequence. The cracking probability is low due to the various factors required to get the secret message. The intruder must not only know which DNA reference or BCR are used, but he/she must also know how the Playfair matrix is constructed, figure out the data hiding locations, and the adopted substitution rule. The drawback of the suggested algorithm is the need to send the random number of seeds used to generate BCR to the receiver. Also, using a fixed substitution table where the same

unsatisfied amino acids always replace each other for every transition session is considered a weak point.

Maintaining the biological features of DNA after embedding the encrypted data in it is a really difficult task to achieve. Any modification or payload applied to the DNA sequence may lead to losing the functionality of this sequence. Although it seems leaving the DNA sequence intact is the only way to succeed in preserving its original signature, there are many other interesting methods to do that. In [57], the main objective is preserving the biological functionality of the DNA sequence after the embedding process. This is accomplished by exploiting a DNA feature, ambiguity, mentioned in section two. Every amino acid is composed of three nucleotides or a codon. Ambiguity arises when more than one codon represents an amino acid. As demonstrated in Table III, there are 20 different types of amino acids. Every amino acid can be represented with one to six codons. The table also includes the number of ambiguities for each amino acid and the number of required bits to represent them. Before initiating the data hiding operation, a preprocessing is deployed. Based on the content of Table III, the whole carrier DNA sequence is converted to amino acid codons. Every bit in the secret key is linked to its corresponding character of the DNA sequence in a specific way. Ones denote amino acids locations where hiding characters is possible, while zeros denote to do not care amino acid locations. In the data hiding process, the codon representing the secret character will substitute a codon in the carrier medium. This does not affect the DNA sequence functionality since both codons belong to the same amino acid. Consequently, the purpose of this work of applying the steganography process without disturbing the biological features of the medium is achieved. Also, the proposed algorithm provides low penetration probability versus different types of attacks like stego-only attack, known cover attack, and known message attack. The weaknesses of this algorithm are adding a new bit for hiding data in some cases which increases the payload. Besides that, the performance of this algorithm depends on the content of the secret message. Every amino acid used in the hiding process has its own effect on parameters like hiding capacity, BPN, and payload. This drawback can be alleviated by using only amino acids that guarantee the best performance.

### B. The Field of Networking

For the mutation/modification detection technique, the author in [56] borrowed a concept used in the field of networking to detect errors in data transmission. A block checksum method is implemented by assigning a number to each nucleotide in the encrypted sequence where ( $A = 0 / T = 1 / G = 2 / C = 3$ ). Then, the summation of nine consecutive nucleotides is divided on 4. The remainder of the division operation will be converted to the equivalent DNA value and attached to the end of the sequence as the tenth location. This operation is repeated for all components of the encrypted message. As shown in Fig. 5, three cases are presented.

TABLE III. NUMBER OF CODONS PER AMINO ACID [57]

Amino Ambiguity			A	B	C	D	E	F	G	H	I	K	L	M	N	P	Q	R	S	T	V	W	Y
			A	B	C	D	E	F	G	H	I	K	L	M	N	P	Q	R	S	T	V	W	Y
A	0	00	G C U	U A A	U G U	G A U	G A A	U U U	G G U	C A U	A U U	A A A	U U A	A U G	A A U	C C U	C A A	C G U	U C U	A C U	G U U	U G G	U A U
A	1	00	G C C	U A G	U G C	G A C	G A G	U U C	G G C	C A C	A U C	A A G	U U G		A A C	C C C	C A G	C G C	U C C	A C C	G U C		U A C
A	2	01	G C A	U G A					G G A		A U A		C U U			C C A		C G A	U C A	A C A	G U A		
A	3	01	G C G						G G G				C U C			C C G		C G G	U C G	A C G	G U G		
A	4	10											C U A					A G A	A G U				
A	5	10											C U G					A G G	A G C				
Number of ambiguities (X)			4	3	2	2	2	2	4	2	3	2	6	1	2	4	2	6	6	4	4	1	2
Number of bits (Y)			2	2	1	1	1	1	2	1	2	1	3	1	1	2	1	3	3	2	2	1	1

In the first case, no mutation has appeared in the encrypted sequence. This is confirmed by matching the last nucleotide with the result of the checksum method. In the second case, a mutation occurs in the first location of the sequence. This is immediately noticed since the last nucleotide in the sequence differs from the resulted sum check calculation. While the proposed mutation detection method works perfectly in the first and second cases, it sometimes flawed as presented in case three. Here, both that attached nucleotide and the result of the checksum are the same. Although the receiver thinks that the sequence has been correctly delivered, it is actually modified in different locations. The proposed mutation detection technique can work properly in the case of single location mutations. Alas, it may stumble in the case of other types of mutations cases with multiple locations frameshifting or swapped nucleotides. An enhanced modification detection technique is required to cover cases like transmission errors and deliberate change by an attacker. This can be accomplished by using two DNA sequences, one for the data hiding and the other for the modification detection. All SNPs locations of the first will be used solely for data hiding while locations in the second sequence are only used to hold data verification values. This will increase the number of locations dedicated for concealing purposes which improve hiding capacity and will make it easier to detect different kinds of changes in the carrier sequence.

C. The Field of Data Structure

Another field in computer science correlated with the field of DNA steganography to increase hiding capacity is data structure. In [58], a framework for hiding based on a balanced tree is suggested. This is accomplished by converting a randomly selected DNA sequence into a balanced tree where every node holds a single nucleotide. The height of the tree depends on the size of the message to be sent. Even levels have at most two children while odd levels have at most three. The

traversing process is done by Depth First Search (DPS) approach. The encryption process starts by converting every character in the message to four nucleotides.

Then, characters in the leaf nodes will be replaced in reverse order with letters of the encrypted message. The last stage is obtaining the fake DNA sequence by assembling the letters based on the references of the nodes in the tree. For example, encrypting letters (ABC) will start by converting them to ASCII form to become (01000001, 01000010, and 01000011). Then, it is converted to (CAAC, CAAG, and CAAT). If the selected DNA sequence to hide the message inside is (ACGGTTCCAATGCCTAAGCTA), it is converted to a balanced tree as shown in Fig. 6.

Cases	Encrypted message	(A = 0 / T = 1 / G = 2 / C = 3)
Case 1	AGT GCC TAT T	021 233 101 13 MOD 4 = 1 » T
Case 2	GGT GCC TAT T	221 233 101 15 MOD 4 = 3 » C
Case 3	GGT GCC TTG T	221 233 112 17 MOD 4 = 1 » T

Fig. 5. Examples of Mutation Detection Method.

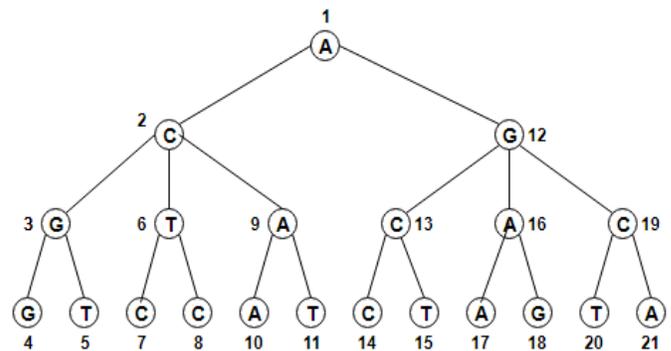


Fig. 6. Balanced tree for Random DNA Sequence [58].

After that, the encrypted message is integrated into the leaf nodes of the tree as shown in Fig. 7. The faked DNA sequence obtained from the balanced tree is (ACGCATATACAGCAGACACAC). The proposed framework offers high hiding capacity and accepts any type of input. Also, hiding spots are scattered all over the reference sequence in non-sequential manner. Nevertheless, the algorithm is pattern-dependent. Once the pattern is revealed, the secret message is compromised. An interesting idea to improve upon this work is using a link list for holding the contents of the DNA sequence instead of the balance tree. Linked lists have higher flexibility, complexity, and more fluent transition from an element to another than a tree.

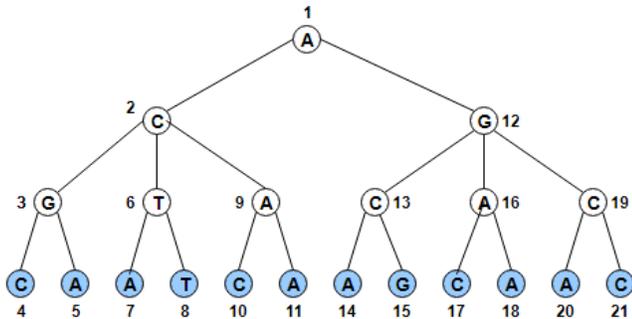


Fig. 7. Balanced Tree after Message Integration [58].

#### D. The Field of Artificial Intelligence

The field of artificial intelligence can also be used to develop a robust DNA steganography algorithm. The authors in [59] used backpropagation artificial neural network (ANN) to achieve high hiding capacity, low cracking probability, and zero payloads. In the embedding process, the inputs are the DNA reference with the secret message and the output is a set of weights from the neural network. At the beginning, every character in the secret message is converted to the equivalent ASCII binary value. Then, this value is converted to the equivalent DNA letter based on the DNA binary coding rule. Each letter in the DNA message will be assigned to a location in the DNA reference. ANN will be used to get a list of binary locations and the weights of the training phase will be stored in a set. This set and the chosen DNA reference are sent to the receiver. Fig. 8 represents a process diagram to illustrate the AI-based data encryption and data hiding processes.

At the receiver side, the extraction process is executed by implementing the steps of the embedding process in reverse order. Firstly, both the DNA sequence and the weights received from the sender are applied to the ANN. The result is a list of positions denoting the hiding locations. A set is constructed of DNA letters assembled from these locations. Based on the binary coding rule table, DNA letters are converted to binary form. The secret message is obtained by converting every 8-bits to a character using the ASCII code. Fig. 9 represents a process diagram to illustrate the data decryption and message extraction.

The proposed algorithm shows good results like 2 BPNs and zero payloads. It also preserves the biological functionality of the DNA sequence because no modification has been done to it. The weak points of this algorithm are the need to send the

original DNA sequence to the receiver. Hence, it is not a blind algorithm. Also, the main defect of using the ANN is the high consumed time, especially in the training phase. This time can be reduced by using only a segment of the DNA sequence as the input to the ANN instead of using the whole sequence. Besides that, it is really interesting to investigate using swarm intelligence techniques like particle swarm optimization (PSO), bee colony, and ant colony to create a hiding locations pattern. This may outperform ANN in terms of complexity and time consumption.

To have a comprehensive look over the classical and modern techniques discussed in this paper, Table IV states the security parameters of these approaches. It can be concluded from this table that the substitution method is more suitable with small size secret messages. It is used when preserving features like blindness, zero payloads, and sequence functionality are crucial. Besides that, the substitution method usually uses only specific locations in the cover medium like LSBase for hiding purposes. This restriction leads to using only long DNA sequences as a cover medium. This issue can be solved by reducing the size of the hidden message with a proper lossless compression method. On the other hand, the insertion method is used when large chunks of data need to be exchanged. It ignores features like blindness and preserving functionality to offer no threshold boundary for the amount of embedded data. Finally, Table V summarizes the modern algorithms in terms of their purpose, advantages and disadvantages, and possible ways to improve them.

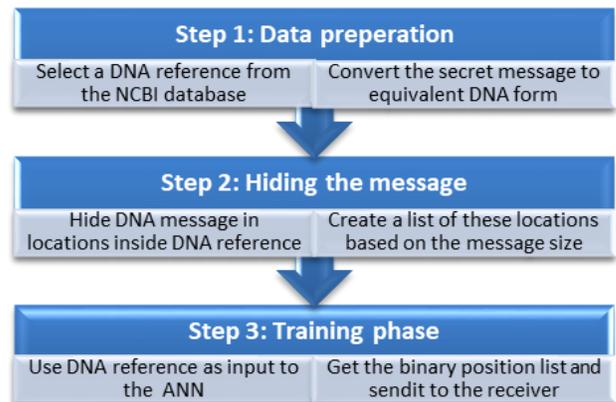


Fig. 8. Data Encryption and Embedding.

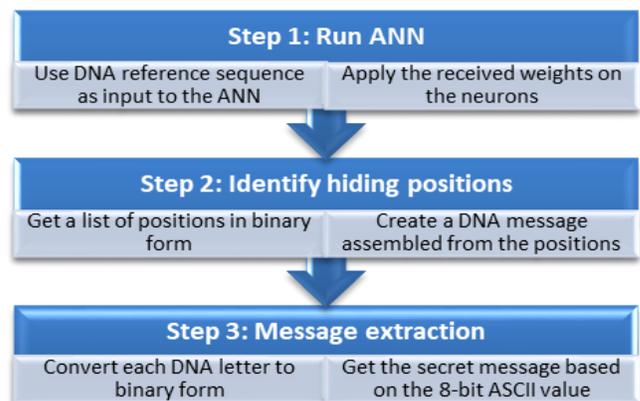


Fig. 9. Data Decryption and Extraction.

TABLE IV. SECURITY MEASUREMENTS OF RECENTLY PROPOSED METHODS

Author & Year	Method	Hiding Capacity	Key Type	Use Data Encryption	Number of Layers	Payload	Modification Rate	Use Random Variable	Blindness	Preserving Functionality
Khalifa et al. 2016 [55]	Insertion	High	Secret Key	Playfair	Single	Yes	High	Yes	Yes	No
Marwan et al. 2017 [46]	Substitution	High	Secret Key	Playfair or Vigenere	Single	No	High	Yes	No	Yes
Malathi et al. 2017 [36]	Insertion	High	Secret Key	No	Single	Yes	Low	Yes	No	No
Sajisha et al. 2017 [41]	Substitution	Low	Secret Key	AES	Single	No	Low	Yes	Yes	Yes
Vijayakumar et al. 2018 [18]	Substitution	Low	No	No	Double (Image)	---	---	No	No	---
Hamed et al. 2018 [23]	Substitution	High	No	Playfair	Single	No	Low	Yes	Yes	Yes
Saha et al. 2019 [58]	Substitution	High	No	No	Single	No	High	No	Yes	No
Sabry et al. 2019 [57]	Substitution	High	Secret Key	No	Single	Yes	High	Yes	Yes	Yes
Mohammed et al. 2019 [59]	Position based	High	Secret Key	No	Single	No	No	No	No	Yes
Dokuyn Na et al. 2020 [56]	Substitution	Low	No	No	Single	No	Low	No	Yes	Yes

TABLE V. SUMMARY OF THE REVIEWED MODERN APPROACHES

Author & Year	Fields	Aim of the paper	Pros	Cons	Suggestions
Hamed et al. 2018 [23]	Biology	Exploit the DNA conservative mutations to develop secured, high capacity, preserved algorithm.	Using advanced Playfair cipher. Very low cracking probability. Scattered hiding locations. High capacity. Preserve biological features.	Using fixed substitution table. BCR table is required to be send to the receiver every transmission session.	Use dynamic and randomly generated substitution table. Integrate the BCR table in the DNA sequence.
Saha et al. 2019 [58]	Data structure	Increase hiding capacity by embedding encrypted characters of the secret message in the leafs of a balanced tree.	Over 50% hiding capacity. Scattered hiding locations. Blind. Zero payload.	Pattern dependent technique. Do not Preserve biological features. High modification rate.	Use more than one nucleotide in leafs nodes will increase hiding capacity. Use a linked list instead of a tree may offer better results.
Mohammed et al. 2019 [59]	Artificial intelligence	Develop a robust DNA steganography algorithm by using ANN.	Preserve biological features. Zero payload. Low cracking probability.	Not blind. High execution time. Sequential hiding pattern.	Lower consumed time in training by reducing the range of ANN's inputs. Use swarm optimization techniques to create a hiding pattern.
Sabry et al. 2019 [57]	Biology	Maintaining DNA signature by exploiting ambiguity feature and hiding data in redundant codons of amino acids.	Preserve biological features. Very low penetration probability versus different types of attacks.	Adding new bit in some cases is required during embedding process. The performance of the algorithm depends on the contents of the secret message.	Hiding data in only locations related to amino acids guarantee best performance.
Na 2020 [56]	Biology Networking	Use SNPs in DNA as hiding locations. Developing a mutation detection method.	SNPs provide good noise cover. Single mutation detection. Zero payload. Blind algorithm. Preserve functionality.	Low hiding capacity. Deal only with alphabets and numbers. Block checksum fails in addition, deletion and swapping cases.	Compress the data before hiding process. Enhance the performance of the checksum technique by using a dedicated DNA sequence for it.

## VI. CONCLUSION AND RECOMMENDATION

DNA has proved it can be the optimal medium for data hiding and transmission. It gives promising solutions to issues that arise when other covering mediums are used. In the last twenty years, many DNA steganography algorithms have been proposed. Despite the wide range of ideas offered by steganography algorithms, there are many gaps and unresolved issues in this field. Some of them are:

- An improved data encoding method is required to convert the binary form of the secret message to genetic letters. The required number of genetic letters to hide the binary form of the secret message can be decreased using the lossless compression method. This will increase the availability of hiding locations and the value of BPN.
- One of the DNA-based cryptography techniques is using a dictionary or a lookup table to link characters of the secret message to a specific codon. Lookup tables have a limited capacity of only 64 locations if codons are used. This is sufficient to encode alphabets and numbers while special characters are ignored. Besides that, lookup tables are static, and using the same table in every data transition session is quite risky. If a third party revealed the contents of the lookup table, the whole steganography algorithm is compromised. One possible solution to this issue is using a dynamic lookup table randomly generated at each transition session. The sender will integrate the new table with the concealed secret message.
- There is a trade-off between providing high hiding capacity and preserving biological features of the DNA sequence. Using all nucleotides to hide data will ruin the functionality of the protein while exploiting biological characteristics like ambiguity or mutations will significantly decrease hiding capacity. Therefore, there is an obvious need for a technique that enables us to hide the maximum amount of data in LSB locations in codons.
- The majority of developed DNA-based steganography algorithms used adjacent or sequential locations in the DNA sequence to hide characters of the secret message. Also, the hiding process is applied to these characters with the same order of their locations in the secret message. Alternatively, scattering hiding locations all over the sequence will make deducing the secret message from the covering medium even harder for a third party. One of the applied techniques in the literature to achieve such a task is using a balanced tree to distribute the message characters all over the sequence. This approach is fairly static and adopting another data structure such as the linked list will offer a more flexible transition from one character to another.
- One of the modern trends in the field of DNA-based steganography is adopting a predefined location-based hiding structure. Both the sender and the receiver agree on a specific method like a neural network with

backpropagation and use its structure in the encryption and decryption phases. The selected method must meet several security and performance measures. For example, minimum deployment speed, variations of hiding locations at each run, and preserving the content of this secret message even if the hiding structure is predicted by an attacker. Identifying the optimal hiding structure method is still an open issue in this field.

- The transmission of the fake DNA sequence from the source to a destination over an untrusted channel may encounter different types of obstacles. Some of these obstacles are mutations, transition errors, and message modification by a third party. To authenticate the integrity of the obtained secret message, a message authentication technique is required. Previously proposed methods are limited to deal with unique cases like single mutations. A comprehensive solution to this issue is using a dedicated DNA sequence to guarantee the integrity of the fake DNA sequence. This will offer more locations for both data hiding and data checking.

All in all, the combination of exploiting biological attributes of the DNA with utilizing the different techniques borrowed from various fields of computer science proved to be fruitful. It offers promising results and solutions for the existing issues in the field of DNA-based steganography. These recently suggested novel approaches are expected to accelerate the movement towards consolidating the rank of DNA as one of the main concealing mediums. Also, they sustain using DNA-based steganography methods in real-life applications.

## REFERENCES

- [1] S. Namasudra, "Cloud computing: A new era," *Journal of Fundamental and Applied Sciences*, 10 (2), pp. 113–135, 2018.
- [2] G. Hamed, M. Marey, S. El-Sayed, and F. Tolba, "DNA based steganography: Survey and analysis for parameters optimization," In *Intelligent Systems Reference Library*, Vol. 96, 2016.
- [3] R. Anusha, M. J. Dileep Kumar, V. S. Shetty, and N. Prajwal Hegde, "Symmetric Key Algorithm in Computer security: A Review," *Proceedings of the 4th International Conference on Electronics, Communication and Aerospace Technology, ICECA 2020*, pp. 765–769.
- [4] P. Chaudhury, S. Dhang, M. Roy, S. Deb, J. Saha, A. Mallik, et al., "ACAFP: Asymmetric key based cryptographic algorithm using four prime numbers to secure message communication. A review on RSA algorithm," *8th Industrial Automation and Electromechanical Engineering Conference, IEMECON, 2017*, pp. 332–337.
- [5] S. S. Baawi, M. R. Mokhtar, and R. Sulaiman, "New text steganography technique based on a set of two-letter words," *Journal of Theoretical and Applied Information Technology*, 95 (22), pp. 6247–6255, 2017.
- [6] M. A. Majeed, and R. Sulaiman, "An improved LSB image steganography technique using bit-inverse in 24 bit colour image," *Journal of Theoretical and Applied Information Technology*, 80 (2), pp. 342–348, 2015.
- [7] A. H. Ali, L. E. George, A. A. Zaidan, and M. R. Mokhtar, "High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain," *Multimedia Tools and Applications*, 77 (23), pp. 31487–31516, 2018.
- [8] S. Kamil, M. A. Authors, S. N. H. S. Abdullah, and Z. Ahmad, "Lightweight and optimized multi-layer data hiding using video steganography paper" *International Journal of Advanced Computer Science and Applications*, 9 (12), pp. 256–262, 2018.
- [9] S. Kamil, M. Ayob, S. N. H. Sheikh Abdullah, and Z. Ahmad, "Optimized Data Hiding in Complemented or Non-Complemented Form in Video Steganography," *Proceedings of the 2018 Cyber Resilience Conference, CRC, 2018*, pp. 1–4.

- [10] M. S. Subhedar, and V. H. Mankar, "Current status and key issues in image steganography: A survey," *Computer Science Review*, 13–14(C), pp. 95–113, 2014.
- [11] C. T. Clelland, V. Risca, and C. Bancroft, "Hiding messages in DNA microdots" *Nature*, 399 (6736), pp. 533–534, 1999.
- [12] D. A. Zebari, H. Haron, and S. R. M. Zeebaree, "Security issues in DNA based on data hiding: A review," *International Journal of Applied Engineering Research*, 12 (24), pp. 15363–15377, 2017.
- [13] E. Passarge, "Color Atlas of Genetics," Fifth edition, Thieme, 2019.
- [14] J. Momand, and A. McCurdy, "Concepts in bioinformatics and genetics," Oxford University Press, 2017.
- [15] NCBI, [Online]. Available: <https://www.ncbi.nlm.nih.gov/genbank/statistics/>.
- [16] (European Bioinformatics Institute). Online website: <https://www.ebi.ac.uk>.
- [17] J.S. Taur, H.Y. Lin, H.L. Lee, and C.W. Tao, "Data hiding in DNA sequences based on table lookup substitution," *Int. J. Innov. Comput. Inf. Control* 8, pp. 6585–6598, 2012.
- [18] P. Vijayakumar, V. Vijayalakshmi, and R. Rajashree, "Increased level of security using DNA steganography," *International Journal of Advanced Intelligence Paradigms*, 10 (1–2), pp. 74–82, 2018.
- [19] H.J. Shiu, K.L. Ng, J.F. Fang, R.C. Lee, and C.H. Huang, "Data hiding methods based upon DNA sequences," *Inf. Sci.* 180, pp. 2196–2208, 2010.
- [20] G. Hamed, M. Marey, S.A. El-Sayed, and M. F. Tolba, "Hybrid technique for steganography-based on DNA with n-bits binary coding rule," *Proceedings of the 2015 7th International Conference of Soft Computing and Pattern Recognition, SoCPaR 2015*, pp. 95–102.
- [21] S. Marwan, A. Shawish, and K. Nagaty, "DNA-based cryptographic methods for data hiding in DNA media," *BioSystems*, 150, pp. 110–118, 2016.
- [22] W. Stallings, "Cryptography and network security principles and practice," 7<sup>th</sup> edition. Pearson. 2017.
- [23] G. Hamed, M. Marey, S. E. S. Amin, and M. F. Tolba, "Hybrid, randomized and high capacity conservative mutations DNA-based steganography for large sized data," *BioSystems*, 167, pp. 47–61, 2018.
- [24] O.A. Al-Harbi, W.E. Alahmadi, and A.O. Aljahdali, "Security analysis of DNA based steganography techniques" *SN Applied Sciences*, 2 (2), 2020.
- [25] A. Atito, A. Khalifa, and S. Z. Rida, "DNA-Based Data Encryption and Hiding Using Playfair and Insertion Techniques" *Journal of Communications and Computer Engineering*, 2 (3), pp. 44, 2011.
- [26] M. Torkaman, N. Kazazi, and A. Rouddini, "Innovative approach to improve hybrid cryptography by using DNA steganography," *International Journal of New Computer Architectures and Their Applications*, 2 (1), pp. 225–236, 2012.
- [27] S. Manna, S. Roy, P. Roy, and S. K. Bandyopadhyay, "Modified technique of insertion methods for data hiding using DNA sequences," *1st International Conference on Automation, Control, Energy and Systems - 2014, ACES 2014*, pp. 1–5.
- [28] E. I. Abd El-Latif, and M. I. Moussa, "Information hiding using artificial DNA sequences based on Gaussian kernel function," *Journal of Information and Optimization Sciences*, 40 (6), pp. 1181–1194, 2019.
- [29] T. Tuncer, and E. Avci, "A reversible data hiding algorithm based on probabilistic DNA-XOR secret sharing scheme for color images," *Displays*, 41, pp. 1–8, 2016.
- [30] R. M. Tank, , H. D. Vasava, and V. Agrawal, "DNA-based Audio Steganography," *An International Open Free Access, Peer Reviewed Research Journal*. Vol. 8, No. (1): pp. 43-48, 2015.
- [31] H. Chaudhary, and V. Bhatnagar, "Hybrid approach for secure communication of data using chemical DNA," *Proceedings of the 5th International Conference on Confluence 2014: The Next Generation Information Technology Summit*, pp. 967–971.
- [32] A. Khalifa, "A Blind DNA-Steganography Approach using Ciphering and Random Sequence Splicing," *10th International Conference on Information Science and Technology, ICIST 2020*, pp. 86–90.
- [33] M. Skariya, and M. Varghese, "Enhanced Double Layer Security using RSA over DNA based Data Encryption System," *International Journal of Computer Science & Engineering Technology (IJCSSET)*, 4 (06), pp. 746–750, 2013.
- [34] P. Das, and N. Kar, "A DNA based image steganography using 2D chaotic map," *2014 International Conference on Electronics and Communication Systems, ICECS 2014*.
- [35] S. Chakraborty, and S. Kumar Bandyopadhyay, "Data Hiding by Image Steganography Applying DNA Sequence Arithmetic," *International Journal of Advanced Information Science and Technology*, 231944 (44), 2015.
- [36] P. Malathi, , M. Manoj, , R. Manoj, , V. Raghavan, , & R. E. Vinodhini, "Highly Improved DNA Based Steganography," *Procedia Computer Science*, 115, pp. 651–659, 2017.
- [37] H. Mousa, K. Moustafa, W. Abdel-Wahed, and M. Hadhoud, "Data hiding based on contrast mapping using DNA medium," *International Arab Journal of Information Technology*, 8 (2), pp. 147–154, 2011.
- [38] Y. H. Huang, C. C. Chang, and C. Y. Wu, "A DNA-based data hiding technique with low modification rates," *Multimedia Tools and Applications*, 70 (3), pp. 1439–1451, 2014.
- [39] H. Liu, D. Lin, and A. Kadir, "A novel data hiding method based on deoxyribonucleic acid coding," *Computers and Electrical Engineering*, 39 (4), pp. 1164–1173, 2013.
- [40] A. Khalifa, "LSBase: A key encapsulation scheme to improve hybrid crypto-systems using DNA steganography," *Proceedings - 2013 8th International Conference on Computer Engineering and Systems, ICCES 2013*, pp. 105–110.
- [41] K. S. Sajisha, and S. Mathew, "An Encryption based on DNA cryptography and Steganography," *International Conference on Electronics, Communication and Aerospace Technology ICECA 2017*.
- [42] R. Agrawal, M. Srivastava, and A. Sharma, "Data hiding using dictionary based substitution method in DNA sequences," *9th International Conference on Industrial and Information Systems, ICIS 2014*.
- [43] P. Das, S. Deb, N. Kar, and B. Bhattacharya, "An improved DNA based dual cover steganography," *Procedia Computer Science*, 46 (Icict 2014), pp. 604–611, 2015.
- [44] K. Santoso, S. Lee, W. Hwang, and K. Kwon, "Sector-based DNA information hiding method," *Security Comm. Networks 2016*, vol 9, pp. 4210–4226.
- [45] A. Khalifa, and A. A. Elhadad, "High-Capacity DNA-based Steganography," *The 8<sup>th</sup> international conference of informatics and systems. 2014*.
- [46] S. Marwan, A. Shawish, and K. Nagaty, "Utilizing DNA strands for secured data-hiding with high capacity," *International Journal of Interactive Mobile Technologies*, 11 (2), pp. 88–98, 2017.
- [47] N. A. Zebari, , D. A. Zebari, , D. Q. Zeebaree, and J. N. Saeed, "Significant features for steganography techniques using deoxyribonucleic acid: a review," *Indonesian Journal of Electrical Engineering and Computer Science*, 21 (1), pp. 338–347, 2021.
- [48] M. R. Abbasy, P. Nikfard, A. Ordi, and N. R. M. Torkaman, "DNA Base Data Hiding Algorithm," *International Journal of New Computer Architectures & Their Applications*, 2 (1), pp. 183–192, 2012.
- [49] A. Majumdar, M. Sharma, and N. Kar, "An Improved Approach to Steganography using DNA Characteristics," 2016.
- [50] Shweta, & S. Indora, "Cascaded DNA cryptography and steganography," *International Conference on Green Computing and Internet of Things (ICGCIoT)*, 2015.
- [51] K. Menaka, "Message encryption using DNA sequences," *Proceedings - 2014 World Congress on Computing and Communication Technologies, WCCCT 2014*, pp. 182–184.
- [52] C. Guo, C. C. Chang, and Z. H. Wang, "A new data hiding scheme based on DNA sequence," *International Journal of Innovative Computing, Information and Control*, 8 (1A), pp. 139–149, 2012.
- [53] C. M. Shyamasree, and S. Anees, "Highly secure DNA-based audio steganography," *2013 International Conference on Recent Trends in Information Technology, ICRTIT 2013*, pp. 519–524.

- [54] Manisha, Parvinder Bangar, and Mohit, "Double layered DNA based cryptography," *IJRET: International Journal of Research in Engineering and Technology*, 2015.
- [55] A. Khalifa, A. Elhadad, and S. Hamad, "Secure blind data hiding into pseudo dna sequences using playfair ciphering and generic complementary substitution," *Applied Mathematics and Information Sciences*, 10 (4), pp. 1483–1492, 2016.
- [56] D. Na, "DNA steganography: Hiding undetectable secret messages within the single nucleotide polymorphisms of a genome and detecting mutation-induced errors," *Microbial Cell Factories*, 19 (1), pp. 1–9, 2020.
- [57] M. Sabry, T. Nazmy, and M. E. Khalifa, "Steganography in DNA Sequence on the Level of Amino acids," *Proceedings - 2019 IEEE 9th International Conference on Intelligent Computing and Information Systems*, ICICIS 2019, pp. 317–324.
- [58] P. Saha, L. Y. Pinky, M. A. Islam, and P. Akter, "Higher Payload Capacity in DNA Steganography using Balanced Tree Data Structure," *International Journal of Recent Technology and Engineering*, 8 (4), pp. 6551–6556, 2019.
- [59] M. H. Mohammed, B. H. Ali, and A. I. Taloba Mohamed, "Self-adaptive dna-based steganography using neural networks," *Information Sciences Letters*, 8 (1), pp. 15–23, 2019.
- [60] N. S. Terkawi, L. Berriche, A. A. Alamar, M. A. Ibrahim, and W. S. Alsaffar, "Comparative Study of Three DNA-based Information Hiding Methods," *International Journal of Computer Science and Security (IJCSS)*, Volume (15), Issue (2), 2021.
- [61] A. Khalifa, "A secure steganographic channel using DNA sequence data and a bio-inspired XOR cipher," *Information (Switzerland)*, 12 (6), 2021.

# Adaptive Logarithmic-Power Algorithm for Preserving the Brightness in Contrast Distorted Images

Navleen S Rekhi<sup>1\*</sup>

Research Scholar & Assistant Professor  
IKG Punjab Technical University, Kapurthala &  
DAV Institute of Engineering & Technology  
Jalandhar, Punjab-India

Jagroop S Sidhu<sup>2</sup>

Associate Professor  
DAV Institute of Engineering & Technology  
Jalandhar, Punjab-India

**Abstract**—The digital images get distorted due to non-uniform light conditions or improper acquisition settings of the digital camera. Such factors lead to distorted contrast objects. In this work, we proposed adaptive enhancement algorithm to improve the contrast while preserving the mean brightness in the image. The method developed is a combination of discrete wavelet transform and gamma correction. Firstly, the gamma scale is computed from multi-scale decomposition using 2D-discrete wavelet transform. The value of scale parameter in gamma was computed from combination of logarithmic and power function. Secondly, the gamma correction is implemented to improve the contrast in the image. Lastly, bilateral filtering is utilized for smoothness of edges in the image. The approach effectively preserved the brightness and optimized the contrast in the image. The objective quality measures used as Peak SNR, AMBE, entropy, entropy based contrast measure and median absolute deviation is computed and compared with other state-of-the-art techniques.

**Keywords**—Non-uniform images; gamma correction; multi-scale 2D- discrete wavelet transform; logarithmic-power; quality metrics

## I. INTRODUCTION

Due to imbalance of energy in the wavelength between RGB (red, green, and blue) colours, the distortion in the contrast is produced in the images. The contrast is the variation of brightness to discriminate between the features present in the image. The Fig. 1 is the exact illustration of what had been discussed by Qing Zhang et al [1]. The figure displayed an image with the distorted contrast, where most of the pixel values lies at the left extrema of the intensity scale. If the pixel values narrows at the extreme left, right, and middle values of the intensity scale, then the image is termed to be dark, bright, and low contrast images. For high contrast, the requisite amount of pixel should be uniformly distributed over the entire intensity scale [2]. Therefore, contrast is an important parameter to indicate the structural information in the image. With contrast stretching, the spread from a low to a high contrast range can be attained. Such mapping is termed to be the adjustment of dynamic range of intensity scale. Therefore, contrast stretching is a transformation technique utilized through linear or non-linear operations. The histogram equalization (HE) is one of the popular linear transformation technique, known for its simplicity and ease of use. It is an

intensity-based transformation which computes the information content based on statistical inference. Fig. 2 shows the full span of range obtained from HE technique. It generates distributed regions all over the intensity scale. But, with the stretch of contrast, contouring artifacts is occurred due to the loss of edges.

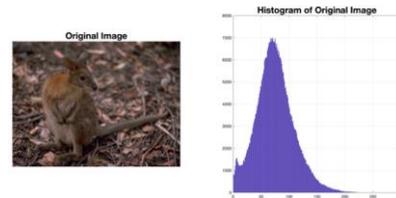


Fig. 1. Original Image.

Moreover, due to poor brightness preservation, the quality of the image is distorted. Hence, it is required to maintain the equilibrium between contrast and brightness in the image.

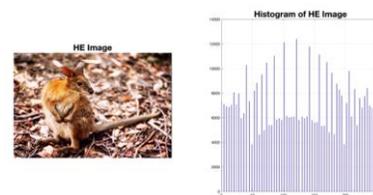


Fig. 2. Enhanced Image using HE Method.

## II. RELATED WORK

To overcome the limitation of HE, different techniques were proposed as mentioned in [3][4][5] to improve the quality of the image. The main idea in most of the techniques was to spread the dynamic range of the images. However, the HE does not provide sufficient information on the composition of fine details and edges. Most of the results obtained from the modified approach to HE, produced over enhancement for the darker scale and under enhancement for the lighter scale of the intensity values. The illustration in Fig. 3 was the enhanced image form the algorithm proposed by Kuldeep Singh and R. Kapoor as ‘MMSIC’ [6]. The modified HE was computed from mean-median based clipped histogram to improve picture quality. With this technique, the large number of pixel values were more towards the left extrema. This effect leads to

\*Corresponding Author

the low quality of contrast. Also, M.M. and M. Abdullah-Al-Wadud [7] had proposed the boosting algorithm for correction in over enhancement. The minor regions were boosted to suppress quantum jumps.

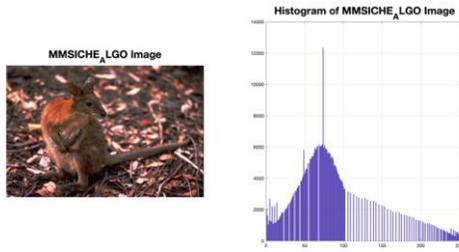


Fig. 3. Enhanced Image from Kuldeep Singh and R. Kapoor [6].

Another approach is the global and local HE methods. In the global HE, the overall picture is enhanced. Whereas in local HE, with the utilization of small windows, the quality of the picture is improved. Qi-Chong Tian and Laurent D. Cohen [8] proposed the combination of global and local HE to preserve the naturalness of the image. Further, fast quadratic HE was proposed by Surabhi Patel [9]. The author claimed the method was computationally faster as compared to global HE and local HE. Lastly, compared to the various modified methods of HE, BPDHE [3] produced effective results in preserving the mean brightness.

Other than HE, discrete wavelet transform is also a useful tool to improve the overall quality of the image. Hafiz Syed Muhammad Muslim et al. [10] had proposed noise reduction using 2-dimensional-discrete wavelet transform (2D-DWT) and a Gaussian low-pass filter. The DWT was used to filter the high frequency content and, for the other part, a Gaussian low pass filter was used. The algorithm was designed for improvement in the visual quality of medical images.

In recent times, the implementation of gamma is used for contrast improvement. Like sigmoid, it is also a non-linear approach to improve the contrast. In this techniques, gamma parameter is a constant value. Due to non-uniform contrast in images, the scale parameter in cannot be held constant. To meet the challenge, Huan S et al [11] developed AGCWD as adaptive gamma correction with weighted distribution mapping of the histogram to improve the contrast. The algorithm designed is limited in approach and mostly over-enhanced the low-contrast images. Gang Cao et al [12] have proposed an effective way to handle the exaggerated enhancement with gamma correction. Rather than correlating with the cumulative density function, gamma scale was used for the negative portion of the images. The modulated value of gamma alleviates the contrast of the image. For the effectiveness of gamma correction, a scale parameter is required to be computed such that, along with the contrast improvement, brightness is preserved in the image. The method of mean- variance computation of scale parameter was proposed by Meriama Mahamdioua and Mohamed Benmohammed was proposed to deal with the non-linear nature of gamma correction. But most of the experimental results were focused on facial recognition in the image. In such condition, the other details of the image could be avoided for overall enhancement. Further G. Jiang et al [13] developed

the golden search algorithm to optimize the scalability of gamma. Through the weighted sum, mean brightness was preserved. Liyun Zhuang and Yepeng Guan [14] proposed the log-exponential method to compute the scale of gamma. The HE was modified through the gamma scale to show the richness in the information details. The objective measures indicated the improvement but the subjective quality of the image was effected due to saturation effects. The hybrid combination of discrete wavelet transform and singular value decomposition was utilized by Sahnoun M. et al [15]. The experiments were restricted to MRI images for utilization of the proposed method and was dealt with grayscale content. Linwei Fan et al [16] explored the pros and cons of denoising techniques for the better visibility of the images. After formulation of denoising problem, various methods and their consequences were explored to conclude the findings of denoising techniques.

Although, HE is the simplest technique to enhance the contrast in the image. Due to serious limitation of over/under-enhancement (as clearly observed in Fig. 2 and 3), alternate approach of gamma is presented in our proposed algorithm. The key point is to preserve the mean brightness while improving the contrast. So, the estimation of brightness is computed through multiscale resolution analysis. And lastly, the scalability of contrast is increased by automated gamma scale calculated from logarithmic-power function.

The organization of the paper will be as followed. In section III, the proposed algorithm is discussed. In section IV, experimental results is demonstrated. Lastly, the conclusion of the proposed algorithm is interpreted.

### III. PROPOSED ALGORITHM

The Fig. 4 demonstrates the flow diagram of the proposed algorithm with gamma correction in contrast distorted images. The course of the work progressively followed with the conversion of raw RGB image to hue (H), saturation (S) and intensity value (I). The luminance value (I) is used for further processing stages. The computation of gamma scale function was obtained from logarithmic-power function. For the optimal value of scale parameter, multiscale resolution is implemented using 2D- discrete wavelet transform. This approach is necessary to extract the maximal luminance information in the intensity component. Lastly, the enhanced image is obtained from bilinear filtering to smooth out the edges.

#### A. Image Transformation

It is difficult to process the information for individual colors. Hence, for the given raw image, given as  $F(x,y)$ , is converted to 'I' [17] such that:

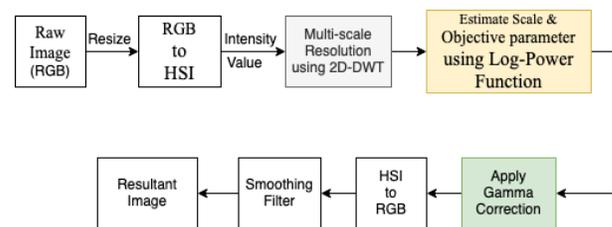


Fig. 4. The Flow Diagram of the Proposed Technique.



Fig. 5. Transformed Image Left: Grayscale and Right: Intensity Component.

$$F_{(x,y)} = T[H_{(x,y)}, S_{(x,y)}, I_{(x,y)}] \quad (1)$$

'T' denotes the transformation of RGB to HSI.

As shown in fig. 5, in comparison to grayscale, the intensity component has the maximal content of brightness in the image.

### B. Multiscale Decomposition

Most of the algorithms were designed to decompose the input image into bright and dark regions or partitioning of histogram [18] [19] [6] to obtain the luminance value in the image. Also, the 2D- DWT is utilized to compute the weighted function for selection of control parameters.

Inspired by the use of 2D-DWT in [15], multiscale resolution to the 'I' component in the HSI space is implemented to compute brightness. The primary objective is to estimate 'brightness' in the image. The information was down-sampled at a scale level of 'two'. The Fig. 6 showed the 2D-DWT decimation of information into four sub samples. The resultant image consisted of low pass filter in rows and columns direction sub-sampled at a scale level of '2'. The other followed by combination of high and low pass filter coefficients. With the profound studies [20][21], multiscale discrete wavelet transform (2D-DWT) was implemented. The 2D decomposition is obtained from one dimensional DWT decomposition. The 2D- discrete wavelet transform is implemented with mother wavelet as 'symlet5'.

$$I_{(u,v,u',v')} = \sum_{x=0, y=0}^{N_{cols}-1, N_{rows}-1} I_{x,y} \frac{1}{\sqrt{vv'}} \psi\left(\frac{x-u}{v}, \frac{y-u'}{v'}\right) \quad (2)$$

Where  $\frac{1}{\sqrt{vv'}} \psi\left(\frac{x-u}{v}, \frac{y-u'}{v'}\right)$  is the specific mother wavelet,  $I_{x,y}$  is the intensity component of the given image and  $I_{(u,v,u',v')}$  is the transformed image as shown in Fig. 5.

The choice of mother wavelet and selection of scale level was based on computation of wavelet energies [22] . The energy was calculated in a two-step formation as follows: (i) compute the wavelet energy at each scale level for different mother wavelets and (ii) the mother wavelet at preferred scale level with highest energy would be the criteria for decomposition.

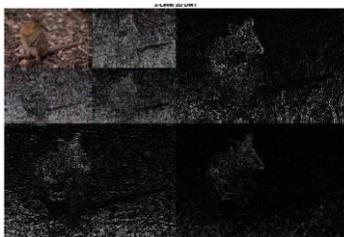


Fig. 6. 2D-DWT at a Scale Level of '2'.

### C. Estimation of Scale Parameter

There could be two possible ways to determine the scale parameter, either it should be chosen a constant value obtained from testing on various images with varying light conditions. Secondly, to make it adaptable for individual intensity scale of the image. Due to unpredictable variations in color distribution, assuming a constant value is difficult to obtain desired objective. Hence, the approach based on assumption of computing the average of minimum intensity of individual colors was taken to define selection criteria. This average value was computed from the original image. Secondly, the scale parameter is computed from the modified form of scale parameter in a logarithmic function. The logarithmic function is defined by the relation as  $s=c \log(1+r)$ . The scaling constant 'c' is chosen such that input intensity is mapped to high values and is calculated as:  $= \frac{J}{\log(1+\max(I))}$ , where J is the maximum scale value (255) and  $\max(I)$  is the maximum input value. This scale constant is modified with the assumption of mean intensity of low pass coefficients and is computed from Eq. 3. From the obtained value in equation (2), the mean intensity of pixel values were calculated as  $\mu = \frac{1}{MN} \sum_{m=0, n=0}^{M-1, N-1} L_{m,n}$  Where 'μ' is the mean intensity of low pass coefficients 'LL'.

$$\gamma = \frac{J - \mu}{\ln(1 + \mu)} \quad (3)$$

Where 'γ' is the scale parameter for gamma correction.

The minimum perceptible value of gamma must be 0.5 for any change in the contrast. And if the value goes greater than 1, will produce low contrast image. Since, the value obtained from Eq. 3 is too large to produce a desirable quality. Hence, the objective function was introduced to balance the scale of gamma parameter.

$$\gamma^{new} = \gamma^{(av(\min(RGB)))} \quad (4)$$

where  $\gamma^{new}$  is the scale parameter and 'av(min(RGB))' defined the objective function and is calculated as average of minimum intensity value in RGB colors. The value of gamma ranges from zero to infinity. However, if the scale value is 1, defines the linear mapping. And if the scale tends towards zero, the mapping is at higher or in other sense, brighter output values. Otherwise, towards darker output values. The intensity range of our referred data does-not constituted darker pixel values. From Eq. 4, it is found that the value of gamma greater than 1.25, over-enhanced the final image. Hence, the primary concern was to keep the scale level less than '1'. To overcome the over or under enhancement, adaptive gamma correction is implemented. As proposed in [23] , the increment value of gamma was computed from mean and variance combination for correction in contrast. But this method is limited to facial recognition, hence the proposed approach computed the average of maximum intensity of each channel in the original image. It is clearly observed in Eq. 5, the range was selected from  $0.65 < \gamma^{new} < 1.2$  for no correction in the gamma scale. However, if the value of gamma ( $\gamma^{new}$ ) is either decreased or increased, the correction in gamma is processed from other relation as stated in Eq. 5. With this approach, the mean brightness is well preserved.

$$\gamma^c = \begin{cases} 0.5 - (\text{av}(\max(\text{RGB}))) & \gamma^{\text{new}} < 0.85 \\ 1 - (\text{av}(\max(\text{RGB}))) & 0.85 \leq \gamma^{\text{new}} < 1.2 \\ 1.25 - (\text{av}(\max(\text{RGB}))) & \gamma^{\text{new}} \geq 1.25 \end{cases} \quad (5)$$

Lastly, gamma correction is implemented on ‘HSI’ transformation. The relation is as shown below:

$$Z_{(u,v)} = (F_{(x,y)})^{1/\gamma^c} \quad (6)$$

Where  $Z_{(u,v)}$  is the final image (HSI) and  $F_{(x,y)}$  is the image obtained from Eq. 1. The Fig. 7 illustrated the comparison of entropy, peak signal to noise ratio (PSNR) and mean brightness error (AMBE) to understand the necessity of change in gamma scale. The quality metrics was compared for the images with gamma correction (M) and without correction (U). The result of ten such images were shown, where gamma scale exceeds the threshold of 1.25. The AMBE [24] is the tool to predict the preservation of mean brightness in the image. Lower the value of AMBE, better will be the preservability. Since, AMBE is not a better metrics to measure noise content in the given information. Hence, PSNR [25] is also stated to predict the noise content in the image. Higher the value of PSNR, lower will be the noise and hence, better quality of image is obtained. The effectiveness of adaptive gamma scale produced the weighted change in AMBE and PSNR. Moreover, the richness of data (entropy) could be clearly observed in comparison to unmodified gamma correction.

Further, the Fig. 8 showed the comparison of variability in gamma correction. The middle image (b) is obtained from  $\gamma^c = [1 - (\text{av}(\max(\text{RGB})))]$  which is the standard form used for every image. With this gamma correction, scale value  $\gamma^{\text{new}}$  is obtained as 1.37. Hence, the gamma scale is modified to  $[1.25 - (\text{av}(\max(\text{RGB})))]$ . The right image (c) is the enhanced image after modification. The over enhancement (color brightness) is observed in the middle image. From the modified scale, the image showed the optimal brightness with improved PSNR.

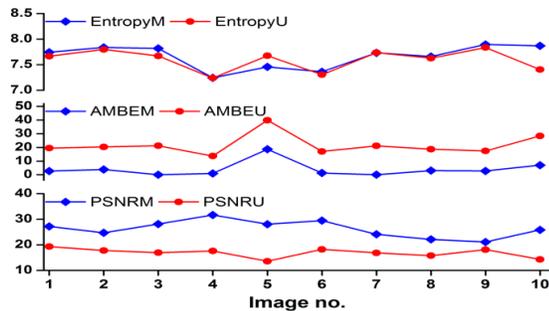


Fig. 7. Comparison of Adaptive Correction with Modified (M) and without Modification (U) based on Threshold Criteria ( $\gamma^c$ ).

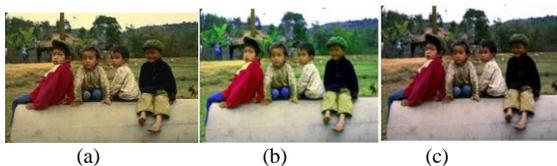


Fig. 8. Illustration of Gamma Scale (Image1): (a) Original Image, (b) without Adaptive Gamma Correction, and (c) Adaptive Gamma Correction (M).

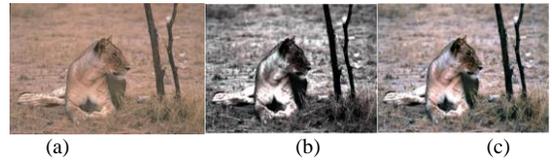


Fig. 9. Illustration of Gamma Scale <0.85, (a) Original Image, (b) without Adaptive Gamma Correction, and (c) Adaptive Gamma Correction (M).

Further, the Fig. 9 demonstrated the quality of the image, when the threshold value was less than 0.85. The middle (b) is low in contrast and when modified with the threshold  $(0.5 - (\text{av}(\max(\text{RGB}))))$ , produced the contrast enhanced image (c).

With point of human perception, ‘I’ is better for color image processing. However, conversion process of ‘rgb’ to ‘hsi’ and vice-versa produced the over-saturated colors. It is stated in [16], that convolutional neural network based denoising technique is well equipped to retain the naturalness in the image. Due to transformation and non-linear approach (gamma), the resultant image in our approach lead to disorientation in formation of colors. Hence, bilateral filtering is implemented to each channel for uniformity in color distribution. So, bilateral filtering was implemented to smooth out the edges for enhanced image. This type of filter is a noise suppression smoothing filter. Each color component is smoothed out while preserving the edges.

In summary, the algorithm proposed could be described as:-

**Algorithm:** Adaptive logarithmic-power function for contrast distorted image

**Input Image:** Original Image  $F_{(x,y)}$

**Step 1:** Convert the original image to HIS channel to obtain ‘I’ component (brightness)

**Step 2:** Decompose the ‘I’ at a scale level of ‘2’ using multiscale 2D discrete wavelet transform

**Step 3:** Using low-pass coefficients (shown in Fig. 6), compute the scale parameter using Eq. 3 and 4.

**Step 4:** Validate the scale value obtained from Eq. 4, using Eq. 5 for individual images.

**Step 5:** Finally, apply the automated gamma correction using Eq. 6 .

**Step 6:** After conversion from HIS to RGB, smooth out the edges using bilateral filtering.

**Step 7:** Obtain the Enhanced image.

#### IV. EXPERIMENTAL ANALYSIS

This section deals with the quality metrics implemented for comparison of proposed method with various state of the art techniques. The experiments were analyzed in the MATLAB 2017, platform. The machine used for evaluation was Apple MacBook, 1.8 GHz CPU and 8 GB of RAM.

### A. Image Dataset

The Berkeley Image dataset BSDS500 [26] and CEED 2016 [27] is used for evaluation of the proposed work. From the referred dataset, 200 images with varying light conditions were selected.

### B. Quality Metrics

The objective was to preserve the mean brightness while improving the overall contrast in the image. So, for our method, three quality metrics used as Entropy, absolute mean brightness error and Peak signal to noise ratio. The assessment of algorithm was based on full reference and no-reference measure. The full reference measure the information of the enhanced image in comparison to original image. Similarly, PSNR [25] and AMBE [28] measure the information as a full reference to predict the noise and mean brightness error in the enhanced image. Whereas, entropy, as a no-reference metrics, measures the richness in the content of the information. It is the full reference technique to assess the quality of image. Typically, high score of entropy and PSNR and low value of AMBE represents the better quality of image. In reference to the experiments conducted on 200 images of BSDS500 dataset, the 20 images with distortion in contrast is chosen for fair comparison with other relevant techniques.

Even though the AMBE is independent of the noise content, but measures the mean brightness content in reference to the original image. The Fig. 10 demonstrated the comparison of proposed technique with other algorithms published in peer reviewed journals. The brightness preserving dynamic (BPDHE) [3] and median-mean based clipped HE (MMSIC) [6] are the state-of-art techniques in modified HE.

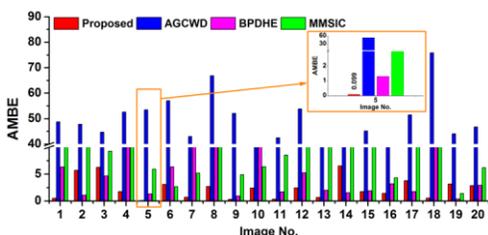


Fig. 10. AMBE Score of Random Selected Images.

Whereas, adaptive gamma weighted distribution (AGCWD) [11] and gradient based image enhancement (IM) [29] are one of the technique referred in most of the published journals. For the proposed method, the minimum AMBE is found to be 0.099 (as shown in inset) in comparison to other methods. The average value of 20 images computed is 2.36, which was far better as compared to MMSIC (8.81), BPDHE (6.11), AGCWD (48.7), and IM (107.34).

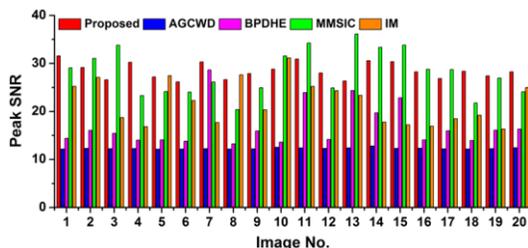


Fig. 11. Comparison of PSNR Value.

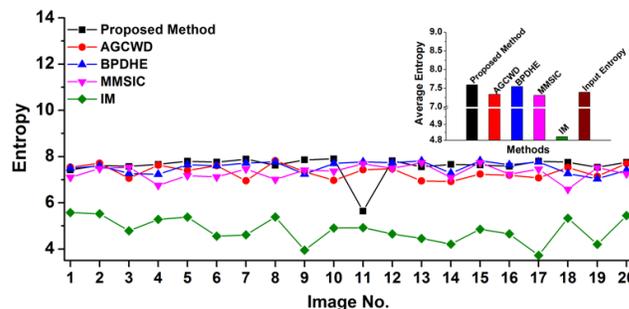


Fig. 12. Comparison of Information Measure (Entropy).

TABLE I. AVERAGE OF QUALITY METRICS FOR RANDOM 20 IMAGES

Metric/Method	BPDHE	MMSIC	AGCWD	IM	Proposed Method
Entropy	7.54	7.31	7.33	4.82	<b>7.59</b>
PSNR	17.03	28.04	12.31	21.91	<b>28.49</b>
AMBE	6.11	8.81	48.70	107.34	<b>2.36</b>
EB	85.30	79.45	<b>133.96</b>	80.53	102.57

\*Bold letters show better results

As stated previously, AMBE is not a good measure of noise content in the information. Hence, the PSNR was computed to show, that with the low value of AMBE, the noise suppression in the enhanced image is appreciably achieved. The Fig. 11 showed the comparison of different methods with our method. From table I, the average value of AGCWD and BPDHE for PSNR computed was 12.31 and 17.03. For lower value of AMBE in BPDHE, the PSNR is found to be poor and as well in the case of AGCWD. The value of 21.97 showed a marginal improvement in PSNR with a very high value of AMBE. But, in case of MMSIC, the value of 28.04 dB was noticed for a low value of AMBE. In our proposed work, both PSNR of 28.493 and AMBE of 2.36 had effectively improved the quality of image.

The entropy is a quantitative analysis to measure the content of information in the image. With low value of entropy, lesser will be the content in the information. For the average original entropy of 7.39, the entropy (Fig. 12) of 7.59 is found in our proposed work. For the different methods: 7.3, 7.54, 7.31, and 4.82 is computed in AGCWD, BPDHE, MMSIC, and IM. Except BPDHE, all other methods showed the loss of information content in the images.

It might be concluded from Table I, even though with marginal increase in PSNR (as compared to MMSIC), considerable change in AMBE and entropy could be observed. Without the loss of information, and with preserved mean brightness, the proposed method proved to be effective in restoration of contrast distorted images. The Fig. 14 showed the enhanced images obtained from proposed method for the middle-left, narrow, spread, and middle-right of the intensity scale. Also, the median based absolute deviation had been shown in reference to the input image. It is visually evident that the enhanced image showed the wide-spread over the entire intensity scale.

The images shown in Fig. 14 is chosen to show, that even for considerable distribution of pixels (boat), the efficacy of the proposed method is proved. From the histogram, it is evident that no peaks could be noticed at the extreme right and

left of the intensity scale. Such pattern indicated no loss of information and under -exposure is found. Moreover, colors in the images did not get overlapped and hence saturation effects is negligible.

C. Comparison with Enhancement Algorithms

In our experiments, hue and saturation is not altered and intensity is enhanced for the better quality of image. Like HE, our approach was also focused to spread the intensity values. With reference to the Fig. 13, for the narrow intensity scale (refer Fig. 1) where most of the information lies in the right half had produced widespread scale value with uniform brightness and contrast. In comparison to Fig. 2 (over enhancement) and Fig. 3 (over saturated colors), the shift of the peaks over the entire region could be observed in Fig. 13. It is attained by adjusting the gamma correction as stated in Eq. 5. The enhanced image produced improved contrast while preserving the mean brightness (in comparison to original image). From the aspect of quality metrics, table II (in reference to the Fig. 1) showed the comparison of different methods with the proposed technique. Except edge based contrast measure, the technique proved to be overall effective in better quality of the image.

The Fig. 15, showed the enhanced image for stat of the art techniques, used for comparison. For the cougar, except IM, the other methods showed the flatness (BPDHE) and over brightness (AGCWD) in the image. The median based absolute deviation is also stated at every histogram of images. It is the robust measure to estimate the distance of intensity value from the referred image. In our case, the referral image is the original and is compared with the enhanced image. With reference to parachute, narrow spread of intensity scale is noticed in comparison to the proposed technique. In case of

MMSIC, color disorientation is observed. For the uniform spread of intensity scale in the boat, over brightness was the major limitation of the AGCWD. Further, visual quality of method showed the over enhancement and color disorientation in the final image. In case of deer, all the methods showed the inconsistency in the spread of intensity values. The overbrightness in AGCWD, low contrast in BPDHE, oversaturation in IM and MMSIC, had adversely affected the detail and edges of the image. With fine details and pleasing quality of the image, the proposed technique effectively enhanced the image. For all the images, the quality metrics shown in table III, proved the efficacy of the approach used in the proposed method.

TABLE II. COMPARISON OF QUALITY METRIC FOR FIG. 1 WITH DIFFERENT METHODS

Metrics/Method	BPDHE	AGCWD	MMSIC	IM	Proposed Method
Entropy	7.23	7.63	6.755	5.28	<b>7.66</b>
AMBE	13.26	52.62	10.48	74.63	<b>1.76</b>
PSNR	14.00	12.28	23.29	24.68	<b>30.24</b>
EB	40.90	<b>102.55</b>	29.28	65.89	68.31

\*Bold letters show better results

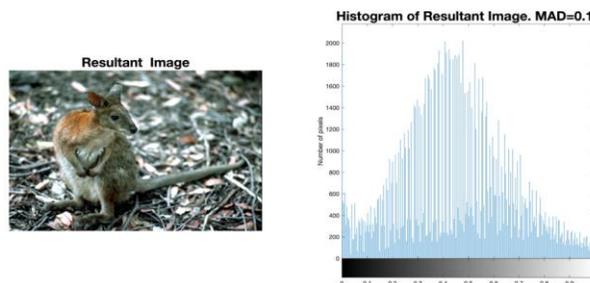


Fig. 13. Enhanced Image Obtained from the Proposed Method.

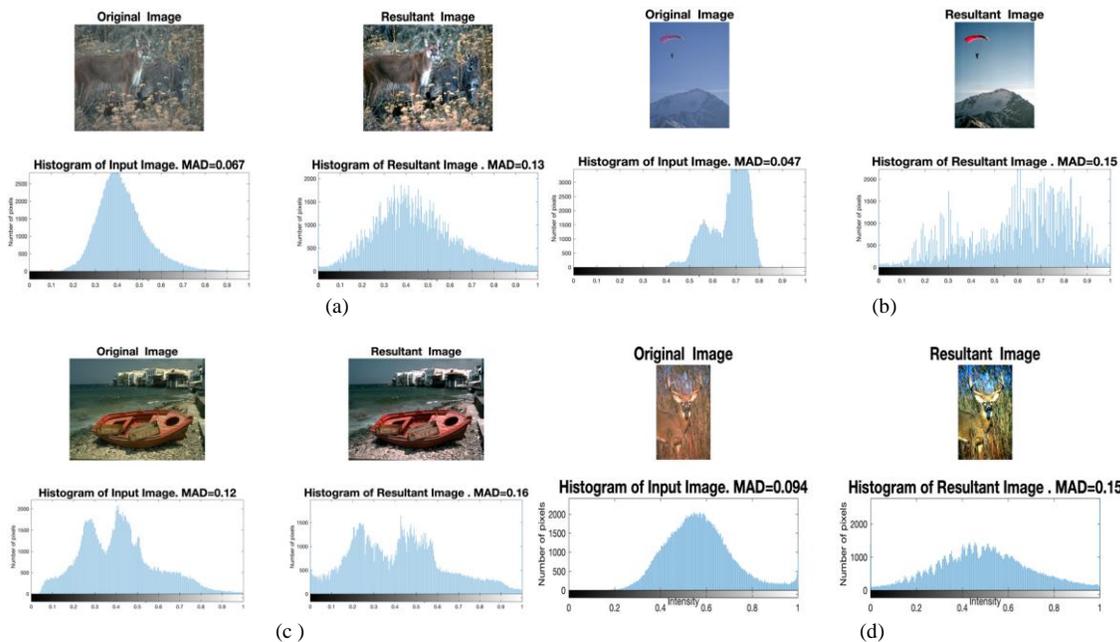


Fig. 14. Enhanced Images Obtained for Various Non- Uniform Contrast at (a) Middle-Left (Cougar) (b) Narrow (Parachute), (c) Spread (Boat) and (d) Mid-Right (Deer) Intensity Scale using Proposed Method.

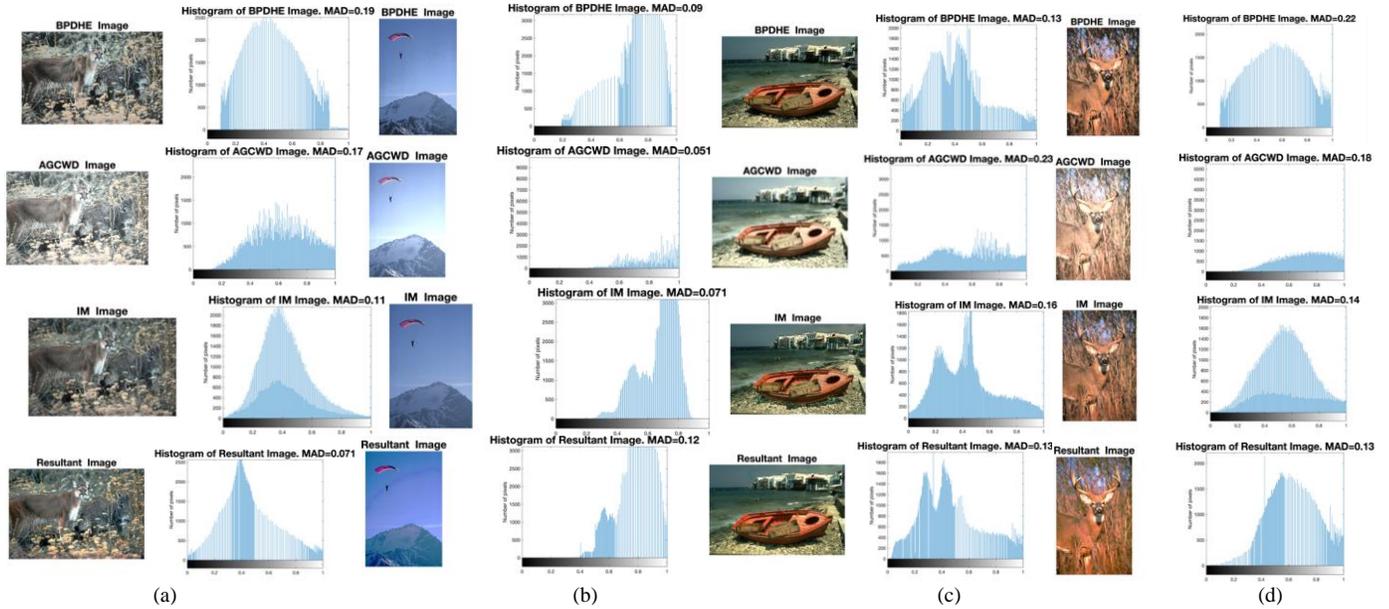


Fig. 15. Enhanced Images Obtained from BPDHE, AGCWD, IM, and MMSIC for (a) Cougar, (b) Parachute, (c) Boat, and (d) Deer.

TABLE III. COMPARISON OF QUALITY METRICS FOR FIG. 14 & 15

Image/Method	BPDHE (AMBE/PSNR)	AGCWD (AMBE/PSNR)	MMSIC (AMBE/PSNR)	IM (AMBE/PSNR)	Proposed Method (AMBE/PSNR)
Cougar	12.11/ 13.38	57.87/ 12.13	5.33/ 21.75	15.24/ 25.89	<b>2.37/ 26.90</b>
Parachute	6.47/ 14.26	62.44/ 12.25	12.13/ 21.13	95.94/ 22.54	<b>0.55/ 28.39</b>
Boat	2.34/ 29.7	55.39/ 12.20	10.50/ 25.25	88.47/ 19.75	<b>1.77/ 30.37</b>
Deer	<b>3.50/ 14.08</b>	53.48/ 12.14	8.56/ 24.14	142.30/116.74	<b>6.59/ 27.38</b>

\*Bold letters show better results

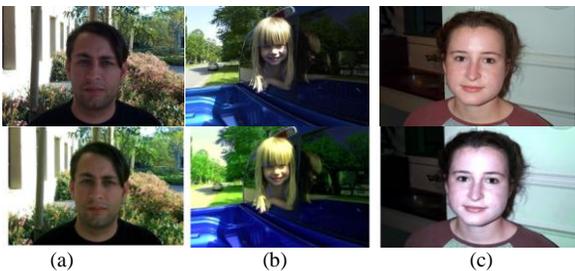


Fig. 16. Enhanced Images Obtained from Proposed Method ((a) Back-Lighting, (b) Side-Lighting, (c) Front-Lighting): Up: Original Image and Down: Enhanced Image.

Lastly, the images with back, side, and front lighting is compared with the method proposed by Liyun Zhuang and Yepeng Guan [14]. The root mean square (RMS) and the entropy of the image was calculated with the same relation prescribed in Sec. 3.3.2 and 3.3.3 of the work referred in [14]. The comparative results as shown in table IV, showed the better quantitative analysis. However, in each image the entropy was more as compared to our method. But, due to over-enhancement (in reference to Fig. 9,10, and 14 of Log-Exp [14]) presented the over saturation of colors. In our

proposed method, neither the detailed information was lost (as compared to input image) and, moreover, the rms value computed is found to be better than published work.

The entropy of the input image shown in Fig. 16 is 7.28, 7.20, and 7.50. From the proposed method, the brightness is preserved for improved visual quality of the image. Also, the proposed method was compared with the method proposed by Rao B [30] using CEED 2016[27] dataset. The comparative images based on visual quality as shown in Fig. 17. The Fig. 17 (a,d and g) is the original image, (b,e, and h) is the enhanced image obtained from proposed method and (c,f and i) is the resultant image from [30].

In comparison to original image, Fig. 17 (c) showed the clipping of histogram at the extreme right of the intensity scale. It indicated the loss of detail information in the image. Whereas in Fig. 17 (b), detail had been well preserved in the proposed method. From fig. 17 (f), the pixel distribution is moved to right of the intensity scale. But in Fig. 17 (e), uniform distribution of pixel is observed.

As compared to dynamic HE [30], the enhanced images had shown spread of intensity scale with an average mean brightness error at 1.89. Similarly, the value of average PSNR is computed to be 27.39. Moreover, the optimal obtained is found to be better as compared to the final image obtained by [30]. In that case, over brightness had decreased the contrast ratio in the enhanced image. In our proposed method, mean brightness is preserved for considerable change in the contrast.

TABLE IV. COMPARISON OF LOG-EXP [14] AND PROPOSED METHOD

Image	Log-Exp (Entropy/RMS)	Proposed Method (Entropy/RMS)
Backlighting	7.79/84.45	7.30/ <b>109</b>
Side Lighting	7.75/77.86	7.26/ <b>105</b>
Front Lighting	7.79/83.59	7.64/ <b>96</b>

\* Bold letters show better results

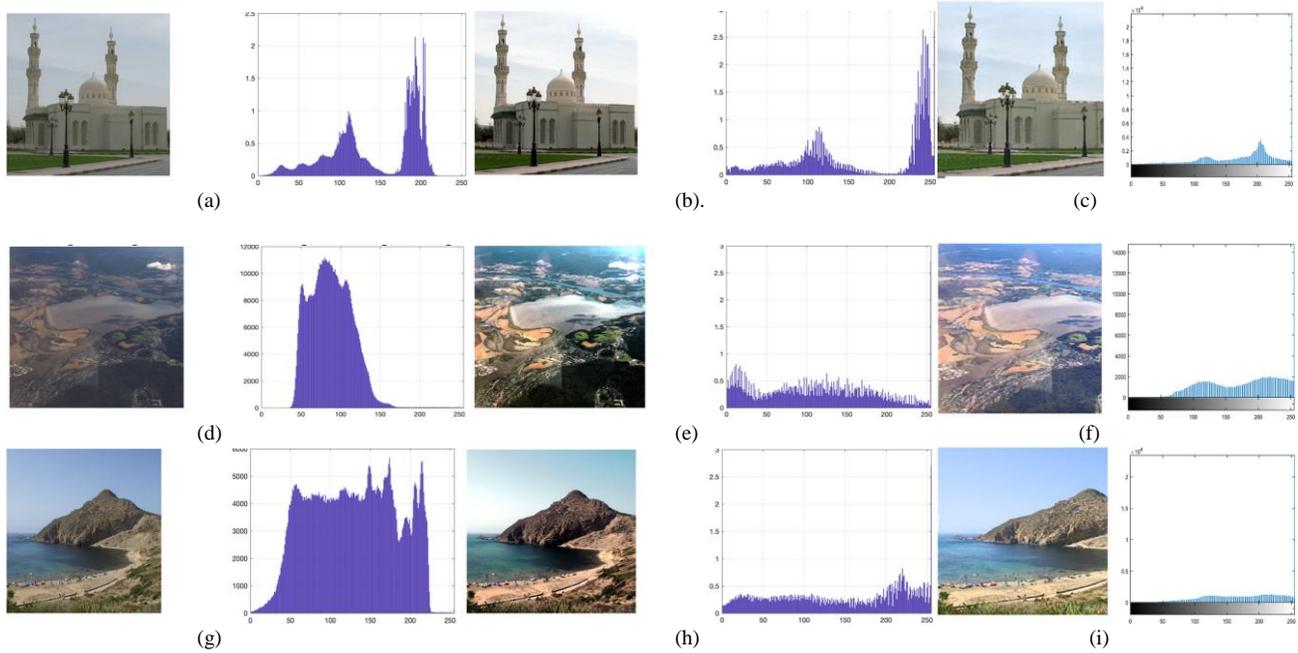


Fig. 17. Comparison of Proposed Method with Dynamic HE [30], (a), (d), and (g) Original Image; (b), (e), and (h) Enhanced Image from Proposed Method and (c), (f), and (i) Enhanced Image from Dynamic HE [30].

Lastly, it might be concluded that the objective of uniform distribution of pixel over the intensity scale, preserving mean brightness and improving the contrast had successfully achieved through the proposed algorithm. From Fig. 13, 14, and 17 (b), (e), and (h), it is clear that enhanced images showed the bell shaped and widespread of pixel values along the intensity scale. The bell shaped distribution represents, that most of the pixel existed at mid-tone values and therefore, minimum pixel distribution at extreme right/left of the histogram. Such representation of graph, is termed to have a better contrast with low under/over-exposure effects of illumination. Hence, with minimum AMBE and good PSNR, the approach in our method had appreciably improved the visual quality of the image.

#### V. CONCLUSION AND FUTURE SCOPE

An adaptive procedure for preservation of mean brightness with improved contrast had been proposed. The alternate and improved use of gamma correction was presented for various low contrast images. The dataset of 200 images from Berkeley BSDS 500 was analyzed for qualitative results. Moreover, some random images from dataset of CEED 2016 was used for different conditions of lightning in the image. From the conclusive results for 200 set of images shown in table V, demonstrated that with improved PSNR and minimum error in brightness, proved the effectiveness of the technique used for contrast distorted images. The measure of information as described by Shannon theory, maximum is the value higher will be the content of information. Hence, the information content is found to be maximum in comparison to other method.

TABLE V. AVERAGE COMPARISON OF BSDS 500 DATASET WITH DIFFERENT METHODS

Metrics/Method	<i>BPDHE</i>	<i>AGCWD</i>	<i>MMSIC</i>	<i>IM</i>	<i>Proposed Method</i>
<b>Entropy</b>	7.57	7.31	7.28	6.78	<b>7.64</b>
<b>AMBE</b>	11.28	49.50	7.67	103.62	<b>3.02</b>
<b>PSNR</b>	16.63	12.32	27.14	19.19	<b>27.67</b>
<b>EB</b>	85.30	<b>121.96</b>	79.45	80.53	105.34

\* Bold letters show better results

The edge based contrast in AGCWD was maximum at the cost of over-brightness as shown in Fig. 15. It is found in our proposed method, that overall quality of the enhanced image had preserved the mean brightness and improved the contrast in the image. The over saturation of colors was also balanced with the use of bilateral filtering.

The objective of our work was to maintain the gamma scale value less than '1'. Even though the visual quality is better in Fig. 17 (b), but the considerable number of pixels could be seen in the right of the intensity scale. That causes the over-exposure of brightness. So, in the future work, thresholding based gamma correction might be implemented in such images to avoid the over exposure effect. Also, for the dark images, the value of scale parameter less than '1.5' could not produce desirable visual quality in the images. Hence, the work would be extended to deal with dark intensity scale values.

#### ACKNOWLEDGMENT

We acknowledge the IKG Punjab Technical University, Kapurthala, Punjab, India and DAV Institute of Engineering & Technology, Jalandhar, and Punjab, India for providing valuable resources and necessary tools for the successful implementation of the work.

REFERENCES

- [1] Q. Zhang, Y. Nie, and W.-S. Zheng, "Dual Illumination Estimation for Robust Exposure Correction," Oct. 2019, [Online]. Available: <http://arxiv.org/abs/1910.13688>.
- [2] R. C. Gonzalez and R. E. (Richard E. Woods, Digital image processing.
- [3] H. Ibrahim and N. Pik Kong, "Brightness Preserving Dynamic Histogram Equalization for Image Contrast Enhancement," IEEE Transactions on Consumer Electronics, vol. 53, no. 4, pp. 1752–1758, Nov. 2007, doi: 10.1109/TCE.2007.4429280.
- [4] N. SinghBagri, S. Sharma, and S. Sahu, "Images Enhancement with Brightness Preserving using MRHRBFN," International Journal of Computer Applications, vol. 40, no. 7, pp. 22–26, 2012, doi: 10.5120/4976-7231.
- [5] K. Santhi and R. S. D. Wahida Banu, "Adaptive contrast enhancement using modified histogram equalization," Optik, vol. 126, no. 19, pp. 1809–1814, 2015, doi: 10.1016/j.ijleo.2015.05.023.
- [6] K. Singh and R. Kapoor, "Image enhancement via Median-Mean Based Sub-Image-Clipped Histogram Equalization," Optik, vol. 125, no. 17, pp. 4646–4651, 2014, doi: 10.1016/j.ijleo.2014.04.093.
- [7] M. M. Naushad Ali and M. Abdullah-Al-Wadud, "Image Enhancement Using a Modified Histogram Equalization," 2012, pp. 17–24. doi: 10.1007/978-3-642-35270-6\_3.
- [8] Q. C. Tian and L. D. Cohen, "A variational-based fusion model for non-uniform illumination image enhancement via contrast optimization and color correction," Signal Processing, vol. 153, pp. 210–220, 2018, doi: 10.1016/j.sigpro.2018.07.022.
- [9] S. Patel and M. Goswami, "Comparative analysis of Histogram Equalization techniques," Proceedings of 2014 International Conference on Contemporary Computing and Informatics, IC3I 2014, vol. 1, no. 2, pp. 167–168, 2014, doi: 10.1109/IC3I.2014.7019808.
- [10] H. S. M. Muslim, S. A. Khan, S. Hussain, A. Jamal, and H. S. A. Qasim, "A knowledge-based image enhancement and denoising approach," Computational and Mathematical Organization Theory, vol. 25, no. 2, pp. 108–121, 2019, doi: 10.1007/s10588-018-9274-8.
- [11] S. C. Huang, F. C. Cheng, and Y. S. Chiu, "Efficient contrast enhancement using adaptive gamma correction with weighting distribution," IEEE Transactions on Image Processing, vol. 22, no. 3, pp. 1032–1041, 2013, doi: 10.1109/TIP.2012.2226047.
- [12] G. Cao, L. Huang, H. Tian, X. Huang, Y. Wang, and R. Zhi, "Contrast enhancement of brightness-distorted images by improved adaptive gamma correction," Computers and Electrical Engineering, vol. 66, pp. 569–582, 2018, doi: 10.1016/j.compeleceng.2017.09.012.
- [13] G. Jiang et al., "Image contrast enhancement with brightness preservation using an optimal gamma correction and weighted sum approach," Journal of Modern Optics, vol. 62, no. 7, pp. 536–547, Apr. 2015, doi: 10.1080/09500340.2014.991358.
- [14] L. Zhuang and Y. Guan, "Image Enhancement Using Modified Histogram and Log-Exp Transformation," Symmetry, vol. 11, no. 8, p. 1062, 2019, doi: 10.3390/sym11081062.
- [15] M. Sahnoun et al., "A Modified DWT-SVD Algorithm for T1-w Brain MR Images Contrast Enhancement," Irbm, vol. 40, no. 4, pp. 235–243, 2019, doi: 10.1016/j.irbm.2019.04.007.
- [16] L. Fan, F. Zhang, H. Fan, and C. Zhang, "Brief review of image denoising techniques," Visual Computing for Industry, Biomedicine, and Art, vol. 2, no. 1, 2019, doi: 10.1186/s42492-019-0016-7.
- [17] A. Ziemba and E. Fornalik-Wajs, "Time performance of RGB to HSI colour space transformation methods," Archives of Thermodynamics, vol. 39, no. 1, pp. 111–128, 2018, doi: 10.1515/aoter-2018-0006.
- [18] Y. T. Kim, "Contrast enhancement using brightness preserving bi-histogram equalization," IEEE Transactions on Consumer Electronics, vol. 43, no. 1, pp. 1–8, 1997, doi: 10.1109/30.580378.
- [19] C. Zuo, Q. Chen, and X. Sui, "Range Limited Bi-Histogram Equalization for image contrast enhancement," Optik, vol. 124, no. 5, pp. 425–431, 2013, doi: 10.1016/j.ijleo.2011.12.057.
- [20] A. K. Bhandari, V. Soni, A. Kumar, and G. K. Singh, "Cuckoo search algorithm based satellite image contrast and brightness enhancement using DWT-SVD," ISA Transactions, vol. 53, no. 4, pp. 1286–1296, 2014, doi: 10.1016/j.isatra.2014.04.007.
- [21] P. D. Boraste and P. K. P. N., "Image Enhancement using DWT," International Journal Of Engineering And Computer Science ISSN:2319-7242, vol. 4, no. 2, pp. 10509–10515, 2015.
- [22] A. J. W. & S. INC., P. K. S. Thyagarajan, "STILL IMAGE AND VIDEO COMPRESSION WITH MATLAB," 2010.
- [23] M. Mahamdioua and M. Benmohammed, "New Mean-Variance Gamma Method for Automatic Gamma Correction," International Journal of Image, Graphics and Signal Processing, vol. 9, no. 3, pp. 41–54, Mar. 2017, doi: 10.5815/ijigsp.2017.03.05.
- [24] A. Shokrollahi, A. Mahmoudi-Aznavah, and B. Mazloom-Nezhad Maybodi, "Image quality assessment for contrast enhancement evaluation," AEU - International Journal of Electronics and Communications, vol. 77, pp. 61–66, 2017, doi: 10.1016/j.aeue.2017.04.026.
- [25] A. Horé and D. Ziou, "Image quality metrics: PSNR vs. SSIM," Proceedings - International Conference on Pattern Recognition, pp. 2366–2369, 2010, doi: 10.1109/ICPR.2010.579.
- [26] D. Martin, C. Fowlkes, D. Tal, and J. Malik, "A Database of Human Segmented Natural Images and its Application to Evaluating Segmentation Algorithms and Measuring Ecological Statistics." Available: <https://www2.eecs.berkeley.edu/Research/Projects/CS/vision/grouping/resources.html>
- [27] M. A. Qureshi, A. Beghdadi, and M. Deriche, "Towards the design of a consistent image contrast enhancement evaluation measure," Signal Processing: Image Communication, vol. 58, no. August 2016, pp. 212–227, 2017, doi: 10.1016/j.image.2017.08.004.
- [28] S. Sahoo, J. Panda, and M. N. Mohanty, "Performance Analysis of HE Methods for Low Contrast Images," Procedia Computer Science, vol. 92, pp. 72–77, 2016, doi: 10.1016/j.procs.2016.07.325.
- [29] M. Tanaka, T. Shibata, and M. Okutomi, "Gradient-Based Low-Light Image Enhancement." Available: <https://arxiv.org/abs/1809.09297>.
- [30] B. S. Rao, "Dynamic Histogram Equalization for contrast enhancement for digital images," Applied Soft Computing Journal, vol. 89, p. 106114, 2020, doi: 10.1016/j.asoc.2020.106114.

# A Meta-analytic Review of Intelligent Intrusion Detection Techniques in Cloud Computing Environment

Meghana G Raj, Dr. Santosh Kumar Pani

Department School of Computer Engineering, Kalinga Institute of Industrial Technology  
Deemed to be University, Bhubaneswar, India

**Abstract**—Security and data privacy continue to be major considerations in the selection and study of cloud computing. Organizations are migrating more critical operations to the cloud, resulting in increase in the number of cloud vulnerability incidents. In recent years, there have been several technological advancements for accurate detection of attacks in the cloud. Intrusion Detection Systems (IDS) are used to detect malicious attacks and reinstate network security in the cloud environment. This paper presents a systematic literature review and a meta-analysis to shed light on intelligent approaches for IDS in cloud. This review focuses on three intelligent IDS approaches- Machine Learning Algorithms, Computational Intelligence Algorithms and Hybrid Meta-Heuristic Algorithms. A qualitative review synthesis was carried out on a total of 28 articles published between 2016 and 2021. This study concludes that IDS based on Hybrid Meta-Heuristic Algorithms have increased Accuracy, decreased False Positivity Rate and increased Detection Rate.

**Keywords**—Intrusion detection system (IDS); machine learning; computational intelligence algorithms; hybrid meta-heuristic algorithms; cloud security; cloud computing

## I. INTRODUCTION

Cloud Computing (CC) provides on-demand network access to a group of configurable computing assets like servers, services, applications, storage, and networks that could be rapidly released with lesser management endeavors or service provider interaction. While it offers many benefits, one of the main challenges for organizations looking to adopt cloud-based solutions is security. This is because of the nature of the cloud infrastructure i.e., fully distributed and open, thus making it more vulnerable to threats and attacks. This environment creates incentives for potential intruders to initiate attacks targeting devices having access to data stored on the cloud. The threats due to attacks are to the integrity, confidentiality, and availability of cloud services and resources [56]. For example, a Distributed Denial of Service attack, is one that aims to prevent availability of data stored on the cloud, by choking the network bandwidth through packet flooding. Other potential attack types include IP Spoofing, Domain Naming System (DNS) Poisoning, Man in the Middle Attack, Port Scanning, etc. [50]. Cloud security is an interesting active field of study and various heuristics have evolved and been proposed. Basic security elements such as a firewall that protects the internal network and adoption of message encryption may be employed as initial lines of defense. However, a firewall may not be able to identify an attack initiated by an insider [33]. In order to

meet the security challenges effectively, a dedicated Intrusion Prevention System (IPS)/ Intrusion Detection System (IDS) should be integrated within the cloud environment. IDS has become an important and irreplaceable part of the network protection system. An intrusion i.e. an attempt to compromise the availability, confidentiality, and integrity of cloud-based resources can be detected utilizing cloud based IDSs [16]. Traditional network security techniques which are not integrated within the cloud environment may not be effective in meeting the requirements of cloud security. This is due to certain limitations of traditional IDS such as incorrect classification of network anomalies as attack, low rate of detection of attacks and high false positive rate among the detected attacks [27]. Techniques in IDS such as anomaly detection and misuse detection are now relying on machine learning to increase performance effectiveness. Machine learning incorporates meta-heuristic algorithms to enhance the performance, and to identify and classify normal and unusual attacks in the network. The IDS should monitor the potential means and ends for attacks, such as network traffic and audit data in a network/ computer system, and employ different methods for detecting unauthorized activities as intrusion. Fig. 1 provides a summary of IDS in cloud environments [44]. Design of an integrated IDS was described in [19] and [54]. The primary goal of IDS is to identify each intrusion in an effective way [60]. The execution of IDS enables network administrators to detect security objective violations. These security objectives include both securing cloud resources from attacks by external sources who are attempting to get unauthorized access, as well as securing them from attacks by internal sources who are attempting to abuse their access privileges. However, the efficient and effective development of IDS is a complex problem due to meeting the twin requirements of achieving low false positive rate and high true positive rate, while consuming minimal computing resources for these purposes [62]. An IDS with a high false positive rate could potentially generate unwarranted alerts and consume significant cloud resources in response to anomalous network states which were not the result of an attempted intrusion. The application of detection methods could then result in initiation of response events within the cloud environment, which eventually cause an overload in the network. Simultaneously, achieving a high true positive rate through accurate and rapid detection of intrusion is crucial in reducing the potential damage caused by an intrusion or unauthorized access to the cloud resources. Within IDS, Host-based Intrusion Detection

Systems (HIDS) functions on data collected from a computer system, and permits analysis of activities of processes and users in the attack on a specific system. It visualizes the attempted attack's outcome, access and observe data files directly and the process of the operating system [25]. It identifies the attacks which may not have been detected by Network-based Intrusion Detection System (NIDS), as it observes the events which are local to the computer system. Host-based Intrusion Detection and Prevention (HIDPS) consist of software involves in observation and analysis of events takes place in the computer and information system in identification and stopping harmful incidents in the system, becomes more important as it protects the computer system and its network activities [33].

IDSs use different methods to detect potential malicious activities during an intrusion. One such method is Signature-based method, which attempts to map the current set of system parameters with the previously recorded system parameters patterns which correspond to known attacks or intrusions which have occurred in the past [51]. A second method is Anomaly-based which attempts to detect attacks or intrusions using machine learning and statistics to create simulations, which are then compared with the current anomalies that may be seen in the cloud environment [51]. The Anomaly-based method has training and testing phases. Learning of normal traffic from data takes place during the training phase, and during the testing phase, tests are performed on previously unseen data. There are two types of IDS approaches- Hybrid and Non-hybrid. Hybrid IDS is the approach which attempts to reduce the limitations of Signature-based and Anomaly-based methods through higher accuracy and detection of known and unknown threats from a large dataset, by combining different intelligent algorithms [29]. Hybrid IDS relies on the reality that it is very difficult to manipulate cyber data without detection to carry out an attack [15]. Non-hybrid IDS is the approach which relies on a single intelligent algorithm to detect potential attacks. Numerous IDS models based on statistical models, machine learning, deep learning (DL), meta-heuristic algorithms, etc. are available in the existing literature. In recent years, hybridization of any of these approaches has been used to enhance intrusion detection performance. However, a comparative review of performance of various IDS approaches, after classifying them into different approach types- Machine Learning Algorithms, Computational Intelligence Algorithms and Hybrid Meta-Heuristic Algorithms- along selected parameters is not available in the literature. This paper provides a review of existing IDS algorithms, particularly developed for the CC environment, with the objective of comparing the performance of IDS approaches along selected parameters. The recent, state of the art IDS techniques consist of both non-hybrid IDS approaches as well as hybrid approaches. The existing IDS algorithms under each approach category have been reviewed and the merits of each algorithm have been identified. In addition, the reviewed algorithms have been compared to one another, based on selected parameters. Finally, the open issues, possible future directions, and limitations of the study have been elaborated.

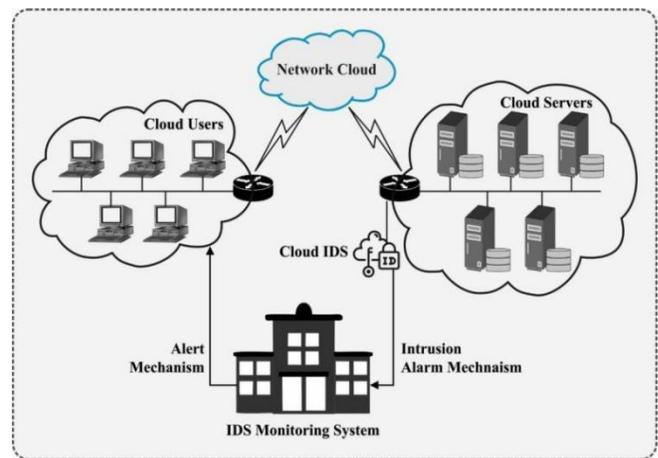


Fig. 1. Overview of IDS in Cloud Environment.

## II. BACKGROUND

Riaz, A., et al., [45] conducted a brief analysis of IDS techniques presented for the cloud environment. To attain this goal, at the initial stage, the unique characteristics and limitations of all the techniques were enumerated. Next, a set of criteria were established for evaluating the IDS framework. In this work, a relative analysis of many current IDSs on different dimensions was elaborated. Lastly, the discussion of open issues and drawbacks was provided in detail. Zouhair, C. et al., in [63] presented the review of cloud infrastructure and summary of distinct intrusions in the cloud. In addition, the essential characteristics and challenges of cloud based IDS techniques were identified. Next, the researchers analyzed 24 cloud based IDS regarding their different positions, types, data sources, and detection times. Also, the strengths and limitations of various IDS, to evaluate whether they meet the security requirement of CC infrastructure or not were listed. Mthunzi, S.N. and Benkhelifa, E. in [41] identified security issues that are of catastrophic nature in the cloud environment and listed out a survey of the counter measures for cloud security with bio-inspired approaches and enumerated the advantages and limitations of the approaches. Mishra, P., et al., in [39] provided a comprehensive study of different IDSs presented for cloud infrastructure with analysis of their attack detection abilities. The researchers proposed an attack taxonomy and threat model in the cloud framework, to list out the various vulnerabilities in the cloud environment. The taxonomy of IDS techniques represented an advanced classification and provided an exhaustive literature survey of techniques using their distinct characteristics. Chattopadhyay, M., et al., in [14] examined the limitations in using machine learning techniques to detect intrusions and compared different techniques on several datasets and calculated the performance merits. The best technological solutions have been identified for various usage patterns. Sharma, S. and Kaul, A., in [53] presented a short overview about the different IDSs for a Vehicular Ad-hoc Network (VANET). Proposals were made to develop IDSs which could have potential application in VANET and VANET Cloud. This study aimed to explore open challenges, research directions in the future aspects, and leading trends in the placement of IDS in VANET. Lee, S.W., et al., in [32] focused on the Deep Learning (DL) IDS approach and

investigated how DL networks may be applied with distinct methods in various phases of the IDS, in order to achieve better results. The researchers categorized the surveyed IDS systems with respect to DL networks employed and described their major contributions. As well, in every classification, basic characteristics such as datasets, evaluated metrics, environments, and simulators were enumerated. In addition, a comparison of the results using DL IDS approach was provided, to compare the major approaches employed. Tama, B.A. and Lim, S., in [58] provided a summary of how ensemble learner may be employed in the IDS, through systematic mapping. The researchers analyzed and collected 124 high quality publications and the selected publications were later mapped to various classes like publication venues, years of publication, ensemble methods, IDS techniques, and datasets used. Furthermore, this survey analyzed and reported the experimental research of a novel classifier ensemble method for abnormality based IDSs. Shamshirband, S., et al., in [50] conducted a complete review of IDSs which used Computational Intelligence (CI) techniques in a (mobile) cloud environment. Initially, a summary of CC paradigm and service models was offered. Next, a review of the security risks in this context was provided. Earlier works related to this subject were surveyed critically, highlighting the limitations and advantages of those earlier studies. Next, a taxonomy for Intrusion Detection System was presented CI based techniques were categorized into hybrid and single approaches, for the different classifications of IDSs.

Based on the above overview of the background for this paper, research questions have been formulated, to focus on two 2 broad approaches to intelligent IDS and on hybridization of algorithms from these 2 broad approaches, to determine whether such hybridization could result in enhanced performance of Intrusion Detection Systems.

### III. RESEARCH METHODOLOGY

A Systematic Literature Review (SLR) denotes evaluation of previous works on a specific set of problems from a critical perspective, with an attempt to list out all relevant studies on the basis of first principles. This study devises a structured method in locating and assembling a body of research studies on IDS in cloud environments [47]. Previous studies state that such methods have overlooked limitations, reduced chance effect and improved data validity process [21]. The SLR structure to review past work on intelligent IDS in cloud computing are presented in this section. This requires an impartial and overall layout of literature in this SLR. First, research questions are proposed as per the objectives of the survey, search query and criteria of inclusion and exclusion bias are illustrated in sections 3.1 and 3.2 with review methodology in 3.3.

**RQ1:** What are the different Computational Intelligence Algorithms- such as Bio-inspired, Swarm Intelligence, Evolutionary Computing- used in intelligent Intrusion Detection Systems in Cloud Computing?

**RQ2:** What are the different Machine Learning Algorithms used in intelligent Intrusion Detection Systems in Cloud Computing?

**RQ3:** What are the performance advantages of hybridization of Computational Intelligence Algorithms and Machine Learning Algorithms, for cloud IDS?

These questions were considered during the process of conducting SLR for intelligent IDS in cloud environments.

#### A. Search Terms

Research articles in reference to keywords such as "Intelligent IDS in cloud computing", "Machine learning based intrusion detection systems in Cloud", "hybrid and non-hybrid approaches", "Bio-inspired IDS in Cloud", "Nature-inspired IDS in Cloud", "Swarm intelligence IDS in Cloud" and "Hybrid Meta-Heuristic IDS in Cloud" were searched from online sources including IEEE, Springer, Taylor & Francis, Scopus, Science direct, and Google Scholar. A total of 140 articles were collected based on these keywords, with preference given to the top research articles from renowned journals. Analysis was conducted in an orderly fashion, to initiate the review process, resulting in identification of 28 articles for Meta Analysis. This process has been summarized in Fig. 2.

#### B. Inclusion and Exclusion Bias

The search was commenced with journals with an overview of the research presented in: (a) articles listed in the peer-reviewed journals; (b) published in English; (c) related to cloud IDS; (d) published between from 2016 to 2021, from databases. Duplicate articles, Conference Publications, Theoretical Research articles were removed from the initial search. Irrelevant articles were excluded further after reading the Title and Abstract. After reading the remaining full text articles, 28 articles were found to be probable sources for the review.

#### C. Qualitative Review Synthesis

These twenty-eight articles were considered probable sources and their contents were streamlined in the SLR. The articles were further categorized into those that were based on machine learning models, computational intelligence (bio-inspired) algorithms and hybrid approaches for IDS. These three approaches were reviewed in terms of Accuracy, False Positive Rate and Detection Rate, as parameters [4].

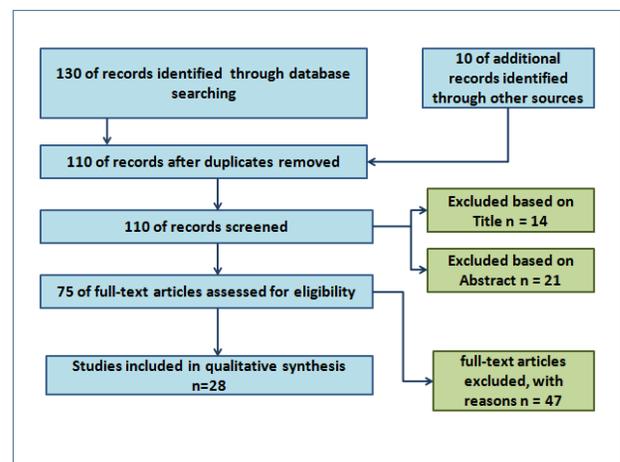


Fig. 2. Flowchart of Article Selection.

#### IV. LITERATURE REVIEW

A detailed review of IDS under each category is given in the following section.

##### A. Machine Learning based Ids Approaches in Cloud

Machine Learning (ML) is used to address the optimal solution for complex problems which have multiple non-linear constraints, high number of dimensions and time limitations in the field of science and engineering. ML techniques have many features to resolve conflicts in classification of patterns as well as regression, optimization and estimation of functions [23]. ML provides computers input or training data to facilitate the process of learning and improving, without manual programming. The main focus of ML is to develop programs that use data in the discovery process without human intervention. ML algorithms can be classified into Supervised ML algorithms— which enable predictions of output from given data; Unsupervised ML algorithms— which enable inferences to be drawn on structures which are not obvious from unknown data; and Semi-supervised ML algorithms— which enable blending of features of both Supervised and Unsupervised ML algorithms and are mostly used to quantify the training data [8]. A detailed comparison of ML based IDS approaches reviewed in this SLR is given in Table I. A brief summary of these models follows. A novel DDoS attack detection technique in CC platform was developed in [31]. The presented model was defined by the use of an ML model called Voting Extreme Learning Machine (V-ELM). A voting scheme was developed and attack class was allotted to a sample, in case of having many votes. The performance of the V-ELM technique was validated using the NSL-KDD and the ISCX intrusion detection datasets. In [59], the researchers aimed to detect the presence of DDoS attacks in SDN. This method classified the SDN traffic as normal or attack traffic with the use of ML models integrated into Neighborhood Component Analysis (NCA). In addition, a public dataset with 23 attributes was used for experimental validation and the results demonstrated the superior performance of the proposed model with limited features. Sharma, P., et al., in [52] developed a multi-layer IDS to classify different types of attacks using the ExtraTress, classification model and the Extreme Learning Machine (ELM) model was employed for the detection of individual attacks.

The outputs from the ELMs were integrated with the use of a Softmax layer. The proposed model's performance was validated using the UNSW and KDDcup99 datasets. Lopez, A.D., et al., in [35] proposed flow based traffic features for analyzing the variance in patterns among normal versus anomalous packets. They evaluated the various supervised classification approaches using parameters such as false negatives, detection accuracy, run time, and time taken to train. The researchers concluded that Decision Tree (DT) based Random Forest (RF) was the promising approach, in which a Dense Neural Network performed well on specific DDoS attack types. Sambangi, S. and Gondi, L., in [48] designed an ML method on the basis of multiple LR analyses and carried out data visualization by taking into account the respective fit charts and residual plots. The aim was to employ the Feature Selection (FS) method and define the significant features which are delivered by various predictive models. Then, the selected feature was subjected to multiple LR analyses, and the performance of the ML method was evaluated as per the set of selected significant features, on the CICIDS2017 dataset. Another study [26] proposed real-time recognition of DDoS attacks using an ML classifier which relied on a distributed processing framework. The DDoS detection rate was computed using the OpenStack based cloud testbed, through the Apache Spark architecture. In [21], a DL based IDS for DDoS attacks was proposed on the basis of 3 methods, namely Convolutional Neural Network (CNN), Deep Neural Network (DNN), and Recurrent Neural Network (RNN). The performance of each method was analyzed on the basis of 2 classification types (multiclass and binary), using 2 real traffic datasets- TON\_IoT and CIC-DDoS2019 [30]. Based on this analysis, a DL based detection method for DoS attacks was proposed, which used the CNN method to carry out multiclass classification and binary classification, and used RNN method to improve efficiency. Aborujilah, A. and Musa, S., in [2] proposed a novel application of Multi Attribute Decision Making (MADM) in CC infrastructure. The results of the experiment showed higher efficacy of MADM in identifying HTTP flooding attacks in the cloud environment, and that a higher MADM threshold value provided better efficiency than a lower MADM threshold value.

TABLE I. MACHINE LEARNING BASED IDS IN CLOUD

Paper	Algorithm Used	Objectives	Accuracy	FPR	DR
Kushwah et al. 2020[1]	V-ELM	To detect DDoS attacks in cloud	High	Low	High
Tonkal et al. 2021[59]	NCA+ML models	To detect DDoS attacks in SDN	High	Low	Medium
Sharma et al. 2019 [52]	ExtraTrees + ELM + Softmax	To classify many attacks	High	High	Low
Lopez et al. 2019 [35]	DT + RF + DNN	To detect DDoS attacks	Low	High	High
Sambangi and Gondi 2020 [48]	MLR model	To detect DDoS attacks	High	Low	Medium
Gumaste and Shinde 2020[26]	Apache Spark	To identify DDoS attacks in OpenStack-based Private Cloud	Low	High	Low
Ferrag et al. 2021 [22]	CNN + DNN + RNN	To detect intrusion in agricultural sector	High	Low	High
Kim et al. 2020[30]	CNN + RNN	To detect intrusion using DL models	Low	-	High
Aborujilah and Musa 2017[2]	Covariance matrix	To detect DDoS HTTP Attacks in cloud	Low	High	Low
Shen et al. 2020 [55]	MKELM	To detect intrusions	High	High	-
Somasundaram 2021[57]	Resource Scaling	To mitigate DDoS attack	High	High	Low

Shen, Y., et al., in [55] proposed a Mixed Kernel Extreme Learning Machine (MKELM) method integrating the ReliefF algorithm with nature inspired algorithms, for IDS. The MKELMs were developed to predict attacks, with the ReliefF algorithm providing inputs to the MKELM for selecting a suitable feature. The nature inspired algorithm determined the fitness function on the basis of kernel alignment, which was then used to build an optimum composite kernel in the MKELM. In [57] a novel approach was presented for evaluating resource consumption through 'scaling down' the resource i.e., through an improvement of the 'scale inside out' approaches. The presented approach utilized two modules- authentication model and elastic load balancing- to detect and mitigate DDoS attacks.

### B. Computational Intelligence based IDS Approaches in Cloud

Computational Intelligence approaches reviewed in this study include Bio-inspired algorithms, Evolutionary Computation algorithms and Swarm Intelligence algorithms. A detailed comparison of Computational Intelligence approaches reviewed in this SLR is given in Table II. A brief summary of these models follows. Bio-inspired algorithms aim to mimic natural biological patterns and behavior to develop novel ways to solve complex optimization problems [17]. Bio-inspired algorithms have been used to address major problems due to their features of adaptability, to attempt achievement of optimal solutions in cloud computing [12]. Bio inspired algorithms have been previously used to meet requirements of the cloud environment such as load balancing, provisioning of resources, and performance improvements, and may prove to be useful for adoption in IDS as well. Comparison of Bio-inspired algorithms for purposes such as sentiment analysis was described in [61]. Evolutionary Computation algorithms have been derived from biological evolution, and essentially aim 'to evolve' from an initial set of solutions to arrive at a best fit solution [20]. It is an approach in which different solutions adapt to different environments through processes similar to natural selection and breeding, so that only those which are truly fit and effective will survive the environment. Those which are not effective will not survive, but extreme conditions may result in mutations, similar to the biological analogy. Through iterations of this process, the best fitting solution to the problem is determined [28]. The population of potential solutions is first initialized randomly and the selection of solutions with the best fit through either survival or mutation mechanisms are devised; the rest are terminated. Evolutionary Computation has also been defined as the probable search performed for test data to be executed for a specific number of times by optimization algorithm based on Charles Darwin's theory of evolution [18]. It works on a potential solution with a permissible value for the variables coded for optimization problems, and is especially known for robustness and suited for complex domains of large numbers of variables [34]. The initialization of a population of solutions for a problem is first set at random, fitness of each individual solution in the

population is calculated, and the algorithm is run until optimization as initially defined is achieved or any of the defined stop conditions are achieved. The results are graded from very poor to good. Then, selection of pairs of individual solutions from the population results in recombination, with the resulting progeny subjected to mutation to maintain diversity. The resulting new generation solutions are evaluated for fitness, and a reinsertion process replaces the older generation solutions with fitness values which are lower than those of the new generation [62]. Swarm Intelligence algorithms emerged from observation of the behavior of social organisms, such as ants, wasps, bees and termites. Swarm Intelligence algorithms aim to mimic natural swarm behavior of organisms to forage for food or resources, to construct nests and to move in their environments. Swarm Intelligence algorithms follow five principles- proximity, quality, diverse response, stability and adaptability. Each possible solution to a problem is analogous to an organism in the swarm and has autonomy in behavior; the resulting emergence of self-organization in the swarm of solutions leads to adaptability to address the problem. The basis of self-organization includes amplification (positive feedback with the use of more resources) as well as stabilization (negative feedback to achieve counter balancing stability), random errors and multiple iterations of interaction between solutions in the swarm. Swarm Intelligence algorithms begin with in initialization phase to set the values of parameters, and continue to execute until defined stop conditions are achieved or stop is executed. Fitness function is evaluated for each solution and the Swarm Intelligence algorithm is updated mathematically based on the results. The fitness functions for each solution or search agent in the swarm leads to proposal of taxonomy and identification of the best fit solution to the problem. Swarm Intelligence algorithms have been used in optimization problems such as Agent Swarm Optimization (ASO) with the coexistence of different agents and their interaction, to ensure problem specificity, facilitation for testing and application to real-life problems [13]. One of the concepts significantly used in cloud computing is virtualization, as it enables higher resource utilization and lower operating costs. During virtualization, Computational Intelligence based optimization algorithms can play a vital role during the process of Virtual Machine Placement (VMP) scheduling. Such algorithms may be adopted for the purpose of IDS as well. Computational Intelligence algorithms are divided into two categories- Single-objective optimization algorithms and Multi-objective optimization algorithms. Examples for Single-objective algorithms include Ant Colony Optimization, Crow Search, Cuckoo Search, Fire Fly, Genetic, Grey Wolf Optimizer, Imperialist Competitive, Memetic, Particle Swarm Optimization, Simulated Annealing, and Whale Optimization Algorithm. Examples for Multi-objective algorithms include Biogeography-based Optimization, Krill Herd, Multi-Objective Evolutionary Algorithm, and Non Dominated Sorting Genetic Algorithm [37]. Taxonomy of Computational Intelligence intrusion detection techniques in mobile cloud computing environments was described in [49].

TABLE II. COMPUTATIONAL INTELLIGENCE BASED IDS IN CLOUD

Paper	Algorithm Used	Objectives	Accuracy	FPR	DR
Reddy et al.,2021 [28]	Crow Search Algorithm	To detect DDoS attacks	High	Low	High
Ahmad et al., 2018 [3]	Dendritic Cell Algorithm	To detect co-residency attack	High	-	-
Prathyusha et al., 2021[44]	Artificial immune system	To mitigate DDoS attacks	High	Low	High
Alharbi et al., 2021[6]	Local-Global best BAT Algorithm	To detect botnet attacks	High	-	-
Alamiedy et al., 2020[5]	Grey wolf optimization algorithm	To detect anomaly-based intrusions.	High	Low	High
Alsharafat 2020 [10]	Cuckoo Algorithm	To achieve intrusion detection	High	Low	High
Niemiec et al. 2021[42]	Multivariable heuristic technique	To detect intrusions using flag and entropy values	High	-	High

### C. Review of Hybrid Meta-Heuristic IDS Approaches in Cloud

Hybridization combines the benefits of different algorithms to form a hybrid algorithm with increased profitable synergy and minimization of disadvantages from the combination. This usually results in improved performance in terms of parameters such as computational speed, storage space and accuracy in detection of attacks. Hybrid algorithms may be classified into two types- Unified purpose hybrid algorithms, where the component algorithms are used to solve the same problem with each used at different stages; and Multiple purpose hybrid algorithms, where one primary component algorithm is used to solve the problem, while other component algorithms are used to alter the parameters of the primary algorithm. Hybrid algorithms may also be categorized as collaborative hybrid, involving a combination of two or more component algorithms run sequentially, or in parallel. These sequential or parallel runs can either comprise a single stage or have multiple stages. Another type of Hybrid algorithm is integrative hybrid, where

one algorithm is considered as a subordinate embedded into a master algorithm. It involves incorporation of operators manipulated by the subordinate algorithm into the master algorithm. The process of hybridization creates additional components but usually increases computational speed [33]. Two different algorithms could be hybridized by optimizing the parameters of both the algorithms to produce the best result. Different hybrid combinations are created and tested, in order to obtain overall best performance through experimentation. Because of the limitations of any standalone ML/DL method or Computational Intelligence algorithm, accomplishing optimum intrusion detection performance in a cloud environment requires hybridization. Since every approach has its merits and demerits, in this view, several authors have integrated the merits of two or more techniques in various aspects. For designing an effective hybrid IDS technique, the concept of mixing algorithms is essential. In this section, the hybrid IDS approaches developed for cloud environments are reviewed and a comparison is made in Table III.

TABLE III. HYBRID METAHEURISTIC INTELLIGENT IDS APPROACHES IN CLOUD

Paper	Algorithm Used	Objectives	Accuracy	FPR	DR
Moghanian et al. 2020 [40]	ANN+GOA	To detect network intrusion patterns	High	Low	High
Ali et al. 2018 [8]	ABC+BPNN	To detect DDoS attacks in cloud	Medium	Low	High
Osaniye et al. 2016 [43]	Ensemble-based multi-filter FS	To design ensemble of four filter approaches	High	-	-
Ghanem et al. 2020 [23]	ABC+DA+MLP	To detect intrusions by optimal training of MLP	High	-	High
Ghosh et al. 2021 [24]	Modified Firefly algorithm	To design IDS using feature selection approach	Low	High	Low
Mazini et al. 2019 [38]	ABC+AdaBoost	To develop a A-NIDS technique	High	-	High
Alharbi et al. 2021 [7]	Enhanced BA	To detect botnets in IIoT	High	Low	High
Bojović et al. 2019 [13]	Feature-based and volume-based detection	To design DDoS detection model	High	Low	High
Lv et al. 2020 [36]	KPCA-DEGSA-HKELM	To design IDS based on attack signatures	High	Low	Medium
Aslahi-Shahri et al. 2016 [11]	SVM+GA	To identify anomalies using hybrid method	High	Low	Low

In [27], a hybrid approach was presented which used an Artificial Neural Network (ANN) approach as a learning approach while a Swarm Intelligence algorithm- Grasshopper Optimization Algorithm- was used to reduce IDS errors. Ali et al. [28] presented a hybrid approach using a combination of Ant Colony Optimization (ACO) and Back Propagation Neural Network (BPNN). This hybrid approach was employed to detect DDoS attacks in the CC environment. Osanaiye, O., et al., in [43] proposed an ensemble based multifilter feature selection approach which integrated the output of 4 filter approaches to achieve optimal selection. The presented approach has been evaluated using standard datasets such as NSL-KDD. Ghanem, et al., [23] proposed a novel binary classification method for detecting intrusions, depending on the hybridization of Artificial Bee Colony (ABC) algorithm and Dragonfly algorithm to train an ANN and thereby increase the classification performance for non-malicious and malicious traffic in the network. The hybrid approach sets the initial parameters and appropriate weights for the ABC and Dragonfly algorithms. Ghosh, P., et al., in [24], proposed an IDS which provides security based on the concept of feature selection using Modified Firefly algorithm. The developed hybrid approach was evaluated on the NSL-KDD dataset and was found to consume lesser storage space due to the decreased number of dimensions from feature selection, and also require lower training time, thereby improving classification performance. A meta-heuristic algorithm based feature selection and recurrent neural network for DoS attack detection was proposed in [46]. Mazini, M., et al., in [38] proposed a novel hybrid approach for an Anomaly Network IDS, using ABC and AdaBoost algorithms to obtain higher detection rate and lower false positive rate. The ABC algorithm was used for feature selection and the AdaBoost algorithm was used for evaluation and classification of features. In [42], a novel multi-variable heuristic IDS was proposed, depending on distinct kinds of flags and values of entropy. The organizations distributed the data to improve the efficacy of IDS. Alharbi, A., in [6] proposed a Local Global Best Bat Algorithm with Neural Network (LGBBA-NN) for selecting hyper parameters and feature subsets for effective detection of botnet attacks. The presented hybrid approach adapted the inertia weights from the LGBB algorithm to update the parameters of the solution in the swarm. In order to address the swarm diversity for the solutions, a Gaussian distribution was employed during the initialization of the population. Bojović, P.D., et al., in [13] introduced a hybrid approach for detecting DDoS attacks, which combined volume and feature based detections. This method was dependent on an exponential moving average approach to make decisions, used on entropy values and packet number time sequences. Lv, L., Wang, et al., in [36] presented an approach for detecting several attacks on the basis of Hybrid Kernel Extreme Learning Machine (HKELM) model. This hybrid approach integrated the Gravitational Search Algorithm (GSA) and Differential Evolution (DE) algorithm to optimize the parameter of HKELM, which in turn enhanced its local and

global optimization capabilities at the time of predictive attack. A Kernel Principal Component Analysis (KPCA) method was presented for feature selection and reduction of number dimensions for the IDS. Aslahi-Shahri, B.M., in [11], presented a hybrid approach of Support Vector Machine (SVM) and Genetic Algorithm (GA) for execution of IDS. The presented hybrid approach was used to decreasing the number of features from forty-five to ten. The features were classified on the basis of priority, using the Genetic Algorithm.

## V. META ANALYSIS

Statistical analysis was performed for the above findings, using three performance metrics- Accuracy, False Positive Rate (FPR) and Detection Rate (DR), by classifying the performance of each algorithm as High, Medium or Low. Fig. 3 shows the ML based IDS approaches used in cloud environment, with the performance of the algorithms specified in terms of the three performance parameters. Algorithms employed in IDS must aim to decrease the FPR, since it represents the number of false alerts or alarms generated by the IDS, which may have a detrimental impact on cloud performance due to increase in computation time and storage space requirements of the IDS due to situations which are not really intrusions [9]. For this reason, having Low FPR is the most significant and important parameter for an effective IDS in the cloud environment. At the same time, algorithms must aim to increase Accuracy and Detection Rate, for obvious reasons.

Fig. 3 shows the comparison of ML based IDSs. First, 7 out of 11 ML based algorithms showed High Accuracy. Secondly, 4 out of the 11 ML based algorithms evaluated showed Low FPR. Thirdly, 4 out of the 11 ML based algorithms showed High Detection Rate. Incidence Rates for the desirable states of these parameters can be computed accordingly.

Fig. 4 shows the comparison of CI based IDSs. First, all 7 CI based algorithms evaluated showed High Accuracy. Secondly, 4 out of 7 CI based algorithms showed Low FPR. Thirdly, 5 out of 7 CI based algorithms showed High Detection Rate. Incidence Rates for the desirable states of these parameters can be computed accordingly.

Fig. 5 shows the comparison of Hybrid Meta-heuristic intelligent IDS approaches. First, 8 out of 10 hybrid approaches showed High Accuracy. Secondly, 8 out of 10 hybrid approaches showed Low FPR. Thirdly, 6 out of 10 hybrid approaches showed High Detection Rate. Incidence Rates for the desirable states of these parameters can be computed accordingly.

Among the three types of IDS- ML based, CI based and Hybrid Meta-heuristic- the Hybrid Meta-heuristic based IDS appear to have the highest overall incidence and scope for achieving the combination of High Accuracy, Low FPR and High Detection Rate.

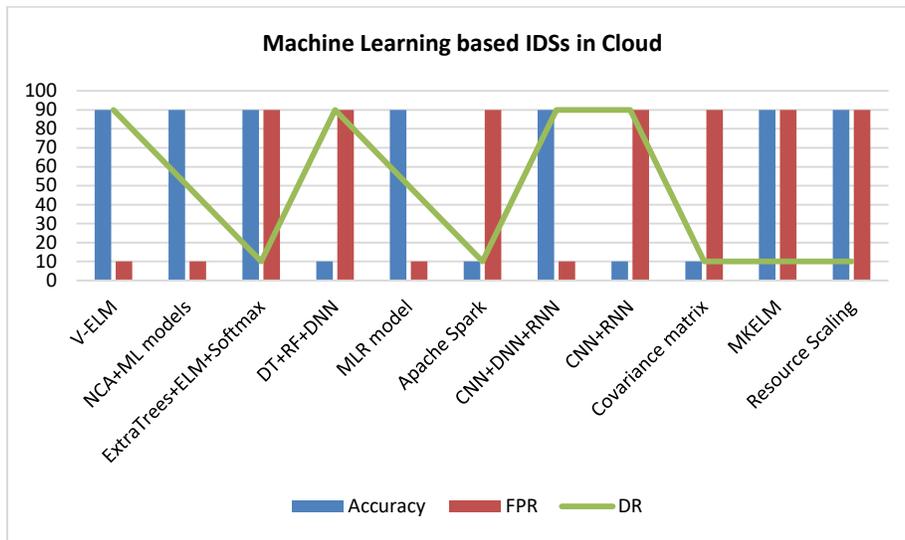


Fig. 3. Performance of Machine Learning based IDSs in Cloud.

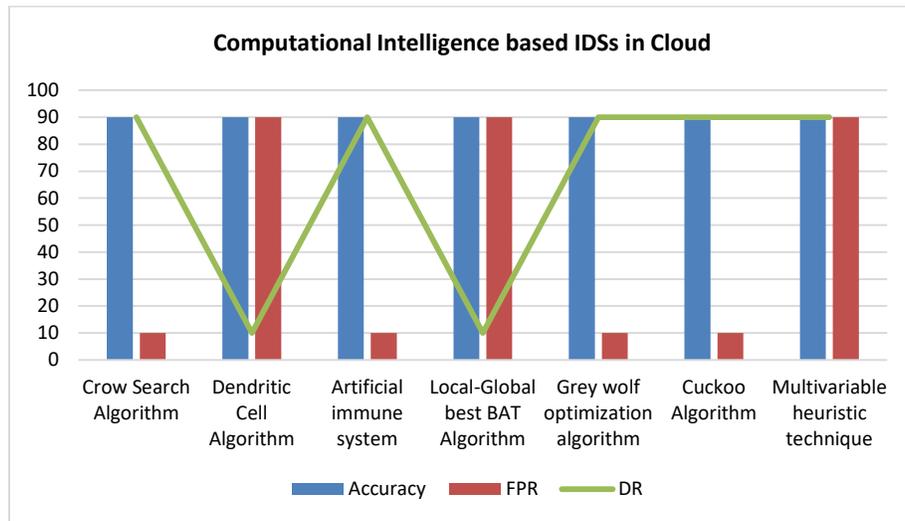


Fig. 4. Performance of Computational Intelligence based IDSs in Cloud.

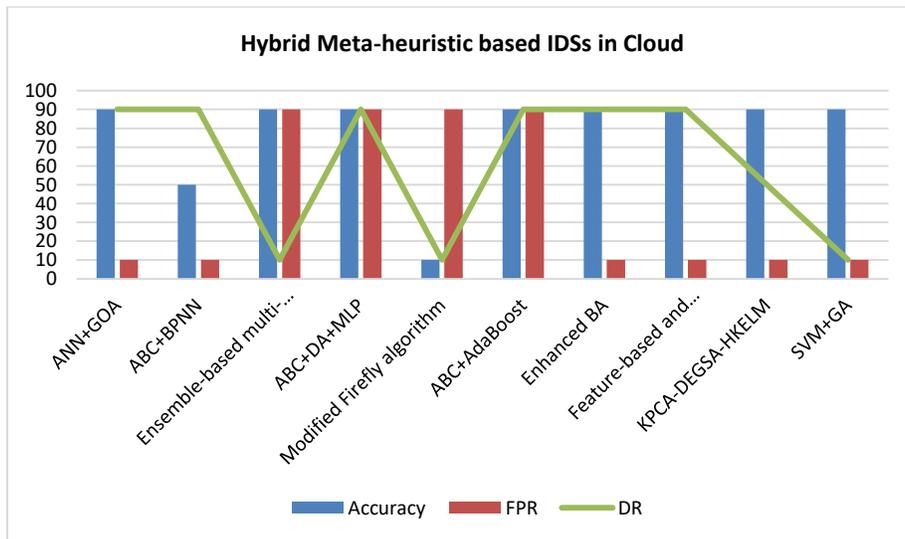


Fig. 5. Performance of Hybrid Meta-Heuristic Intelligent IDS Approaches.

TABLE IV. WEIGHTED SCORE ANALYSIS FOR INCIDENCE RATES FOR DESIRABLE STATES OF PARAMETERS

Type of IDS	High Accuracy	Low FPR	High Detection rate	Weight for Accuracy	Weight for FPR	Weight for Detection Rate	Weighted Score for IDS
Machine learning IDS	63.64%	36.36%	36.36%	20.00%	60.00%	20.00%	41.82%
Computational Intelligence IDS	100.00%	57.14%	71.43%	20.00%	60.00%	20.00%	68.57%
Hybrid IDS	80.00%	80.00%	60.00%	20.00%	60.00%	20.00%	76.00%

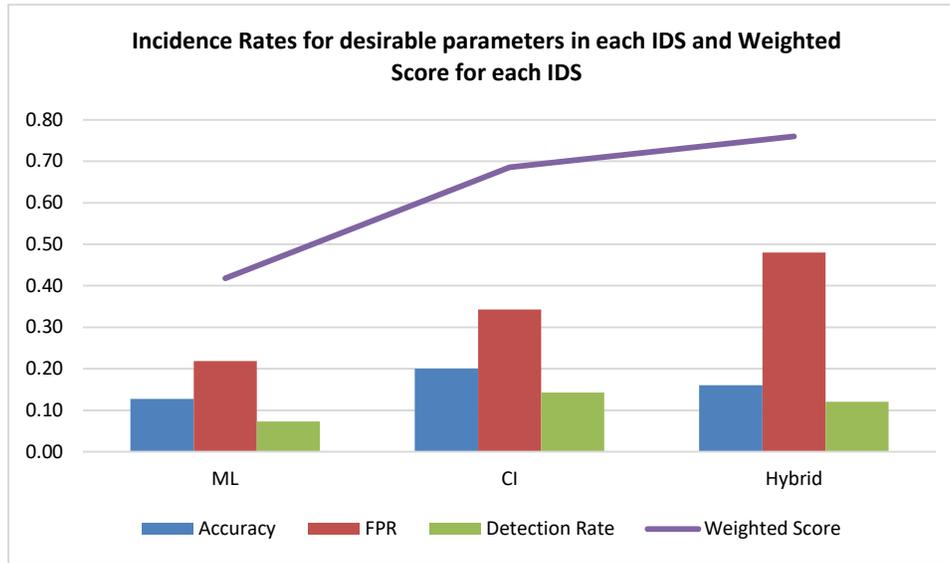


Fig. 6. Performance Comparison of IDS Approaches in Cloud.

Computation of incidence rates for desirable states of the three parameters (High Accuracy, Low FPR and High Detection Rate) across algorithms within each IDS was carried out, and using these incidence rates and associated weights assigned to parameters, a Weighted Score computed for each type of IDS. The results are presented in Table IV and plotted in Fig. 6. While the performance of Hybrid Meta-heuristic intelligent algorithms in terms of Detection Rate and Accuracy is marginally lower than that seen in Computational Intelligence algorithms, the performance is higher in terms of False Positive Rate, which is the parameter which has been assigned higher weight in determining the overall weighted performance score across the three parameters. From the results, the significance of potential adoption of Hybrid Meta-heuristic intelligent algorithms in IDS, to achieve the desirable performance states of High Accuracy, Low FPR and High Detection Rate is apparent.

## VI. OPEN CHALLENGES

This section discusses the major challenges that exist in the reviewed IDS models in the cloud environment.

- Existing IDS in the cloud environment only detect security-based events and are unable to block it. If many such events occur simultaneously, they could overwhelm the system. If the number of attacks or data breaches are very high in number, a valid threat may not be detected on time. Existing studies have not focused much on intrusion prevention.

- One of the major challenges in network-based IDS is that it cannot detect encrypted traffic without interception and decryption. In some organizations, the IDS decrypts traffic as it flows into the network. However, it will not be able to decrypt the traffic if the attacker uses a key to initiate encryption and decrypts the host.
- A high False Positive Rate is a significant and material open challenge to the execution of successful IDS. A system that generates high number of false alerts can potentially create serious business challenges for organizations, which may outweigh the benefits of even implementing the IDS itself.
- From the reviewed papers, it is evident that most of the IDS models have been developed using Machine Learning (ML) models and only a few works have concentrated on Deep Learning (DL) models. In addition, the experimental validation of the reviewed approaches should be extended to larger and real time datasets.
- In addition, the high number of dimensions of the IDS data-set should be carefully reviewed to reduce and discard irrelevant, and repetitive features. Feature selection techniques should be highly focused on minimizing the count of features in the data-set, to retain only essential features. Feature reduction and cluster techniques can be designed to boost the detection performance in large scale IDS datasets.

- Furthermore, the reviewed approaches are not designed for multi-objective formulation or multiple attacks detection, which needs to be further explored. Lastly, the offline IDS process needs to be extended to real time intrusion detection.
- The hybrid IDS technique should incorporate the combination of improved meta-heuristic optimization algorithms, to utilize their benefits.
- Most of the studies have focused on DoS and DDoS attacks. In future, IDS techniques should be designed to handle new and emerging types of attacks. The CC makes use of wireless networks for communication with the user system. Owing to few features of wireless networks such as resource limitations, mobility, and restricted bandwidth, issues related to network management and security need to be addressed. Based on the reviewer's works, hybrid methods may be employed for the detection of anomaly and signature based IDS in cloud environments.
- The choice of appraising classification model and feature selection is a major challenging issue in IDS. Therefore, it is important to design a rapid and precise IDS with minimal false positives and maximum true positives in a cloud environment.
- The choice of parameters has a significant influence in comparative analysis of various IDS approaches. Therefore, it is important to take into account any other parameter apart from the 3 parameters used in this study, which is considered significant and material for a particular IDS.
- On the other hand, the description of the implementation on setup can be a serious challenging problem for the cloud environment to accomplish security. In some cases, the models developed to improve the outcome of the IDS might be ineffective, resulting in false alarms owing to the inappropriate choice of evaluation criteria. The data integrity and security of information handled by cloud providers and probable susceptibilities which may result in data breaches need to be addressed in future. Based on the open issues and possible future directions, an effective IDS can be designed with respect to the consideration of the dimensions and features of the cloud environment.

#### VII. LIMITATIONS OF THE STUDY

The authors utilize Google scholar as a reliable electronic database that recommends highly relevant and effective studies depending upon the previous empirical works. But It could not be guaranteed that all selection is applicable studies. There is a chance that few significant works are not considered in the article selection process. Although this literature will provide an overall understanding utilization of an intelligent Intrusion Detection System in cloud environments and could be applied practically, this review article and its findings are theoretical only, which is one of the limitations of this study as it could not be reproduced in terms of practical implications. There is also a

limitation arising due to the 3 performance parameters selected, since some of the IDS approaches may theoretically perform better if other performance parameters were to be considered. Practical implementations are required to prove the benefits of the study.

#### VIII. CONCLUSION

This paper conducted SLR and Meta Analysis in order to evaluate the efficacy of Hybrid Meta-heuristic based IDSs in the cloud environment along three performance parameters, compared to two other types of IDS- ML based and CI based. The significance of various recent studies was summarized, and the performance of different algorithms/ approaches within each type of IDS was reviewed along the parameters of Accuracy, FPR and Detection Rate. The reviewed approaches were briefly explained, along with the merits and demerits. The open research issues which have to be addressed in future study have been discussed. The highlight of the study is the significance of potential adoption of Hybrid Meta-heuristic intelligent algorithms in IDS, to achieve High Accuracy, Low FPR and High Detection Rate. We strongly believe the outcome of this review study will be helpful to design new hybrid IDS approaches for cloud environments, particularly utilizing Meta-heuristic techniques.

#### REFERENCES

- [1] A. Chonka, Y. Xiang, W. Zhou, and A. Bonti, "Cloud security defence to protect cloud computing against HTTP-DoS and XML-DoS attacks," *J. Netw. Comput. Appl.*, vol. 34, no. 4, pp. 1097–1107, 2011
- [2] Aborujilah, A. and Musa, S., 2017. Cloud-based DDoS HTTP attack detection using covariance matrix approach. *Journal of Computer Networks and Communications*.
- [3] Ahmad, A., Zainudin, W.S., Kama, M.N., Idris, N.B. and Saudi, M.M., 2018, December. Cloud Co-residency denial of service threat detection inspired by artificial immune system. In *Proceedings of the 2018 Artificial Intelligence and Cloud Computing Conference* (pp. 76-82).
- [4] Aiyanyo, I.D., Samuel, H. and Lim, H., 2020. A Systematic Review of Defensive and Offensive Cybersecurity with Machine Learning. *Applied Sciences*, 10(17), p.5811.
- [5] Alamiedy, T.A., Anbar, M., Alqattan, Z.N. and Alzubi, Q.M., 2020. Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm. *Journal of Ambient Intelligence and Humanized Computing*, 11(9), pp.3735-3756.
- [6] Alharbi, A., Alosaimi, W., Alyami, H., Rauf, H.T. and Damaševičius, R., 2021. Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things. *Electronics*, 10(11), p.1341.
- [7] Alharbi, A., Alosaimi, W., Alyami, H., Rauf, H.T. and Damaševičius, R., 2021. Botnet Attack Detection Using Local Global Best Bat Algorithm for Industrial Internet of Things. *Electronics*, 10(11), p.1341.
- [8] Ali, U., Dewangan, K.K. and Dewangan, D.K., 2018. Distributed denial of service attack detection using ant bee colony and artificial neural network in cloud computing. In *Nature Inspired Computing* (pp. 165-175). Springer, Singapore.
- [9] Almseidin, M., Alzubi, M., Kovacs, S., & Alkasasbeh, M., 2017. Evaluation of machine learning algorithms for intrusion detection system. In *2017 IEEE 15th International Symposium on Intelligent Systems and Informatics (SISY)* (pp. 000277-000282). IEEE.
- [10] Alsharafat, W., 2020 The Cuckoo Feature Filtration Method for Intrusion Detection (Cuckoo-ID). *International Journal of Advanced Computer Science and Applications*, 11(5), pp. 341-347.
- [11] Aslahi-Shahri, B.M., Rahmani, R., Chizari, M., Maralani, A., Eslami, M., Golkar, M.J. and Ebrahimi, A., 2016. A hybrid method consisting of GA and SVM for intrusion detection systems. *Neural computing and applications*, 27(6), pp.1669-1676.

- [12] Balusamy, B., Sridhar, J., Dhamodaran, D. and Krishna, P.V., 2015. Bio-inspired algorithms for cloud computing: a review. *International Journal of Innovative Computing and Applications*, 6(3-4), pp.181-202.
- [13] Bojović, P.D., Bašičević, I., Ocovaj, S. and Popović, M., 2019. A practical approach to detection of distributed denial-of-service attacks using a hybrid detection method. *Computers & Electrical Engineering*, 73, pp.84-96.
- [14] Chattopadhyay, M., Sen, R. and Gupta, S., 2018. A comprehensive review and meta-analysis on applications of machine learning techniques in intrusion detection. *Australasian Journal of Information Systems*, 22.
- [15] Chavez, A., Lai, C., Jacobs, N., Hossain-McKenzie, S., Jones, C.B., Johnson, J. and Summers, A., 2019, April. Hybrid intrusion detection system design for distributed energy resource systems. In *2019 IEEE CyberPELS (CyberPELS)* (pp. 1-6). IEEE.
- [16] Chiba, Z., Abghour, N., Moussaid, K. and Rida, M., 2019. Intelligent approach to build a Deep Neural Network based IDS for cloud environment using combination of machine learning algorithms. *computers & security*, 86, pp.291-317.
- [17] Darwish, A., 2018. Bio-inspired computing: Algorithms review, deep analysis, and the scope of applications. *Future Computing and Informatics Journal*, 3(2), pp.231-246.
- [18] Elbeltagi, E., Hegazy, T. and Grierson, D., 2005. Comparison among five evolutionary-based optimization algorithms. *Advanced engineering informatics*, 19(1), pp.43-53.
- [19] Elmasry, W., Akbulut, A. and Zaim, A.H., 2021. A Design of an Integrated Cloud-based Intrusion Detection System with Third Party Cloud Service. *Open Computer Science*, 11(1), pp.365-379.
- [20] Elsayed, S.; Sarker, R.; Essam, D. Survey of Uses of Evolutionary Computation Algorithms and Swarm Intelligence for Network Intrusion Detection. *Int. J. Comput. Intell. Appl.* 2015, 14, 1550025
- [21] F. Gonçalves et al., "A Systematic Review on Intelligent Intrusion Detection Systems for VANETs," 2019 11th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT), 2019, pp. 1-10, doi: 10.1109/ICUMT48472.2019.8970942.
- [22] Ferrag, M.A., Shu, L., Djallel, H. and Choo, K.K.R., 2021. Deep Learning-Based Intrusion Detection for Distributed Denial of Service Attack in Agriculture 4.0. *Electronics*, 10(11), p.1257.
- [23] Ghanem, W.A.H., Jantan, A., Ghaleb, S.A.A. and Nasser, A.B., 2020. An efficient intrusion detection model based on hybridization of artificial bee colony and dragonfly algorithms for training multilayer perceptrons. *IEEE Access*, 8, pp.130452-130475.
- [24] Ghosh, P., Sarkar, D., Sharma, J. and Phadikar, S., 2021. An Intrusion Detection System Using Modified-Firefly Algorithm in Cloud Environment. *International Journal of Digital Crime and Forensics (IJDCF)*, 13(2), pp.77-93.
- [25] Giovanni Vigna and Christopher Kruegel. 2005. Host-Based Intrusion Detection, JWBS001C.
- [26] Gumaste, S. and Shinde, S., 2020. Detection of DDoS attacks in OpenStack-based private clouds using Apache spark. *Journal of Telecommunications and Information Technology*.
- [27] Iyengar, N.C.S., Banerjee, A. and Ganapathy, G., 2014. A fuzzy logic based defense mechanism against distributed denial of service attacks in cloud computing environments. *International journal of communication networks and Information security*, 6(3), p.233.
- [28] K. R. Krishnanand, S. K. Nayak, B. K. Panigrahi and P. K. Rout, "Comparative study of five bio-inspired evolutionary optimization techniques," 2009 World Congress on Nature & Biologically Inspired Computing (NaBIC), 2009, pp. 1231-1236, doi: 10.1109/ NABIC. 2009.5393750.
- [29] Khraisat, A., Gondal, I., Vamplew, P., Kamruzzaman, J. and Alazab, A., 2020. Hybrid intrusion detection system based on the stacking ensemble of c5 decision tree classifier and one class support vector machine. *Electronics*, 9(1), p.173.
- [30] Kim, J., Kim, J., Kim, H., Shim, M. and Choi, E., 2020. CNN-based network intrusion detection against denial-of-service attacks. *Electronics*, 9(6), p.916.
- [31] Kushwah, G.S. and Ranga, V., 2020. Voting extreme learning machine based distributed denial of service attack detection in cloud computing. *Journal of Information Security and Applications*, 53, p.102532.
- [32] Lee, S.W., Mohammadi, M., Rashidi, S., Rahmani, A.M., Masdari, M. and Hosseinzadeh, M., 2021. Towards secure intrusion detection systems using deep learning techniques: Comprehensive analysis and review. *Journal of Network and Computer Applications*, p.103111.
- [33] Letou, K., Devi, D. and Singh, Y.J., 2013. Host-based intrusion detection and prevention system (HIDPS). *International Journal of Computer Applications*, 69(26), pp.28-33.
- [34] Liang, Y., 2012. A Splicing/Decomposable Binary Encoding and Its Novel Operators for Genetic and Evolutionary Algorithms. *Bio-Inspired Computational Algorithms and Their Applications*, p.83.
- [35] Lopez, A.D., Mohan, A.P. and Nair, S., 2019. Network traffic behavioral analytics for detection of DDoS attacks. *SMU data science review*, 2(1), p.14.
- [36] Lv, L., Wang, W., Zhang, Z. and Liu, X., 2020. A novel intrusion detection system based on an optimal hybrid kernel extreme learning machine. *Knowledge-based systems*, 195, p.105648.
- [37] Masdari, M., Gharehpasha, S., Ghobaei-Arani, M. and Ghasemi, V., 2020. Bio-inspired virtual machine placement schemes in cloud computing environment: taxonomy, review, and future research directions. *Cluster Computing*, 23(4), pp.2533-2563.
- [38] Mazini, M., Shirazi, B. and Mahdavi, I., 2019. Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. *Journal of King Saud University-Computer and Information Sciences*, 31(4), pp.541-553.
- [39] Mishra, P., Pilli, E.S., Varadharajan, V. and Tupakula, U., 2017. Intrusion detection techniques in cloud environments: A survey. *Journal of Network and Computer Applications*, 77, pp.18-47.
- [40] Moghanian, S., Saravi, F.B., Javidi, G. and Sheybani, E.O., 2020. GOAMPLP: Network intrusion detection with multilayer perceptron and grasshopper optimization algorithm. *IEEE Access*, 8, pp.215202-215213.
- [41] Mthunzi, S.N. and Benkhelifa, E., 2017, September. Trends towards bio-inspired security countermeasures for cloud environments. In *2017 IEEE 2nd International Workshops on Foundations and Applications of Self\* Systems (FAS\* W)* (pp. 341-347). IEEE.
- [42] Niemiec, M., Kościej, R. and Gdowski, B., 2021. Multivariable Heuristic Approach to Intrusion Detection in Network Environments. *Entropy*, 23(6), p.776.
- [43] Osanaiye, O., Cai, H., Choo, K.K.R., Dehghantanha, A., Xu, Z. and Dlodlo, M., 2016. Ensemble-based multi-filter feature selection method for DDoS detection in cloud computing. *EURASIP Journal on Wireless Communications and Networking*, 2016(1), pp.1-10.
- [44] Prathyusha, D.J. and Kannayaram, G., 2021. A cognitive mechanism for mitigating DDoS attacks using the artificial immune system in a cloud environment. *Evolutionary Intelligence*, 14(2), pp.607-618.
- [45] Riaz, A., Ahmad, H.F., Kiani, A., Qadir, J., Rasool, R. and Younis, U., 2017. Intrusion Detection Systems in Cloud Computing: A contemporary review of techniques and solutions. *Journal of Information Science and Engineering*, 33, pp.611-634.
- [46] SaiSindhuTheja, R. and Shyam, G.K., 2021. An efficient metaheuristic algorithm based feature selection and recurrent neural network for DoS attack detection in cloud computing environment. *Applied Soft Computing*, 100, p.106997.
- [47] Salo, F., Injadat, M., Nassif, A.B., Shami, A. and Essex, A., 2018. Data mining techniques in intrusion detection systems: A systematic literature review. *IEEE Access*, 6, pp.56046-56058.
- [48] Sambangi, S. and Gondi, L., 2020. A Machine Learning Approach for DDoS (Distributed Denial of Service) Attack Detection Using Multiple Linear Regression. In *Multidisciplinary Digital Publishing Institute Proceedings* (Vol. 63, No. 1, p. 51).
- [49] Shamshirband, S., Fathi, M., Chronopoulos, A.T., Montieri, A., Palumbo, F. and Pescapè, A., 2020. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *Journal of Information Security and Applications*, 55, p.102582.

- [50] Shamshirband, S., Fathi, M., Chronopoulos, A.T., Montieri, A., Palumbo, F. and Pescapè, A., 2020. Computational intelligence intrusion detection techniques in mobile cloud computing environments: Review, taxonomy, and open research issues. *Journal of Information Security and Applications*, 55, p.102582.
- [51] Sharma, J., Giri, C., Granmo, O.C. and Goodwin, M., 2019. Multi-layer intrusion detection system with ExtraTrees feature selection, extreme learning machine ensemble, and softmax aggregation. *EURASIP Journal on Information Security*, 2019(1), pp.1-16.
- [52] Sharma, P., Sengupta, J. and Suri, P.K., 2019. Survey of intrusion detection techniques and architectures in cloud computing. *International Journal of High Performance Computing and Networking*, 13(2), pp.184-198.
- [53] Sharma, S. and Kaul, A., 2018. A survey on Intrusion Detection Systems and HoneyPot based proactive security mechanisms in VANETs and VANET Cloud. *Vehicular communications*, 12, pp.138-164.
- [54] Shelke, M.P.K., Sontakke, M.S. and Gawande, A.D., 2012. Intrusion detection system for cloud computing. *International Journal of Scientific & Technology Research*, 1(4), pp.67-71.
- [55] Shen, Y., Zheng, K., Wu, C. and Yang, Y., 2020. A Nature-inspired Multiple Kernel Extreme Learning Machine Model for Intrusion Detection. *KSII Transactions on Internet and Information Systems (TIIS)*, 14(2), pp.702-723.
- [56] Singh, S., Kubendiran, M. and Sangaiah, A.K., 2019. A review on intrusion detection approaches in cloud security systems. *International Journal of Grid and Utility Computing*, 10(4), pp.361-374.
- [57] Somasundaram, A., 2021. DDOS Mitigation In Cloud Computing Environment By Dynamic Resource Scaling With Elastic Load Balancing. *Turkish Journal of Computer and Mathematics Education (TURCOMAT)*, 12(11), pp.3346-3362.
- [58] Tama, B.A. and Lim, S., 2021. Ensemble learning for intrusion detection systems: A systematic mapping study and cross-benchmark evaluation. *Computer Science Review*, 39, p.100357.
- [59] Tonkal, Ö., Polat, H., Başaran, E., Cömert, Z. and Kocaoğlu, R., 2021. Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking. *Electronics*, 10(11), p.1227.
- [60] Wang, W., Du, X. and Wang, N., 2018. Building a cloud IDS using an efficient feature selection method and SVM. *IEEE Access*, 7, pp.1345-1354.
- [61] Yadav, A. and Vishwakarma, D.K., 2020. A comparative study on bio-inspired algorithms for sentiment analysis. *Cluster Computing*, 23(4), pp.2969-2989.
- [62] Yassin, W., Udzir, N.I., Muda, Z., Abdullah, A. and Abdullah, M.T., 2012, June. A cloud-based intrusion detection service framework. In *Proceedings Title: 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic (CyberSec)* (pp. 213-218). IEEE.
- [63] Zouhair, C., Abghour, N., Moussaid, K., El Omri, A. and Rida, M., 2018. A review of intrusion detection systems in cloud computing. *Security and Privacy in Smart Sensor Networks*, pp.253-283.

# Machine Learning Mini Batch K-means and Business Intelligence Utilization for Credit Card Customer Segmentation

Firman Pradana Rachman, Handri Santoso, Arko Djajadi

Master of Information Technology Department, Faculty of Science and Technology  
Pradita University, Tangerang, Indonesia

**Abstract**—An effective marketing strategy is a method to identify the customers well. One of the methods is by performing a customer segmentation. This study provided an illustration of customer segmentation based on the RFM (Recency, Frequency, Monetary) analysis using a machine learning clustering that can be combined with customer segmentation based on demography, geography, and customer habit through data warehouse-based business intelligence. The purpose of classifying the customers based on the RFM and machine learning clustering analyses was to make a customer level. Meanwhile, customer segmentation based on demography, geography, and behavior was to classify the customers with the same characteristics. The combination of both provided a better analysis result in understanding customers. This study also showed a result that minibatch k-means was the machine learning model with the rapid performance in clustering 3-dimension data, namely recency, frequency, and monetary.

**Keywords**—Customer segmentation; machine learning; business intelligence; data warehouse

## I. INTRODUCTION

Knowing customer needs is a way to win the competition in the market and increase company profits. By knowing what customers want, companies can create effective marketing strategies. Every customer has different needs and expectations, but some have similar or the same characteristics. One way to group several customers who have the same characteristics is to create customer segmentation. Customer segmentation is also the key to improving customer relationships. The process of information analysis to understand the market and customer is a part of a marketing strategy known as marketing intelligence.

Previous research used machine learning for customer segmentation. The type of machine learning used is unsupervised machine learning. One of them is using k-means [1] or using Hierarchical Clustering which is combined with PCA (Principal Component Analysis) technique [2]. Several other studies combine RFM (Recency, Frequency, Monetary) Analysis with K-means to determine customer ratings [3]. Some of these studies only make segmentation based on numerical values or predictive numbers generated by machine learning such as annual income and spending scores [1] or RFM Score [3], but do not grouping them with categorical and descriptive data. When there is a question, which city does the

customer group live in with the highest annual income? So, to get the answer, we must explore the data further.

Another problem is how to make the data well integrated. Well-organized data will facilitate analysis and report generation better. The quality of the data must also be considered. Problems in data such as duplication, different formats, incomplete and dirty data are things that must be overcome for better data governance [4].

Based on that fact, a research idea emerged that utilizes machine learning and business intelligence to create customer segmentation in a data warehouse platform. The information technology advancement enables the data to be processed and analyzed better. One of the examples is machine learning and business intelligence technology utilization. The use of machine learning can display predictive data, while business intelligence displays descriptive data. The integration and the combination of both will provide knowledge for a company in making an accurate business need. Data warehouse will make the data well integrated, stored for a long time and not interfere with data in the main system or transaction operations. Data quality can be handled well through the ETL (Extract, Transform, Load) process in the data warehouse [5].

This study discussed the utilization of machine learning and business intelligence built in the data warehouse platform using SQL Server. The outcome can be analyzed by marketing through dashboard and business intelligence reports. The data used here were the credit card transaction data for three months from banking companies in Indonesia. A machine learning model that can be used is unsupervised learning known as clustering. This study also tested some machine learning models of clustering to find a model with a rapid performance.

## II. THEORETICAL FRAMEWORK

Banking is any kind of activity in banks, including organizational business activities and the process. Meanwhile, a bank is a business entity operating the business activity. The function of a bank is collecting funds and also a distributor of credit to both individuals and business entities [6]. A bank has several types of loan products, such as working capital loans, investment loans, and consumer loans. A credit card is a part of consumer credit given to an individual in the form of a card that can be used for purchasing goods and services in shops, supermarkets, restaurants, etc.

Marketing Intelligence is a process of analyzing information to understand consumers, attitudes, and market behavior for accessing changes in a business and industrial environment to support the decision-making process [7]. Marketing intelligence consists of two parts, namely marketing research and customer relationship marketing database. Marketing research focuses more on the process of marketing planning, analyzing a situation, and building a strategy, while customer relationship marketing database focuses on data processing in a database.

Customer segmentation consists of a group of customers having the same needs and wants [8]. A segmentation group can be divided into 4 parts, namely.

- 1) Geography. It divides a market based on the location of the domicile, for instance, country, province, and city.
- 2) Demography. It divides a segmentation based on age, family, income, occupation, education, religion, etc.
- 3) Psychography. It is a part of psychological and demographic science in understanding consumers better, such as lifestyle or the value of life.
- 4) Behavior. This segmentation divides customers into several groups based on their habits, knowledge, or responses to a certain product.

Customer segmentation can also be performed based on Cost to Serve, Net Price, and relationship value [9]. Net Price and Cost to Serve are types of costs that can be measured. Relationship value has qualitative characters, and the value is determined intuitively by managers. This matrix is able to provide variability in making customer segmentation.

Another method in making customer segmentation is by using the RFM (Recency, Frequency, and Monetary) analysis. The purpose is to determine the customer level based on their purchase history [10]. This method consists of 3 dimensions, namely.

- 1) Recency. The last time a customer does a transaction. The Recency value is calculated from the difference of total days by subtracting the last date of transaction from the date of the current process. The lower value will be better.
- 2) Frequency. The frequency of a customer does a transaction. The higher value will be better.
- 3) Monetary. The amount of money spent. It is equal to Frequency that the higher value will be better.

A data warehouse is separate data storage from the primary application operating an operational transaction process. In this process, the data are transformed into information that can be analyzed by consumers [11]. The data process starts from data integration that has been extracted from the primary operational application and is transformed and loaded into a format that is appropriate to the data structure in the data warehouse. This process is known as ETL (Extract Transform Load).

The ETL process contains data cleaning, filtering, aggregate, and types of transformation. After the data are collected orderly, the data can be used for data mining or business intelligence. Business intelligence (BI) is defined as

data presentation to entrepreneurs to be used for gaining knowledge or making a business decision [11]. Business intelligence is an important part of business analytics because it produces effective analysis [12].

In making a business intelligence model, two tabulated models are generally used, namely.

- 1) A fact table is a table containing a transaction table consisting of numeric data that can be changed every day. For example, sales, purchase, finance, etc.
- 2) A dimension table is a table containing data category that generally the content rarely changes, and it will be used for data classification and aggregation contained in the fact table. For example, the Customer dimension table contains customer id, customer name, date of birth, address, and the like.

A schema in business intelligence is a group of tables consisting of dimension, fact, and attribute designed in differently according to the necessity. A schema consists of several types. They are as follows.

- 1) Star Schema. This schema puts the fact table in the center and the dimension table is placed around the fact table forming a star pattern. In the star schema, the dimension table with the same hierarchical data structure is placed in one table.
- 2) Snowflake Schema. This schema is different from the star schema model, whereby the dimension table is separated for the main category. For example, in the star schema, the data in the product table for product and product group is merged, while in the snowflake schema, both data are separated. Thus, in the end, the snowflake schema model looks like a snowflake.

Machine learning is a part of Artificial Intelligence (AI) allowing a system to learn from data rather than by explicit programming. Machine learning uses several repetitive algorithms by learning from data to improve, describe data, and predict results [13].

Unsupervised learning is a process of grouping unlabeled data. One of the utilizations is for clustering. The machine learning models for clustering are as follows.

- 1) Hierarchical Clustering. It works by forming a hierarchy or based on a certain level to appear like a tree structure. Thus, the clustering process is performed according to the level or step by step. Hierarchical clustering consists of two clustering, namely Agglomerative (bottom-up) and Divisive (Top-Down).
- 2) Balanced Iterative Reducing and Clustering using Hierarchies (BIRCH). It is an algorithm that can cluster big data by making a small and brief summary at first and storing information as much as possible. The smaller and brief summary is then grouped as a substitute for the larger data cluster. The mechanism of the first BIRCH algorithm is summarizing a group of big data into a smaller one that is known as Clustering Feature (CF) tree. Each node of this tree consists of some Clustering features (CF). Then, each node,

including a leaf node, has some CF; besides, the internal node CF has a pointer to sub-node, and all leaf nodes are linked by a doubly linked list.

3) K-means. This clustering algorithm is one of the non-hierarchical clustering methods that try to make partitions for the existing objects into one or more clusters or object groups according to the characteristics. Thus, the object with the same characteristics is grouped in one cluster and the object with different characteristics is grouped in another cluster.

4) Mini Batch K-means. This algorithm forms a minibatch consisting of a collection of small randomized data with a constant size enable to be stored in a memory. The mechanism is that the sample is taken randomly from the dataset to form a minibatch, and then it is assigned to the nearby centroid. In the second step, the centroid is updated and so on.

One of the ways to find the optimal total cluster is by using an elbow method. It is done by seeing the percentage of the comparison between the total clusters that will form an elbow in a certain point. This method can be illustrated through a line plot between SSE (Sum of Squared error) compared to the total cluster and finding a point that represents ‘an elbow point’ (the point after SSE or inertia starts decreasing in a linear fashion). Elbow method is often used in previous studies for determining the optimal number of clusters [14], [15], in addition to the silhouette coefficient method [16].

### III. RELATED WORK

A study on Customer segmentation using a machine learning method was the Fuzzy C-Means Clustering utilization for Customer Relationship Management (CRM) database on an online shop, namely tokodiapers.com [17]. Subsequently, another study focused on the implementation of k-means clustering on Recency-Frequency-Monetary (RFM)-based customer segmentation [18], [19]. Customer segmentation using PCA was combined with machine learning to make clustering [20]. The combination of K-means and ANN methods used SOM [21], [22]. Some other studies compared the clustering models between k-means, fuzzy c-means, Repetitive median K-Means [10], and between k-means, k-medoids, and DBSCAN [23].

Previous studies showed that business intelligence can be used for descriptive data in marketing strategy [24], social media analysis [25], travel companies [26], and can also be implemented in small-scale companies [27]. The business intelligence implementation can be combined with the data warehouse implementation. For example, business intelligence implementation using Higher Education data in Iran [28].

Based on literature studies and previous research, this study offers a complete and different solution for customer segmentation. First, customer segmentation based on RFM analysis creates customer levels combined with Geographic, Demographic, Psychographic and Behavioral to classify customers with the same characteristics. Second, the data is presented in business intelligence reports and is based on a data warehouse. Finally, the research will test several clustering models to find the fastest model.

### IV. RESEARCH METHODOLOGY

This study was conducted through several phases as shown below.

#### A. Understanding the Business Process

In this phase, it was done by seeking information on how customer segmentation was implemented. There were two methods. They are as follows.

1) Literature study. It was performed by reading relevant books and journals.

2) Conducting a field observation and interview with users.

Based on these processes, it can be inferred that 2 methods of customer segmentation will be implemented. First, customer segmentation was ranked based on the RFM (Recency, Frequency, Monetary) analysis [10], and the second method was customer segmentation based on Geography, Demography, Psychography, Behavior [8].

#### B. Analysis Data

The study used secondary data taken from the credit card transaction history in bank XYZ in Indonesia for three months, namely October to December 2020. There are five CSV (Comma Separated File) format files that will be used, namely.

1) Cc\_transaction.csv is credit card transaction data whose information consists of customer id, category id, transaction date, amount in foreign currency, currency, card number, payee account and payee name.

2) Category.csv is shopping category data whose columns consist of category id, category name and group category.

3) Currency.csv contains a list of currencies consisting of the following columns currency id, currency code and currency name.

4) Customer.csv contains data from customer profiles consisting of customer id, customer name, gender, marital, grade, profession, address1, address2, postal code, open date, birthday, city, and province.

5) Rate.csv contains exchange rate information for all currencies consisting of currency id, date and rate.

#### C. Designing a Data Architecture and Data Flow

This phase consisted of designing tables, data architecture, and the data flow. The column structure of the created table must match the format and content of the data.

#### D. Preparation Process in the Data Warehouse

This phase consisted of an ETL (extract, transform, and load) process. The data in this phase were processed through cleaning, filtering, and normalization, thus, the data entering the database were neat and clean data. The data from the ETL process were imported into a staging table and then processed into a fact and dimension table for the needs of business intelligence and a table of RFM analysis for the machine learning process.

#### E. The Process of Machine Learning

It consisted of several stages as seen below.

1) Feature selection. The data were taken from the table of RFM analysis that was made in the preparation process in the data warehouse.

2) The production of a machine learning model. This stage consisted of several tests for machine learning clustering to find the rapid model. The models being tested here were agglomerative hierarchical clustering, Balanced Iterative Reducing and Clustering Using Hierarchies (BIRCH), K-means, and Mini Batch K-means.

3) Optimizing the total clustering. This stage was done to find the optimum total clusters using an Elbow method.

4) Implementation of clustering model. The machine learning model selected is the fastest from the previous testing process. The number of clusters is in accordance with the recommendations of the elbow method.

**F. Business Intelligence Process**

It consisted of several steps as follows.

1) The tables of load from the machine learning process and ETL at data warehouse.

2) Making a dimension model and the relationship between those tables. At this stage, it will be decided to use the star schema or snowflake model.

3) Design and dashboard visualization. This stage aims to design and present data in a business intelligence portal. The data displayed is a summary of the clustering results of machine learning and demography, geography, and customer habits. On the other hand, it displays detailed data from transaction history and customer profiles. History data is also available for each transaction and customer grouping. All data can be selected and filtered based on the results of machine learning clustering, year and month.

**V. RESULT AND DISCUSSION**

**A. The Process in the Data Warehouse**

The result from the observation and analysis was an illustration of how to design the data architecture and data

flow. The following is an illustration of the data architecture and data flow.

From the Fig. 1 we can see that the first process is data processing from the server of core banking and then it is integrated into SQL server database as data warehouse through an ETL (Extract, Transform, and Load) process using SQL commands (bulk insert method). The result of the ETL process was stored in the staging table. Subsequently, two processes were done; first, the data from the staging table were processed into a fact table and dimension table through the SQL demand. Second, the data from the staging table formed an RFM \_analysis table that would be used as a feature selection for a clustering process in machine learning. Processes in machine learning using Python with the Scikit-learn library. The result obtained from the machine learning process was exported into a dimension table and a fact table.

The outcome of the machine learning process and the ETL process in the data warehouse was forming a dimension table and a fact table used for a modeling process in the business intelligence. The detail of processes and data structure can be seen in Fig. 2.

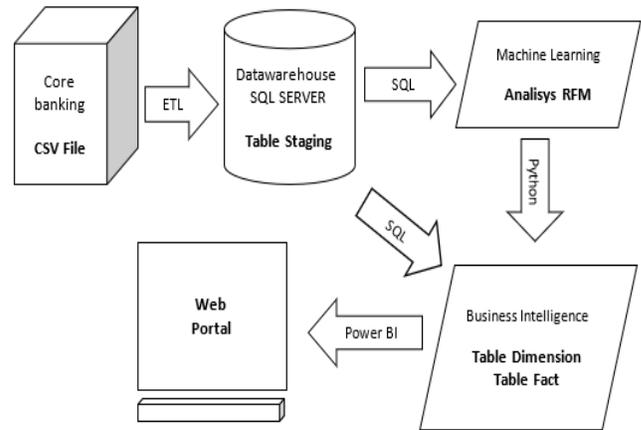


Fig. 1. The Design of Data Architecture and Data Flow.

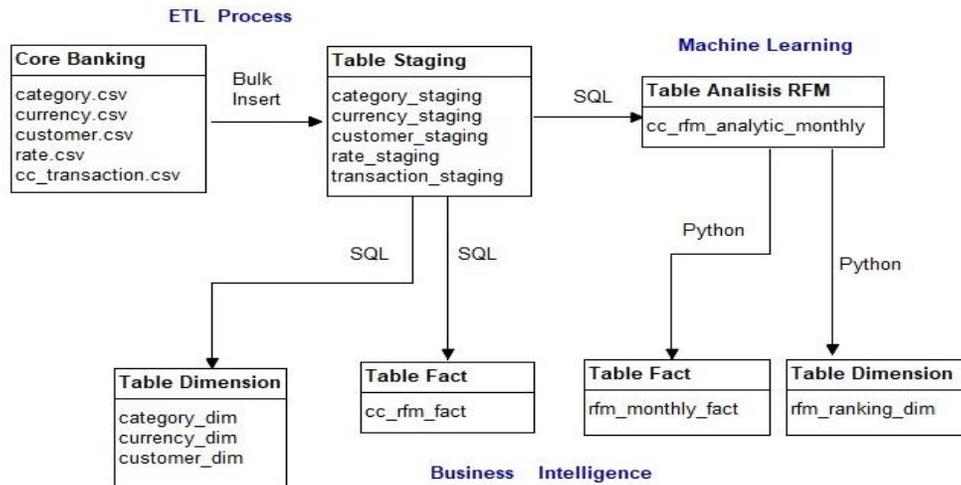


Fig. 2. Detail of Data Flow.

B. Machine Learning Process

The data used in this process was an RFM analysis table that was made in the ETL process previously. The content consisted of the summary of recency, frequency, and monetary values based on customer per month and per year as shown in Table I.

TABLE I. CC\_RFM\_ANALYTIC\_MONTHLY TABLE

Customer id	Recency	Frequency	Monetary	Month	Year
190003214887	22	1	79000	12	2020
190000291053	1	4	845800	12	2020
190001424933	1	2	831608	12	2020
190002882666	3	1	540000	11	2020
190001940395	8	3	3317177	10	2020
190003283225	7	5	1611053	12	2020
190003229073	11	1	79000	12	2020

The next process was testing the machine learning clustering model aiming at seeking a clustering model with a rapid performance. The first trial test was conducted using the data with a range of 3 months from the staging table. Overall, the total data was 46.079 rows. The test was conducted using a trial test on 2 up to 5 clusters. The computer specification used here was Intel Core i3 6006U 2 GHz, Memory 12 GB, Hard disk SSD 512 GB, and VGA Nvidia GeForce 940MX with 2GB dedicated VRAM. The Table II illustrates the detail of the test result showing the speed of the clustering process done in a second.

TABLE II. THE SPEED DIFFERENCES BETWEEN CLUSTERING MODELS

Model	2 Clusters (second)	3 Clusters (second)	4 Clusters (second)	5 Clusters (second)
Agglomerative	Error Memory	2856	2700	2239
BIRCH	31	20.36	20.03	20.01
Kmeans	1.32	1.45	1.76	2.24
Minibatch Kmeans	1.47	1.40	1.18	1.08

From the Table II, agglomerative clustering has the longest clustering process; even when trying to perform a clustering process with 2 clusters, an error message appears stating that not enough memory. BIRCH occupies the third rank for better performance than agglomerative clustering. Meanwhile, K-means reaches a far better performance than BIRCH and agglomerative clustering. Nevertheless, in general, the performance of minibatch k-means is faster with the longest duration of 1.47 seconds for 2 Clusters.

TABLE III. THE CALCULATION RESULT OF RFM TABLE IN OCTOBER 2020

Cluster	R_means	R_score	F_means	F_score	M_means	M_score	Score	Segment	Label
0	0.81	1	0.01	1	0.08	3	5	113	At Rsik
1	0.46	2	0.02	2	0.08	1	5	221	Keep
2	0.16	3	0.06	3	0.37	4	11	344	Royal
3	0.13	4	0.03	4	0.08	2	9	432	Potensial

The experimental results in Table II show that when the number of clusters increases, the clustering process becomes faster. This happens for clustering using agglomerative, birch and minibatch kmeans, but for kmeans the opposite happens. The unique thing is that when using 2 clusters, the kmeans algorithm is better than the mini batch kmeans. However, when trying 3 or more clusters, the minibatch kmeans performance is superior.

The machine learning Mini Batch K-Means model is finally chosen because it is the rapid model in performing a clustering. The next phase was selecting the optimal number of clusters from the data. The method used here was the elbow method. The result shows that the total optimal cluster in each month is 4 clusters. It is shown from the intersection of lines forming a perpendicular line as a visualization of an elbow method in Fig. 3.

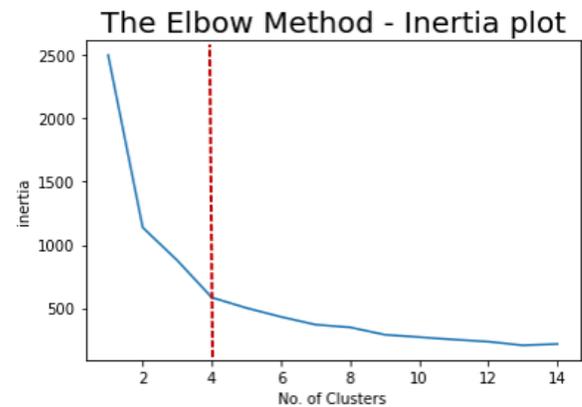


Fig. 3. A Graph of an Elbow Method in December 2020.

Before the data modeling, it was normalized using a Min-Max score. This process was aimed at making the data have the same range from 0 to 1. Therefore, data visualization in the form of a graphic becomes more precise. The formula used in this Min-Max method as shown in (1).

$$X_{new} = \frac{(X_{old} - X_{min})}{(X_{max} - X_{min})} \tag{1}$$

Xold is the former score. Xmin is the minimum score and Xmax is the maximum score in the data range.

The clustering prediction was done using minibatch k-means with a total of 4 clusters. After grouping the data using machine learning, the recency, frequency, and monetary scores of each datum were calculated. The scoring was done by ranking the data. The best one was scored 4 and the lower one was scored 3 and so on. The following is the calculation result of the RFM score for October 2020 in Table III.

From the Table III, it can be inferred that the highest score is cluster 3 with a score of 11 points. Even though the score is the highest, cluster 3 does not have the highest recency score since the best recency score is occupied by cluster 1. Meanwhile, the lowest score is occupied by clusters 0 and 2 with the same score of 5. However, cluster 0 is considered the lowest since it has the lowest recency and frequency scores. Subsequently, each of these clusters is labeled according to their class. The highest cluster is cluster 3 labeled with Royal; the cluster below cluster 3 is cluster 1 labeled with Potential. Then, clusters 2 and 0 are labeled with Keep and At-Risk respectively.

Clusters with the Royal label are the most important and loyal customers because the number of shopping transactions is the largest and the shopping frequency is the most frequent. Meanwhile, the group of potential clusters are customers who have the potential to become loyal credit card users, because the recency value is higher even though the amount and frequency of shopping are smaller. It is possible that the group from this cluster is a new customer. Clusters with the labels At Risk and Keep must be considered, because in this group they rarely shop in large quantities. The same grouping was also done for the data in November and December 2020. The following is the 3D visualization of customer clustering in October 2020 in Fig. 4.

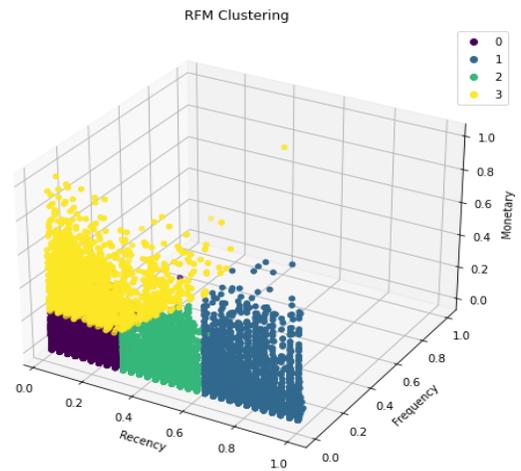


Fig. 4. 3D Visualization of Clustering for the Data in October 2020.

### C. Business Intelligence Process

The table containing the result of ETL and Machine Learning processes is loaded into the business intelligence model. The modeling schema is made using a Star Schema by placing two fact tables, namely *cc\_rfm\_fact* and *rfm\_monthly\_fact*. Meanwhile, the other dimension tables are around the two fact tables as shown in Fig. 5.

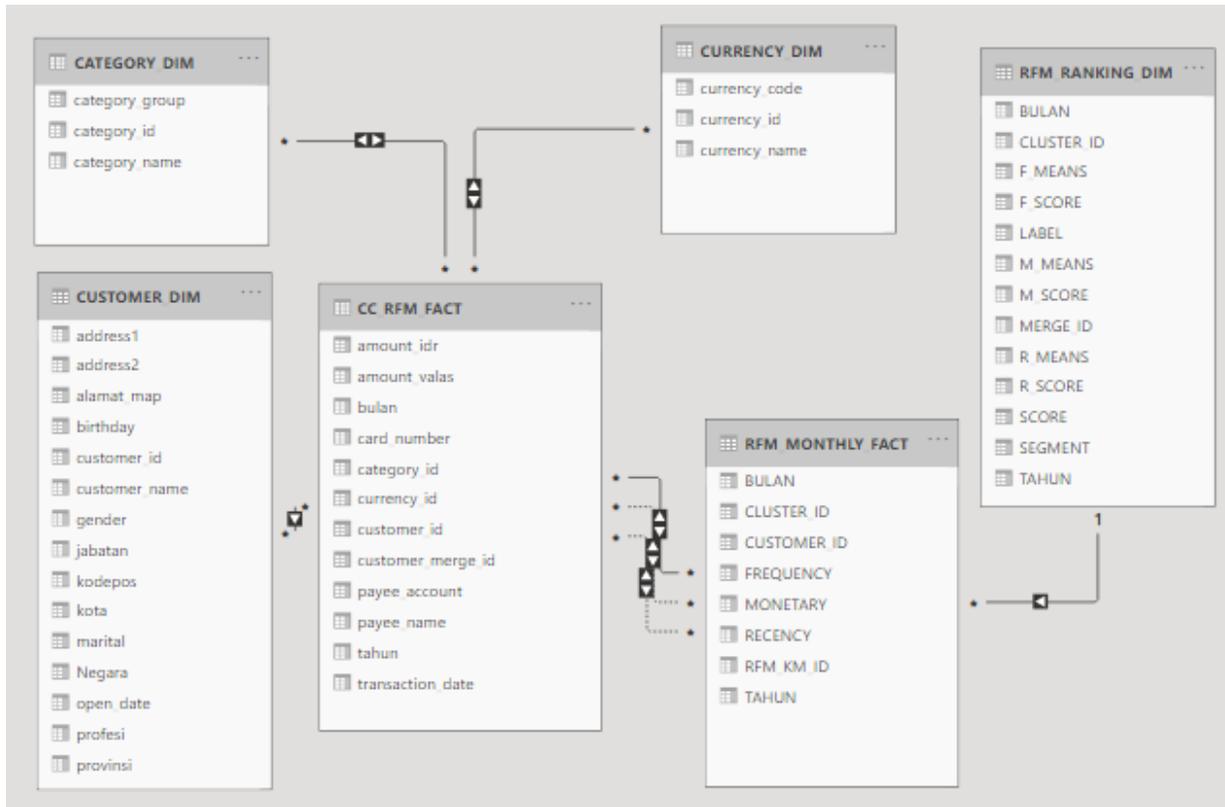


Fig. 5. Dimensional Modeling with a Star Schema.

The dashboard in the business intelligence consists of several parts as follows.

1) Main Dashboard. It displays a summary and aggregate data from all data. The top side has filtering based on year, month, and cluster choices. Besides filtering, there is a scorecard containing segmentation information of cluster, RFM score, and total customer, average recency score, average frequency score, and average monetary score. Meanwhile, the central side has a bar graph showing data on shopping habits based on the shopping category. The

demographic data, such as profession, sex, and marital status, are in the form of a pie chart or doughnut chart. On the right side, there is information about transaction amount based on the currency. The complete illustration can be seen in Fig. 6.

2) Distribution map. It shows the number of customer distribution based on the province and regency. The data are presented in the form of an Indonesian map. There is filtering on the top side according to customer segmentation, year, and month as shown in Fig. 7.

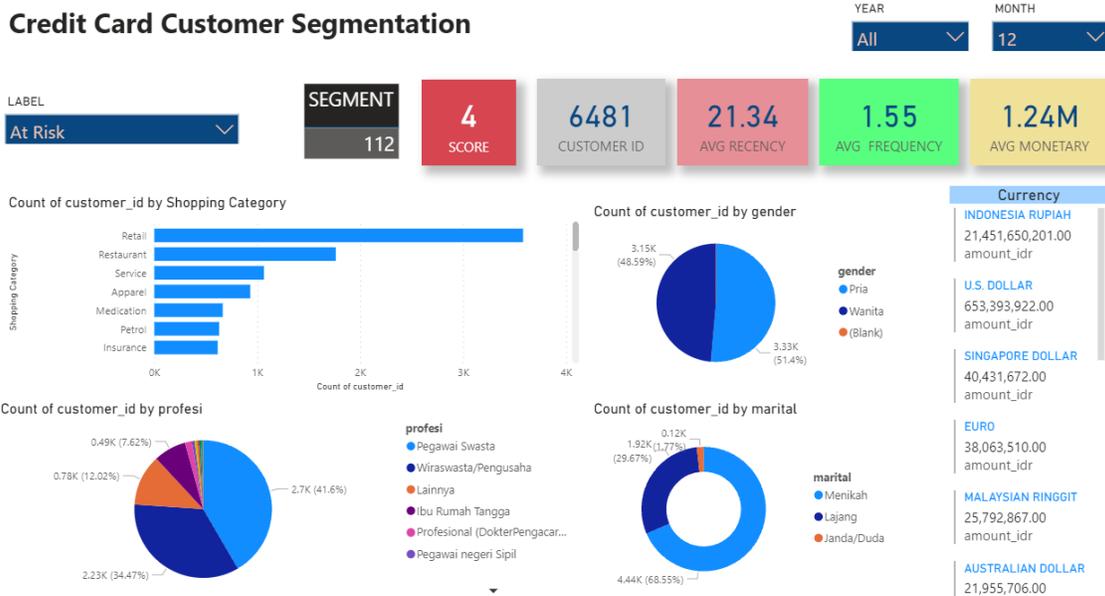


Fig. 6. The Dashboard Main Menu of Business Intelligence Portals.



Fig. 7. Customer Distribution in the Form of a Geographic Map.

3) Transaction detail. It displays detailed data of each customer transaction. The column consists of customer-id, transaction date, category id, payee account, payee name, and the amount in Indonesian rupiah (IDR). This information can be filtered based on the label, year, and month through a slicer on the top side as shown in Fig. 8.

customer_id	transaction_date	category_id	payee_account	payee_name	amount_idr
19000332885	04 November 2020	34	0000000000	(L)HYEONDAEBAE@HDAEJOM HINCHEON KR	175.000,00
19000210676	11 December 2020	20	0008000265	*ASTRA (SUZU) FRAMUKA JAKARTA TIMURID	153.855,00
19000152352	15 October 2020	20	0003999021	*AUTO 2000 DENPASAR ID	640.992,00
19000151795	14 November 2020	20	0008000831	*AUTO 2000 WAY HALIM BANDARLAMPUNGID	793.402,00
19000320147	14 December 2020	20	0002198115	*AUTO0000 KAPUK (SS) JAKARTA BARATID	2.439.273,00
190003256716	05 November 2020	20	0002198115	*AUTO0000 KAPUK (SS) JAKARTA BARATID	3.060.624,00
19000185648	20 November 2020	20	0002198117	*AUTO0000 YOS SUDARSO (SS)JAMKARTID (UTARAD)	1.536.817,00
190002189018	15 December 2020	20	0002198117	*AUTO0000 YOS SUDARSO (SS)JAMKARTID (UTARAD)	2.539.288,00
190003502727	11 December 2020	20	0008000499	*TSD A YANI BANJARMASIN BANJARMASIN ID	629.400,00
190002419887	10 December 2020	20	0005009741	0K29-SALD-GREEN LAKE TN TANGERANG ID	1.169.000,00
19000390463	03 November 2020	34	0704146170	07SC RADI RAVIA CIRVUNG Jakarta TimurID	232.294,00
19000358859	09 November 2020	35	45467812993	1 MONTH PLAN RIVERDALE US	132.300,00
19000288859	09 November 2020	35	45467812993	1 MONTH PLAN RIVERDALE US	128.983,00
19000288859	09 December 2020	35	45467812993	1 MONTH PLAN RIVERDALE US	128.990,00
19000305607	19 October 2020	20	07040223334	1 STATION TAMAN SUREJA Jakarta BaratID	5.562.000,00
<b>Total</b>					<b>22.324.527.686,00</b>

Fig. 8. The Detail of Credit Card Transaction.

4) Customer Detail. It displays the data of customer-id, customer name, sex, position, profession, marital status, zip code, and date of birth. As in the transaction detail, on the top side, there is a slicer to filter the data based on the segmentation, year, and month.

5) Forecasting Credit Transaction. It contains credit card transaction predictions in the next few days. Forecasting uses an Exponential Smoothing method that has been available in the Power BI application. Exponential Smoothing is a forecasting method of a moving average providing an exponential or graded weight in the latest data [29]. The graph can be seen in Fig. 9.

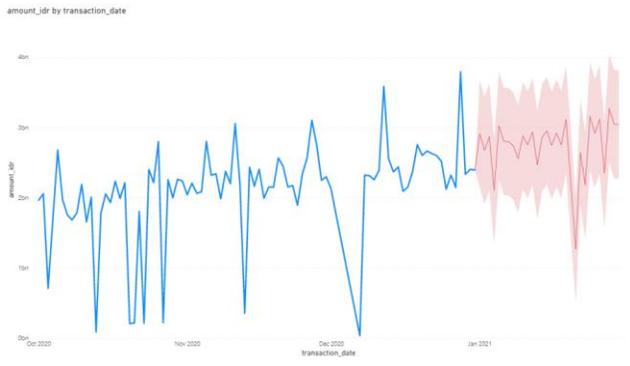


Fig. 9. Forecasting of the Amount of Credit Card Transactions.

6) Transaction History. Show in Fig. 10, displays the transaction history based on the shopping category per month in tabular form to the side part. The far-right column contains a difference in the amount in December takes away the amount in November. If the difference is positive, it shows a green color. Meanwhile, if the difference is negative, it shows red color. The top side has filtering according to year.

category_name	October	November	December	Des - Nov
Apparel	3,075,197,591.00	4,254,841,188.00	4,236,944,676.00	-17,896,512.00
Audiovisual	118,202,603.00	342,195,575.00	311,534,295.00	-30,661,280.00
Beauty	1,199,893,787.00	1,508,490,744.00	1,243,242,324.00	-265,248,420.00
Cable TV	508,488,413.00	535,240,027.00	435,049,743.00	-100,190,284.00
Cafe	195,890,266.00	282,546,223.00	252,343,846.00	-30,202,377.00
Donation	82,429,750.00	85,649,935.00	40,145,798.00	-45,504,137.00
Education	162,083,988.00	178,586,153.00	190,599,805.00	12,013,652.00
Electronic	1,472,025,933.00	1,640,861,952.00	1,600,953,704.00	-39,908,248.00
Entertainment	897,517,521.00	725,555,122.00	477,125,279.00	-248,429,843.00
E-Wallet	2,655,443.00	4,944,338.00	10,524,936.00	5,580,598.00
Food & Drink	269,773,613.00	369,991,721.00	432,750,513.00	62,758,792.00
Gadget	46,924,224.00	31,810,850.00	31,070,300.00	-740,550.00
Games	451,596,632.00	448,844,763.00	385,277,388.00	-63,567,375.00
Gas & Electricity & Water	12,039,276.00	25,681,028.00	17,643,363.00	-8,037,665.00
Hobby	250,683,519.00	314,949,311.00	315,424,782.00	475,471.00
Insurance	4,737,119,517.00	6,383,239,183.00	4,938,243,182.00	-1,444,996,001.00
Lodging	1,028,829,942.00	1,403,979,509.00	1,594,240,926.00	190,261,417.00
<b>Total</b>	<b>53,169,212,314.00</b>	<b>67,723,124,723.00</b>	<b>62,164,839,832.00</b>	<b>-5,558,285,285.00</b>

Fig. 10. Monthly Credit Card Transaction History.

7) Customer History. The data show a monthly customer history shown in a tabular form. There is a column showing a gap between the amount in December and the amount in November. If the value is positive, it shows green; if the value is negative, it shows red. The variable of the data presented according to year can be selected, either frequency, recency, monetary, or RFM score. The illustration can be seen in Fig. 11.

CUSTOMER_ID	OKTOBER	NOVEMBER	DECEMBER	DEC-NOV
190000000882	3	0	0	0
190000001432	1	1	2	1
190000001467	3	2	11	9
190000001950	1	1	2	1
190000002584	1	2	2	0
190000002884	5	0	0	0
190000003577	0	1	2	1
190000003672	1	4	3	-1
190000004082	1	0	0	0
190000004200	1	2	0	-2
190000004706	1	0	4	4
190000007237	2	0	0	0
190000007238	2	4	4	0
190000007606	0	0	2	2
190000007617	0	1	4	3
190000008250	0	1	0	-1
<b>Total</b>	<b>101445</b>	<b>121569</b>	<b>110791</b>	<b>-10778</b>

Fig. 11. Monthly Credit Card Customer History.

## VI. CONCLUSION

This study makes a segmentation using a machine learning clustering model and business intelligence in the customers of data warehouse-based credit cards. The data warehouse concept utilization is used for constructing an integrated data management system that can handle a large amount of data. The machine learning clustering model is used for grouping customers according to a rank to know the most loyal customers and inactive customers. This clustering uses the RFM (Recency, Frequency, and Monetary) analysis as the measurement variable and feature selection in the clustering process. The RFM analysis is chosen because it can present customer loyalty based on their shopping behavior, such as the last time of shopping (recency), the frequency of shopping (frequency), and the amount of money spent for shopping (monetary).

The data from the machine learning clustering process are combined with other data and presented in the form of a business intelligence portal dashboard. The dimension modeling process uses a star schema because it is superior in terms of speed compared to the snowflake schema. The data and graphics displayed in the business intelligence portal present the segmentation data according to demography, geography, and behavior.

The combination of machine learning clustering segmentation for ranking customers with segmentation based on the demography, geography, and behavior provides complete and strong information as a support in a business decision for a marketing department. For example, the marketing department wants to increase the customers' credit card transactions by a limited promotional budget. First, he/she will see a group of customers having a relatively low RFM score. Then, from the group, the city with the highest number of customers is observed. Thus, the marketing department can effectively promote to a group of customers with the same characteristics.

This study also shows the minibatch k-means clustering algorithm has faster performance than that of agglomerative hierarchical clustering, BIRCH, and k-means algorithms. The result shows that out of 46.097 rows of data, the minibatch k-means method is superior to agglomerative clustering, BIRCH is superior with a thin margin to k-means. Some clusters are tested using an elbow method. The result shows that the best and optimal cluster is 4 clusters.

### REFERENCES

- [1] M. Pradana, "Maximizing Strategy Improvement in Mall Customer Segmentation using K-means Clustering," *J. Appl. Data Sci.*, vol. 2, no. 1, pp. 19–25, 2021, doi: 10.47738/jads.v2i1.18.
- [2] A. Abdulhafedh, "Incorporating K-means, Hierarchical Clustering and PCA in Customer Segmentation," *J. City Dev.*, vol. 3, no. 1, pp. 12–30, 2021, doi: 10.12691/jcd-3-1-3.
- [3] J. Wu et al., "An Empirical Study on Customer Segmentation by Purchase Behaviors Using a RFM Model and K -Means Algorithm," *Math. Probl. Eng.*, vol. 2020, no. November 2017, 2020, doi: 10.1155/2020/8884227.
- [4] M. McCaig and D. Rezanía, "A Scoping Review on Data Governance," *SSRN Electron. J.*, no. Iccinis, 2021, doi: 10.2139/ssrn.3882450.
- [5] M. Souibgui, F. Atigui, S. Zammali, S. Cherfi, and S. Ben Yahia, "Data quality in ETL process: A preliminary study," *Procedia Comput. Sci.*, vol. 159, pp. 676–687, 2019, doi: 10.1016/j.procs.2019.09.223.
- [6] M. Supriyono, *Buku pintar perbankan*. JOGjakarta: Andi Offset, 2011.
- [7] A. Amborowati and M. Suyanto, "Studi Dukungan Marketing Intelligence pada Strategi Pemasaran," *Semin. Nas. Inform.* 2015, vol. 2015, no. November, pp. 49–53, 2015.
- [8] P. Kotler and K. L. Keller, *Marketing Management*, 15th ed. Harlow: Pearson, 2016.
- [9] P. Kolarovszki, J. Tengler, and M. Majerčáková, "The New Model of Customer Segmentation in Postal Enterprises," *Procedia - Soc. Behav. Sci.*, vol. 230, no. May, pp. 121–127, 2016, doi: 10.1016/j.sbspro.2016.09.015.
- [10] A. J. Christy, A. Umamakeswari, L. Priyatharsini, and A. Neyaa, "RFM ranking – An effective approach to customer segmentation," *J. King Saud Univ. - Comput. Inf. Sci.*, 2018, doi: 10.1016/j.jksuci.2018.09.004.
- [11] R. Sherman, *Business Intelligence Guidebook From Data Integration to Analytics*. Waltham: Elsevier Inc, 2015.
- [12] Y. Zhao, "Transformation of Business Analytics from Business Intelligence," *E3S Web Conf.*, vol. 253, pp. 3–6, 2021, doi: 10.1051/e3sconf/202125303013.
- [13] J. Hurwitz and D. Kirsch, *Machine Learning For Dummies IBM Limited Edition*, 2018th ed. New Jersey: John Wiley & Sons, Inc, 2018.
- [14] J. D'Silva and U. Sharma, "Unsupervised Automatic Text Summarization of Konkani Texts using K-means with Elbow Method," *Int. J. Eng. Res. Technol.*, vol. 13, no. 9, pp. 2380–2384, 2020, doi: 10.37624/ijert/13.9.2020.2380-2384.
- [15] H. Humaira and R. Rasyidah, "Determining The Appropriate Cluster Number Using Elbow Method for K-Means Algorithm," 2020, doi: 10.4108/eai.24-1-2018.2292388.
- [16] B. N. Sari, "Identification of Tuberculosis Patient Characteristics Using K-Means Clustering," *Sci. J. Informatics*, vol. 3, no. 2, pp. 129–138, 2016, doi: 10.15294/sji.v3i2.7909.
- [17] L. Zahrotun, "Implementation of data mining technique for customer relationship management (CRM) on online shop tokodipers.com with fuzzy c-means clustering," *Proc. - 2017 2nd Int. Conf. Inf. Technol. Inf. Syst. Electr. Eng. ICITISEE 2017*, vol. 2018-Janua, pp. 299–303, 2018, doi: 10.1109/ICITISEE.2017.8285515.
- [18] R. D. F. Ruly, Purbandini, and E. Wuryanto, "Penerapan Clustering K-Means Pada Customer Segmentation Berbasis Recency Frequency Monetary ( Rfm ) ( Studi Kasus : Pt . Sinar Kencana Intermoda Surabaya )," *Semin. Nas. Mat. Dan Apl.*, pp. 418–427, 2017.
- [19] J. Jamal and D. Yanto, "Analisis RFM dan Algoritma K-Means untuk Clustering Loyalitas Customer," *Energy*, vol. 9, no. 1, pp. 1–8, 2019.
- [20] A. Aziz, "Customer Segmentation basedon Behavioural Data in E-marketplace," 2017, [Online]. Available: <https://www.diva-portal.org/smash/record.jsf?pid=diva2:1145508>.
- [21] W. Qadadeh and S. Abdallah, "Customers Segmentation in the Insurance Company (TIC) Dataset," *Procedia Comput. Sci.*, vol. 144, pp. 277–290, 2018, doi: 10.1016/j.procs.2018.10.529.
- [22] J. Silva, N. Varela, L. A. B. López, and R. H. R. Millán, "Association rules extraction for customer segmentation in the SMES sector using the apriori algorithm," *Procedia Comput. Sci.*, vol. 151, no. 2018, pp. 1207–1212, 2019, doi: 10.1016/j.procs.2019.04.173.
- [23] R. W. Sembiring Brahmana, F. A. Mohammed, and K. Chairuang, "Customer Segmentation Based on RFM Model Using K-Means, K-Medoids, and DBSCAN Methods," *Lontar Komput. J. Ilm. Teknol. Inf.*, vol. 11, no. 1, p. 32, 2020, doi: 10.24843/lkjiti.2020.v11.i01.p04.
- [24] K. K. Halim, S. Halim, and Felecia, "Business intelligence for designing restaurant marketing strategy: A case study," *Procedia Comput. Sci.*, vol. 161, pp. 615–622, 2019, doi: 10.1016/j.procs.2019.11.164.
- [25] J. Choi, J. Yoon, J. Chung, B. Y. Coh, and J. M. Lee, "Social media analytics and business intelligence research: A systematic review," *Inf. Process. Manag.*, vol. 57, no. 6, p. 102279, 2020, doi: 10.1016/j.ipm.2020.102279.
- [26] P. L. Bourbonnais and C. Morency, "A robust datawarehouse as a requirement to the increasing quantity and complexity of travel survey data," *Transp. Res. Procedia*, vol. 32, pp. 436–447, 2018, doi: 10.1016/j.trpro.2018.10.054.

- [27] C. D'Arconte, "Business intelligence applied in small size for profit companies," *Procedia Comput. Sci.*, vol. 131, pp. 45–57, 2018, doi: 10.1016/j.procs.2018.04.184.
- [28] V. Khatibi, A. Kheramati, and F. Shirazi, "Deployment of a business intelligence model to evaluate Iranian national higher education," 2020, [Online]. Available: [www.elsevier.com/locate/ssaho](http://www.elsevier.com/locate/ssaho).
- [29] H. Yonar, "Modeling and Forecasting for the number of cases of the COVID-19 pandemic with the Curve Estimation Models, the Box-Jenkins and Exponential Smoothing Methods," *Eurasian J. Med. Oncol.*, no. April, 2020, doi: 10.14744/ejmo.2020.28273.

# Intrusion Detection System for Energy Efficient Cluster based Vehicular Adhoc Networks

M V B Murali Krishna M<sup>1</sup>, Dr. C.Anbu Ananth<sup>2</sup>, Dr. N. Krishna Raj<sup>3</sup>

Research Scholar: Department of CSE, FEAT, Annamalai University, Chidambaram-608002, India<sup>1</sup>

Associate Professor: Department of CSE, FEAT, Annamalai University, Chidambaram- 608002, India<sup>2</sup>

Associate Professor, School of Computing, SRM Inst. of Sci & Tech, Kattankulathur- 603203, Tamil Nadu, India<sup>3</sup>

**Abstract**—A vehicular Adhoc Network, a subfield of Mobile Adhoc Network is defined by its high mobility and by demonstrating dissimilar mobility patterns. So, VANET clustering techniques are needed with the consideration of the mobility parameters amongst nearby nodes to construct stable clustering techniques. At the same time, security is also a major design issue in VANET which can be resolved by the Intrusion Detection Systems. In contrast to the conventional IDS, VANET based IDS are required to be designed in such a way that the functioning of the system does not affect the real-time efficiency of the performance of VANET applications. With this motivation, this paper presents an efficient Fuzzy Logic based Clustering with optimal Fuzzy Support Vector Machine, called FLC-OFSVM based Intrusion Detection System for VANET. The proposed FLC-OFSVM model involves two stages of operations namely clustering and intrusion detection. Primarily, FLC technique is employed to select an appropriate set of cluster heads and construct clusters. Besides, a lightweight anomaly IDS model named FSVM optimized with krill herd optimization algorithm is developed to detect the existence of malevolent attacks in VANET. The KH algorithm which is based on the herding behavior of krills is used to optimally tune the parameters of the FSVM model. In order to investigate the performance of the FLC-OFSVM model, an extensive set of simulations are carried out and the results are investigated in terms of several performance measures.

**Keywords**—Clustering; intrusion detection; vehicular communication; VANET; machine learning; krill herd optimization; fuzzy logic

## I. INTRODUCTION

Vehicle ad hoc networks (VANET) were developed as a part of a mobile ad hoc network (MANET) [1] application. It is deliberated a significant method for intelligent transportation systems (ITS). Recently, it is an emphasis of many scientists in the field of wireless mobile data transmission. In VANET, vehicles are utilized as network nodes. It contains three main kinds of data transmission feasible in VANET: a) Vehicle to Vehicle (V2V), b) Vehicle to Infrastructure (V2I), and c) Hybrid. However, this current data transmission kind suffers from several drawbacks like huge amount of Road Side Units (RSU) are required at standard location in V2I data transmission that aren't financially possible, security and privacy problems in V2V based data transmissions [2], hence clustering data transmission is chosen currently that has benefits on above three data transmission types [3]. This method is very congested traffic scenario that increases further load on cluster

head (CH) that finally presents delay in the data transmission and affect entire network performances. For handling this, a novel clustering framework stimulated from dolphin swarm behavior was introduced in this study where many nodes could perform as a CH in a cluster and therefore could allocate their load in heavy traffic situations which enhances the entire network efficiency. Fig. 1 depicts the architecture of cluster VANET.

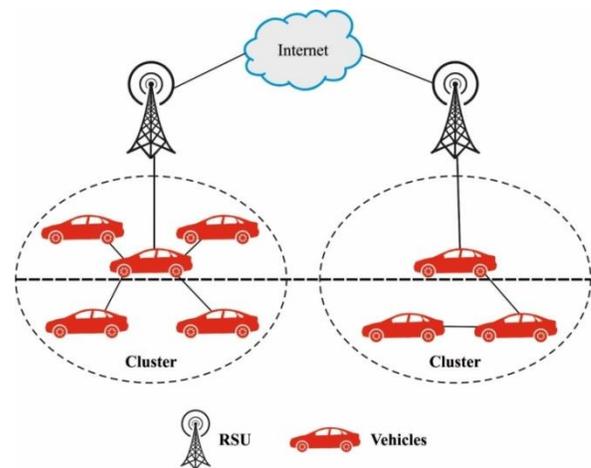


Fig. 1. Architecture of Clustered VANET.

VANET provides several applications and services to the clients that are involved with the security of the navigational aid, drivers, and infotainment. It contains 2 kinds of data allocated in VANET: safety (curve warning, vehicle speed warning) and non-safety data (value added comfort application) [4]. Standard safety data provides high priority in VANET related to non-safety data, then safety data inform driver of predictable danger to permit earlier response. In spite of the advantages provided by VANET, it has several problems based on transmitted messages, security, and privacy of clients. Since vehicles exit and enter highways, they need specific safety information's like traffic road conditions and congestions, decision making on that route for taking to their destination. It is vital that this data be sent at an appropriate time; or else, it can lead to delay in attaining the destination securely [5]. In particular conditions, few malicious nodes refuse to transmit or even purposefully change the needed safety message beforehand transferring to the requested client that can lead to long delays or mortalities. Moreover, the features of VANET (such as volatility, higher mobility) are different from other wireless data transmission networks that

have made VANET vulnerable to several external and internal attacks [6]. Because of the dynamic topology and decentralized structure of VANET, the safety of the vehicles, clients, and data become significant, as the detection of faulty nodes/malicious/user becomes complex [7].

Alternatively, different from conventional Intrusion Detection Systems (IDS), VANET based IDS should be placed with care in this manner where the process shouldn't delay the real-time efficiency of VANET application. It contains several based resolutions for VANET in survey [8]. Mostly, it contains challenges such as higher false positives, lower detection rate, additional overhead on the network, higher detection time, and so are related with them. But it cannot detect modified and newer attacks. Abnormality based IDS has benefits over rule based IDS in the manner that it can detect novel attacks where the signature isn't existing in the database. However, this class of IDS requires settings of an optimum threshold and large trained set to make it proficient for differentiating among the normal and malicious nodes.

This paper presents an efficient Fuzzy Logic based Clustering with optimal fuzzy support vector machine (FSVM), called FLC-OFSVM based Intrusion Detection System for VANET. The proposed FLC-OFSVM model involves FLC technique with different input parameters to select cluster heads (CHs) and organize clusters. In addition, a lightweight anomaly IDS model named FSVM optimized with krill herd (KH) optimization algorithm is developed to detect the existence of malevolent attacks in VANET. For optimal tuning of the parameters involved in the FSVM model, the KH algorithm is employed in such a way that the intrusion detection ate can be enhanced. For examining the outcomes of the FLC-OFSVM model, a comprehensive set of experimental analyses were performed and the results are inspected interms of several aspects.

Section 2 describes the Literature Survey and Section 3 briefly explains proposed model followed by performance evaluation in section 4, finally section 5 discusses with conclusion and future directions,

## II. LITERATURE REVIEW

Several security systems have been presented by numerous scientists for addressing privacy and security problems in VANETs. This segment emphasizes few present methods which focus on related issues in VANET with same methods. An anonymous and lightweight authentication system smart card (ASC) is presented in Ying and Nayak [9] for addressing privacy preserving issues like legitimacy of the user and message transferred over the network. The verification of user and message is made by low-cost cryptographic operation. This protocol doesn't authenticate the user identity and also verify transmitted messages, however it assurances privacy of user. Wazid et al. [10] introduced a decentralized lightweight authentication and key agreement protocol (LAKAP) for VANET, that utilizes bitwise exclusive OR (XOR) operation and one way hash function.

Rajput et al. [11] presented a hybrid method for privacy preserving authentication scheme (HEPPA), that integrates the feature of pseudonym and group signature based methods,

with conditional anonymity. This technique utilizes lightweight and simple pseudonyms that provide conditional privacy. Tangade and Manvi [12] presented an efficient, scalable, and privacy preserving authentication (ESPA) protocol by a hybrid cryptography method for inter-vehicle data transmissions.

Cui et al. [13] projected a secure privacy preserving authentication scheme for VANET with cuckoo filter (SPACF) for enhancing the privacy and security of clients, and reduce data transmission overhead. Moreover, the investigators projected a novel authentication system with no bilinear pairings that could lead to heavy computation costs. The cuckoo filter is a data structure which gives an optimum search time and searches accuracy and utilizes hash function. The present methods deliberated have been chosen as the standard protocol for this work since this approach focuses on improving security and privacy preserving of user in the network. It is viewed that the present methods mainly focus on authentication and privacy preserving systems. But, another security necessity of VANET like non-repudiation, availability, and integrity, wasn't paid more interest. This provides a gap for additional development in VANET security with the deliberation of executing a novel security-based technique which is available in the present times. Hence, the resolution presented in this work tries to enhance the VANET security by employing a modern technology which can tackle the security needs and enhance road security with the help of vehicles resource and data transmission scheme.

## III. THE PROPOSED MODEL

The overall system architecture of the proposed FLC-OFSVM model is demonstrated as under. Initially, the vehicles in the VANET are placed randomly in the target area. Then, the network initialization process takes place where the single hop neighboring vehicles interact with one another. Next, the FLC technique is performed to optimally select the CHs and construct clusters proficiently. Followed by, the FSVM model is employed for the identification of intrusions in the network. Finally, the KH algorithm is used to optimally choose the parameters involved in the FSVM model.

### A. Design of FLC Technique

At this stage, the FLC technique with three input parameters is utilized to select CHs, as shown in Fig. 2. In this presented scheme, every node transmits its mobility data, average velocity to its neighbor via HELLO packet with the succeeding formats: Average Velocity, Node ID, Direction, and Location.

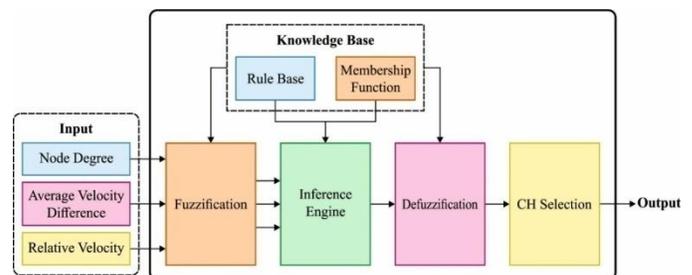


Fig. 2. Process Involved in FLC Technique.

1) *Node degree*: The amount of the velocity variances between adjacent vehicles is the main problem to construct relatively stable clustering topology. The neighborhood relation is made by the location data embedding from periodic message transmits by vehicles. Vehicles transmit their present state to every node with their broadcast range  $R$ :

$$N_i = \{v_j; \text{dis}_{i,j} \leq R\} \quad (1)$$

Whereas  $\text{dis}_{i,j}$  denotes average distance among vehicles  $i$  and  $j$ . According to this determination, they acquire other terms named node degree of a node ( $\psi_i$ ), that is determined by overall amount of  $R$ -neighbors. Then clusters are made with vehicles travel in a similar direction, every  $R$ -neighboring vehicle travel in the opposite direction isn't deliberated [14]. Thus, every  $R$ -neighboring nodes utilized in this analyses are restricted to this vehicle travels in a similar direction, located in other lanes and estimated by:

$$\psi_i = |N_i| \quad (2)$$

2) *Average velocity differences*: In all time intervals, every vehicle, have data regarding each vehicle with its transmission range and therefore, it would estimate its average velocity variance  $\phi_i$  from every vehicle by:

$$\phi_i = \frac{1}{\psi_{i-1}} \sum_{j=1}^{\psi_{i-1}} |v_j - v_i| \quad (3)$$

Whereas  $j$  denotes possible neighboring vehicle, and  $v_i, v_j$  indicates velocity of vehicle  $i$  and  $j$ , correspondingly in m/s. The node could attain its velocity by commercial navigation services, like Garmin Traffic.

3) *Relative velocity*: For building relative stable cluster, they assume the vehicles related to optimum neighborhood degree ( $\psi_i$ ). A low relatively velocity simply implies that the neighbor of a particular node has consumed a long time in its broadcast range. Thus, they could accomplish that the stated node comprises additional stable situations. The relative velocity of a node  $i$  is estimated by:

$$\omega_i = \frac{\phi_i}{v_i} \quad (4)$$

The lesser the value of  $\omega_i$ , the nearer the velocity of node for an average velocity of their neighbour that improves neighbourhood steadiness. In this presented system, every node calculates its neighbors based on link connectivity, average velocity difference, and relative velocity. If a node should transmit a packet, the node utilized FL for calculating fit factor value for every neighbor in terms of link connectivity duration, average absolute distance, and average velocity.

4) *Fuzzification process*: Fuzzification is the procedure of transforming mathematical values to fuzzified values by a MF. The transmitter node utilizes average absolute distance and MF for calculating the degree to which the distance factors belong to Large, Small, and Medium. The transmitter node utilizes average velocity and MF for calculating that degree the average velocity comes under Fast, Slow, Medium. The transmitter node utilizes link connectivity duration and MF for

calculating the link connectivity. When the fuzzy values of link connectivity, duration average absolute distance, and average velocity were estimated, fuzzy inference engine map the fuzzy values to the IF or THEN rules and restricted in the knowledge base for calculating the fit factor for every node. The fuzzy inference scheme is implemented according to twenty seven rules are introduced. Therefore, their equivalent calculation result should be integrated.

5) *Defuzzification process*: Defuzzification is the procedure of generating a numerical result on the basis of output MF and equivalent membership degree. Now, they utilize center of gravity (CoG) technique for defuzzifying the fuzzy results. Particularly, they cut the output MF with a straight horizontal line based on equivalent degree, and eliminate the top part. Later, they estimate the Centroid of this shape.

### B. Design of IDS Technique

Once the vehicles in the VANET are clustered, the next stage is to identify the presence of intruders in the network using the OFSVM model. In addition, the KH algorithm is employed to optimally tune the parameters of the FSVM model in such a way that the intrusion detection ate can be enhanced.

1) *FSVM model*: In conventional SVM, every data point is deliberated with equivalent significance and allocated a similar penal variable in its objective function. To resolve this problem, the system of FSVM was presented by [15]. Fuzzy membership to every instance point is presented; thus, distinct instance points could create various contributions to the creation of decision surface. Assume the trained instance is

$$S = \{(x_1, y_i, s_i), i = 1, \dots, N\} \quad (5)$$

Whereas  $x_1 \in R^n$  denotes  $n$ -dimension instance point,  $y_i \in \{-1, +1\}$  denotes class label, and  $s_i (i = 1, \dots, N)$  indicates fuzzy membership that fulfills  $\sigma \leq s_i \leq 1$  with adequately smaller constant  $\sigma > 0$ . Re quadratic optimization problem for classification is deliberated by:

$$\min_{w, s, \xi} \frac{1}{2} w^T w + C \sum_{i=1}^l s_i \xi_i \quad (6)$$

$$s. t. y_i (w^T x_i + b) \geq 1 - \xi_i, \xi_i \geq 0, i = 1, \dots, l,$$

Whereas  $w$  denotes normal vector of the splitting hyperplane,  $b$  indicates bias term, and  $C$  represents variable that should be defined before for controlling the trade-off among classification margin and cost of misclassification error [16]. Then  $s_i$  denotes attitude of equivalent point  $x_1$  to single class and the slack parameters  $\xi_i$  denotes measure of error, later the expression  $s_i \xi_i$  is deliberated a measure of error with distinct weights. It can be stated that the larger  $s_i$  is, the more prominently the equivalent point is processed; the lesser the  $s_i$  is, the lesser prominently the equivalent point is processed; therefore, distinct input points could create various contributions to learn of decision surface. Hence, FSVM could detect stronger hyperplane by increasing the margin allowing few misclassifications of lesser significant points.

To resolve the FSM optimum problem, (6) is converted to the succeeding two problems by presenting Lagrangian multipliers  $\alpha_i$ :

$$\max \sum_{i=1}^N \alpha_i - \frac{1}{2} \sum_{i=1}^N \sum_{j=1}^N \alpha_i \alpha_j y_i y_j x_i x_j \quad (7)$$

$$s. t. \sum_{i=1}^N y_i \alpha_i = 0, 0 \leq \alpha_i \leq s_i C, i = 1, \dots, N.$$

Related to regular SVM, the aforementioned representation has a slight variance, that is the upper bound of the values of  $\alpha_i$ . By resolving these two problems in (3) for optimum  $\alpha_i, w$  and  $b$  are recovered in a similar manner as in the regular SVM.

2) *Overview of KH Algorithm:* The KH algorithm is a type of swarm intelligence technique that is inspired by the herding characteristics of krills. In the procedure of predation, the predator would alter the distribution of krill population, that would create them to move quickly, and later causes their distribution density for decreasing and the distance among the predator and the food becomes farther that is the first stage of KH. In this method, the distribution of krill population is defined as the succeeding 3 conditions: the impact of other krill individuals, arbitrary diffusion, and behavior of getting food. The KH method is defined by:

$$dX_i dt = N_i + F_i + D_i \quad (8)$$

Whereas  $N_i$  denotes impact of another krill individuals,  $F_i$  represents behavior of getting food, and  $D_i$  indicates behavior of arbitrary diffusion;  $i = 1, 2, \dots, N$ , and  $N$  represents the population size.

For the impact of another krill individuals, the movement  $N_{i,new}$  of krill  $i$  induced by another krill can be determined:

$$N_{i,new} = N_{max} \alpha_i + \omega_n N_{i,old} \quad (9)$$

Whereas  $N_{max}$  denotes maximal induced velocity,  $N_{i,old}$  indicates earlier induced motion,  $\omega_n$  denotes inertia weight and the value range zero and one and  $\alpha_i$  represents individual  $i$  is caused by the induction direction of the adjacent neighbors [17].

The succeeding behavior  $F_i$  is to get food, by:

$$F_i = V_f \beta_i + \omega_f F_{i,old} \quad (10)$$

whereas  $V_f$  represents maximal foraging speed, and its value is a constant, that is  $0.02 \text{ (ms}^{-1}\text{)}$ ;  $\omega_f$  indicates inertia weight of foraging motion, and its range is zero and one;  $F_{i,old}$  denotes earlier foraging motion, and  $\beta_i$  represents foraging direction. Fig. 3 demonstrates the flowchart of KH technique. The individual  $D_i$  in the final behavior is given by:

$$D_j = D_{max} \left(1 - \frac{I}{I_{max}}\right) \delta \quad (11)$$

Where  $D_{max}$  denotes maximal arbitrary diffusion speed;  $\delta$  indicates direction of arbitrary diffusion; and  $I$  and  $I_{max}$  denotes present amount and the maximal number of iterations,

correspondingly. From aforementioned procedure, they could attain the krill upgrade procedure of the KH method by:

$$X_i(t + \Delta t) = X_i(t) + \Delta t \frac{dX_i}{dt} \quad (12)$$

$$\Delta t = Ct \sum_{j=1}^{NV} (UB_j - LB_j) \quad (13)$$

Where  $\Delta t$  denotes time interval relevant to the certain application;  $NV$  represents dimension of the decision parameter; step factor  $Ct$  indicates constant among  $(0,2)$ ; and  $UB_j$  and  $LB_j$  denotes upper and lower bounds of equivalent parameter  $j(j = 1, 2, \dots, NV)$ , correspondingly.

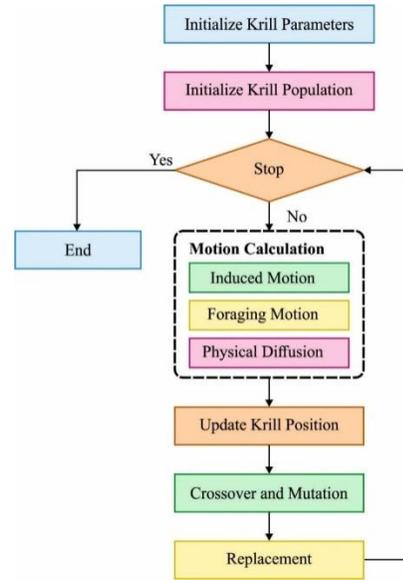


Fig. 3. Flowchart of KH.

The process of the KH algorithm (Algorithm 1) is given as follows.

Algorithm1. Pseudo code of KH algorithm
<p>Begin</p> <p>Step 1: Initiation. Initiate the generation counter <math>G</math>, the population <math>P</math>, <math>V_f</math>, <math>D_{max}</math>, and <math>N_{max}</math>.</p> <p>Step 2: Fitness evaluation. Evaluate fitness to every krill based on early position.</p> <p>Step 3: While <math>G &lt; \text{Max Generation}</math> do</p> <p>    Arrange the population based on its fitness.</p> <p>    for <math>i = 1: N</math> (all krill) do</p> <p>        Execute the succeeding movement evaluation.</p> <p>        Movement induced by other individuals</p> <p>        Foraging movement</p> <p>        Physical diffusion</p> <p>        Execute the genetic operator.</p> <p>        Upgrade the krill location from search space.</p> <p>        Evaluate fitness to every krill based on its novel place</p> <p>    end for <math>i</math></p> <p>        <math>G = G + 1</math>.</p> <p>Step 4: end while.</p> <p>End.</p>

3) *Parameter tuning of FSVM model using KH algorithm:*

In OFSVM model, the parameters (weight and bias) in the FSVM model are optimally adjusted by the use of KH algorithm. The FSVM model is trained with the parameters of the KH algorithm. Besides, 10 fold cross validation process is employed for determining the fitness function where the training data is split arbitrarily into 10 parts. Then, 9 sets of data are employed for training process and the final one is utilized for testing process. This process gets iteration ten times; therefore, every set is utilized once to test the model. The fitness function can be represented as  $1 - CA_{validation}$  of the 10-fold cross-validation (CV) technique in the training data, as given in Eqs. (14) and (15). Besides, the solution with higher CA validation holds lower fitness value.

$$Fitness = 1 - CA_{validation} \tag{14}$$

$$CA_{validation} = 1 - \frac{1}{10} \sum_{i=1}^{10} \left| \frac{y_c}{y_c + y_f} \right| \times 100 \tag{15}$$

Where  $y_c$  and  $y_f$  refers the count of true and false classifications correspondingly.

IV. PERFORMANCE VALIDATION

A brief comparative study of the FLC with other techniques in terms of NLT, EC, and throughput is made in Table 1. Fig. 4 examines the NLT analysis of the FLC technique with other methods under varying number of vehicles. The proposed FLC technique has gained maximum NLT under all distinct numbers of vehicles. For instance, with 20 vehicles, the proposed FLC technique has accomplished a higher NLT of 4600 rounds whereas the HEPPA, ASC, and LAKAP techniques have attained a lower NLT of 4400, 4000, and 3800 rounds respectively. In addition, with 60 vehicles, the presented FLC approach has accomplished a superior NLT of 4100 rounds whereas the HEPPA, ASC, and LAKAP techniques have attained a lower NLT of 3700, 3600, and 3500 rounds correspondingly. Also, with 100 vehicles, the proposed FLC technique has accomplished a higher NLT of 3600 rounds whereas the HEPPA, ASC, and LAKAP methodologies have obtained a minimum NLT of 3300, 3200, and 3100 rounds correspondingly.

An EC analysis of the proposed FLC technique with recent methods is made in Fig. 5. The figure has shown that the FLC technique has offered superior results with minimal EC over the other techniques whereas the LAKAP technique has displayed insufficient performance with the maximum EC. For instance, with 20 vehicles, the proposed FLC technique has resulted in the least EC of 32mJ whereas the HEPPA, ASC, and LAKAP techniques have demonstrated a maximum EC of 40mJ, 46mJ, and 56mJ, respectively. Additionally, with 60 vehicles, the proposed FLC method has resulted in the lesser EC of 79mJ whereas the HEPPA, ASC, and LAKAP approaches have showcased a maximal EC of 91mJ, 94mJ, and 114mJ, correspondingly. Besides, with 100 vehicles, the presented FLC algorithm has resulted in the least EC of 103mJ whereas the HEPPA, ASC, and LAKAP techniques have revealed a higher EC of 136mJ, 153mJ, and 172mJ, correspondingly.

TABLE I. RESULT ANALYSIS OF PROPOSED FLC WITH OTHER TECHNIQUES

Network Lifetime (Rounds)				
Number of Vehicles	Proposed FLC	HEPPA	ASC	LAKAP
20	4600	4400	4000	3800
40	4400	4100	3700	3600
60	4100	3700	3600	3500
80	3700	3500	3300	3200
100	3600	3300	3200	3100
Energy Consumption (mJ)				
Number of Vehicles	Proposed FLC	HEPPA	ASC	LAKAP
20	32	40	46	56
40	58	64	69	79
60	79	91	94	114
80	94	109	118	127
100	103	136	153	172
Throughput (Kbps)				
Number of Vehicles	Proposed FLC	HEPPA	ASC	LAKAP
20	67.01	65.75	57.00	53.28
40	72.42	70.35	64.45	60.65
60	77.27	74.23	69.24	64.72
80	81.61	78.75	72.21	69.19
100	83.91	80.85	78.36	73.48

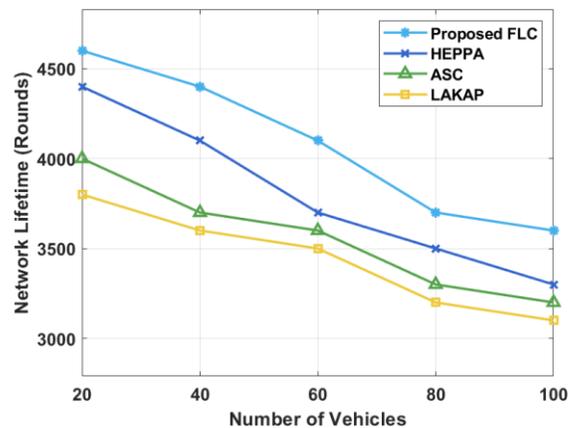


Fig. 4. Network Lifetime Analysis of FLC Model.

Fig. 6 examines the throughput analysis of the FLC technique with other methods under varying number of vehicles. The proposed FLC technique has gained maximum throughput under all distinct number of vehicles. For instance, with 20 vehicles, the proposed FLC technique has accomplished a higher throughput of 67.01Mbps whereas the HEPPA, ASC, and LAKAP techniques have attained a lower throughput of 65.75Mbps, 57Mbps, and 53.28Mbps respectively. Moreover, with 60 vehicles, the presented FLC manner has accomplished a maximum throughput of 77.27Mbps whereas the HEPPA, ASC, and LAKAP techniques have achieved a lesser throughput of 74.23Mbps, 69.24Mbps, and 64.72Mbps correspondingly. Furthermore, with 100 vehicles, the projected FLC technique has accomplished a maximal throughput of 83.91Mbps whereas the HEPPA, ASC, and LAKAP approaches have attained a lower throughput of 80.85Mbps, 78.36Mbps, and 73.48Mbps rounds correspondingly.

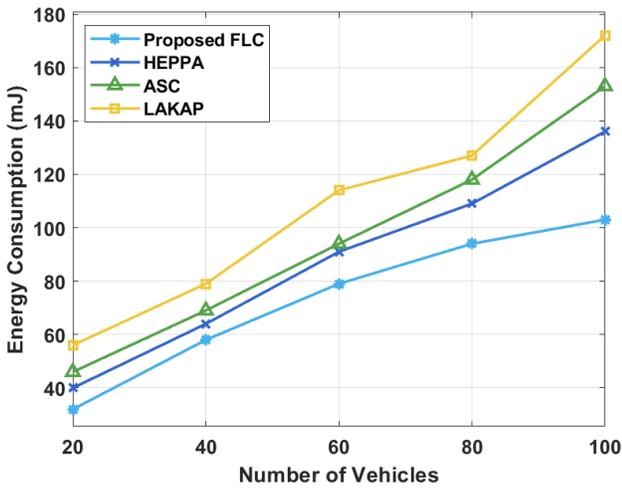


Fig. 5. Energy Consumption Analysis of FLC Model.

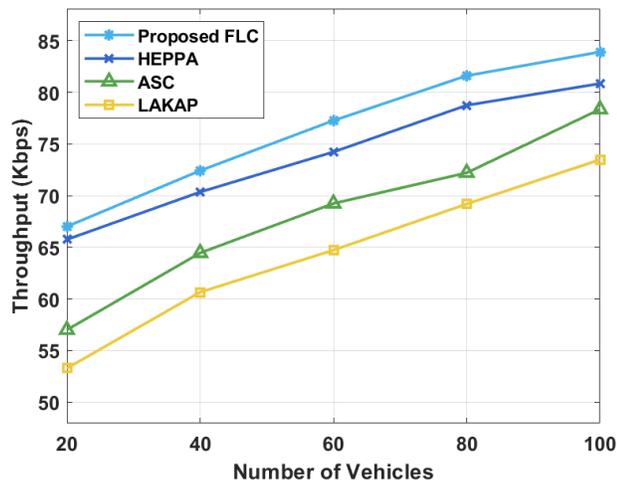


Fig. 6. Throughput Analysis of FLC Model.

TABLE II. PDR AND ETE DELAY ANALYSIS OF PROPOSED FLC WITH OTHER TECHNIQUES

Packet Delivery Ratio (%)				
Number of Vehicles	Proposed FLC	HEPPA	ASC	LAKAP
20	0.98	0.95	0.93	0.82
40	0.87	0.84	0.80	0.71
60	0.78	0.74	0.71	0.62
80	0.72	0.67	0.60	0.55
100	0.69	0.63	0.55	0.48
End-to-End Delay (ms)				
Number of Vehicles	Proposed FLC	HEPPA	ASC	LAKAP
20	7.57	7.97	8.07	10.57
40	8.13	8.47	8.69	11.11
60	8.39	9.04	9.57	11.61
80	8.92	9.80	10.17	12.04
100	9.38	10.14	10.40	13.11

A brief comparison study of the FLC with other techniques in terms of PDR and ETE delay is made in Table 2 [18]. Fig. 7 inspects the PDR analysis of the FLC algorithm with other techniques under varying number of vehicles. The presented FLC technique has gained maximal PDR under all distinct number of vehicles. For instance, with 20 vehicles, the proposed FLC technique has accomplished a higher PDR of 0.98% whereas the HEPPA, ASC, and LAKAP techniques have attained a lesser PDR of 0.95%, 0.93%, and 0.82% correspondingly. In the meantime, with 60 vehicles, the proposed FLC method has accomplished a superior PDR of 0.78% whereas the HEPPA, ASC, and LAKAP approaches have achieved minimal PDR of 0.74%, 0.71%, and 0.62% respectively. At the same time, with 100 vehicles, the proposed FLC method has accomplished a higher PDR of 0.69% whereas the HEPPA, ASC, and LAKAP methodologies have attained a lower PDR of 0.63%, 0.55%, and 0.48% correspondingly.

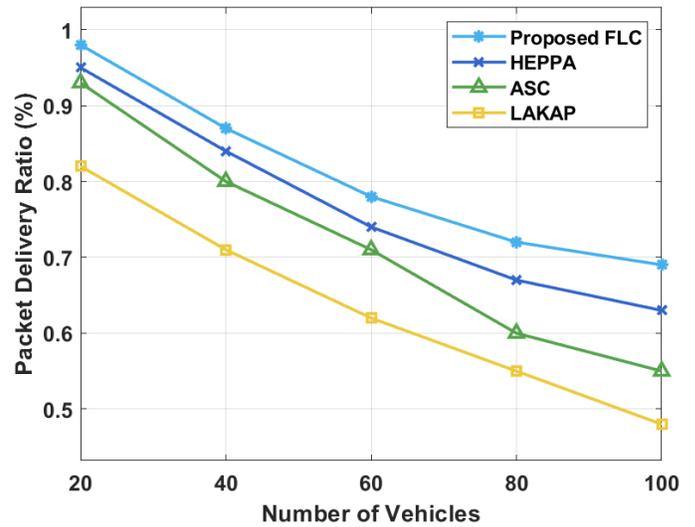


Fig. 7. PDR Analysis of FLC Model.

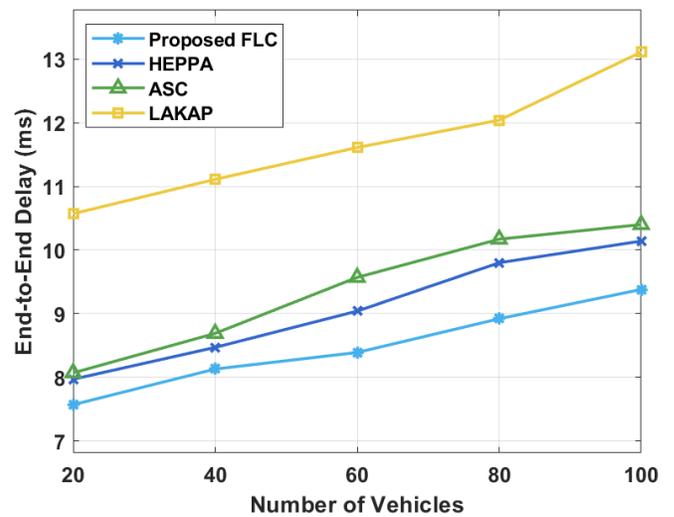


Fig. 8. ETE Delay Analysis of FLC Model.

An ETE delay analysis of the proposed FLC technique with recent techniques is made in Fig. 8. The figure has demonstrated that the FLC approach has offered superior results with the minimal ETE delay over the other methods whereas the LAKAP algorithm has portrayed insufficient performance with the higher ETE delay. For instance, with 20 vehicles, the proposed FLC technique has resulted in a least ETE delay of 7.57ms whereas the HEPPA, ASC, and LAKAP manners have demonstrated a maximal ETE delay of 7.97ms, 8.07ms, and 10.57ms, correspondingly. Meanwhile, with 60 vehicles, the proposed FLC technique has resulted in the least EC of 8.39ms whereas the HEPPA, ASC, and LAKAP techniques have outperformed a higher EC of 9.04ms, 9.57ms, and 11.61ms, correspondingly. Eventually, with 100 vehicles, the projected FLC technique has resulted in the least EC of 9.38ms whereas the HEPPA, ASC, and LAKAP methods have showcased a maximal EC of 10.14ms, 10.4ms, and 13.11ms, correspondingly.

For validating the IDS performance of the OFSVM method, it is tested using NSL-KDD 2015 dataset which includes a set of 125973 instances with 51 class labels and 2 classes. Table 3 and Fig. 9 demonstrate the detailed detection accuracy analysis of the OFSVM with other methods [19]. The table values showcased that the CS-PSO algorithm has gained lowest performance with the accuracy of 75.51% whereas a certainly enhanced performance is obtained by the DNN-SVM and Cuckoo optimization methods with the accuracy of 92.03% and 96.88% correspondingly. Besides, the behaviour based IDS, PSO-SVM, MLIDS, and DBN models have exhibited moderately closer accuracy of 98.89%, 99.1%, 99.93%, and 99.96% respectively. However, the proposed OFSVM model has gained maximum outcome with an accuracy of 99.98%.

TABLE III. RESULT ANALYSIS OF PROPOSED OFSVM METHOD WITH EXISTING METHODS FOR APPLIED DATASET

Methods	Accuracy
Proposed OFSVM	99.98
Deep Belief Network (2020)	99.96
MLIDS (2019)	99.93
CS-PSO (2019)	75.51
PSO-SVM (2019)	99.10
Behaviour Based IDS (2019)	98.89
Cuckoo Optimization (2018)	96.88
DNN+SVM (2018)	92.03

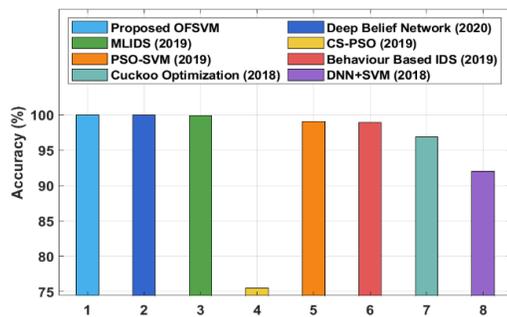


Fig. 9. Accuracy Analysis of OFSVM Model with Existing Techniques.

## V. CONCLUSION

This paper has presented an effective FLC-OFSVM model to achieve security and effective communication in VANET. The proposed FLC-OFSVM model begins with the deployment of vehicles in a random way and is initialized together. Then, the FLC technique is executed to determine the proper set of CHs in VANET and neighboring vehicles join the CH to develop the cluster. Moreover, the OFSVM model is applied for identifying the existence of intruders from VANET. In order to optimally tune the parameters involved in the FSVM model, the KH algorithm is employed in such a way that the intrusion detection rate can be enhanced. For examining the outcomes of the FLC-OFSVM model, a comprehensive set of experimental analyses were performed and the results are inspected in terms of several aspects. The resultant experimental values highlighted the promising performance of the FLC-OFSVM model over the state of art methods. As a part of future work, the security of the VANET is improved by the design of secure multihop routing protocols for privacy preserving data transmission with reliable vehicles in VANET.

## REFERENCES

- [1] M.R.Ghori, K.Z.Zamli, N.Quosthoni, M.Hisyam and M.Montaser, May 2018. Vehicular ad-hoc network (VANET). In 2018 IEEE international conference on innovative research and development (ICIRD) (pp. 1-6). IEEE.
- [2] S.K.Biswal, 2014. "On Board unit based authentication for V2V communication in VANET (Doctoral dissertation)".
- [3] H Lu, J. Li and M. Guizani, 2013. "Secure and efficient data transmission for cluster-based wireless sensor networks". *IEEE transactions on parallel and distributed systems*, 25(3), pp.750-761.
- [4] S.K.Bhoi, P.M.Khilar, M.Singh, R.R.Sahoo and R.R.Swain, 2018. "A routing protocol for urban vehicular ad hoc networks to support non-safety applications". *Digital Communications and Networks*, 4(3), pp.189-199.
- [5] C.Lai, K.Zhang, N.Cheng, H Li, and X.Shen, 2016. SIRC: "A secure incentive scheme for reliable cooperative downloading in highway VANETs". *IEEE Transactions on Intelligent Transportation Systems*, 18(6), pp.1559-1574.
- [6] R.G.Engoulou, M.Bellaïche, S.Pierre and A.Quintero, 2014. "VANET security surveys". *Computer Communications*, 44, pp.1-13.
- [7] N.J.Patel and R.H.Jhaveri, 2015. "Trust based approaches for secure routing in VANET": A Survey. *Procedia Computer Science*, 45, pp.592-601.
- [8] O.Depren, M.Topallar, E.Anarim and M.K.Ciliz, 2005. "An intelligent intrusion detection system (IDS) for anomaly and misuse detection in computer networks". *Expert systems with Applications*, 29(4), pp.713-722.
- [9] B.Ying. and A.Nayak, 2017. "Anonymous and lightweight authentication for secure vehicular networks". *IEEE Transactions on Vehicular Technology*, 66(12), pp.10626-10636.
- [10] M.Wazid, A.K Das, N.Kumar, V.Odelu, A.G Reddy, K. Park and Y.Park, 2017. "Design of lightweight authentication and key agreement protocol for vehicular ad hoc networks". *IEEE Access*, 5, pp.14966-14980.
- [11] U.Rajput, F.Abbas, H.Eun and H.Oh, 2017. "A hybrid approach for efficient privacy-preserving authentication in VANET". *IEEE Access*, 5, pp.12014-12030.
- [12] S.Tangade and S.S.Manvi, 2016, November. "Scalable and privacy-preserving authentication protocol for secure vehicular communications". In *2016 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS)* (pp. 1-6). IEEE.
- [13] J.Cui, J.Zhang, H.Zhong and Y.Xu, 2017. SPACF: "A secure privacy-preserving authentication scheme for VANET with cuckoo filter". *IEEE Transactions on Vehicular Technology*, 66(11), pp.10283-10295.

- [14] M.Aissa,B.Bouhdid,A.Ben Mnaouer,A.Belghith and S.AiAhmadi, 2020. SOFCluster: “Safety-oriented, fuzzy logic-based clustering scheme for vehicular ad hoc networks”. *Transactions on Emerging Telecommunications Technologies*, p.e3951.
- [15] C.F.Lin and S.D.Wang, 2002. “Fuzzy support vector machines. *IEEE transactions on neural network*’s, 13(2), pp.464-471.
- [16] X.Gu,T.Ni and H.Wang, 2014. “New fuzzy support vector machine for the class imbalance problem in medical datasets classification”. *The scientific world journal*, 2014.
- [17] C.L.Wei and G.G.Wang, 2020. “Hybrid Annealing Krill Herd and Quantum-Behaved Particle Swarm Optimization”. *Mathematics*, 8(9), p.1403.
- [18] A.S.Khan, K.Balan,Y.Javed,S.Tarmizi and J.Abdullah, 2019. “Secure trust-based blockchain architecture to prevent attacks in VANET”. *Sensors*, 19(22), p.4954.
- [19] M.Maheswari and R.A.Karthika, 2021. “A Novel QoS Based Secure Unequal Clustering Protocol with Intrusion Detection System in Wireless Sensor Networks”. *Wireless Personal Communications*, pp.1-23.

# Chest Diseases Prediction from X-ray Images using CNN Models: A Study

Latheesh Mangeri<sup>1</sup>

Research Scholar, Computer Science  
& Engineering  
CHRIST University  
Bangalore, India

Gnana Prakasi O S<sup>2</sup>, Kanmani P<sup>4</sup>

Assistant Professor, Computer  
Science & Engineering  
CHRIST University  
Bangalore, India

Neeraj Puppala<sup>3</sup>

Research Scholar, Electronics &  
Communication Engineering  
CHRIST University  
Bangalore, India

**Abstract**—Chest Disease creates serious health issues for human beings all over the world. Identifying these diseases in earlier stages helps people to treat them early and save their life. Conventional Neural Networks play an important role in the health sector especially in predicting diseases in the earlier stages. X-rays are one of the major parameters which help to identify Chest diseases accurately. In this paper, we study the prediction of chest diseases such as Pneumonia, COVID-19, and Tuberculosis (TB) from the X-ray images. The prediction of these diseases is analyzed with the support of three CNN Models such as VGG19, Resnet50V2, and Densenet201, and results are elaborated in the terms of Accuracy and Loss. Though all three models are highly accurate and consistent, considering the factors like architectural size, training speed, etc. Resnet50V2 is the best model for all three diseases. It trained with F1 score accuracies of 0.98,0.92,0.97 for pneumonia, tuberculosis, covid respectively.

**Keywords**—Convolutional neural networks; VGG19; ResNet50V2; DenseNet201

## I. INTRODUCTION

Historically, Chest diseases are very serious health problems in the life of people. These diseases include chronic obstructive pulmonary disease, pneumonia, asthma, tuberculosis, and lung diseases. The timely infectious diseases have had civilization-altering consequences. so, diagnosis of chest diseases in the early stage is very important. To estimate the importance of diseases, different measures such as morbidity and mortality can be used. An X-ray is a quick, painless test that produces images of the structures inside your body. pneumonia, tuberculosis, or lung cancer can show up on chest X-rays. Generally, however, radiation exposure from an X-ray is low, and the benefits from these tests far outweigh the risks [1].

The study of major diseases from x-rays becomes a most challenging task. In this study, we have considered 3 diseases Pneumonia, COVID-19, and Tuberculosis (TB) these diseases can be easily identified using chest X-rays and CT scans. Chest X-rays are normally painless and non-invasive radiological tests to screen and diagnose many lung diseases also other methods such as CT and MRI can be used. Chest X-ray is fast, easy and inexpensive than CT and MRI and they are mostly used in emergency diagnosis and treatment of lungs, hearts, and chest wall diseases. Coronavirus disease 2019 (COVID-19) is an infectious disease caused by a

coronavirus strain called severe acute respiratory syndrome coronavirus [2]. Results show that chest X-rays correctly diagnosed COVID-19 in 99% of people who had COVID-19. However, it incorrectly identified COVID-19 in 1% of people who did not have COVID-19 [3]. Pneumonia is a form of acute respiratory infection that is most commonly caused by viruses or bacteria [4,5]. The X-rays scans show 92 % of accuracy. Tuberculosis (TB) is caused by a bacterium called *Mycobacterium tuberculosis*. A total of 1.4 million people died from TB in 2019 [6,7]. X -rays help in 99% of the identification of tuberculosis.

The challenges and the increase in the number of cases for these diseases motivate us to explore the methods that help to study how to accurately identify this disease to help humans. Currently, Artificial Intelligence (AI) especially Machine Learning (ML) and Deep Learning (DL) algorithms help to effectively identify these diseases. For our study, we considered pre-trained deep Convolutional Neural Networks (CNNs) as feature extractors to extract powerful and discriminative deep features from brain magnetic resonance (MR) images and Chest X-ray images for various ML classifiers and deep learning networks to identify the infected and uninfected images. Also, to investigate the benefits of combining features from different pre-trained CNN models by comparing their Accuracies.

Our experiment results demonstrate that the ensemble of deep features can help to improve performance significantly. In this paper, we considered 3 datasets of disease X-rays namely COVID19, Pneumonia, Tuberculosis, and performed comparisons on various CNN pre-trained models VGG19, Resnet50V2, Densenet201. In summary, our contributions are listed as follows:

- We designed and implemented a fully automatic disease classification, in which the pre-trained CNN VGG19, Resnet50V2, Densenet201 models extract the deep features from X-ray images.
- This is executed in three steps: (1) Training the model using CNN models (2) Comparing the pre-trained models based on their accuracies and losses (3) Selecting the top fine-tuned model to achieve state-of-the-art performance for disease classification in X-ray images.

- We conducted extensive experiments on 3 datasets namely Pneumonia, COVID, Tuberculosis, and for each 3 pre-trained models namely VGG19, Resnet50V2, and Densenet201 to analyze the classification accuracy and precision for these models.

The Related works are described in section 2. Section 3 highlights the datasets and methodology, section 4 with model architecture section 5 shows a more detailed performance analysis. The Conclusion and future work are discussed in Section 6.

## II. LITERATURE SURVEY

Many papers addressed CT scan and x-ray diagnosis of COVID, Irfan Ullah Khan et al. [8] compared the COVID-19 x-ray images by performing different deep learning techniques DenseNet121, ResNet50, VGG16, and VGG19 with accuracies of 96-99% and stated overall accuracy of 99.33% VGG16 and VGG19. Kumar [9] used ResNet50 and Support Vector Machine (SVM) classification for the diagnosis of COVID in x-ray images and got an accuracy of 95.38% for binary classes. Also, Ali [10] found the highest accuracy of 98% for ResNet50 using X-ray datasets [11]. However, most of the research is carried out for small datasets. When the size of the dataset increases it shows some in-efficiencies. Hence in our paper, we analyze the performance of the X-ray dataset in a large volume and the implications are measured.

In the research of classification of X-ray images, Rachna Jain[12] performs several pre-trained convolutional neural networks(CNN) on pneumonia x-rays to classify x-ray images into two classes i.e. pneumonia and non-pneumonia by varying different parameters and layers. She had compared 4 pre-trained models VGG16, VGG19, ResNet50, and Inception-v3 with accuracies of 87.28%, 88.46%, 77.56%, and 70.99% respectively. Similarly [13,14] examines various deep convolutional neural networks (DCNNs) for the prediction of tuberculosis and shows Densenet201 has better accuracy when compared to other algorithms. And [15] shows the analysis of various CNN algorithms in the prediction of Tuberculosis with different classification theories of tuberculosis. [16,17] proposed a deep learning-based approach using Densenet-121 with the radiology image learned by the CheXnet model to detect COVID-19 patients and performance analysis of these algorithms in the detection. [18, 19] also describes the study on pneumonia with two convolutional neural network models Xception and VGG16.

Megha Chandra et al. [20] proposed a CNN-based MobileNet architecture for detecting diseases in plants. Authors in [21,22] proposed a method performing by combining clustering and classification for the effective diagnosis of tuberculosis. This model has various algorithms such as K-means, C4.5 decision tree, K-NN, Naive Bayes, and SVM which produced an accuracy of 98.7%. They concluded that the SVM algorithm provided better accuracy in predicting tuberculosis. Lakhani P. [23] trained a deep CNN for the automated classification of pulmonary tuberculosis from chest radiographs. AlexNet and GoogLeNet, which are dual CNNs, were used for classification purposes. The dataset was pre-processed before evaluation. Their model had a high accuracy of 0.99. Their model had a specificity of 100% and a

sensitivity of 97.3%. Anthimopoulos M. et al [24] The input dataset images are of size 256X256 pixels. The accuracy of the model is 0.964 on an average specificity and sensitivity of 91% showing that deep convolutional neural networks can be developed with high classification accuracy and can help in the diagnosis procedure. [25] proposed a Reliable Learning with Partial differential equation to detect various diseases from Chest X-rays.

Along with x-rays, MRI reports also play a major role in the diagnosis of brain diseases. Studying MRI reports is much more difficult than x-rays, a researcher named Ahmed Kharrat [26], proposed a hybrid approach for classifying Brain tissues in MRI based on a Genetic Algorithm(GA) and Support Vector Machine(SVM). He performed his research with fewer datasets consisting of 83 images, due to the small size of the dataset SVM classifier is employed. These two algorithms give heady results in classifying brain tumors. 94.44% accuracy is obtained while performing the following technique SGLDM+GA+SVM and 96.29% accuracy is obtained for WT+SGLDM+GA+SVM.

From the survey, X-ray images are very helpful in detecting most chest-related diseases. As a continuation of this, we began our research in analyzing these Chest diseases once again with three CNN models and the results are discussed.

## III. METHODOLOGY

The methodology includes the analysis of the 3 datasets for three chest diseases with the three different CNN models. The execution steps include pre-processing of the x-ray images and the classification of data into normal cases and infected cases.

The dataset underwent different image processing techniques for the image analysis and to retrieve the values from those images. The given dataset is divided into three sets for the processing train data, test data, and validation data. The Pneumonia dataset is split before computation. Other datasets COVID, Tuberculosis are split with the ratios of 75:10:15 for train, test, and validation. The processed image sets are passed through the different layers present in the pre-trained model, which generates a model for disease classification by comparing it with the untrained imageset.

### A. Data Pre-Processing

The pre-processing execution starts once the images are resized and augmented. NumPy tensor is used as the function for preprocessing and it produces the output image of the same shape. In the data pre-processing image will be resized to 224x224x3 and then it is converted to an array to store the values. Each value in an array is rescaled by 255. The tensor input will insert a dimension of length at the index axis of the input's shape to refer to the values. The dimension index follows indexing rules which are given as: It's zero-based, a negative index is counted backward from the end. It helps in aligning axes for broadcasting, to add an inner vector length axis to a tensor of scalars.

**B. Classification**

Classification is a task that requires the use of machine learning algorithms that learn how to assign a class label to examples from the problem domain. The pre-trained architecture generated a model with various arguments by validating the trained set with a validation set for 50 epochs to learn from the losses of previous epochs gives good accuracy. This validation process plays a major role in the detection to classify infected and uninfected images. In the end, it tries to draw some conclusions from the input values given for training in the form of the confusion matrix and line graphs. It will predict the class labels/categories for the new data. The execution procedure is shown in Fig. 1.

In this model, we are using the algorithms of Conventional Neural Networks. VGG19, DenseNet201, and ResNet50V2 models of CNN are used for training the different datasets and the prediction accuracy is measured for these models.

**C. Datasets**

Below datasets are extracted from Kaggle namely Pneumonia, COVID, Tuberculosis dataset with the size of 1.15GB, 1.97GB, 662.49MB respectively.

The pneumonia dataset contains 5856 images of which 5216 are used for training with all three models, 624 for the test, and 16 for validation as shown in Fig. 2. This dataset consists of two categories of images – Pneumonia cases, Normal cases. The dataset was obtained from

Kaggle:<https://www.kaggle.com/paultimothymooney/chest-xray-pneumonia>.

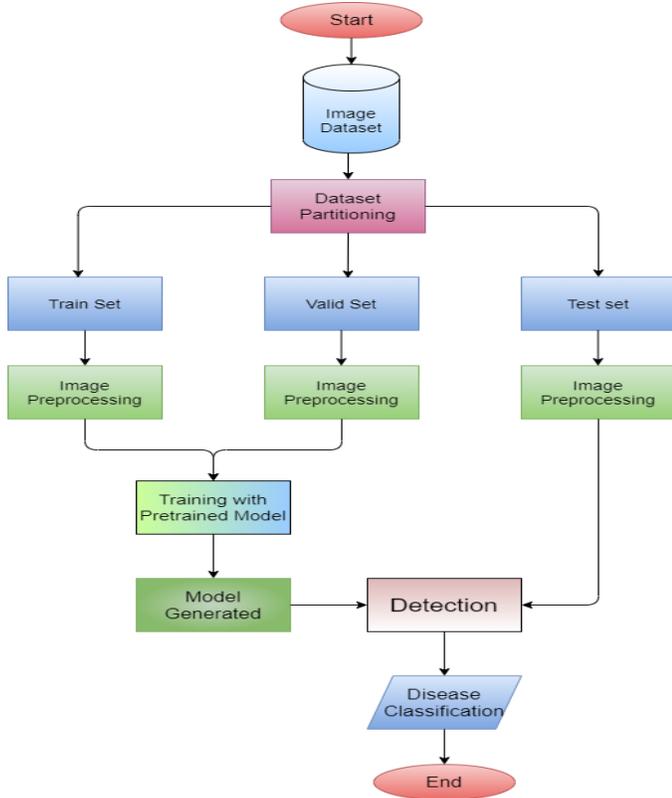


Fig. 1. Data Flow Model of the Execution Procedure.

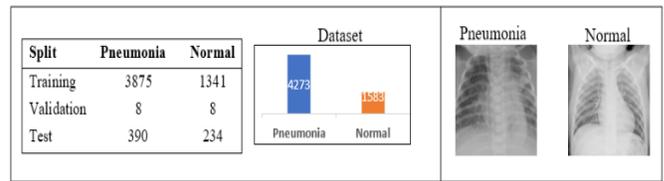


Fig. 2. Data Classification Pneumonia.

COVID dataset contains 4606 captured images in which 3470 are used for training the model, 562 for the test, and 674 for validation as shown in Fig. 3. This dataset consists of two categories of images – COVID, Normal. The dataset obtained from Kaggle:<https://www.kaggle.com/amanullahasraf/covid19-pneumonia-normal-chest-xray-pa-dataset?select=covid>.

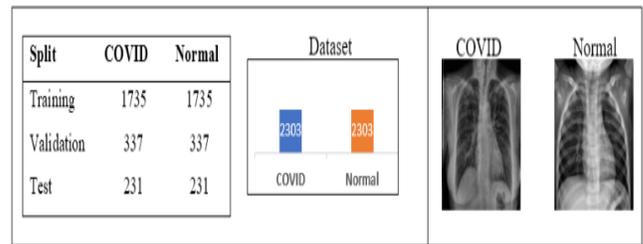


Fig. 3. Data Classification COVID 19.

The tuberculosis dataset contains 4606 images in which 3470 are used for training the model, 562 for the test, and 674 for validation as shown in Fig. 4. This dataset consists of two categories of images – Tuberculosis infected chest, Normal chest. The dataset obtained from Kaggle:<https://www.kaggle.com/tawsifurrahman/tuberculosis-tb-chest-xray-dataset>.

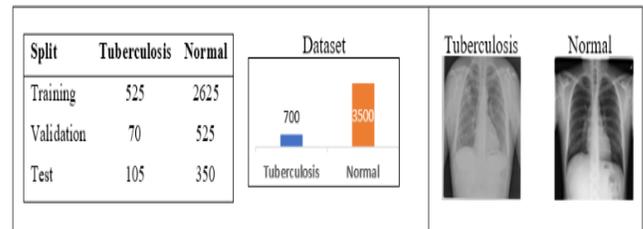


Fig. 4. Data Classification Tuberculosis.

**IV. EVALUATION OF THE MODEL**

The untrained test set has gone through the same pre-processing steps and is used to test the generated model which predicts the image with a suitable label, where end users can test their x-rays and uses the result for their study. The saved trained model can be further converted to an API for a mobile application to create a better user interface for users.

**A. VGG19 Architecture**

VGG model consists of a variety of models like VGG11, VGG16, and many more, among them VGG19 consists of 19 layers (16 convolution layers, 3 fully connected layers, 5 MaxPool layers, and 1 SoftMax layer) and 19.6 billion FLOPs. The input to VGG based convNet is a 224x224 grayscale image. Preprocessing layer takes the grayscale image with pixel values in the range of 0 to 255. The processing model for the VGG 19 is shown in Fig. 5.

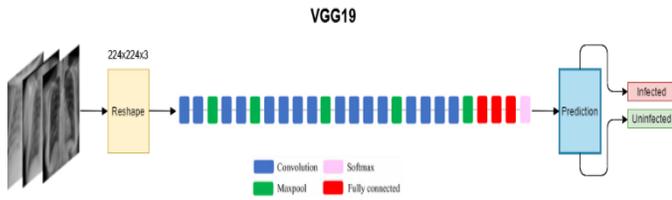


Fig. 5. VGG19 Processing Model.

B. ResNet50V2 Architecture

Resnet50V2 is a huge architecture, it is taken and modified from Resnet50 in later years for better performance than previous architectures like resnet101. It is a contemporary convolution neural network (CNN) which addresses vanishing gradient problems using residual blocks in the architecture. In a residual network, multiple residual blocks are stacked up one after another. Each residual block is formed of short-cut connections skipping one or more layers. Resnet50V2 uses the pre-activation of weight layers. ResNet50V2 achieves accurate predictions on the datasets. The processing model for Resnet50V2 is shown in Fig. 6.

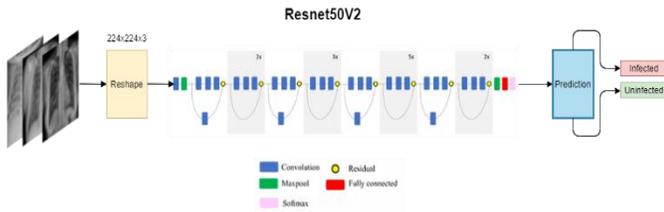


Fig. 6. Resnet50V2 Processing Model.

C. DenseNet201 Architecture

DenseNet-201 is a convolutional neural network that is 201 layers deep. Recent work has shown that convolutional networks can be substantially deeper, more accurate, and efficient to train if they contain shorter connections between layers close to the input and those close to the output. DenseNet connects each layer to every other layer in a feed-forward fashion. Whereas traditional convolutional networks with L layers have L connections - one between each layer and its subsequent layer - the DenseNet network has  $L(L+1)/2$

direct connections. For each layer, the feature maps of all preceding layers are used as inputs, and their feature maps are used as inputs into all subsequent layers[21,22]. DenseNets have several compelling advantages: they alleviate the vanishing gradient problem, strengthen feature propagation, encourage feature reuse, and substantially reduce the number of parameters. The processing model for Densenet201 is shown in Fig. 7.

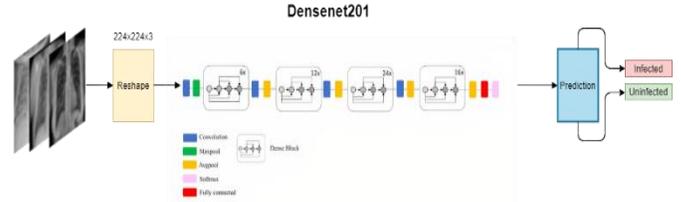


Fig. 7. Densenet201 Processing Model.

V. PERFORMANCE ANALYSIS

The performances of these three VGG19, Resnet50V2, and Densenet201 algorithms are analyzed for all the diseases data set COVID, Pneumonia, and Tuberculosis. The metrics used for performance analysis are defined in terms of Accuracy, Loss, Confusion matrix, and Classification report. The simulation is done in python with TensorFlow and Keras. Keras Layers are the functional building blocks of Keras Models. These layers are fed with input information, they process this information, do some computation and hence produce the output. Also, we used matplotlib for data visualization and a few standard libraries like NumPy and Pandas for calculations of image arrays.

A. Classification Report

a) Pneumonia: Pneumonia causes the lungs that fill with fluid and make breathing difficult. The analysis is made with the help of 624 values. Table 1. a and Table 1.b shows the confusion matrix and classification report of all Pneumonia datasets which is compared for all three algorithms. From the analysis, it can be identified that Resnet50V2 and VGG19 show high prediction accuracy with 92% and Densenet201 shows 91% of accuracy.

TABLE I. (A) PNEUMONIA-CONFUSION MATRIX

	Predicted Normal			Predicted Pneumonia		
	VGG 19	Resnet50V2	Densenet201	VGG 19	Resnet50V2	Densenet201
Actual Normal	376	383	384	37	41	51
Actual Pneumonia	14	7	6	197	193	183

(B) PNEUMONIA-CLASSIFICATION REPORT

	Precision			Recall			F1-Score			Support
	VGG 19	Resnet50V2	Densenet201	VGG 19	Resnet50V2	Densenet 201	VGG 19	Resnet50V2	Densenet201	
Normal	0.91	0.96	0.97	0.84	0.82	0.78	0.89	0.89	0.87	234
Pneumonia	0.93	0.90	0.88	0.96	0.98	0.88	0.94	0.94	0.93	390
Accuracy							0.92	0.92	0.91	624
Macro Avg	0.92	0.93	0.93	0.90	0.90	0.88	0.91	0.92	0.90	624
Weighted Avg	0.92	0.93	0.91	0.92	0.92	0.91	0.92	0.92	0.91	624

b) *Tuberculosis*: Tuberculosis caused by bacteria usually attacks the lungs, but TB bacteria can attack any part of the body such as the kidney, spine, and brain. TB is spread from person to person through the air. The analysis is made with the help of 422 values. VGG19 and Densenet201 show 99% of accuracy for Tuberculosis as shown in Table 2.a and Table 2.b and ResNet50V2 show 98% of prediction accuracy.

c) *COVID19*: COVID-19 is an infectious disease caused by a coronavirus strain called severe acute respiratory syndrome coronavirus. The analysis is made with the help of 422 values for testing. The result is shown in Table 3.a and Table 3.b shows VGG19 shows 98% whereas 97% for

ResNet50V2 and 96% for Densenet201. This shows that Though all the models are similar the VGG19 shows better accuracy in the prediction.

The overall analysis shows VGG19 and the Resnet50V2 show more accuracy when compared to Densenet201.

**B. Training Vs Validation Set**

This section shows the comparative analysis of the algorithms concerning Loss and Accuracy of the data during the training and the validation process of the dataset. Table 4 shows the values of performance measures in terms of loss and accuracy achieved by models VGG19, ResNet50V2 and DenseNet201.

TABLE II. (A). TUBERCULOSIS-CONFUSION MATRIX

	Predicted Normal			Predicted Tuberculosis		
	VGG 19	Resnet50V2	Densenet201	VGG 19	Resnet50V2	Densenet201
Actual Normal	104	94	103	4	0	1
Actual Tuberculosis	1	11	2	346	350	349

(B). TUBERCULOSIS-CLASSIFICATION REPORT

	Precision			Recall			F1-Score			Support
	VGG 19	Resnet50V2	Densenet201	VGG 19	Resnet50V2	Densenet 201	VGG 19	Resnet50V2	Densenet201	
Normal	0.96	0.97	0.99	0.99	1.00	1.00	0.99	0.98	1.00	350
Tuberculosis	1.00	1.00	0.99	0.99	0.90	0.98	0.98	0.94	0.99	105
Accuracy							0.99	0.98	0.99	455
Macro Avg	0.98	0.95	0.99	0.99	0.95	0.99	0.98	0.96	0.99	455
Weighted Avg	0.99	0.98	0.99	0.99	0.98	0.99	0.99	0.98	0.99	455

TABLE III. (A). COVID-CONFUSION MATRIX

	Predicted Normal			Predicted COVID		
	VGG 19	Resnet50V2	Densenet201	VGG 19	Resnet50V2	Densenet201
Actual Normal	226	231	231	2	13	18
Actual COVID	5	0	0	229	218	213

(B). COVID-CLASSIFICATION REPORT

	Precision			Recall			F1-Score			Support
	VGG 19	Resnet50V2	Dense-net201	VGG 19	Resnet50V2	Densenet 201	VGG 19	Resnet50V2	Densenet201	
Normal	0.99	0.95	0.93	0.98	1.00	1.00	0.98	0.97	0.96	231
COVID	0.98	1.00	1.00	0.99	0.94	0.92	0.98	0.97	0.96	231
Accuracy							0.98	0.97	0.96	462
Macro Avg	0.98	0.97	0.96	0.98	0.97	0.96	0.98	0.97	0.96	462
Weighted Avg	0.98	0.97	0.96	0.98	0.97	0.96	0.98	0.97	0.96	462

TABLE IV. PERFORMANCE MEASURES

Disease name	CNN Model	Train Loss	Train accuracy	Validation Loss	Validation Accuracy
Pneumonia	VGG19	0.0308	0.9879	0.1036	0.9375
	ResNet50V2	0.1396	0.9916	4.8358	0.8750
	DenseNet201	0.0889	0.9904	0.000001	0.1000
Tuberculosis	VGG19	0.1041	0.9699	0.0469	0.9899
	ResNet50V2	0.0125	0.9971	0.0212	0.9916
	DenseNet201	0.0068	0.9996	0.00009	0.1000
COVID 19	VGG19	0.0721	0.9716	0.1201	0.9555
	ResNet50V2	0.0848	0.9930	0.9956	0.9570
	DenseNet201	0.1172	0.9823	0.4328	0.9599

a) *Train Loss*: The training loss for the pneumonia are 0.0308, 0.1396, 0.0889 for the models VGG19, ResNet50V2, and DenseNet201 shown in Table 4 and the training loss for each epoch is shown in Fig. 8. (a). Similarly, the training loss for tuberculosis is 0.1041, 0.0125, 0.0068 for the models VGG19, ResNet50V2, and DenseNet201 shown in Table 4 and the training loss for each epoch is shown in Fig. 8. (b). Finally, the training loss for the COVID19 are 0.0721, 0.0848, 0.1172 for the models VGG19, ResNet50V2, and DenseNet201 shown in Table 4 and the training loss for each epoch is shown in Fig. 8. (c).

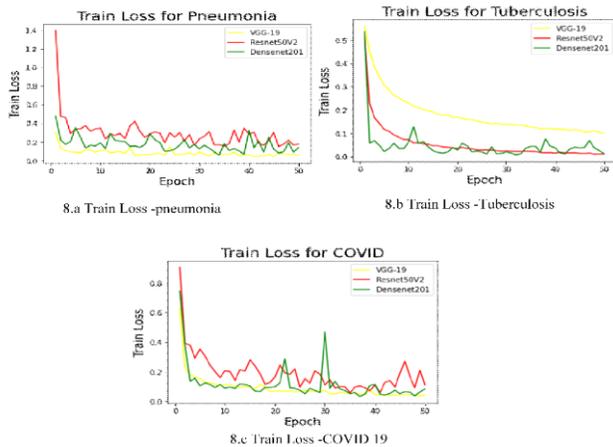


Fig. 8. Train Loss Vs Epoch.

b) *Validation Loss*: The Validation loss for the pneumonia is 0.1036, 4.8358, 0.000001 for the models VGG19, ResNet50V2, and DenseNet201 shown in Table 4 and the Validation loss for each epoch is shown in Fig. 9. (a). Similarly, the Validation loss for tuberculosis are 0.0469, 0.0212, 0.00009 for the models VGG19, ResNet50V2, and DenseNet201, and the Validation loss for each epoch is shown in Fig. 9. (b). Finally, the Validation loss for the COVID19 are 0.1201, 0.9956, 0.4328 for the models VGG19, ResNet50V2, and DenseNet201, and the validation loss for each epoch is shown in Fig. 9. (c).

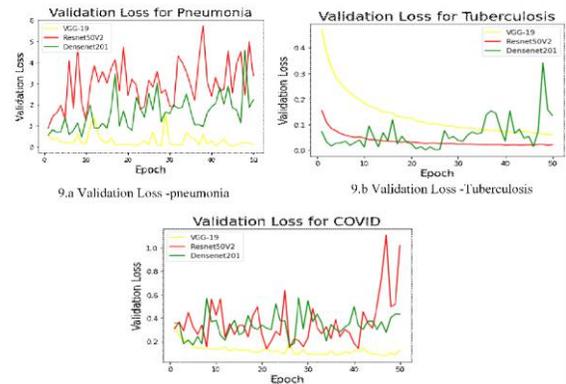


Fig. 9. Validation Loss Vs Epoch.

c) *Training Accuracy*: The training accuracy for the pneumonia is 0.9879, 0.9916, 0.9904 for the models VGG19, ResNet50V2, and DenseNet201 shown in Table 4 and the training accuracy for each epoch is shown in Fig. 10. (a). Similarly, the training accuracy for tuberculosis is 0.9699, 0.9971, 0.9996 for the models VGG19, ResNet50V2, and DenseNet201 shown in Table 4 and the training accuracy for each epoch is shown in Fig. 10. (b). Finally, the training accuracy for the COVID19 are 0.9716, 0.9930, 0.9823 for the models VGG19, ResNet50V2, and DenseNet201 shown in Table 4 and the training accuracy for each epoch is shown in Fig. 10. (c).

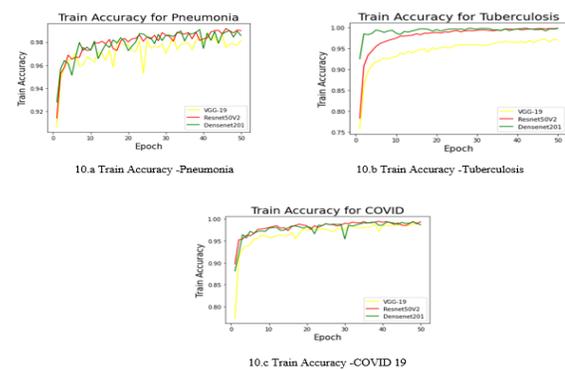


Fig. 10. Train Accuracy Vs Epoch.

d) *Validation Accuracy*: The validation accuracy for the pneumonia are 0.9375, 0.8750, 0.1 for the models VGG19, ResNet50V2 and DenseNet201 shown in Table 4 and the validation accuracy for each epoch is shown in Fig. 11. (a). Similarly, the Validation accuracy for tuberculosis are 0.9899, 0.9916, 0.1 for the models VGG19, ResNet50V2 and DenseNet201 shown in Table 4 and the validation accuracy for each epoch is shown in Fig. 11. (b). Finally, the validation accuracy for the COVID19 are 0.9555, 0.9570, 0.9599 for the models VGG19, ResNet50V2 and DenseNet201 shown in table 4 and the validation accuracy for each epoch is shown in Fig. 11. (c).

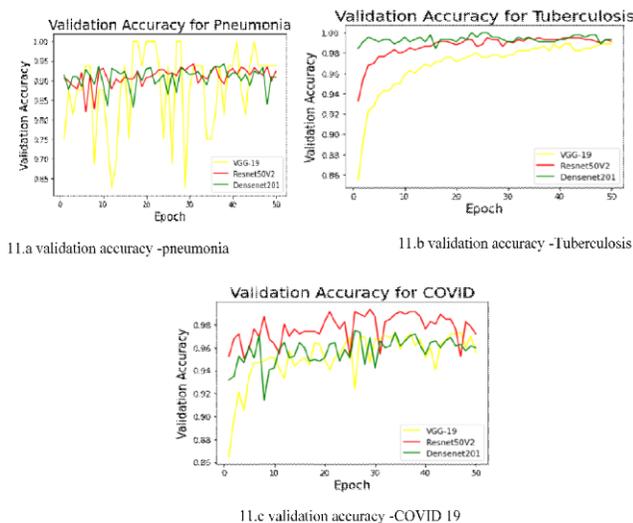


Fig. 11. Validation Accuracy vs Epoch.

## VI. CONCLUSION AND FUTURE WORK

High precise diagnostic results are expected in helping the healthcare system to provide efficient services to the patient in less time. To attain this goal a CNN model was built in our research to study x-rays images of covid 19, pneumonia, tuberculosis. For this, we study VGG19, ResNet50V2, DenseNet201 architectures, and their performances have been analyzed with the X-ray images. We used Adam optimizer and trained for 50 epochs. Though all three models are highly accurate and consistent, considering the factors like architectural size, training speed, etc. Resnet50V2 is the best model for all three diseases. It trained with F1 score accuracies of 0.98,0.92,0.97 for pneumonia, tuberculosis, covid respectively.

In this study, we can't predict the diseases at the earlier stages. So, to predict the above chest diseases in earlier stages with the support of other parameters can be extended as part of future work.

### REFERENCES

[1] X-Ray: Imaging Test Quickly Helps Diagnosis - Mayo Clinic. <https://www.mayoclinic.org/tests-procedures/x-ray/about/pac-20395303>. Accessed 16 Aug. 2021.

[2] Martínez Chamorro, E., et al. "Radiologic Diagnosis of Patients with COVID-19." *Radiologia (English Edition)*, vol. 63, no. 1, Jan. 2021, pp. 56–73. [www.elsevier.es, https://doi.org/10.1016/j.rxeng.2020.11.001](https://doi.org/10.1016/j.rxeng.2020.11.001).

[3] Hwang, Eui Jin, et al. "COVID-19 Pneumonia on Chest X-Rays: Performance of a Deep Learning-Based Computer-Aided Detection System." *PLOS ONE*, vol. 16, no. 6, June 2021, p. e0252440. [PLoS Journals, https://doi.org/10.1371/journal.pone.0252440](https://doi.org/10.1371/journal.pone.0252440).

[4] "Health topics", *Who.int*, 2021. [Online]. Available: <https://www.who.int/health-topics/>. [Accessed: 12- Sep- 2021].

[5] *Stoppneumonia.org*, 2021. [Online]. Available: <https://stoppneumonia.org/wp-content/uploads/2019/11/India-12.11.2019-Web.pdf>. [Accessed: 12- Sep- 2021].

[6] CDCTB. "Tuberculosis (TB)- Basic TB Facts." Centers for Disease Control and Prevention, 19 June 2019, <https://www.cdc.gov/tb/topic/basics/default.htm>.

[7] Mar 02, Published: and 2021. "The U.S. Government and Global Tuberculosis Efforts." KFF, 2 Mar. 2021, <https://www.kff.org/global-health-policy/fact-sheet/the-u-s-government-and-global-tuberculosis-efforts/>

[8] Khan, Irfan Ullah, and Nida Aslam. "A Deep-Learning-Based Framework for Automated Diagnosis of COVID-19 Using X-Ray Images." *Information*, vol. 11, no. 9, Sept. 2020, p. 419. [www.mdpi.com, https://doi.org/10.3390/info11090419](https://doi.org/10.3390/info11090419).

[9] Sethy, Prabira Kumar, and Santi Kumari Behera. Detection of Coronavirus Disease (COVID-19) Based on Deep Features. Mar. 2020. [www.preprints.org, https://doi.org/10.20944/preprints202003.0300.v1](https://doi.org/10.20944/preprints202003.0300.v1).

[10] Cohen, Joseph Paul, et al. "COVID-19 Image Data Collection." *ArXiv:2003.11597 [Cs, Eess, q-Bio]*, Mar.2020. [arXiv.org, http://arxiv.org/abs/2003.11597](http://arxiv.org/abs/2003.11597).

[11] Chest X-Ray Images (Pneumonia). <https://kaggle.com/paultimothymooney/chest-xray-pneumonia>. Accessed 16 Aug. 2021.

[12] Jain, Rachna, et al. "Pneumonia Detection in Chest X-Ray Images Using Convolutional Neural Networks and Transfer Learning." *Measurement*, vol. 165, Dec. 2020, p. 108046. [DOI.org \(Crossref\), https://doi.org/10.1016/j.measurement.2020.108046](https://doi.org/10.1016/j.measurement.2020.108046).

[13] Ho, Thi Kieu Khanh ; Gwak, Jeonghwan ; Prakash, Om ; Song, Jong In ; Park, Chang Min. / Utilizing Pretrained Deep Learning Models for Automated Pulmonary Tuberculosis Detection Using Chest Radiography. *Intelligent Information and Database Systems - 11th Asian Conference, ACIIDS 2019,17*.

[14] Jian Liu and Yidi Huang. 2020. Comparison of Different CNN Models in Tuberculosis Detecting. *KSII Transactions on Internet and Information Systems*, 14, 8, (2020), 3519-3533. DOI: 10.3837/tiis.2020.08.021.

[15] T. Rahman et al., "Reliable Tuberculosis Detection Using Chest X-Ray With Deep Learning, Segmentation and Visualization," in *IEEE Access*, vol. 8, pp. 191586-191601, 2020, doi: 10.1109/ACCESS.2020.3031384.

[16] Sarker, L.; Islam, M.M.; Hannan, T.; Ahmed, Z. COVID-DenseNet: A Deep Learning Architecture to Detect COVID-19 from Chest Radiology Images. *Preprints* 2020, 2020050151 (doi: 10.20944/preprints202005.0151.v1).

[17] E. Ayan and H. M. Ünver, "Diagnosis of Pneumonia from Chest X-Ray Images Using Deep Learning," 2019 Scientific Meeting on Electrical-Electronics & Biomedical Engineering and Computer Science (EBBT), 2019, pp. 1-5, doi: 10.1109/EBBT.2019.8741582.

[18] Shazia, A., Xuan, T.Z., Chuah, J.H. et al. A comparative study of multiple neural network for detection of COVID-19 on chest X-ray. *EURASIP J. Adv. Signal Process.* 2021, 50 (2021). <https://doi.org/10.1186/s13634-021-00755-1>.

[19] Asnaoui, Khalid & Youness, Chawki & Idrı, Ali. (2020). Automated Methods for Detection and Classification Pneumonia based on X-Ray Images Using Deep Learning.

[20] N. V. Megha Chandra Reddy, K. A. Reddy, Sushanth. G and Sujatha. S, "Plant Disease Diagnosis and Solution System Based on Neural Networks", *Indian Journal of Computer Science and Engineering (IJCSE)*, vol. 12, no. 4, pp. 1084-1092, 2021, doi: 10.21817/indjcs/2021/v12i4/211204218.Link:<https://doi.org/10.21817/indjcs/2021/v12i4/211204226>.

[21] Subramanyam, Natarajan. A Data Mining Approach to the Diagnosis of Tuberculosis by Cascading Clustering and Classification. [www.academia.edu](http://www.academia.edu)

- [https://www.academia.edu/19259905/A\\_Data\\_Mining\\_Approach\\_to\\_the\\_Diagnosis\\_of\\_Tuberculosis\\_by\\_Cascading\\_Clustering\\_and\\_Classification](https://www.academia.edu/19259905/A_Data_Mining_Approach_to_the_Diagnosis_of_Tuberculosis_by_Cascading_Clustering_and_Classification). Accessed 16 Aug. 2021.
- [22] K. A. Reddy, N. V. M. C. Reddy and S. Sujatha., "Precision Method for Pest Detection in Plants using the Clustering Algorithm in Image Processing," 2020 International Conference on Communication and Signal Processing (ICCSP), 2020, pp. 894-897, doi: 10.1109/ICCSP48568.2020.9182190.
- [23] Lakhani, Paras, and Baskaran Sundaram. "Deep Learning at Chest Radiography: Automated Classification of Pulmonary Tuberculosis by Using Convolutional Neural Networks." *Radiology*, vol. 284, no. 2, Aug. 2017, pp. 574–82. [pubs.rsna.org](https://pubs.rsna.org) (Atypon), <https://doi.org/10.1148/radiol.2017162326>.
- [24] Anthimopoulos, Marios, et al. "Lung Pattern Classification for Interstitial Lung Diseases Using a Deep Convolutional Neural Network." *IEEE Transactions on Medical Imaging*, vol. 35, no. 5, May 2016, pp.1207–16. PubMed, <https://doi.org/10.1109/TMI.2016.2535865>.
- [25] Marginean AN, Muntean DD, Muntean GA, Priscu A, Groza A, Slavescu RR, Timbus CL, Munteanu GZ, Morosanu CO, Cosnarovici MM, Pinteá C-M. Reliable Learning with PDE-Based CNNs and DenseNets for Detecting COVID-19, Pneumonia, and Tuberculosis from Chest X-Ray Images. *Mathematics*. 2021; 9(4):434. <https://doi.org/10.3390/math9040434>.
- [26] Kharrat, Ahmed & Karim, Gasmi & ben messaoud, Mohamed & Benamrane, Nacéra & Mohamed, Abid. (2010). A Hybrid Approach for Automatic Classification of Brain MRI Using Genetic Algorithm and Support Vector Machine. *Leonardo Journal of Sciences*. 17.

# Detection of Acute Myeloid Leukemia based on White Blood Cell Morphological Imaging using Naïve Bayesian Algorithm

Esti Suryani<sup>1</sup>, Wiharto<sup>2\*</sup>, Adi Prasetya Putra<sup>3</sup>, Wisnu Widiarto<sup>4</sup>  
Department of Informatics, Universitas Sebelas Maret, Surakarta, Indonesia

**Abstract**—The process of diagnosing AML is based on the complete blood-count analysis of the patients. As such, it involves high energy consumption, long completion times, and is rather expensive compared to conventional medical practices. One of the methods for identifying tumor cells involves the utilization of image-processing techniques based on the morphology of white blood cells (WBCs). The principal objective of this study involves the identification of AML cells—especially of the AML M1 and AML M2 types—through morphological imaging of WBCs using the Naïve Bayes' Classifier. The Image-processing methods used in this study include YCbCr color space classification, image thresholding, morphological operations, chain code representation, and the use of bounding boxes. Regardless of the processing technique used, all identification procedures, performed in this study, were based on the Naïve Bayes' Classifier. The test process was performed on 30 images of each of the AML M1 and M2 cell types. The use of the cell identification method proposed in this study demonstrated an accuracy of 73.33%. While the accuracy of cell type identification is 54.92%. Based on the results obtained in this study, it is inferred that the Naïve Bayes' Classifier method can be employed in the process of identifying dominant AML cell types amongst AML M1 and AML M2 (myeloblast, promyelocyte, myelocyte, and metamyelocyte) based on the morphology of WBCs.

**Keywords**—Leukemia; acute myeloid leukemia; morphology; image processing; Naïve Bayes

## I. INTRODUCTION

Leukemia is a type of cancer, where the bone marrow tends to produce abnormal white blood cells (WBCs) [1]. Leukemia may be divided into four main types—acute myeloid leukemia (AML), chronic myeloid leukemia (CML), acute lymphoblastic leukemia (ALL), and chronic lymphocytic leukemia (CLL). AML is the most commonly diagnosed type of leukemia; of all cases of AML diagnosed to date, 80% have been found to occur in adults, and 15–20% cases have been found to occur in children [2].

National Cancer Institute, 2013 maintains a record of the occurrence of AML amongst adults belonging to different age groups. It is seen that in the age group of 30–34 years, a single case of leukemia is recorded per 100,000 people; between 65–69 years, these numbers increase by ten times to 10 cases per 100,000 people. This number increases still further for adults beyond 70 years of age and the trend continues to rise until the age group of 80–84 years[3]. In general, the process of diagnosing AML involves analysis of the complete blood count of the patient, wherein the pathologist counts the number of red

blood cells, WBCs, platelets, and checks for the presence of abnormal WBCs[4]. However, this method is time-consuming, requires energy, and is one of the most expensive routine tests performed in clinical hematological laboratories[5].

According to the French–America–British (FAB) classification, AML is classified into eight types—M0, M1, M2, M3, M4, M5, M6, M7[6]. This classification is based on the calculation of the cell-maturity level as well as the lineage from blast cells[7]. Utilization of various image-processing techniques offers an alternate approach aiding the identification of blood cells[8]-[9]. Cell identification could be performed through process analysis of digital images of a leukemia-positive blood cell preparation, captured using a digital microscope.

Previously, research has been conducted on the identification of blood cells using image processing techniques on AML images based on the white morphology of white blood cells[6],[8], as well as classification of the types of AML[8][9]. The technique used there are four stages of image acquisition, segmentation, feature extraction, and identification. The segmentation process aims to separate white blood cells and red blood cells. The techniques used in image segmentation include colour filter, Canny Edge Detection, Ellipse Detection. While the identification process uses a Fuzzy Rule-Based System with the Sugeno Order Zero method[9]. Another study used K-means data mining to separate the nucleus into white blood cells. After separating the nucleus and white blood cells, the next step is to extract the characteristics of the shape and the characteristics of densitometry, then perform the process of classification of white blood cell types using the Naïve Bayes Classifier algorithm[8].

Segmentation of the cell nucleus can be performed through the use of the C–Y color space[10]. The C–Y color space serves to transform an RGB image of WBCs into a YCbCr image. The white-blood-cell nucleus can then be segmented based on luminance (Y) [10]. WBC segmentation with other methods has also been used, namely, Active Contour Without Edge[11]. The opening morphology operation and median filter have been used to remove noise[12]. The study presented in this paper aims to identify AML cells, especially the ones belonging to the M1 and M2 types, based on the morphology of WBCs. The proposed study involves the utilization of the C–Y color space to achieve the conversion of an RGB image into a YCbCr image[12][13]. Segmentation of the nucleus and

\*Corresponding Author

WBCs is accomplished through the use of the thresholding method followed by median filtering to make the nucleus and WBC [10]. Methods to classify cell and AML types were based on naïve Bayes' classifier algorithm. The use of this method is favored because it includes an algorithm that makes use of training data to identify similarities with test data [14][15]. Additionally, the naïve Bayes classifier method has previously been used to identify cell types from digital images, which is an added advantage[8]. The Naïve Bayes Classifier is also used to classify texture images from the Describable Textures Dataset (DTD) and Brodatz albums. The classification results show very accurate results[16]. In another study, Naïve Bayes was used to classifying tomatoes into three classes, namely raw, ripe and rotten based on the histogram characteristics, the experimental results obtained an accuracy of 76%[17]. Naïve Bayes is also used to classify the type of hepatitis from the results of blood smear images using the Fuzzy C-Means Clustering and random forest methods. The segmented image is subjected to feature extraction with SITCA (Spatio-Temporal Independent Component Analysis) which extracts every required feature. The experimental results show an accuracy of 89%[18]. Other research on image classification was also carried out using the Naïve Bayes method, based on the histogram gray feature, SIFT feature, SURF feature, and dataset dimension reduction from the image data set. The Naive Bayesian method is used to obtain the accuracy, recall, and F1 values of the image for each feature. The analysis is done by comparing the features with Naïve Bayes. The evaluation results show that the image representation using the SURF feature description can achieve better classification results[19].

## II. MATERIAL AND METHOD

The data used in this study is a WBC image that identified leukemia type AML M1 and AML M2 Data in the form of a WBC image that is identified AML type AML M1 and AML M2. The process of identification is performed by and, subsequently, obtained from a clinical pathologist—RSUD Dr. Moewardi—at the Clinical Pathology Installation, Surakarta, Central Java. The data comprises 30 images of each of the M1- and M2-type AML cells. Each image was obtained through observations performed using a digital microscope at 1000 times magnification of blood-cell preparations identified as AML M1 and AML M2. Sample data images, used in this study, are shown in Fig. 1.

Acute myeloblastic leukemia with little maturation (AML M1) possesses a myeloblast cell count of more than 90% and is found in the spinal cord with fine chromatin and a prominent nuclear form at locations where azurophilic granules (blue color) may be present[20] Myeloblastic cells predominate in the AML M1 cell type.

In contrast to AML M1, AML M2 is more common in children to the extent that approximately 30–45% of all AML cases in children belong to this type. In terms of cell types, AML M2 is comprised of more than myeloblast cells (more than 20% of the total cell count), found in the blood and spinal cord, and neutrophil cells (roughly 10% of total cell count) in various stages of maturity, such as Promyelocyte, Myelocyte, and Metamyelocyte. The cytoplasm of the myeloblast cells

may or may not be comprised of azurophilic grains and Auer stems[20]. Morphological features of the dominant cells in AML M1 and M2 are listed in Table I.

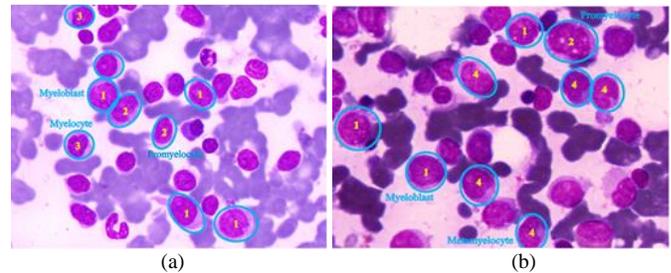


Fig. 1. Identification Type of AML M1 & AML M2 by Expert; (a) AML M1, (b) AML M2.

### Information:

- 1) Myeloblast cells
- 2) Promyelocyte cells
- 3) Myelocyte cells
- 4) Metamyelocyte cells

The selection of features in the form of WBC diameter, nuclear ratio, and roundness ratio because they are the dominant features found in every granulocyte cell (Myeloblast, Promyelocyte, Myelocyte, Metamyelocyte) besides being able to see whether the cytoplasm is granular or not[21][6], as shown in Table I. However, to determine whether the cytoplasm is granular (azurophilic) or not, it is quite difficult to do because it is in the form of spots, some of which are pink, dark red, and some are purplish in the cytoplasm. It is difficult to separate the colors, so the most feasible feature was selected by measuring WBC diameter, nucleus ratio, and cell nucleus sphericity ratio in feature extraction on image data.

TABLE I. FEATURES OF DOMINANT CELLS OF AML M1 & AML M2

Cell Types	WBC Diameter (µm)	Nucleus Ratio	Nucleus Roundness
Myeloblast	15 – 20	7:1 – 5:1	Roundness
Promyelocyte	12 – 24	5:1 – 3:1	Roundness
Myelocyte	10 – 18	2:1 – 1:1	Oval
Metamyelocyte	10 – 18	1.5:1 – 1:1	Curve

Image enhancement is performed to reduce noise by converting the captured RGB image into a YCbCr image in the C–Y color space[22].

Post conversion, the YCbCr image is processed through mean and median filtering. The processes of mean and median filtering are performed to obtain a more solid image and reduce the noise that may be induced during image segmentation[23].

Image segmentation is performed to detect and segregate nuclei from WBCs by subjecting the YCbCr image to a thresholding operation based on the Y, Cr, and Cb components. The result of image segmentation is a binary image. Segmentation results are subsequently subjected to an opening operation to reduce unnecessary noise during the feature-extraction process.

The feature-extraction process relates to the quantization of image characteristics into numerical values. The methods used in this phase include those based on chain code and the bounding box algorithm. The characteristics of WBCs sought in this study are the WBC diameter, nuclear ratio, and roundness ratio [24].

1) *WBC diameter* The WBC diameter can be calculated based on the area of the detected WBC area and can be calculated using the following equation (1)[25]:

$$Diameter = 2 \sqrt{\frac{WBC\ Area}{\pi}} \quad (1)$$

2) *Nucleus ratio* This is a ratio that compares the area of the nucleus with the WBC area and can be calculated using the following equation:

$$Nucleus\ Ratio = \frac{Nucleus\ Area}{WBC\ Area} \quad (2)$$

3) *Roundness ratio* The roundness ratio of serves to quantify the curvature of a nucleus. Its value approaching unity implies that the nucleus has a high curvature. The roundness ratio can be calculated using the following equation:

$$Roundness\ Ratio = \frac{4\pi L_{Nucleus}}{Perimeter^2} \quad (3)$$

where  $L_{Nucleus}$  represents the area of the nucleus and perimeter represents the number of pixels from the edge of the nucleus.

The purpose of this step is to identify the cell and AML types. As mentioned earlier, the naïve Bayes classifier is the algorithm used in this process. Inputs for identification of the cell type include WBC diameter, nuclear ratio, and roundness ratio, while that for identification of the AML type includes number of dominant cells—myeloblast, promyelocyte, myelocyte, and metamyelocyte. The naïve Bayes' classifier method employs the Bayes' theorem, wherein laws of probability determine a possible outcome of the classification process. This method approach uses probability as a determinant of the possible outcomes of the classification process. Bayes' theorem is stated by the following formula.

$$P(H|X) = \frac{P(X|H)P(H)}{P(X)} \quad (4)$$

The Bayes classifier assumes attributes that have independent distributions. For this reason, there is the following formula:

$$P(H|X) = P(X_1|H)P(X_2|H)P(X_3|H) \dots P(X_n|H) \quad (5)$$

Where  $X$  is data with an unknown class.  $H$  is hypothesis data is a specific class.  $P(H|X)$  is the probability of hypothesis  $H$  based on condition  $X$  (posteriori probability).  $P(H)$  represents Hypothesis probability  $H$  (prior probability).  $P(X|H)$  Probability of  $X$  based on the conditions on the hypothesis  $H$ , and  $P(X)$  is Probability of  $X$ .

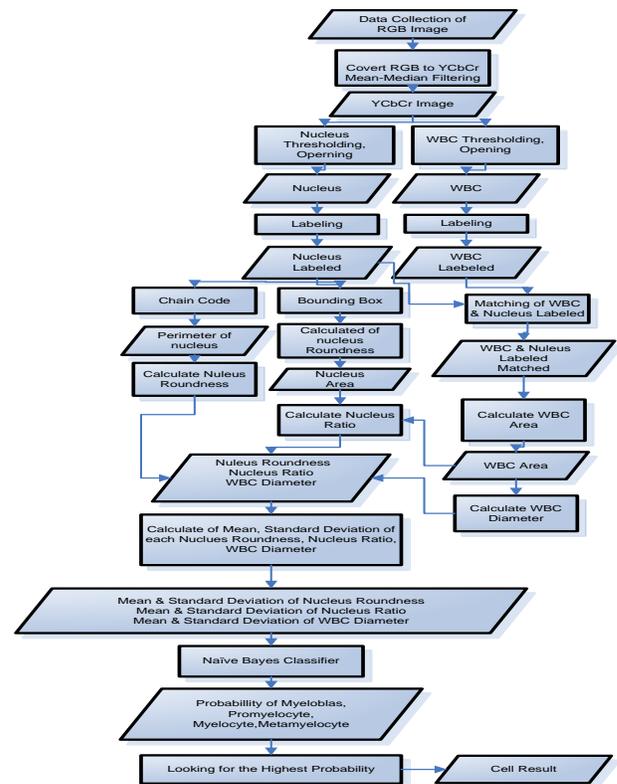


Fig. 2. The Research Methods.

The research methods of the steps can be shown in Fig. 2, from data collection, preprocessing, segmentation, characteristic extraction, and classification process with naive Bayes classifier, to find identified cell results.

### III. RESULT AND DISCUSSION

#### A. Results

As previously mentioned, a YCbCr image is obtained as a result of image enhancement and subsequent mean and median filtering. Fig. 2 depicts the result of image enhancement performed on the RGB image depicted in Fig. 1(a). Conversion of the RGB image to the YCbCr color space is performed to obtain optimum reproduction of the red-colored image components since red is a dominant color in WBC images. The red component in the YCbCr image is the Cr component, while the RGB image is the R component. Differences in the reproduction of red-colored components in the RGB and YCbCr color spaces can be recognized as shown in Fig. 4.

The result of the nucleus segmentation performed on the YCbCr image shown in Fig. 3 is depicted in Fig. 5(a) whereas WBC segmentation is shown in Fig. 5(b).

The feature-extraction process begins with the process of labeling the segmented images of the nuclei and WBCs. This is followed by the selection process performed on the segmented nucleus and WBC images using the bounding box method. Fig. 6(a) depicts results of the selection process performed on images of the nucleus, Fig. 6(b) shows selection results for WBC images, and Fig. 6(c) depicts the result of WBC selection

with the label. The characteristics of the extraction result shown in Fig. 6(c) are listed in Table II.

The attributes of feature extraction—WBC diameter, nuclear ratio, and roundness ratio—are used as test data. Based on the above feature extraction result, AML image characteristics (cell 6 in Fig. 6(c)) have WBC diameter, 18.161  $\mu\text{m}$ ; nucleus ratio, 0.647; and roundness ratio, 0.706. The percentage similarity of the cell types obtained through calculations based on the naïve Bayes' classifier algorithm is as quoted, Myeloblast = 40.1%, Promyelocyte = 39.1%, Myelocyte = 7.6%, Metamyelocyte = 13.2%.

Cell 6 in Fig. 6(c) is identified by the system as a myeloblast cell, because it has the highest percentage of 40.1%. A comparison of the results of cell type identification performed by a laboratory expert and that corresponding to Fig. 6(c) performed by the proposed system is presented in Table III.

As can be seen in Table III, there exist two cells—3 and 8—for which the result obtained using the proposed method did not match the identifications made by the expert. Cell 3 with characteristics of WBC diameter, 13.035  $\mu\text{m}$ ; nuclear ratio, 0.768; and roundness ratio of 0.815 is identified as a myeloblast cell because it has the following similarity percentages, Myeloblast = 61.2%, Myelocyte = 25.4%, Promyelocyte = 8.6%, Metamyelocyte = 4.8%. The WBC diameter of cell 3 demonstrates similarity percentages of 54.5%, 14.8%, 22.7%, and 8% with myeloblast, promyelocyte, myelocyte, and metamyelocyte cells, respectively. Thus, the proposed method identifies cell 3 as a myeloblast cell.



Fig. 3. Image Enhancement Result.

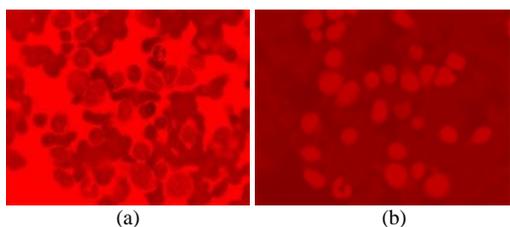


Fig. 4. The Difference of the Red Components in RGB Image and YCbCr Image (a) The Red Components (R) in RGB Image (b) The Red Components (Cr) in YCbCr Image.

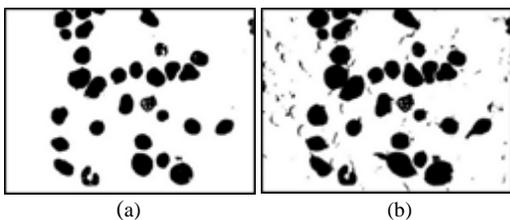


Fig. 5. Segmentation Result (a) Nucleus Segmentation, (b) WBC Segmentation.

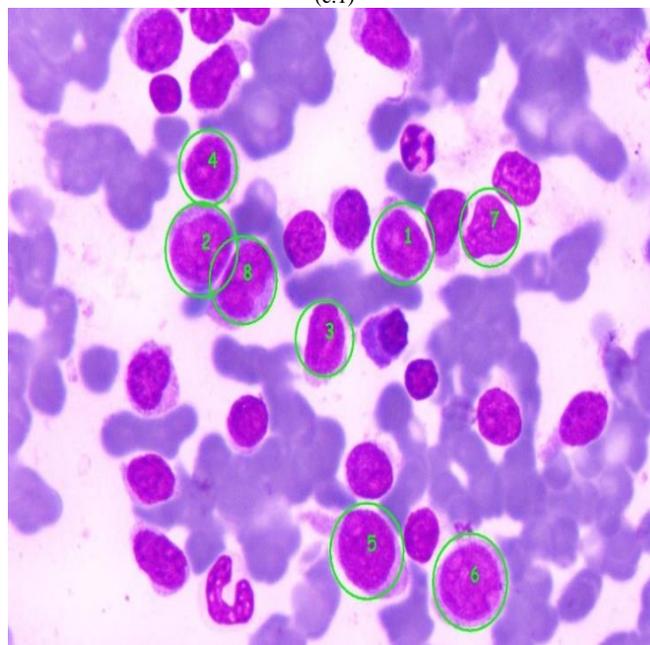
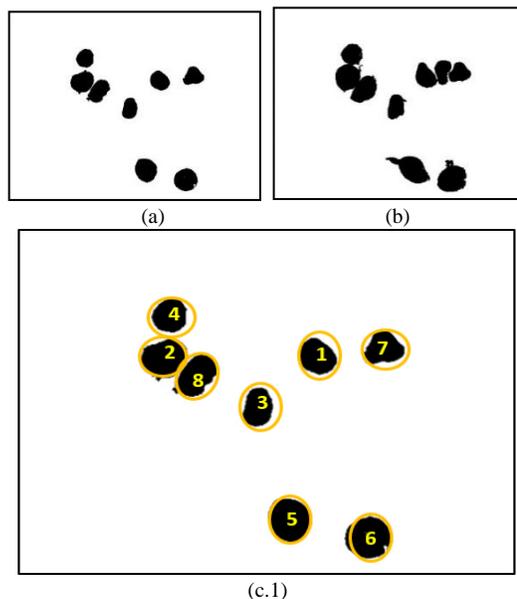


Fig. 6. Selection Result of Nucleus and WBC (a) Selection Result of Nucleus, (b) Selection Result of WBC (c.1.c.2) WBC Labelling.

TABLE II. RESULTS OF CELL-FEATURE EXTRACTION

Label	Wbc Diameter ( $\mu\text{m}$ )	Nucleus Ratio	Nucleus Roundness
1	14.161	0.7428	0.866
2	17.306	0.676	0.720
3	13.035	0.768	0.815
4	13.552	0.718	0.869
5	18.212	0.640	0.855
6	18.161	0.647	0.706
7	12.987	0.833	0.771
8	16.569	0.645	0.621

TABLE III. COMPARISON OF CELLS IDENTIFICATION PERFORMED BY AN EXPERT AND THE PROPOSED SYSTEM

Label	Cell Identification by System	Cell Identification by Expert	Explanation
1	Myeloblast	Myeloblast	Matched
2	Myeloblast	Myeloblast	Matched
3	Myeloblast	Promyelocyte	Not matched
4	Myeloblast	Myeloblast	Matched
5	Myeloblast	Myeloblast	Matched
6	Myeloblast	Myeloblast	Matched
7	Myeloblast	Not Identified	Not Identified
8	Myeloblast	Promyelocyte	Not matched

The nucleus ratio of cell 3 demonstrates similarity percentages of 62.3%, 13.85%, 12.35%, and 11.5% with myeloblast, promyelocyte, myelocyte, and metamyelocyte cells, respectively. The nucleic feature of cell 3 demonstrates similarity ratios of 55.7%, 24.1%, 14.9%, and 5.3% with myeloblast, promyelocyte, myelocyte, and metamyelocyte cells, respectively. So, the nucleus ratio and roundness ratio of cell 3 has similarities to myeloblast characteristics.

Cell 8 with characteristics of WBC diameter, 16.569 μm; nuclear ratio, 0.645; and roundness ratio of 0.621 is identified as a myeloblast cell because it has the following similarity percentages, Myeloblast = 46.4%, Myelocyte = 11.3%, Promyelocyte = 23.3%, Metamyelocyte = 19%.

The WBC diameter of cell 8 demonstrates similarity percentages of 59.2%, 18%, 14.4%, and 8.4% with myeloblast, promyelocyte, myelocyte, and metamyelocyte cells, respectively. As such, the feature of WBC diameter for cell 8 has a strong resemblance to myeloblast cells. The nucleus ratio corresponding to cell 8 demonstrates similarity percentages of 44.5%, 31.3%, 14.1%, and 10.1% with myeloblast, promyelocyte, myelocyte, and metamyelocyte cells, respectively. At the same time, the nucleic feature of 8 demonstrates similarity percentages of 49.3%, 21.7%, 8.3%, and 20.7% with myeloblast, promyelocyte, myelocyte, and metamyelocyte cells, respectively. Thus, cell 8 has been assumed to possess a strong resemblance to myeloblast cells. The differences in the characteristics of WBC diameter, nuclear ratio, and roundness ratio between myeloblast cells and neutrophil cells (promyelocyte cells, myelocyte cells, and metamyelocyte cells) are almost indistinguishable in the above cases since each feature has an uncertain range of values. For example, cell 3 is identified by the expert as a promyelocyte cell, whereas cell 4, which possesses characteristic values similar to those of cell 3, is identified by the specialist as a myeloblast cell.

Results of the cell type feature extraction comprise 264 cell type data obtained from 50 AML images. Based on identifications made by the laboratory expert, these 264 cells comprised 143 myeloblasts, 62 promyelocytes, 33 myelocyte, and 26 metamyelocyte cells.

Table IV presents a comparison of these results with those obtained from cell type identification performed by the proposed system.

TABLE IV. RESULTS OF CELL TYPE IDENTIFICATION PERFORMED BY EXPERTS AND THE PROPOSED SYSTEM

Identification By Expert	Identification By System			
	Myeloblast (A)	Promyelocyte (B)	Myelocyte (C)	Metamyelocyte (D)
Myeloblast (A)	125	13	0	5
Promyelocyte (B)	41	20	0	1
Myelocyte (C)	31	2	0	0
Metamyelocyte (D)	20	6	0	0

An example of testing myeloblast cells using a confusion matrix based on Table IV. TP (True Positive): The number of myeloblast cells detected by the system and experts as myeloblast cells is 125 cells. FN (False Positive): The number of myeloblast cells identified by the expert but detected by the system as other cells (promyelocyte, myelocyte, and metamyelocyte) is 13 + 5 = 18 cells. FP (False Positive): The number of other cells (promyelocyte, myelocyte, and metamyelocyte) identified by the expert but detected by the system as myeloblast cells is 41 + 31 + 20 = 92 cells. TN (True Negative): The number of other cells (promyelocyte, myelocyte, and metamyelocyte) identified by the expert and the system as other cells (promyelocyte, myelocyte, and metamyelocyte) is 20 + 0 + 1 + 2 + 0 + 0 + 6 + 0 + 0 = 29 cells.

$$Precision = \frac{TP}{TP+FP} = \frac{125}{125+92} = 0.576$$

$$Sensitivity = \frac{TP}{TP+FN} = \frac{125}{125+18} = 0.8741$$

$$Spesificity = \frac{TN}{TN+FP} = \frac{29}{29+92} = 0.2396$$

The analysis of each cell is done by using a confusion matrix with precision, sensitivity, and specificity of each type of cell test. The results of confusion matrix testing can be seen in Table V. As seen in Table V, the precision of the myeloblast cells is 57.6% implying that the number of myeloblast cells was correctly identified as 57.6% of the total cell count. Sensitivity is the level of success achieved by the system in rediscovering information. As seen, the sensitivity of myeloblast cells is 87.41%, which means that 87.41% of the actual number of myeloblast cells was correctly identified by the system.

TABLE V. CONFUSION MATRIX TEST RESULT

Cell Type	Precision	Sensitivity	Specificity
Myeloblast	57.6 %	87.41 %	23.96 %
Promyelocyte	48.78 %	32.25 %	90.00 %
Myelocyte	0	0	100.00 %
Metamyelocyte	0	0	97.47 %
Overall Cells	54.92 %	54.92 %	85.14 %

Each cell type in the proposed study was subjected to a different mean test to examine the differences in the characteristics of WBC diameter, nucleus ratio, and roundness ratio between each cell type. The testing was performed using the T-test to know the significant value (p-value) of each cell.

An error rate of 5% was set meaning that if the p-value exceeds 0.05, it implies that the character of the compared cell is significantly different. The mean difference of the test results corresponding to each cell is listed in Table VI.

The WBC diameter of myeloblast cells, in theory, measures between 15–20 μm, and that of promyelocyte cells measures between 12–24 μm. Myeloblast and promyelocyte cells have similar typical WBC diameters between 15–20 μm. However, this similarity is not identified by the mean difference test result, which states that WBC diameters of myeloblast and promyelocyte cells are significantly different. Similarly, the nuclear ratio of the myeloblast cell, in theory, ranges from 7:1–5:1, while that of promyelocyte cells lies in the range of 5:1–3:1. This is in line with the mean difference test result that the nuclear ratios of the two cell types differ significantly.

The mean test result for the roundness ratio demonstrates that there exists no significant difference between the two cell types, which corresponds to the theoretical basis that myeloblast and promyelocyte cells have a still-filled nucleus.

K-fold cross-validation of the cell type data was performed to determine the accuracy of naive Bayes' classifier algorithm applied to new data. The test was performed using the Leave One Out Cross Validation (LOO-CV) method on the naive Bayes' classifier algorithm using the experimental values k = 2 to k = 10. The test results demonstrate that the algorithm possessed the highest accuracy at k = 4 with an accuracy of 54.92%. The complete cross-validation test results are presented in Table VII.

Out of the 60 AML images that were processed using the proposed technique, 44 were identified correctly. A summary of the results of AML identification can be seen in Table VIII.

The obtained accuracy results of the AML type identification are as follows:

$$Accurate\ of\ System = Acc = \frac{\text{The amount of data is correct}}{\text{Total data tested}} \\ = \frac{44}{60} \times 100\% = 73.33\%$$

**B. Discussion**

Many studies on the diagnosis of leukemia based on image processing have been carried out, including research on ALL (Acute Myeloid Leukemia) classification using the Naïve Bayes Classifier method on WBC segmentation results with k-NN (k-Nearest Neighbor), with a calcification accuracy of 75% [8]. Another study was conducted to classify AML M0 and AML M1 on the results of WBC segments with RGB to YCbCr conversion using the k-NN classification method, obtaining an accuracy of 59.87% [12]. Then the classification of AML M2 and AML M3 diseases with the Momentum backpropagation method from the results of WBC segmentation with the Watershed Distance Transform method obtained an accuracy of 94.285% [26]. While the classification on AML M1, M2 and M3 using the Backpropagation Momentum Method from the results of WBC segmentation with the ACWE method obtained an average precision of 84.754%, Sensitivity 75.88%, specificity 95.090%, and accuracy 94.285% [11]. In the same year, cell classification was carried out in AML M4, AML M5, and AML M7 with the

Support Vector Machine method on the results of WBC segmentation with K-NN and Watershed Distance Transform. The cell types were myeloblast, promyelocyte, granulocyte, monoblast, promonocyte, monocyte, megakaryoblast. and supporting cells with accuracy of 98.67%, 98.01%, 84.05% 99.67%, 95.35%, 89.70%, 99.34% and 98.01%, respectively [27]. The classification of AML M0 and AML M1 diseases has also been carried out using the Naïve Bayes Classification method from the results of WBC segmentation with Multi-Otsu Thresholding compared to Static Thresholding, respectively, the accuracy is 83.81% and 75.35% [28]. Then a comparison of the accuracy of the segmentation results on WBC in AML MI obtained an accuracy of 90.67% with the ACWE segmentation method, the results are higher than the accuracy obtained with the Sheet Region Growing and Otsu Thresholding segmentation [29].

Another study was also conducted regarding the classification of leukocyte cells in AML with the random forest method from the WBC segmentation process with Multi-Otsu Thresholding, which obtained 93.45% classification accuracy and 65% precision [30]. Then the classification is carried out on the case for ALL classification using the Naïve Bayes Classification method from the results of WBC segmentation with thresholding, 80% accuracy is obtained [31]. From the results of several studies that have been carried out for the classification of AML from the segmentation results of WBC cells in Acute Myeloid Leukemia, it is true that for this study the precision, sensitivity, specificity, and accuracy are relatively small compared to other similar studies that have been carried out.

TABLE VI. MEAN DIFFERENCE TEST OF EACH CELL TYPES

The Type of Cells That Are Compared	P-Value		
	WBC Diameter	Nucleus Ratio	Roundness Ratio
Myeloblast – Promyelocyte	0.000	0.000	0.105
Myeloblast – Myelocyte	0.008	0.169	0.922
Myeloblast – Metamyelocyte	0.092	0.515	0.001
Promyelocyte – Myelocyte	0.000	0.052	0.188
Promyelocyte – Metamyelocyte	0.468	0.014	0.010
Myelocyte – Metamyelocyte	0.002	0.542	0.002

TABLE VII. IDENTIFICATION RESULT OF CELL TYPES WITH K-FOLD CROSS VALIDATION TEST

K	2	3	4	5	6	7	8	9	10
Correct	144	142	145	144	141	140	144	143	143
Acc	54.5 5%	53.7 9%	54.9 2%	54.5 5%	53.4 1%	53.0 3%	54.5 5%	54.1 7%	54.1 7%

TABLE VIII. IDENTIFICATION RESULT OF AML

Type of Aml	Identification By System	
	AML M1	AML M2
AML M1	29	1
AML M2	15	15

#### IV. CONCLUSION

From the above analysis and supporting discussion, it can be inferred that the naïve Bayes' classifier algorithm could be used in the identification of dominant cell AML types—myeloblast, promyelocyte, myelocyte, and metamyelocyte—based on WBC morphological imaging. The AML type identification performed in this study using the naïve Bayes classifier algorithm demonstrated a system accuracy of 73.33% in a sample space comprising 60 AML images. Additionally, cell type identification accuracy of 54.92% was achieved in a sample space comprising 264 cell type data. The above accuracy was achieved with a precision of 54.92%, sensitivity of 54.92%, and specificity of 85.14%. As part of a future endeavor, the authors suggest normalization of the contrast in the image before the segmentation process to reduce noise generated in the segmentation process.

#### ACKNOWLEDGMENT

We would like to thank the National Research and Innovation Agency of the Republic of Indonesia for providing research funding under the Basic Research Grant scheme with Contract Number: 221.1/UN27.22/HK.07.00/2021. We would like to thank all those who have assisted in the completion of this research.

#### REFERENCES

- [1] Kumar et al., "Automatic Detection of White Blood Cancer From Bone Marrow Microscopic Images Using Convolutional Neural Networks," IEEE Access, vol. 8, pp. 142521–142531, 2020, doi: 10.1109/ACCESS.2020.3012292.
- [2] A. Vakiti and P. Mewawalla, "Acute Myeloid Leukemia," 2021.
- [3] American Cancer Society. (2013). Leukemia: Acute Myeloid ( Myelogenous ) Overview. American Cancer Society.
- [4] College of American Pathologists. (2011). Blood Cancer Acute Myeloid Leukemia. College of American Pathologists.
- [5] B. Houwen, "The Differential Cell Count," Laboratory Hematology, vol. 7, pp. 89–100, 2001.
- [6] A. Bell and S. Sallah, The Morphology of Human Blood Cells: Seventh Edition, Seventh. English: Bookbaby, 2020.
- [7] Mitchell, Kumar, Abbas, and Fausto, Robbins amp Cotran Buku Saku Dasar Patologis Penyakit Edisi 7 Mitchell. Elsevier Inc, 2009.
- [8] S. Selvaraj and B. Kanakaraj, "Naïve Bayesian classifier for Acute Lymphocytic Leukemia detection," ARPN Journal of Engineering and Applied Sciences, vol. 10, no. 16, pp. 6888–6892, 2015.
- [9] E. Suryani, W. Wiharto, and N. Polvonov, "Identification and Counting White Blood Cells and Red Blood Cells using Image Processing Case Study of Leukemia," International Journal of Computer Science & Network Solutions, vol. 2, no. 6, pp. 35–49, 2015.
- [10] R. Mohammed, O. Nomir, and I. Khalifa, "Segmentation of Acute Lymphoblastic Leukemia Using C-Y Color Space," ijacsa, vol. 5, no. 11, 2014, doi: 10.14569/IJACSA.2014.051117.
- [11] A. Harjoko, T. Ratnaningsih, E. Suryani, Wiharto, S. Palgunadi, and N. P. T. Prakisyana, "Classification of acute myeloid leukemia subtypes M1, M2 and M3 using active contour without edge segmentation and momentum backpropagation artificial neural network," in MATEC Web of Conferences, Yogyakarta, 2018, vol. 154, p. 01041. doi: 10.1051/mateconf/201815401041.
- [12] E. Suryani, Wiharto, S. Palgunadi, and Y. R. Putra, "Cells identification of acute myeloid leukemia AML M0 and AML M1 using K-nearest neighbour based on morphological images," Proceedings of 2017 International Conference on Data and Software Engineering, ICODSE 2017, vol. 2018-Janua, pp. 1–6, 2018, doi: 10.1109/ICODSE.2017.8285851.
- [13] W. Wiharto, E. Suryani, and Y. R. Putra, "Classification of blast cell type on acute myeloid leukemia (AML) based on image morphology of white blood cells," TELKOMNIKA (Telecommunication Computing Electronics and Control), vol. 17, no. 2, p. 645, 2018, doi: 10.12928/telkomnika.v17i2.8666.
- [14] J. Han, M. Kamber, and J. Pei, Data Mining: Concepts and Techniques., Third Edition. USA: Morgan Kaufmann is an imprint of Elsevier, 2012.
- [15] H. Hamidi and A. Daraei, "Analysis of Pre-processing and Post-processing Methods and Using Data Mining to Diagnose Heart Diseases," IJE, vol. 29, no. 7, pp. 921–930, Jul. 2016, doi: 10.5829/idosi.ije.2016.29.07a.06.
- [16] A. M. Mansour, "Texture Classification Using Naive Bayes Classifier," IJCSNS International Journal of Computer Science and Network Security, VOL.18 No.1, January 2018.
- [17] A. Kusuma, D. R. I. M. Setiadi, and M. D. M. Putra, "Tomato Maturity Classification using Naive Bayes Algorithm and Histogram Feature Extraction," Journal of Applied Intelligent System (e-ISSN : 2502-9401 | p-ISSN : 2503-0493), Vol. 3 No. 1, August 2018, pp. 39 – 48
- [18] V. Vanitha and D. Akila, "Image Segmentation and classification Hepatitis viral infection in human blood smear with a hybrid algorithm combining Naive Bayes Classifier," Turkish Journal of Computer and Mathematics Education, Vol.12 No.11 (2021), 5873-5881.
- [19] K. Fang, "Naive Bayes Image Classification Based on Multiple Features," Computer Software and Media Applications (2019), Volume 2, doi: 10.24294/csma.v2i1.1171.
- [20] A. Kaur and B. V. Kranthi, "Comparison between YCbCr Color Space and CIELab Color Space for Skin Color Segmentation," International Journal of Applied Information Systems, vol. 3, no. 4, pp. 30–33, 2012.
- [21] College of American Pathologists. (2016). Hematology and Clinical Microscopy Glossary. College of American Pathologists.
- [22] A. Bacarea, "Diagnosis of Acute Myeloid Leukaemia," in Myeloid Leukemia - Clinical Diagnosis and Treatment, S. Koschmieder, Ed. InTech, 2012. doi: 10.5772/26177.
- [23] M. A. Fattahzadeh and A. Saghaei, "A Statistical Method for Sequential Images-based Process Monitoring," IJE, vol. 33, no. 7, pp. 1285–1292, Jul. 2020, doi: 10.5829/ije.2020.33.07a.15.
- [24] M. Ghaderzadeh, F. Asadi, A. Hosseini, D. Bashash, H. Abolghasemi, and A. Roshanpour, "Machine Learning in Detection and Classification of Leukemia Using Smear Blood Images: A Systematic Review," Scientific Programming, vol. 2021, pp. 1–14, Jun. 2021, doi: 10.1155/2021/9933481.
- [25] E. S. A. Baquero, "Methodology for Automatic Classification of Atypical Lymphoid Cells from Peripheral Blood Cell Images," Disertation, Universitat Politècnica de Catalunya • BarcelonaTech, Barcelona, 2015.
- [26] E. Suryani, Wiharto, S. Palgunadi, and N. P. T. Prakisyana, "Classification of Acute Myelogenous Leukemia (AML M2 and AML M3) using Momentum Back Propagation from Watershed Distance Transform Segmented Images," International Conference on Computing and Applied Informatics 2016, IOP Conf. Series: Journal of Physics: Conf. Series 801 (2017) 012044, IOP Publishing, doi:10.1088/1742-6596/801/1/012044.
- [27] A. Setiawan 1, A. Harjoko2, T. Ratnaningsih, E. Suryani, Wiharto, S., and Palgunadi, "Classification of Cell Types In Acute Myeloid Leukemia (AML) of M4, M5 and M7 Subtypes With Support Vector Machine Classifier," 2018 International Conference on Information and Communications Technology (ICOIACT), 978-1-5386-0954-5/18/\$31.00 ©2018 IEEE.
- [28] E. Suryani, E I Asmari, and B Harjito, "Image Segmentation of Acute Myeloid Leukemia Using Multi Otsu Thresholding," ICERIA 2020, Journal of Physics: Conference Series 1803 (2021) 012016, IOP Publishing, doi:10.1088/1742-6596/1803/1/012016.
- [29] N. P. T. Prakisyana and A. Setiawan, "A Comparative Study of Digital Image Segmentation Algorithms for Acute Myeloid Leukemia M1 White Blood Cells Images," Indonesian Journal of Informatics Education (IJE), ISSN: 2549-0389.

- [30] S. Dasariraju, M. Huo, and S. McCalla, "Detection and Classification of Immature Leukocytes for Diagnosis of Acute Myeloid Leukemia Using Random Forest Algorithm," *Bioengineering* 2020, 7, 120; doi:10.3390/bioengineering7040120.
- [31] S. Shidada, B. Hariyanto, "Identifikasi Acute Lymphoblastic Leukemia pada Citra Mikroskopis Menggunakan Algoritma Naïve Bayes," *Journal of Science and Technology*, <https://journal.trunojoyo.ac.id/rekayasa>, *Rekayasa*, 2021; 14(1): 78-83, ISSN: 0216-9495 (Print), ISSN: 2502-5325 (Online).

# Automatic Essay Scoring: A Review on the Feature Analysis Techniques

Ridha Hussein Chassab, Lailatul Qadri Zakaria, Sabrina Tiun

The Asean Natural Language Processing (ASLAN), Faculty of Information Science and Technology  
Universiti Kebangsaan Malaysia, Bangi, Selangor Darul Ehsan, Malaysia

**Abstract**—Automatic Essay Scoring (AES) is the automatic process of identifying scores for a particular essay answer. Such a task has been extensively addressed by the literature where two main learning paradigms have been utilized: Supervised and Unsupervised. Within these paradigms, there is a wide range of feature analyses has been utilized, Morphology, Frequencies, Structure, and semantics. This paper aims at addressing these feature analysis types with their subcomponent and corresponding approaches by introducing a new taxonomy. Consequentially, a review of recent AES studies is being conducted to highlight the utilized techniques and feature analysis. The finding of such a critical analysis showed that the traditional morphological analysis of the essay answer would lack semantic analysis. Whereas, utilizing a semantic knowledge source such as ontology would be restricted to the domain of the essay answer. Similarly, utilizing semantic corpus-based techniques would be impacted by the domain of the essay answer as well. On the other hand, using essay structural features and frequencies alone would be insufficient, but rather as an auxiliary to another semantic analysis technique would bring promising results. The state-of-the-art in AES research concentrated on neural-network-based-embedding techniques. Yet, the major limitations of these techniques are represented as (i) finding an adequate sentence-level embedding when using models such as Word2Vec and Glove, (ii) ‘out-of-vocabulary when using models such as Doc2Vec and GSE, and lastly, (iii) ‘catastrophic forgetting’ when using BERT model.

**Keywords**—Automatic essay scoring; automatic essay grading; semantic analysis; structure analysis; string-based; corpus-based; word embedding

## I. INTRODUCTION

The last decade has witnessed a dramatic evolution in employing Artificial Intelligence (AI) in the educational domain. This has been represented in classifying questions [32], question answering [10], or question generation [23]. Another challenging area in the educational domain is Automatic Essay Scoring (AES) or Automatic Essay Grading (AEG). AES refers to the task of automatically determining an exact or nearly score for an essay answer [26]. This would require an extensive analysis of the answer’s textual characteristics to identify an accurate score. The common method depicted in the literature for doing such an analysis is to acquire a reference answer (sometimes referred to as a model or template answer) and compare it with the student’s answer. The comparison would have taken a wide range of forms depending on the technique used for scoring.

Generally speaking, AES’s scoring techniques belong to two major categories; Supervised and Unsupervised. According to the machine learning paradigms, such categories refer to the learning mechanism [47]. For instance, in the supervised learning paradigm, a previous or example dataset is being prepared to train the classification algorithm. In this regard, previous students’ answers along with reference answers are being arranged along with their actual score given by the teacher and the aim is to train the machine learning algorithm to predict the score of upcoming, testing, or unseen answers. This process of learning is known as regression where the goal is to predict a numeric value rather than a predefined class label (i.e., machine learning classification).

After acquiring the example or training data of answers, a set of numeric features will be generated to predict the score. Such features could be derived from the answer’s textual characteristics such as morphology, semantic, structure, or frequency of terms. Regarding the regressor itself, there are a wide range of algorithms have been depicted in the AES literature where it can be categorized into two main classes; traditional regressors and deep learning regressors. Traditional regressors refer to the Linear Regression which is a statistical algorithm that intends to identify the most accurate coefficients that would turn the numeric features of the answers (i.e., X variables) into its actual score (i.e., Y output) [33]. On the other hand, deep learning regressors refer to the latest and sophisticated neural network architectures such as Long Short-Term Memory (LSTM) and Convolutional Neural Network (CNN). Such architectures are intended to process the numeric features of the answers through a neural network to predict the output score. Such a prediction is performed through a learning mechanism by randomly generated weights that are linked between the input and output layers within a hidden layer that aims at determining deep relationships [36].

On the other hand, the unsupervised learning paradigm refers to the task of categorizing data without the use of a predefined example or training set, but rather through a distance/similarity function or curated set of rules. The simple and most straightforward mechanism of unsupervised AES is where each answer is compared with reference answer or other student answers for identifying a similarity score which will be used afterward as the final score of the answer. This kind of pairwise similarity can be used separately or through a clustering technique that aims at grouping the similar answers into multiple groups [4].

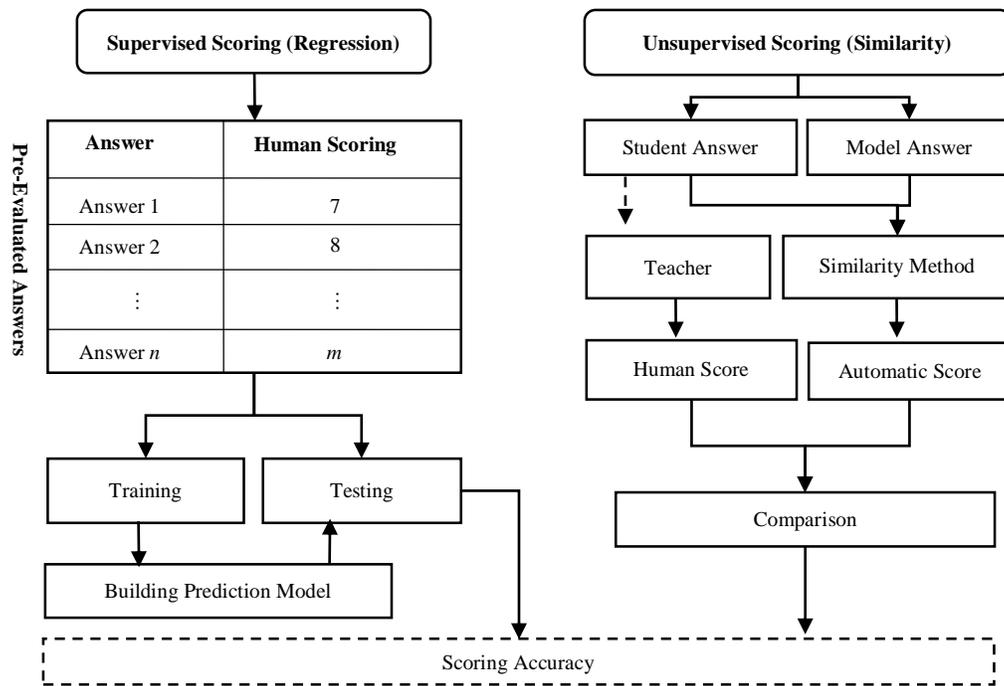


Fig. 1. General Workflow of AES Task.

Another unsupervised technique that has been depicted in the AES literature is the rule-based or ranking approach, the characteristics of the textual answer information in this method are ranked or encoded into a numeric value. Using a predefined set of rules, the numeric values associated with a particular answer would have undergone a summation or averaging procedure to get the overall score. Fig. 1 depicts the general workflow of the AES task.

Based on the general workflow of the AES task in Fig. 1, an extensive literature review is accommodated in this paper where Section 2 will depict such a review. Section 3 will depict the proposed taxonomy where the techniques used by the literature for the AES task are being categorized. Lastly, Section 4 provides a discussion on the techniques where the pros, cons, and ongoing challenges will be determined.

## II. RELATED WORK

In this section, an extensive literature review will be conducted on the recent AES research studies. The related works will be divided into two major parts; supervised AES and unsupervised AES. The following subsections will tackle these parts.

### A. Supervised AES

In a study of lexical sophistication for evaluating second language writing proficiency (L2), [25] examined two main approaches of lexical techniques. First, the authors have utilized the word frequency where the statistics of the terms within the answers are being exploited. Second, the authors have utilized the n-gram sequences (i.e., bigram) to capture multi-word sequences. Besides, the authors have adopted some ranks for the academic writing and word range. Lastly, a simple regression has been used to predict the score of the

answers. Using a corpus for the English placement test (i.e., TOFEL), the proposed method showed 92.6% of accuracy.

The author in [15] has treated the AES task as a regression problem where a Support Vector Regressor (SVR) has been used to predict the score of Portuguese student answers. For this purpose, a dataset obtained from Brazilian Schools has been used. In addition, the input of the SVR was represented as a set of numeric features that have been obtained by the structure of the answer, lexical diversity, theme, and coherence. The authors have defined scores for each feature and then use them as input to the SVR. The authors reported 74.7% as a value of correlation between regression result and teacher score. However, this study has used an imbalance dataset where five scores are used as 0, 50, 100, 150, and 200. The classes of the students' answers were imbalanced therefore, latterly the authors have proposed an improvement in their work of [14]. Using some statistical algorithms, the authors have managed to improve the accuracy of assessment by obtaining 75% of correlation.

The author in [11] has treated the AES task as regression problem where SVR algorithm has been utilized. In order to input the answer text to the regressor, the authors have used a method called Bag-of-Super-Word-Embeddings (BOSWE). This method works on existing embedding vector of words to accommodate clustering where the centroid terms will be represented as super words. Hence, the semantic meaning of terms would be converted into group of clusters. Consequentially, the authors have utilized a string similarity called Histogram Intersection String Kernel (HISK) which is a measure that has been widely used to calculate similarity between images' histograms. In this regard, the histogram of word embedding clusters would be targeted. To obtain the word embedding vectors, the authors have used a pre-trained

model based on Word2Vec introduced by [31]. An English benchmark dataset of Automated Student Assessment Prize (ASAP) has been used where the accuracy result was 78.8%.

The author in [19] established a comparison between pre-trained word embedding models and paragraph embedding models. For the pre-trained word embedding, the authors used Google Word2Vec, Glove, FastText and Elmo models. Whereas, for the paragraph embedding, the authors used Doc2Vec, InferSent and SkipThought models. Lastly, cosine similarity used to determine the similarity between student's answer vector and teacher's answer vector. Such similarity will be fed into a Ridge regression classifier. Using a benchmark dataset of English questions and answers brought from University of North Texas, the authors have concluded that the paragraph embedding using Doc2Vec has achieved the highest correlation of 56.9%.

The author in [27] proposed a self-attention method that captures long-distanter relationship for AES task. The authors first utilize the self-attention network to process two inputs including word vector embedding and word position. The word embedding has been brought from a pre-trained model of Glove where the average of each word's vector within a sentence is gained through padding approach. Another input will be depicted for the word position where each word would have a position embedding. The output of the self-attention will be processed via a Long Short-Term Memory (LSTM) architecture to accommodate the scoring. Using the benchmark of ASAP, the proposed method showed an accuracy of 77.6%.

The author in [45] proposed a deep learning architecture for the AES task. The proposed architecture begins with Word2Vec embedding for the words within the student's answer. Consequentially, the resulted embedding will be processed via a bidirectional LSTM in order to extract semantic features. Lastly, an attention layer will process the extracted features in order to give the score. The benchmark dataset of ASAP has been used in the experiments where the acquired accuracy was 83%.

The author in [41] has proposed a hybrid method of Support Vector Machine (SVM) and LSA to provide automated assessment of answers in Indonesian languages. The authors used a dataset contains students answers along with lecturer answers. Then, they treated the problem as topic modeling where SVM has been used to classify the answers into multiple generated number of topics. If a particular student answer has been classified into an irrelevant topic in respect to the lecturer answer, it would be assessed as zero.

The author in [17] examined the lexical sophistication for evaluating second language writing proficiency (L2) where Korean students are being tested on English placement test. The authors have treated the problem as regression in which the n-gram features of multi-word sequences are being addressed. For this purpose, the authors prepared answers from native speakers and compare it with the tested answers. Within such a comparison the authors addressed the occurrence of bigram and trigram sequences. A corpus of English placement test has been used to accommodate the comparison. The comparison aims at computing the associate measure between n-gram sequences. Lastly, the statistical measures' values will

be fed to a step-wise regression in order to predict the automatic score. Results of correlation between automatic and human score were 84.64%.

The author in [9] has treated the task of AES differently where the problem has been handled as a regression task. Instead of accommodating feature engineering on the answer text, the authors have used the answer as an input to a Convolutional Neural Network (CNN) architecture that has been incorporated with a regression layer. Such regression layer will predict the score of the answer based on a non-linearized function. To do so, the authors have input the embedding of words inside the answer to the architecture. Such embedding has been obtained via a pre-trained Glove model proposed by [48]. An English benchmark dataset of Automated Student Assessment Prize (ASAP) has been used. Results of accuracy obtained were 82.6%.

The author in [28] proposed a multi-way attention architecture for AES task. The proposed architecture contains a transformer layer at first which process pre-trained Glove word embedding of student's answer and model's answer. Then, the following layer represents the multi-way attention where three self-attention vectors are represented for the student's answer, model's answer and their cross vector respectively. This will be followed with an aggregation layer where word's position vectors will be added. The final layer contains the regressor where the score of the essay is being predicted. For this purpose, the authors have used a real-word educational dataset of questions and answers. Result of accuracy was 88.9%.

The author in [46] proposed a deep learning architecture for AES task. The proposed architecture begins with pre-trained word embedding vectors brought from Glove and processed via CNN layer. Then, the resulted features will be processed via LSTM in order to generate sentence embedding for each answer. The key distinguishes of this study lies in adding a co-attention layer that consider the similar sentences between student's answer and model's answer. Lastly, the final layer will give the score for each answer. Using ASAP benchmark dataset, the proposed architecture produces an accuracy of 81.5%.

The author in [34] has examined the possibility of incorporating embedding features with structural features or so-called feature-engineered. The authors have utilized an LSTM where sentence-level embedding incorporated with a set of feature-engineered. Using ASAP dataset, the proposed method showed an accuracy of 77.5%.

The author in [24] examined the lexical sophistication for evaluating second language writing proficiency (L2). The authors have used a corpus for English placement test (i.e., TOFEL). Using some lexical features such as word and n-gram overlapping along with a semantic approach of LSA, the authors have applied a simple regression in order to predict the score of the tested answers.

The author in [26] has proposed a deep learning method for AES task where two architectures of CNN and LSTM are being employed. First, the authors have processed the words' vectors of each answer through the CNN architecture in order to get the sentence embedding. For this purpose, a pre-trained

model of Glove word embedding has been used. In addition, the resulted sentence embedding from CNN has been furtherly processed via the LSTM architecture in order to get the score. Using the benchmark dataset of ASAP, the authors have shown an accuracy of 72.65%.

The author in [44] has proposed a deep learning architecture for AES task. The proposed architecture begins with word embedding vectors generated by Word2Vec and process via CNN layer in order to extract n-gram features. Lastly, a recurrent layer called Bidirectional Gated Recurrent Unit (BGRU) is being used to predict the score of the answer. Using the benchmark dataset of ASAP, the proposed architecture showed an accuracy of 86.5%.

The advancement of deep learning architecture led to the emergence of Transformers which yield a novel mechanism in learning. Such mechanism lies in the synchronized bidirectional learning. Such an architecture led to the emergence of Bidirectional Encoder Representations from Transformers (BERT) embedding. BERT has a fixed and indexed pretrained model of embedding where a vocabulary of 30,000 English terms is being stored. BERT has shown remarkable superior performance in text generation applications.

However, recently, [43] have utilized the BERT architecture for the AES task. Using ASAP dataset, BERT showed an accuracy of 74.75%. The authors have compared the BERT against the LSTM and the comparison showed that LSTM is still a competitor where it achieved an accuracy of 74.63%. The authors have justified such a miscarriage of BERT regarding a problem known as 'catastrophic forgotten' where the BERT architecture would forget quickly what it had learnt previously.

Similarly, [30] has proposed a BERT architecture for the AES task. The authors have utilized the pretrained BERT embedding and then apply the fine-tune. Using ASAP dataset, results of accuracy showed an average of 64.6% achieved by the proposed BERT.

The author in [42] has examined a Multi-Task Learning (MTL) of AES where the essay is being assessed as traits rather than holistic (i.e., Single-Task Learning). The authors have utilized structural features as traits such as the organization of the essay, the discourse of topic, and the vocabulary size of the essay; in addition, a word embedding CNN architecture using through Glove along with a sentence embedding through LSTM. The traits have been encoded through a pooling attention layer. Using ASAP dataset, the proposed MTL showed an accuracy of 76.4%.

The author in [35] has utilized much more efficient architectures derived from BERT such as Albert and Reformer for the AES task. In fact, BERT suffers from the tremendous extent of parameters (around 60 million). Therefore, the authors have concentrated on architectures that derived from BERT with considerably lower number of parameters. Using the ASAP dataset, the authors have demonstrated that the proposed architectures maintained fair accuracy of 78.2% with significant drop in the computational requirements.

## B. Unsupervised AES

The author in [18] has introduced the first benchmark of Arabic dataset for automatic scoring essays which contains 610 students' answers written in Arabic language. The domain of question was geography. The authors have applied several similarity measures including string-based, n-gram and corpus-based specifically Distributional Semantic Co-occurrence (DISCO) similarity measures independently and with combination. Then they have applied k-means clustering approach in order to scale the obtained similarity values. Results of correlation between manual and automatic score were 83%.

The author in [37] has established a comparative study on two main similarity approaches through an unsupervised paradigm for AES task. The authors have firstly used the Cosine measure to compute the similarity between student's answer and model's answer. Then, the authors have used a corpus-based method of LSA to compute the similarity between the two answers. Using a real-word dataset of questions and answers, LSA showed better performance by obtaining a correlation of 59.7%.

The author in [22] has proposed a ranking algorithm for Automatic Essay Scoring (AES) based on structural and semantic features. The structural features included number of words, number of verbs, number of sentences, and number of paragraphs in an essay, whereas semantic features brought from a corpus-based approach known as Kullback - Leibler divergence. An English benchmark dataset of Automated Student Assessment Prize (ASAP) has been used.

The author in [1] proposed an automatic essay grading system that has been utilizing ontology-based approach. The proposed approach aimed at focusing on the subject of the answer given by the students. For this purpose, the WordNet ontology has been exploited which can provide domain-specific semantic correspondences. The authors have prepared a teacher guide answer in order to be used as a benchmark when evaluating student's answer. Comparing both the guide answer and the student's answer through querying the included terms over WordNet, the authors have computed the similarity using semantic relatedness measure known as Least Common Sub-sumer (LCS). Results of the comparison were set as the automatic score where the Pearson metric has been used to compute the correlation between the automatic score and the teacher score. Experimental results showed an average correlation of 80% has been achieved.

The author in [2] has proposed a system for Arabic AES for a Saudi Intermediate school children. The criteria used for assessing the students' answers were based on spelling, grammar, structure of the answer, relation of the answer to the desired topic, and following the Modern Standard Arabic (MSA) words. For evaluating a particular answer, the authors have adopted a hybrid method of LSA RST. LSA was intended to measure the semantic similarity of the tested answer while, RST was intended to measure the cohesion and the writing style of the answer. The authors have collected a set of pre-evaluated answers of 300 essays where such answers have been written by the intermediate level students from different topics with a score out of 10. Consequentially, the authors have re-

typed the answers to the computer in order to use them for training and testing purposes. Using Pearson Correlation, the authors have compared the automatic score to the teacher score. Experimental result showed an average of 78.3% of Pearson Correlation.

The author in [39] has proposed a fingerprinting method for automatic essay scoring in Japanese language. The authors have utilized a hashing method for each essay answer by computing the ASCII values of the characters within the answer's words. This would provide a distinctive fingerprint for every answer. Then, using a model answer, answers that have been assessed with full mark, the fingerprints of the students' answers will be compared to the fingerprint of the model answer. Since the fingerprint values are numeric thus, Cosine similarity has been used to compute the distance. Based on a set of pre-assessed answers by human (i.e., teachers), the automatic score has been compared to the human's score in order to calculate the accuracy. Lastly, the authors have manipulated some parameters of fingerprint calculation such as number of N-gram characters to get the best accuracy. The proposed method managed to obtain 86.86%.

In another study, [12] described a system called TAALES which has been proposed for the AES task. The proposed system utilizes traditional features to evaluate student answer such as word frequency, academic language, N-gram frequency and other structural features. The proposed system works on user generated text.

The author in [19] has focused on the preprocessing tasks utilized for the AES task in the Indonesian language. The authors have used a corpus of questions, students' answers and teacher answers written in Indonesian. Five preprocessing tasks have been applied including lower-case, tokenization, punctuation removal, stopword removal and stemming. Lastly, Cosine similarity has been used to compute the distance between teacher's answer and student's answer. Results of correlation between manual and automatic scoring were 47%.

The author in [38] has extended the fingerprinting algorithm presented in (A. Agung Putri Ratna et al., 2018) by adding a semantic similarity of LSA. Using a real-word of Japanese questions and answers, the proposed method obtained 87.78% of accuracy. At the same year, the authors have also presented another study (A. A. P. Ratna, Noviandriani, Santiar, Ibrahim, & Purnamasari, 2019) where the authors have addressed the use of k-means clustering with LSA for AES in Japanese language. Using the same dataset, the proposed method showed an 89% of accuracy.

The author in [38] has proposed an LSA method to provide automated assessment of answers in Indonesian languages. The authors used a dataset contains students answers along with lecturer answers. Then, LSA has been used to calculate the similarity between the two answers. Using a comparison between the automatic score and human score, the proposed method showed an accuracy of 72.01%.

The author in [3] has proposed a rule-based system for Arabic AES that is evaluating the answers based on style issues such as spelling, structure, and coherence. The proposed

system utilizes a predefined set of rules that check each essay answer in terms of the aforementioned style aspect. The authors have used online dialogues and discussions among university students in order to train their system. Results of correlation between the automatic and human grading were 73% (Unsupervised).

The author in [5] has proposed an AES system that utilizes LSA along with RST. The authors have built a dataset from the scratch where a set of religious questions has been initiated along with their model answers. Then, such questions have been given to school students in order to answer them. Lastly, a set of teachers has been assigned to give a human / manual scoring that will be used later for training both the LSA and RST. Experimental result showed a 75.6% of correlation between the proposed method's scoring and the teacher's scoring.

The author in [21] has established a comparison among different embedding approaches for the AES task. The authors have utilized the benchmark dataset of ASAP. In addition, traditional vector representations such as TFIDF and Jaccard have been utilized. Furthermore, different embedding approaches such as Glove, Elmo, Google Sentence Encoder (GSE) have been also used. Lastly, using cosine similarity, the authors have identified the similarity between vectors of student answers and vectors of teacher answers. Results showed that the highest correlation achieved by GSE where it obtained 74.3%.

### III. TAXONOMY OF AES FEATURE ANALYSIS

Within the textual analysis of answers by either the supervised or unsupervised techniques, there is a wide range of features that could be used. Based on the review of literature in the previous section, this section attempts to provide a taxonomy of the AES feature analysis. As shown in Fig. 2, the taxonomy of AES's techniques is divided through the two topologies of supervised and unsupervised paradigms. However, the key characteristics of utilizing the two paradigms lies on the type of feature analysis. In fact, there are four main categories of feature analysis: Structure, Frequency and Term Occurrence, Morphology, and Semantic. Following subsections will tackle each category independently.

#### A. Structure

In this type of feature analysis, the essay answer is analyzed in terms of its structure where the coherence, writing style and spelling mistakes are being considered. The common approach for this type of feature analysis is the Rhetorical Structure Theory (RST) (Al-Jouie & Azmi, 2017). RST is a linguistic method that aims at analyzing parts of text in order to identify relations among them; it has been widely used for text summarization.

Usually, this type of feature analysis is exploited by the unsupervised technique through a ranking procedure that gives score for each criterion [22], or it could be exploited within a set of rules ([2]; [5]; [12]). On the other hand, this feature analysis can be utilized by a supervised technique through the ranking procedure where the numeric ranks would be fed to a regressor ([14]; [15]).

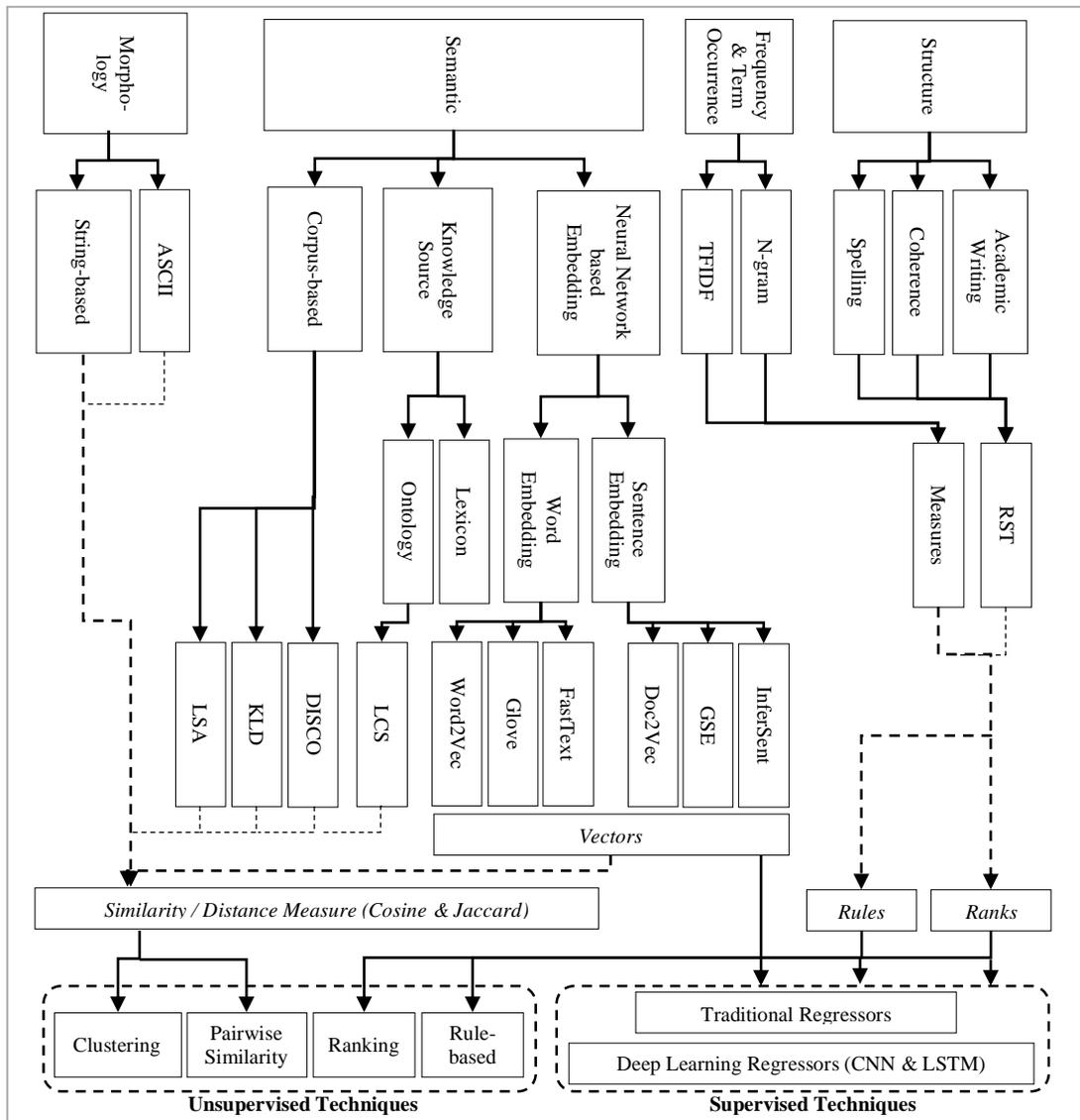


Fig. 2. Taxonomy of AES Feature Analysis.

### B. Frequency and Term Occurrence

This type of feature analysis aims at analyzing the frequencies of specific terms or the number of words, sentences and paragraphs. The common approach for counting word frequencies is the Term Frequency Inverse Document Frequency (TFIDF). On the other hand, this feature analysis focuses on the occurrence of specific term and its surrounding words to assess the student’s answer. The common approach for this occurrence analysis is the N-gram where the occurrence of unigram (i.e., single term), bigram (i.e., two terms), and trigram (i.e., three terms) can be considered.

The way of utilizing such feature analysis by an unsupervised technique is represented by a set of rules that determine the consequences of capturing specific frequencies or occurrences [12]. Otherwise, the statistics of frequency and occurrence could be exploited directly by a supervised regression technique [25].

### C. Morphology

This type of feature analysis concentrates on the lexical morphology of terms within the essay answer. The most straightforward example of this analysis is the string-based similarity between words which can be identified through similarity measures such as Cosine and Jaccard. In addition, sometimes the morphology of words could be extended to consider the ASCII code representation of characters within the essay answer ([38]; [39]; [40]). The way of adopting this feature analysis into an unsupervised technique is simply represented through the use of clustering where similarity values between answers (produced by Cosine or Jaccard) are being used to aggregate similar answers in a single cluster [18]. Otherwise, it could be adopted through a supervised regression technique by processing the similarity values and predicting the score [19].

#### D. Semantic

This type of feature is considered to be much more sophisticated where the semantic meaning of the answer's words is being analyzed. Apparently, the common way to utilize the semantic aspect is to utilize an external knowledge source such as a dictionary. However, there are other two techniques that can analyze the semantic without using knowledge source depicted in the literature; corpus-based and neural-network-based embedding. The three aforementioned techniques will be illustrated in the following.

1) *Knowledge source*: In this technique a lexicon, dictionary or ontology is being used to clarify semantic correspondences. Using a knowledge source would offer different semantic relationship between the words such as hypernymy and synonymy which might enhance the comparison between the student answer and the reference answer. WordNet is the most popular ontology that has been used for this purpose. Usually, this feature is utilized by an unsupervised technique through semantic relatedness measures such as Least Common Subsumer (LCS) [1].

2) *Corpus-based*: In this technique the semantic is being analyzed statistically and without utilizing any knowledge source. In fact, this technique aims at exploiting a corpus of text in order to identify similar contexts which usually yield semantically matching terms. To do that, a matrix of the terms along with their corresponding documents is being initiated. Consequentially, some dimensionality reduction such as Singular Value Decomposition (SVD) is applied to determine semantic correspondences. The most popular corpus-based approaches are the Latent Semantic Analysis (LSA), Latent Dirichlet Allocation (LDA), Distributional Semantic Co-occurrence (DISCO), and Kullback - Leibler Divergence (KLD). The utilization of these approaches for supervised AES is simply represented by feeding a regression technique with answer document vectors [38]. Otherwise, a distance measure such as Cosine can be used to determine similarity between answers documents through an unsupervised technique ([2]; [6]; [18]; [40]).

3) *Neural-Network-based-embedding*: Similar to the corpus-based approaches, this technique aims at analyzing the semantic aspect of the text without the use of knowledge source. The key distinguishes here is the utilization of neural

network architectures to produce special embedding. The earliest effort of this technique was represented by generating distinctive embedding vector for words which referred to as Word Embedding. The most common architectures of word embedding are Word2Vec [45], Glove [9], and FastText [19]. Afterwards, other textual levels have been examined in terms of neural network embedding such as Document Embedding, Sentence Embedding, and Paragraph Embedding. The common architectures for these levels are Doc2Vec, Google Sentence Encoder (GSE), and InferSent [19]. The way of utilizing word and sentence embedding by an unsupervised technique is simply through vector similarity computed by either Cosine or Jaccard. Otherwise, the embedding vectors would be fed to a supervised regression technique in order to predict the score.

Recent years reveal a new embedding architecture of BERT which is based on transformer learning. Such an architecture has the ability to overcome the 'out-of-vocabulary' problem. In addition, it has the capability to handle word-level and sentence-level embedding. The common way of utilizing BERT architecture for the AES task is through a supervised learning ([30]: [43]).

#### E. AES Datasets

The literature depicts a diversity in using various types of datasets for the AES task. First, there were several languages depicted by the literature such as English, Arabic, Indonesian, Japanese, Portuguese, and others. On the other hand, some efforts utilized synthesis data where students are tested to collect their results. Other efforts utilized real-world data where students' answers from previous exams have been collected. Lastly, the rest of the studies concentrated on benchmark datasets. There are two main benchmark datasets for AES, namely, Automated Student Assessment Prize (ASAP) [29] which has been presented in Kaggle.com as a challenge, and the second dataset is the ETS Corpus of Non-Native Written English from the Linguistic Data Consortium (LDC) [8].

#### F. Summary of Related Work

To conclude all the researches in AES, Table I shows the summary that briefly describes each related work, whereas, Table II depicts the summary of techniques used by the literature.

TABLE I. SUMMARY OF RELATED WORK

Author	Learning Paradigm	Method	Features	Dataset & Language	Accuracy	Limitations
Gomaa & Fahmy (2014)	Unsupervised	K-means clustering	string-based and corpus-based (DISCO)	Benchmark Arabic dataset of questions and answers	83%	String-based similarity suffers from ignoring semantic aspect. Whereas, corpus-based similarity of DISCO suffers from domain dependent
Kyle and Crossley (2016)	Supervised	Simple regression	Word frequency, n-gram, and academic writing	Real-world student answers (English Placement Test)	92.6%	More semantic features are needed
Pramukantoro and Fauzi (2016)	Unsupervised	LSA + Cosine	String-similarity + semantic similarity	Real-world student answers (English)	59.7%	corpus-based similarity of LSA suffers from domain dependent

Kopparapu and De (2016)	Unsupervised	Ranking algorithm	Structural features (# words, sentences and paragraphs) + Semantic corpus-based (Kullback - Leibler divergence)	English Benchmark Automated Student Assessment Prize (ASAP)	-	corpus-based similarity of Kullback - Leibler divergence suffers from domain dependent
Ajetunmobi and Daramola (2017)	Unsupervised	Ontology-based approach (WordNet)	Semantic relatedness (LCS)	Synthesis (English)	80%	ontology offers domain-specific semantic correspondences where open domain answers would not be assessed effectively
Al-Jouie and Azmi (2017)	Unsupervised	LSA + RST	Semantic similarity + Spelling + structure + grammar	Real-world student answers (Arabic)	78.3%	corpus-based similarity of LSA suffers from domain dependent
Crossley and Kyle (2018)	Unsupervised	Rule-based	Word frequency, n-gram frequency and academic writing	Synthesis (based on user-generated data)	-	more semantic analysis is needed
Hasanah et al. (2018)	Unsupervised	Cosine Similarity	Lowercasing, tokenization, punctuation removal, stopword removal and stemming	Real-world student answers (Indonesian)	47%	more semantic analysis is needed
Ratna et al. (2018)	Unsupervised	Fingerprinting algorithm	Characters ASCII values of the answer's words	Real-world student answers (Japanese)	86.86%	Focusing on ASCII values of characters would only determine morphological similarity and ignore the semantic similarity
Filho et al. (2018)	Supervised	SVR	Predefined numeric scores of features (Structure+ lexical diversity + theme + coherence)	Real-world student answers (Portuguese)	74.7%	More semantic analysis is needed. In addition, much more sophisticated regressor is needed (SVR is considered shallow neural network and not deep learning)
Cozma et al. (2018)	Supervised	Bag-of-Super-Word-Embeddings (BOSWE) + SVR	Histogram Intersection String Kernel (HISK)	English Benchmark Automated Student Assessment Prize (ASAP)	78.8%	This method could suffer from 'out-of-vocabulary' problem. In addition, much more sophisticated regressor is needed (SVR is considered shallow neural network and deep learning)
Hassan et al. (2018)	Supervised	Ridge regression based on vector cosine similarity	Word embedding models (Word2Vec, FastText, Glove, Elmo) + Paragraph embedding models (Doc2Vec, InferSent, Skipthought)	English Benchmark dataset (University of North Texas)	56.9%	Much more sophisticated regression is needed. In addition, regression can benefit from embedding vector features rather than feeding only on similarity values produced by cosine
Li et al. (2018)	Supervised	LSTM regression	Self-attention with Glove embedding and word position	ASAP	77.6%	Glove embedding suffers from 'out-of-vocabulary' problem.
Wang et al. (2018)	Supervised	Bidirectional LSTM with attention layer	Word2Vec word embedding	ASAP	83%	Word2Vec embedding suffers from 'out-of-vocabulary' problem.
Ratna et al. (2019)	Unsupervised	Fingerprinting algorithm + LSA	Characters ASCII values of the answer's words + semantic similarity	Real-world student answers (Japanese)	87.78%	corpus-based similarity of LSA suffers from domain dependent
Ratna et al. (2019)	Unsupervised	K-means clustering + LSA	Semantic similarity	Real-world student answers (Japanese)	89%	corpus-based similarity of LSA suffers from domain dependent
Garner et al. (2019)	Supervised	Stepwise regression	Association measures of bigram and trigram	Real-world student answers (English Placement Test)	84.64%	More semantic analysis is needed. In addition, much more sophisticated regressor is needed

Filho et al. (2019)	Supervised	SVR to solve imbalance classes	Predefined numeric scores of features (Structure+ lexical diversity + theme + coherence)	Real-world student answers (Portuguese)	75%	More semantic analysis is needed. In addition, much more sophisticated regressor is needed (SVR is considered shallow neural network and not deep learning)
Ratna et al. (2019)	Combination: Supervised (topic-modeling) Unsupervised (answer similarity)	SVM + LSA	Topic modeling (SVM) + semantic similarity (LSA)	Real-world student answers (Indonesian)	72.01%	corpus-based similarity of LSA suffers from domain dependent
Nadeem et al. (2019)	Supervised	LSTM	Doc2Vec + Structural Features	ASAP	77.5%	Doc2Vec embedding suffers from 'out-of-vocabulary' problem.
Alqahtani and Alsaif (2019)	Unsupervised	Rule-based	Spelling + structure + coherence	Real-world student answers (Arabic)	73%	More semantic analysis is needed. In addition, the dataset used was relatively small and not adequately adjusted
Azmi et al. (2019)	Unsupervised	LSA + RST	Semantic similarity + Spelling + structure + grammar	Real-world student answers (Arabic)	75.6%	corpus-based similarity of LSA suffers from domain dependent
Chen and Zhou (2019)	Supervised	CNN + Ordinal Regression	Pre-trained word embedding based on Glove	ASAP	82.6%	Glove embedding suffers from 'out-of-vocabulary' problem.
Liu et al. (2019)	Supervised	Multi-way attention architecture	Pre-trained Glove word embedding	Real-world student answers (English)	88.9%	Glove embedding suffers from 'out-of-vocabulary' problem.
Zhang & Litman (2019)	Supervised	LSTM with co-attention layer	Glove pre-trained embedding	ASAP	81.5%	Glove embedding suffers from 'out-of-vocabulary' problem.
Rodriguez et al. (2019)	Supervised	BERT architecture	BERT pretraining embedding	ASAP	74.75%	BERT architecture suffers from 'catastrophic forgetting' problem
Hendre et al. (2020)	Unsupervised	vector embedding cosine similarity	TFIDF, Jaccard, Glove, Elmo, GSE-lite, GSE-large	ASAP	74.3%	Relying on cosine to compute similarity between vectors would seem insufficient, utilizing the embedding features of GSE for a regression task can be seen promising
Kyle (2020)	Supervised	Simple regression	Word frequency, n-gram and LSA	Real-world student answers (English Placement Test)	-	corpus-based similarity of LSA suffers from domain dependent
Li et al. (2020)	Supervised	LSTM regression	Sentence embedding using CNN based on Glove word embedding	ASAP	72.65%	Glove embedding suffers from 'out-of-vocabulary' problem.
Tashu (2020)	Supervised	BGRU	Word embedding Word2Vec processed via CNN	ASAP	86.5%	Word2Vec embedding suffers from 'out-of-vocabulary' problem.
Mayfield and Black (2020)	Supervised	BERT architecture	Pretraining BERT embedding	ASAP	64.6%	BERT architecture suffers from 'catastrophic forgetting' problem
Ridley et al. (2021)	Supervised	Bidirectional LSTM with attention layer	Glove word embedding and LSTM sentence embedding with traits attention layer	ASAP	76.4%	Glove embedding suffers from 'out-of-vocabulary' problem.
Ormerod et al. (2021)	Supervised	Efficient BERT architecture	Efficient architectures derived from BERT such as Albert and Reformer	ASAP	78.2%	Still suffers of 'catastrophic forgetting' problem

TABLE II. SUMMARY OF TECHNIQUES

Author	Morphology		Corpus-based			Embedding					Knowledge	Frequencies & Structural
	String	ASCII	LSA	DISCO	KLD	Word2Vec	Glove	Doc2Vec	GSE	BERT	Ontology	
Gomaa & Fahmy (2014)				√								
Kyle and Crossley (2016)												√
Pramukantoro and Fauzi (2016)	√		√									
Kopparapu and De (2016)					√							√
Ajetunmobi and Daramola (2017)											√	
Al-Jouie and Azmi (2017)			√									√
Crossley and Kyle (2018)												√
Hasanah et al. (2018)	√											
Filho et al. (2018)												√
Cozma et al. (2018)						√						
Hassan et al. (2018)						√	√	√				
Li et al. (2018)							√					
Wang et al. (2018)						√						
Ratna et al. (2019)		√	√									
Ratna et al. (2019)			√									
Garner et al. (2019)												√
Filho et al. (2019)												√
Ratna et al. (2019)			√									
Nadeem et al. (2019)								√				√
Alqahtani and Alsaif (2019)												√
Azmi et al. (2019)			√									√
Chen and Zhou (2019)							√					
Liu et al. (2019)							√					
Zhang & Litman (2019)							√					
Rodriguez et al. (2019)										√		
Hendre et al. (2020)							√		√			√
Kyle (2020)			√									√
Li et al. (2020)							√					
Tashu (2020)						√						
Mayfield and Black (2020)										√		
Ridley et al. (2021)							√	√				√
Ormerod et al. (2021)										√		

#### IV. DISCUSSION

AES task has been depicted in the literature through various techniques. The traditional ones were concentrating on the essay structure, spelling and grammatical errors ([2]; [3]; [6]; [12]; [22]). Obviously, these techniques are focusing on general features of the essay and cannot provide an accurate scoring based on such general features. However, the structural features showed feasibility when combined with other semantic features.

Another type of features depicted in the literature is the ones focused on morphological aspect of the words within the essay. This has been represented by utilizing the string-based similarity ([18]; [39]; [40]). On the other hand, the statistics of words within the essay have been also utilized ([12]; [21]). The main limitation behind the aforementioned techniques lies in the absence of semantic analysis in which focusing only on the morphology of the words would discard the semantic factor.

For this purpose, some studies have utilized a semantic knowledge source in order to enhance semantic analysis. For instance, [1] have utilized the ontology of WordNet for AES task. Yet, the problem of such external knowledge source is that it can provide general synonyms of the words where the aim sometime is to focus on specific domain. On other hand, some studies attempted to include the semantic analysis without the use of any external knowledge source, but rather through corpus-based approaches ([2]; [6]; [18]; [40]). These approaches are being fed with specific corpus to analyze the similar contexts which reflects on finding semantic correspondences. The common example of these approaches is the Latent Semantic Analysis (LSA). However, the main limitation behind the corpus-based approaches, in contrary to the use of knowledge source, is that they become domain-dependent after being fed by specific corpus. This makes them too sensitive toward the domain of the answers.

Further research attempts showed different techniques for semantic analysis; in particular, the Neural-Network-based techniques. Such techniques aim at processing a set of token words as input to a neural network architecture for the purposed of outputting distinctive embedding for each term. Such an embedding would capture the semantic, lexical and other important features of the word and represent them in a vector. This vector then would be utilized for other tasks such as the AES. The common example of these techniques is the Word2Vec architecture [45]. The problem of this architecture is represented by the need to train the model on large text, meanwhile, fine tune the parameters of the network; otherwise, it would generate inaccurate embedding.

To solve the aforementioned problem, further researches have presented a pre-trained model in which the model is being trained on large text and its parameters are fine tuned. The literature showed the utilization of a pre-trained Word2Vec models [11] along with another pre-trained model known as Glove ([9]; [26]; [27]; [28]; [45]; [46]). The main limitation behind these architectures is that they only work with word-level which obstructs them from working on document/sentence-level. Since the AES task is mainly depending on sentence/document answers, the traditional word embedding architectures seem insufficient.

Other studies have utilized much more sophisticated architecture to handle document/sentence embedding such as Doc2Vec [20] or Google Sentence Encoder (GSE) [21]. However, these architectures suffer from a common limitation known as 'out-of-vocabulary'. This problem occurs when an embedding architecture is being tested with a word that has no embedding vector within its training model.

In fact, the embedding techniques are considered as the state-of-the-art techniques that have shown remarkable performance in the AES task. Therefore, it is a significant effort to overcome the 'out-of-vocabulary' problem in order to enhance the semantic analysis which indeed would reflect on improving the essay answer scoring.

A remarkable overcome for the aforementioned problems has been depicted by the emergence of Bidirectional Encoder Representation from Transformer (BERT) architecture [13]. Such an architecture has the ability to overcome the averaging embedding for larger text units (e.g., document and paragraph) by utilizing a pretrained embedding that works by treating the sentence as a combination of words with fixed an indexed embedding. In addition, it has the ability to overcome 'out-of-vocabulary' problem by dividing unseen words into an indexed and recognized words from its vocabulary repository. BERT has two models; language modeling and fine-tuning. The first model aims at understand the language of a text and its latent contextual information. Whereas, the second model aims at accommodating the desired task such as question answer, document classification or ranking.

However, multiple recent researches showed that BERT architecture has non-outstanding performance on AES task compared to techniques ([16]; [30]; [43]). Although BERT showed magnificent performance in problems like question answering, its architecture failed to give an accurate scoring for an answer. The reason behind such failure lies on a problem called 'catastrophic forgetting' where its language model forgets significant contextual information that impact the scoring. In addition, BERT suffers from the tremendous extent of parameters where around 60 million parameters represent a highly computational requirement [35].

According to [7], the application of most sophisticated embedding techniques including BERT on AES task is still lacking of latent rubrics. This is because the scoring task is still challenging for humans themselves. Hence, the language modeling architectures show an outstanding ability of capturing semantic of text. Yet, it is still lacking the writing style or structural features.

#### V. CONCLUSION

This paper has provided a review on the feature analysis used for either supervised or unsupervised AES. Within such a review, a taxonomy has been represented for the feature analysis which included four main types; Morphology, Frequencies, Structure, and Semantic. Inside each type, various subcomponents and approaches have been illustrated. After that, a critical review has been provided on the recent AES studies by linking each feature analysis type to these studies. The finding of such a critical analysis showed that the traditional morphological analysis of the essay answer would

lack the semantic analysis. Whereas, utilizing a semantic knowledge source such as ontology would be restricted to the domain of the essay answer. Similarly, utilizing semantic corpus-based techniques would be impacted by the domain of the essay answer as well. On the other hand, using essay structural features and frequencies alone would be insufficient, but rather as an auxiliary to another semantic analysis technique would bring promising results. The state-of-the-art in AES researches concentrated on neural-network-based-embedding techniques. Yet, the major limitations of these techniques are represented as (i) finding an adequate sentence-level embedding when using models such as Word2Vec and Glove, (ii) 'out-of-vocabulary' when using models such as Doc2Vec and GSE, and lastly, (iii) 'catastrophic forgetting' when using BERT model.

#### ACKNOWLEDGMENT

This study is supported by the University Kebangsaan Malaysia (UKM).

#### REFERENCES

- [1] Ajetunmobi, S. A., & Daramola, O. (2017, 29-31 Oct. 2017). Ontology-based information extraction for subject-focussed automatic essay evaluation. Paper presented at the 2017 International Conference on Computing Networking and Informatics (ICCN).
- [2] Al-Jouie, M. F., & Azmi, A. M. (2017). Automated Evaluation of School Children Essays in Arabic. *Procedia Computer Science*, 117, 19-22. doi:https://doi.org/10.1016/j.procs.2017.10.089.
- [3] Alqahtani, A., & Alsaif, A. (2019, 10-12 Dec. 2019). Automatic Evaluation for Arabic Essays: A Rule-Based System. Paper presented at the 2019 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT).
- [4] Alshaikhdeeb, B., & Ahmad, K. (2015). Integrating correlation clustering and agglomerative hierarchical clustering for holistic schema matching. *Journal of Computer Science*, 11(3), 484-489.
- [5] Azmi, A. M., Al-Jouie, M. F., & Hussain, M. (2019). AAEE—Automated evaluation of students' essays in Arabic language. *Information Processing & Management*, 56(5), 1736-1752.
- [6] Azmi, A. M., Al-Jouie, M. F., & Hussain, M. (2019). AAEE – Automated evaluation of students' essays in Arabic language. *Information processing & management*, 56(5), 1736-1752. doi:https://doi.org/10.1016/j.ipm.2019.05.008.
- [7] Beseiso, M., & Alzahrani, S. (2020). An Empirical Analysis of BERT Embedding for Automated Essay Scoring.
- [8] Blanchard, D., Tetreault, J., Higgins, D., Cahill, A., & Chodorow, M. (2013). TOEFL11: A corpus of non - native English. *ETS Research Report Series*, 2013(2), i-15.
- [9] Chen, Z., & Zhou, Y. (2019, 25-28 May 2019). Research on Automatic Essay Scoring of Composition Based on CNN and OR. Paper presented at the 2019 2nd International Conference on Artificial Intelligence and Big Data (ICAIBD).
- [10] Choi, E., He, H., Iyyer, M., Yatskar, M., Yih, W.-t., Choi, Y., . . . Zettlemoyer, L. (2018). Quac: Question answering in context. arXiv preprint arXiv:1808.07036.
- [11] Cozma, M., Butnaru, A. M., & Ionescu, R. T. (2018). Automated essay scoring with string kernels and word embeddings. arXiv preprint arXiv:1804.07954.
- [12] Crossley, S. A., & Kyle, K. (2018). Assessing writing with the tool for the automatic analysis of lexical sophistication (TAALES). *Assessing Writing*, 38, 46-50. doi:https://doi.org/10.1016/j.asw.2018.06.004.
- [13] Devlin, J., Chang, M.-W., Lee, K., & Toutanova, K. (2018). Bert: Pre-training of deep bidirectional transformers for language understanding. arXiv preprint arXiv:1810.04805.
- [14] Filho, A. H., Concato, F., Nau, J., Prado, H. A. d., Imhof, D. O., & Ferneda, E. (2019). Imbalanced Learning Techniques for Improving the Performance of Statistical Models in Automated Essay Scoring. *Procedia Computer Science*, 159, 764-773. doi:https://doi.org/10.1016/j.procs.2019.09.235.
- [15] Filho, A. H., do Prado, H. A., Ferneda, E., & Nau, J. (2018). An approach to evaluate adherence to the theme and the argumentative structure of essays. *Procedia Computer Science*, 126, 788-797. doi:https://doi.org/10.1016/j.procs.2018.08.013.
- [16] Fukuda, H., Tsunakawa, T., Oshima, J., Oshima, R., Nishida, M., & Nishimura, M. (2020). BERT-based Automatic Text Scoring for Collaborative Learning. Paper presented at the 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE).
- [17] Garner, J., Crossley, S., & Kyle, K. (2019). N-gram measures and L2 writing proficiency. *System*, 80, 176-187. doi:https://doi.org/10.1016/j.system.2018.12.001.
- [18] Gomaa, W. H., & Fahmy, A. A. (2014). Automatic scoring for answers to Arabic test questions. *Computer Speech & Language*, 28(4), 833-857.
- [19] Hasanah, U., Astuti, T., Wahyudi, R., Rifai, Z., & Pambudi, R. A. (2018, 13-14 Nov. 2018). An Experimental Study of Text Preprocessing Techniques for Automatic Short Answer Grading in Indonesian. Paper presented at the 2018 3rd International Conference on Information Technology, Information System and Electrical Engineering (ICITISEE).
- [20] Hassan, S., Fahmy, A. A., & El-Ramly, M. (2018). Automatic Short Answer Scoring based on Paragraph Embeddings. *International Journal of Advanced Computer Science and Applications*, 9(10), 397-402.
- [21] Hendre, M., Mukherjee, P., Preet, R., & Godse, M. (2020). Efficacy of Deep Neural Embeddings based Semantic Similarity in Automatic Essay Evaluation. *International Journal of Computing and Digital Systems*, 9, 1-11.
- [22] Kopperapu, S. K., & De, A. (2016, 21-24 Sept. 2016). Automatic ranking of essays using structural and semantic features. Paper presented at the 2016 International Conference on Advances in Computing, Communications and Informatics (ICACCI).
- [23] Kumar, V., Ramakrishnan, G., & Li, Y.-F. (2018). A framework for automatic question generation from text using deep reinforcement learning. arXiv preprint arXiv:1808.04961.
- [24] Kyle, K. (2020). The relationship between features of source text use and integrated writing quality. *Assessing Writing*, 45, 100467. doi:https://doi.org/10.1016/j.asw.2020.100467.
- [25] Kyle, K., & Crossley, S. (2016). The relationship between lexical sophistication and independent and source-based writing. *Journal of Second Language Writing*, 34, 12-24. doi:https://doi.org/10.1016/j.jslw.2016.10.003.
- [26] Li, X., Chen, M., & Nie, J.-Y. (2020). SEDNN: Shared and enhanced deep neural network model for cross-prompt automated essay scoring. *Knowledge-Based Systems*, 210, 106491. doi:https://doi.org/10.1016/j.knsys.2020.106491.
- [27] Li, X., Chen, M., Nie, J., Liu, Z., Feng, Z., & Cai, Y. (2018). Coherence-Based Automated Essay Scoring Using Self-attention Chinese Computational Linguistics and Natural Language Processing Based on Naturally Annotated Big Data (pp. 386-397): Springer.
- [28] Liu, T., Ding, W., Wang, Z., Tang, J., Huang, G. Y., & Liu, Z. (2019). Automatic short answer grading via multiway attention networks. Paper presented at the International Conference on Artificial Intelligence in Education.
- [29] Mathias, S., & Bhattacharyya, P. (2018). ASAP++: Enriching the ASAP automated essay grading dataset with essay attribute scores. Paper presented at the Proceedings of the Eleventh International Conference on Language Resources and Evaluation (LREC 2018).
- [30] Mayfield, E., & Black, A. W. (2020). Should You Fine-Tune BERT for Automated Essay Scoring? Paper presented at the Proceedings of the Fifteenth Workshop on Innovative Use of NLP for Building Educational Applications.
- [31] Mikolov, T., Sutskever, I., Chen, K., Corrado, G. S., & Dean, J. (2013). Distributed representations of words and phrases and their compositionality. Paper presented at the Advances in neural information processing systems.
- [32] Mohamed, O. J., ZAKAR, N. A., & Alshaikhdeeb, B. (2019). A combination method of syntactic and semantic approaches for

- classifying examination questions into Bloom's taxonomy cognitive. *Journal of Engineering Science and Technology*, 14(2), 935-950.
- [33] Montgomery, D. C., Peck, E. A., & Vining, G. G. (2015). *Introduction to linear regression analysis*: John Wiley & Sons.
- [34] Nadeem, F., Nguyen, H., Liu, Y., & Ostendorf, M. (2019). Automated Essay Scoring with Discourse-Aware Neural Models. Paper presented at the Proceedings of the Fourteenth Workshop on Innovative Use of NLP for Building Educational Applications.
- [35] Ormerod, C. M., Malhotra, A., & Jafari, A. (2021). Automated essay scoring using efficient transformer-based language models. arXiv preprint arXiv:2102.13136.
- [36] Pouyanfar, S., Sadiq, S., Yan, Y., Tian, H., Tao, Y., Reyes, M. P., . . . Iyengar, S. (2018). A survey on deep learning: Algorithms, techniques, and applications. *ACM Computing Surveys (CSUR)*, 51(5), 1-36.
- [37] Pramukantoro, E. S., & Fauzi, M. A. (2016, 15-16 Oct. 2016). Comparative analysis of string similarity and corpus-based similarity for automatic essay scoring system on e-learning gamification. Paper presented at the 2016 International Conference on Advanced Computer Science and Information Systems (ICACSIS).
- [38] Ratna, A. A. P., Khairunissa, H., Kaltsum, A., Ibrahim, I., & Purnamasari, P. D. (2019, 2-3 Oct. 2019). Automatic Essay Grading for Bahasa Indonesia with Support Vector Machine and Latent Semantic Analysis. Paper presented at the 2019 International Conference on Electrical Engineering and Computer Science (ICECOS).
- [39] Ratna, A. A. P., Luhurkinanti, D. L., Ibrahim, I., Husna, D., & Purnamasari, P. D. (2018, 21-22 Sept. 2018). Automatic Essay Grading System for Japanese Language Examination Using Winnowing Algorithm. Paper presented at the 2018 International Seminar on Application for Technology of Information and Communication.
- [40] Ratna, A. A. P., Noviaindriani, R. R., Santiar, L., Ibrahim, I., & Purnamasari, P. D. (2019, 22-24 July 2019). K-Means Clustering for Answer Categorization on Latent Semantic Analysis Automatic Japanese Short Essay Grading System. Paper presented at the 2019 16th International Conference on Quality in Research (QIR): International Symposium on Electrical and Computer Engineering.
- [41] Ratna, A. A. P., Santiar, L., Ibrahim, I., Purnamasari, P. D., Luhurkinanti, D. L., & Larasati, A. (2019, 23-25 Oct. 2019). Latent Semantic Analysis and Winnowing Algorithm Based Automatic Japanese Short Essay Answer Grading System Comparative Performance. Paper presented at the 2019 IEEE 10th International Conference on Awareness Science and Technology (iCAST).
- [42] Ridley, R., He, L., Dai, X., Huang, S., & Chen, J. (2021). Automated Cross-prompt Scoring of Essay Traits.
- [43] Rodriguez, P. U., Jafari, A., & Ormerod, C. M. (2019). Language models and Automated Essay Scoring. arXiv preprint arXiv:1909.09482.
- [44] Tashu, T. M. (2020, 3-5 Feb. 2020). Off-Topic Essay Detection Using C-BGRU Siamese. Paper presented at the 2020 IEEE 14th International Conference on Semantic Computing (ICSC).
- [45] Wang, Z., Liu, J., & Dong, R. (2018, 23-25 Nov. 2018). Intelligent Auto-grading System. Paper presented at the 2018 5th IEEE International Conference on Cloud Computing and Intelligence Systems (CCIS).
- [46] Zhang, H., & Litman, D. (2019). Co-attention based neural network for source-dependent essay scoring. arXiv preprint arXiv:1908.01993.
- [47] Zhu, X. (2006). Semi-supervised learning literature survey. *Computer Science, University of Wisconsin-Madison*, 2(3), 4.
- [48] Zou, W. Y., Socher, R., Cer, D., & Manning, C. D. (2013). Bilingual word embeddings for phrase-based machine translation. Paper presented at the Proceedings of the 2013 Conference on Empirical Methods in Natural Language Processing.

# Forensic Analysis on False Data Injection Attack on IoT Environment

Saiful Amin Sharul Nizam<sup>1</sup>, Zul-Azri Ibrahim<sup>2</sup>, Fiza Abdul Rahim<sup>3</sup>  
Hafizuddin Shahril Fadzil<sup>4</sup>, Haris Iskandar Mohd Abdullah<sup>5</sup>, Muhammad Zulhusni Mustafa<sup>6</sup>  
UNITEN R&D Sdn. Bhd., Selangor, Malaysia<sup>1, 4, 5, 6</sup>  
College of Computing and Informatics, Universiti Tenaga Nasional, Malaysia<sup>2</sup>  
Razak Faculty of Technology and Informatics, Universiti Teknologi Malaysia, Malaysia<sup>3</sup>  
Institute of Informatics and Computing Energy, Universiti Tenaga Nasional, Malaysia<sup>2, 3</sup>

**Abstract**—False Data Injection Attack (FDIA) is an attack that could compromise Advanced Metering Infrastructure (AMI) devices where an attacker may mislead real power consumption by falsifying meter usage from end-users smart meters. Due to the rapid development of the Internet, cyber attackers are keen on exploiting domains such as finance, metering system, defense, healthcare, governance, etc. Securing IoT networks such as the electric power grid or water supply systems has emerged as a national and global priority because of many vulnerabilities found in this area and the impact of the attack through the internet of things (IoT) components. In this modern era, it is a compulsion for better awareness and improved methods to counter such attacks in these domains. This paper aims to study the impact of FDIA in AMI by performing data analysis from network traffic logs to identify digital forensic traces. An AMI testbed was designed and developed to produce the FDIA logs. Experimental results show that forensic traces can be found from the evidence logs collected through forensic analysis are sufficient to confirm the attack. Moreover, this study has produced a table of attributes for evidence collection when performing forensic investigation on FDIA in the AMI environment.

**Keywords**—Advanced Metering Infrastructure (AMI); False Data Injection Attack (FDIA); man in the middle (MITM); internet of things (IoT); forensic analysis

## I. INTRODUCTION

Internet of Things (IoT) offers many benefits and advantages to people in the current modern era [1]. Besides, even in our daily life, IoT has proven to be beneficial. IoT is a system of interrelated intelligent devices that are provided with unique identifiers and given the ability to connect with other devices by exchanging information over a communication network. The IoT is seen as one of the foremost important zones in future development and is expanding tremendous consideration from a wide scope of businesses [2]. IoT will play a major role in improving many sectors such as manufacturing, public security, health care, accommodation, entertainment, environment protection, agriculture, industrial monitoring, intelligent transportation, and traditional metering system.

However, little consideration has been paid to IoT adoption that may affect the IoT device's security measure, such as lack of authentication and insecure communication are among the main problems in most IoT devices [3]. These vulnerabilities will lead to many forms of attacks taking place, such as

malware injection, SQL injection [4], false data injection (FDI), man-in-the-middle (MITM) [5], zero-day exploit, distributed denial-of-service (DDoS), DNS tunnelling [6], and many more cyber-attacks. Since the case of the Mirai botnet in 2016, over 600,000 IoT devices were targeted to launch cyberattacks that reached 620 Gigabits at the peak. The number of malware in the cyber world has been growing, giving threats to cybersecurity to face other types of aggravated attacks.

There is also concern about one of the IoT environments, the Advanced Metering Infrastructure (AMI). AMI is a system consisting of modern electronic-digital hardware and software, which enables data measurement intermittently and remote communication continuously. The system gives a few important capacities that were not already possible or had to be performed manually. For instance, the ability to remotely and automatically measure power usage, connect and disconnect service, and voltage monitoring. FDIA is one of the popular attacks that can impact AMI as countries around the globe are implementing an AMI in their infrastructure. Like the MITM attack, FDIA is more toward creating falsified data, which the attacker injected from compromised smart meters to change the actual value sent by another smart meter in AMI. This threat can negatively affect both utilities and customers as it is difficult to investigate from the available log in the AMI [7]. This paper aims to simulate the impact of FDIA on the IoT environment and perform forensic analysis on digital traces from data obtained.

In the next section of this paper, related literature on cyber attacks in the smart grid was reviewed. Subsequently, Section III presents the development of a testbed that is used to simulate the cyber attack in components of the smart grid. Section IV presents the result from the simulation and how forensic investigations are done to investigate FDI attacks in the smart grid environment. Section V provides a conclusion to the paper.

## II. LITERATURE REVIEW

### A. False Data Injection Attack (FDIA)

The operation of the smart grid faces extreme consequences when the smart meters have been compromised and reporting false power consumption. Most current cases include the crime of electricity stealing. However, a few other sorts of data falsification attacks are conceivable such as FDIA. AMI would

be affected by this kind of attack badly as data falsification is difficult to detect.

Based on [8], they work on detecting falsification of data injection attacks focusing on smart grid systems. They made a successful and real-time scheme to distinguish FDIA in smart grids where they evaluate the reliabilities of state estimations by misusing spatial-temporal correlations and trust-based voting. The study's objective is to minimize the harm from the threat of FDIA in smart grids by using these solutions to conduct detection of an attack. This case study was done by simulation of the smart grid and the proposed solutions to detect malicious FDIA. It is suggested that powerful countermeasures are necessary as these kinds of attacks can become highly potential threats as those FDIA are evolving by implementing anti-forensic techniques to prevent detection of the attack.

In [9], the study proposed a system to detect cyber-attacks that aim to sabotage the Instrumentation and Control (I&C) environment. The study intends to provide a last line of defense to sabotage attacks. A system called Goosewolf was produced which has the capability to detect when an adversary has manipulated the process control of the Programmable Logic Controller (PLC). The result obtained in that study shows that the proposed system is effective in checking the capabilities of the PLC and the ability to detect FDIA.

Another study by [10] has focused their work on statistical anomaly detection techniques to solve the difficulties in detecting data falsification in AMI. To identify compromised smart meters for deductive and additive attacks, they have proposed a trust model based on Kullback-Leibler divergence. Moreover, techniques such as the generalized linear and Weibull function-based kernels were proposed for camouflage and conflict attacks. After investigation on comparison under various attacks, which is additive, deductive, camouflage, and conflict, they found out that their models have good high true positive detection and the average false positive is just 8 per cent for most attacks conducted.

### B. IoT Testbeds

For the purpose of better understanding on vulnerabilities of IoT devices, researchers utilized a security testbed designed to simulate the attack in a particular environment. The author in [11] illustrated a testbed for securing IoT devices by producing a testbed that can be used as a penetration testing platform to evaluate risks and vulnerabilities of IoT devices. The penetration testing included were port scanning, vulnerability scanning, downgrading attack, search exploits, brute force directories, passwords, port services, and SSL configuration. The software used to perform the testing were Snitch, ZAP, Wascan, Skipfish, Nmap, TLS proper, SSLScan, Nikto, Wireshark, Ettercap, Dirb, SQLmap, WAFwoof, Metasploit, Dex2jar, Binwalk, and UART. The network protocols used was WIFI and BLE. Penetration testing for this analysis was conducted on a smart bulb and IP camera. Vulnerabilities found were very common problems in IoT-based products such as no firewall, authentication in plain text, open ports, lack of certificate, etc.

Moreover, paper [12] displayed a testbed designed to analyze security issues in IoT devices. This testbed indicated design and architecture prerequisites to support the development of penetration testing for the purpose of cybersecurity forensic investigation. They conducted the tests based on the security vulnerabilities in the IoT products such as Amazon Echo, Nest Cam, Phillips hue, SENSE Mother, Samsung SmartThings, Witching HOME, WeMo Smart Crock-Pot, and Netatmo Security Camera. The study was conducted using WIFI and Bluetooth. For control and administration, they handle the process and events using NI TestStand software. A closed source software runs only on Windows OS, which is intensely prohibitive and proprietary. Following a huge downside from limitation in network penetration testing capabilities, the software used to avoid testing from handling passive capture of packets, wireless cards, and other network or low-level functionalities.

In [13], researchers used SecuWear to recognize the weaknesses of commercial hardware. The testbed collects the data needed for distinguishing different attacks, thereby assessing the security of wearables devices. Besides, it gives a method for mitigating information and performing attacks in a network that used WIFI and BLE. The software used to perform the vulnerability assessments, and penetration testing was Wireshark. In that study, the eavesdropping and the Denial of Service (DOS) attack were executed. The results of the study found that SecuWear vulnerabilities may be similar to certain open sources such as false positives when recognizing security issues.

### III. TESTBED DEVELOPMENT

Fig. 1 shows the topology of our testbed that is used to perform FDIA. The testbed consists of 4 main hardware components, two units Raspberry Pi 4 Model B, a computer and a switch. The smart meter (192.168.1.13) generates random data to mimic a real smart meter then sends the generated data to the data collector containing one virtual machine running Ubuntu Version 21.04 operating system to act as a data collector using the MYSQL version 10.14.9-MariaDB database which receives incoming data from the smart meter. Attacker smart meter (192.168.1.11) will act as an attacker to perform FDIA that will attempt to tamper the smart meter data to the data collector.

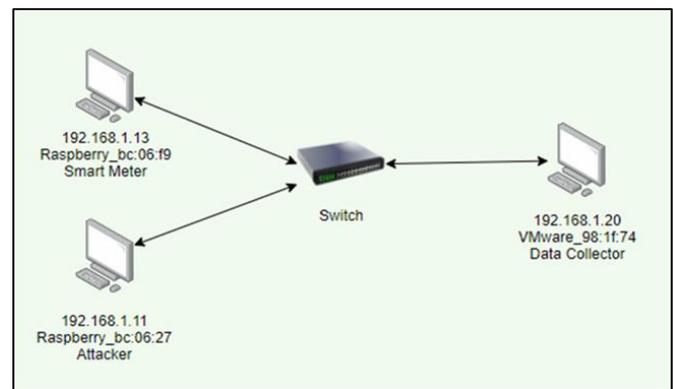


Fig. 1. Testbed Topology.

A comparative analysis between normal traffic logs and logs during the attack was made to verify the FDIA investigations in the IoT environment. Forensic evidence was analyzed based on the packet captured using Wireshark in the form of PCAP files.

#### IV. DISCUSSION OF FINDINGS

The experiments conducted on the testbed were carried out in two phases. The first phase of the experiment was the 'Normal operation', and the second phase was the 'Under Attack'. The details of the experiments will be explained later on in this chapter. Fig. 2 shows the flow of the experiment during normal traffic and under attack.

##### A. Normal Operations

During the normal traffic phase, the smart meter as shown in Fig. 1 with an IP address of 192.168.1.13 with MAC address of Raspberry bc : 06: f9 will send data to the data collector where the IP address of the database is 192.168.1.20 with MAC address of VMware\_98:1f:74. The smart meter will send power consumption data with an interval of 10 seconds between each data to imitate data for 1 week with an interval of 30 minutes between each data interval. In this experiment, 137 data will be collected using the Wireshark version 3.4.5 packet capturing tool. The consumption transmission script will run in 25 minutes to collect data in a total range of 135 to 140 data. Fig. 3 shows the data sent by the smart meter to the data collector, the value of power consumption with the timestamp.

Fig. 4 shows the sample data sent by the smart meter to the data collector in the MySQL database. The first column shows the numbers of data in the database. The second column shows the ID of the smart meter, the third and fourth rows display the timestamp of when the data was accepted, and the last row shows the data value of the power consumption.

```
[POWER CONSUMPTION] 3719 kWh
[TIMESTAMP] 2020-12-17 17:52:42
MAC00003 - 3719 - 01:53:02 - 2020-12-18
('MAC ID: ', 'MAC00003', '| Power Consumption: ', 3719)

[POWER CONSUMPTION] 3349 kWh
[TIMESTAMP] 2020-12-17 17:52:42
MAC00003 - 3349 - 01:53:12 - 2020-12-18
('MAC ID: ', 'MAC00003', '| Power Consumption: ', 3349)

[POWER CONSUMPTION] 6674kWh
[TIMESTAMP] 2020-12-17 17:52:42
MAC00003 - 6674 - 01:53:22 - 2020-12-18
('MAC ID: ', 'MAC00003', '| Power Consumption: ', 6674)

[POWER CONSUMPTION] 7542 kWh
[TIMESTAMP] 2020-12-17 17:52:42
MAC00003 - 7542 - 01:53:32 - 2020-12-18
('MAC ID: ', 'MAC00003', '| Power Consumption: ', 7542)
```

Fig. 3. Smart Meter Sending Data in Normal Traffic.

9015	MAC00003	2020-12-18	01:53:02	3719
9016	MAC00003	2020-12-18	01:53:12	3349
9017	MAC00003	2020-12-18	01:53:22	6674
9018	MAC00003	2020-12-18	01:53:32	7542
9019	MAC00003	2020-12-18	01:53:42	1971

Fig. 4. Accepted Data in a Database.

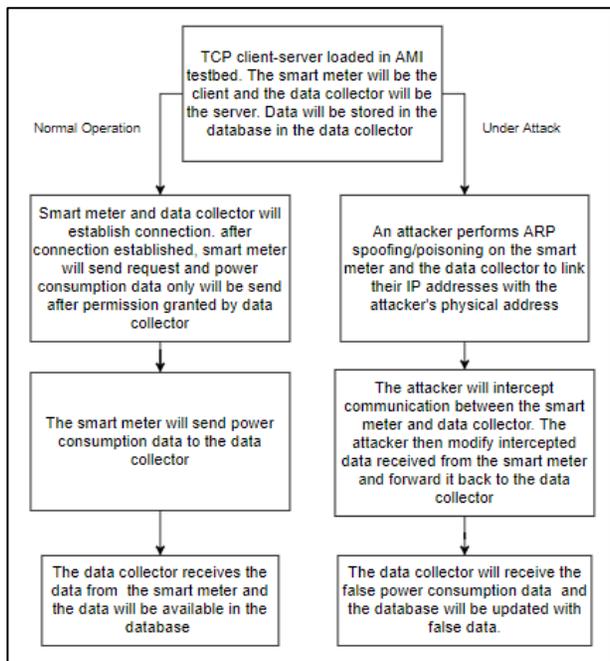


Fig. 2. Flow of Experiments.

Fig. 5 shows only the ARP packet for this communication. The results show that the smart meter with MAC address Raspberry\_bc:06:f9 with IP address 192.168.1.13 made a broadcast asking for the MAC address of the default gateway with the IP address 192.168.1.1. Moreover, it shows that the data collector is asking for the MAC address of the destination with the IP address of 192.168.1.13. As highlighted in Fig. 5, it is shown that the destination or the data smart meter answer the ARP request of the smart meter by giving its MAC address Raspberry\_bc:06:f9. The smart meter also give ARP, a reply to its MAC address as shown in Fig. 5. Sample of ARP tables for smart meter and data collector are shown in Fig. 6 and Fig. 7.

Fig. 6 shows the ARP cache of the smart meter during normal traffic, while Fig. 7 also shows the ARP cache of the data collector when there is no attack on the network.

Source MAC	Destination	Dest MAC	Protocol	Length	Info
Vmware_c0:00:01	Broadcast	Broadcast	ARP	60	Who has 192.168.1.0? Tell 192.168.1.2
Raspberr_bc:06:f9	Broadcast	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.13
Raspberr_bc:06:f9	Broadcast	Broadcast	ARP	42	Who has 192.168.1.1? Tell 192.168.1.13
Raspberr_bc:06:27	Broadcast	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.11
Raspberr_a8:be:24	Broadcast	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.12
Vmware_98:1f:74	Raspberr_bc:06:f9	Raspberr_bc:06:f9	ARP	60	Who has 192.168.1.13? Tell 192.168.1.20
Raspberr_bc:06:f9	Vmware_98:1f:74	Vmware_98:1f:74	ARP	42	192.168.1.13 is at dc:a6:32:bc:06:f9
Raspberr_bc:06:27	Broadcast	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.11
Raspberr_c3:7d:10	Broadcast	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.14
Raspberr_a8:be:24	Broadcast	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.12
Raspberr_bc:06:27	Broadcast	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.11
Raspberr_c3:7d:10	Broadcast	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.14
Raspberr_a8:be:24	Broadcast	Broadcast	ARP	60	Who has 192.168.1.1? Tell 192.168.1.12

Fig. 5. ARP Reply Captured by Wireshark during Normal Traffic.

```
pi@raspberrypi:~$ arp -a
? (192.168.1.1) at <incomplete> on eth0
? (192.168.1.11) at dc:a6:32:bc:06:27 [ether] on eth0
? (192.168.1.20) at 00:0c:29:98:1f:74 [ether] on eth0
? (192.168.1.2) at 00:50:56:c0:00:01 [ether] on eth0
```

Fig. 6. ARP Cache on the Smart Meter.

```
dc@ubuntu:~$ arp -a
? (192.168.1.11) at dc:a6:32:bc:06:27 [ether] on ens33
? (192.168.1.14) at dc:a6:32:c3:7d:10 [ether] on ens33
? (192.168.1.12) at dc:a6:32:a8:be:24 [ether] on ens33
? (192.168.1.13) at dc:a6:32:bc:06:f9 [ether] on ens33
```

Fig. 7. ARP Cache on the Data Collector.

Based on the data gathered during the normal operations experiment, no anomalies were detected in Wireshark, ARP cache on the smart meter and ARP cache on the data collector. The data sent from the smart meter has the same value as the data stored in the database.

### B. Under Attack

The smart meter with an IP address of 192.168.1.13 will send data as usual for the attack simulation. However, another Raspberry Pi will be included that will imitate the attacker for this phase. The attacker with IP address 192.168.1.11 and the corresponding MAC address of Raspberry\_bc:06:27 will perform ARP spoofing on the respective smart meter and data collector in the topology. Once the attacker managed to intercept and change the power consumption value, the tampered packet will be forward back to the data collector using IPV4.

By performing ARP spoofing on a legitimate smart meter and data collector, the attacker machine will be the gateway for both of these devices. The attacker can now sniff and perform further attacks as the attacker already has access to data transferred. All communication between the smart meter and data collector now needs to go through the attacker's machine first before reaching the destination.

Packet manipulation script is used to change the value of power consumption. In this experiment, the power consumption is increased by 12 on every reading. The difference is shown in Fig. 8, where the data generated and sent to the data collector is not tally with Fig. 9 which displays that the data accepted by the data collector was not the legitimate data sent by the smart meter. The data in the database has been modified because the data has been intercepted and sent to the data collector by the attacker.

Fig. 10 shows the view of the attacker machine. The data from the smart meter will be intercepted, modified, and then forwarded to the destination. Fig. 10 shows that every data intercepted will be applied increment by 12. For the MITM part, this study successfully perform packet manipulation by using pattern searching tools and some modifications on the iptables to filter only the packet that needs to be modified to come through.

```
[POWER CONSUMPTION] 9576 kWh
[TIMESTAMP] 2020-12-17 18:26:34
MAC00003 - 9576 - 02:26:45 - 2020-12-18
('MAC ID: ', 'MAC00003', '| Power Consumption: ', 9588)

[POWER CONSUMPTION] 2011 kWh
[TIMESTAMP] 2020-12-17 18:26:34
MAC00003 - 2011 - 02:26:55 - 2020-12-18
('MAC ID: ', 'MAC00003', '| Power Consumption: ', 2023)

[POWER CONSUMPTION] 3662 kWh
[TIMESTAMP] 2020-12-17 18:26:34
MAC00003 - 3662 - 02:27:05 - 2020-12-18
('MAC ID: ', 'MAC00003', '| Power Consumption: ', 3674)

[POWER CONSUMPTION] 1883 kWh
[TIMESTAMP] 2020-12-17 18:26:34
MAC00003 - 1883 - 02:27:15 - 2020-12-18
('MAC ID: ', 'MAC00003', '| Power Consumption: ', 1895)
```

Fig. 8. Smart Meter Sending Data during FDIA.

9173	MAC00003	2020-12-18	02:26:45	9588
9174	MAC00003	2020-12-18	02:26:55	2023
9175	MAC00003	2020-12-18	02:27:05	3674
9176	MAC00003	2020-12-18	02:27:15	1895
9177	MAC00003	2020-12-18	02:27:25	4722

Fig. 9. Database Accepted Falsified Data.

```
root@raspberrypi:/home/pi/Desktp# python3 testingfinal.py
[*] waiting for data

Original Data is: 9576
New Data: 9588
Payload sent!

Original Data is: 2011
New Data: 2023
Payload sent!

Original Data is: 3662
New Data: 3674
Payload sent!

Original Data is: 1883
New Data: 1895
Payload sent!

Original Data is: 4710
New Data: 4722
Payload sent!
```

Fig. 10. View on Attacker's Machine during FDIA.

The evidence captured using Wireshark is explained based on Fig. 11. Note on the highlighted line, the attacker sending a broadcast reply telling the data collector that the smart meter's MAC address is now at his MAC address which is Raspberry\_bc:06:27. Also, there are presents of duplicate use in the collected evidence.

Source MAC	Destination	Dest MAC	Protocol	Length	Info
Raspberr_c3:7d:10	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.14
Raspberr_a8:be:24	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.12
Vhware_c0:00:01	Broadcast	Broadcast	ARP	60	who has 172.17.88.1? Tell 192.168.1.2
Raspberr_bc:06:27	Vhware_98:1f:74	Vhware_98:1f:74	ARP	60	192.168.1.13 is at dc:a6:32:bc:06:27 (0)
Raspberr_bc:06:27	Raspberr_bc:06:f9	Raspberr_bc:06:f9	ARP	60	192.168.1.20 is at dc:a6:32:bc:06:27 (0)
Raspberr_bc:06:27	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.11
Raspberr_c3:7d:10	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.14
Raspberr_a8:be:24	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.12
Raspberr_c3:7d:10	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.14
Raspberr_bc:06:27	Vhware_98:1f:74	Vhware_98:1f:74	ARP	60	192.168.1.13 is at dc:a6:32:bc:06:27 (0)
Raspberr_bc:06:27	Raspberr_bc:06:f9	Raspberr_bc:06:f9	ARP	60	192.168.1.20 is at dc:a6:32:bc:06:27 (0)
Raspberr_a8:be:24	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.12
Raspberr_bc:06:27	Vhware_98:1f:74	Vhware_98:1f:74	ARP	60	192.168.1.13 is at dc:a6:32:bc:06:27 (0)
Raspberr_bc:06:27	Raspberr_bc:06:f9	Raspberr_bc:06:f9	ARP	60	192.168.1.20 is at dc:a6:32:bc:06:27 (0)
Raspberr_a8:be:24	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.12
Raspberr_a8:be:24	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.12
Raspberr_bc:06:27	Vhware_98:1f:74	Vhware_98:1f:74	ARP	60	192.168.1.13 is at dc:a6:32:bc:06:27 (0)
Raspberr_bc:06:27	Raspberr_bc:06:f9	Raspberr_bc:06:f9	ARP	60	192.168.1.20 is at dc:a6:32:bc:06:27 (0)
Raspberr_bc:06:27	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.11
Raspberr_bc:06:27	Vhware_98:1f:74	Vhware_98:1f:74	ARP	60	192.168.1.13 is at dc:a6:32:bc:06:27 (0)
Raspberr_bc:06:27	Raspberr_bc:06:f9	Raspberr_bc:06:f9	ARP	60	192.168.1.20 is at dc:a6:32:bc:06:27 (0)
Raspberr_bc:06:27	Broadcast	Broadcast	ARP	60	who has 192.168.1.1? Tell 192.168.1.11

Fig. 11. ARP Traffic Captured by Wireshark during under Attack.

Fig. 12 and Fig. 13 show the difference in ARP cache when there is no attack and under attack. During the attack, it is shown that there are two IP addresses with the MAC addresses. Supposedly, the MAC address for 192.168.1.13 was Raspberry\_bc:06:f9 but after ARP spoofing, the attacker managed to link the victim's IP address to his MAC address.

```
pi@raspberrypi:~$ arp -a
? (192.168.1.1) at <incomplete> on eth0
? (192.168.1.11) at dc:a6:32:bc:06:27 [ether] on eth0
? (192.168.1.20) at 00:0c:29:98:1f:74 [ether] on eth0
? (192.168.1.2) at 00:50:56:c0:00:01 [ether] on eth0
```

Fig. 12. ARP Cache on the Smart Meter.

```
dc@ubuntu:~$ arp -a
? (192.168.1.11) at dc:a6:32:bc:06:27 [ether] on ens33
? (192.168.1.14) at dc:a6:32:c3:7d:10 [ether] on ens33
? (192.168.1.12) at dc:a6:32:a8:be:24 [ether] on ens33
? (192.168.1.13) at dc:a6:32:bc:06:27 [ether] on ens33
```

Fig. 13. ARP Cache on the Data Collector.

Based on the data gathered during the under attack experiment, anomalies were detected in Wireshark, ARP cache on the smart meter, and ARP cache on the data collector. The data sent from the smart meter has a different value from the data stored in the database as it was changed by the attacker.

### C. Forensic Analysis

In this section, the PCAP file that stored all the digital evidence was extracted and analyzed. The analysis and comparison of the collected evidence in this study are used for in-depth analysis. Fig. 14 shows the steps taken during the forensic analysis.

The analysis process begins by collecting packets captured using Wireshark from the client during normal traffic and during under attack. The packets are also collected from the data collector during normal traffic and during the network under attack. The records from the normal traffic phase will be used as a benchmark for comparative analysis to investigate the FDIA in AMI.

Fig. 15 shows that Wireshark captured another MAC address (bc:06:27). In addition, Fig. 16 shows the use of duplicate IP addresses was reported. This strengthens the evidence collected, as shown in Fig. 12 and Fig. 13. It could be observed that the IP address 192.168.137.13, which was earlier known to be the IP address of the smart meter, now has

two MAC bindings: Raspberr\_bc:06:f9 (initial MAC address), and Raspberry\_bc:06:27 (owned by the attacker machine in the network), which was the outcome of ARP poisoning/spoofing.

Fig. 16 shows that the time to live (TTL) of the packet from the client was 64 (left), and it was still 64 when it reached the data collector (right). This is normal as there is no router involved in this topology. However, Fig. 17 shows that TTL is different when the data was sent from the smart meter (left) and when it was accepted at the data collector (right) during the network was under attack.

As shown in Fig. 17, when the data was sent out from the smart meter (left), the TTL was 64 but when it reached the database, the TTL of the packet was 63, indicate that the packet had travel somewhere else before reached the data collector. The normal topology is assumed that the smart meter should directly deliver data to the data collector with a switch and not include a router, so it should not modify the TTL of the packet. This happens because the attacker intercepted the packet and modified the packet's data before forwarding it to the real destination.

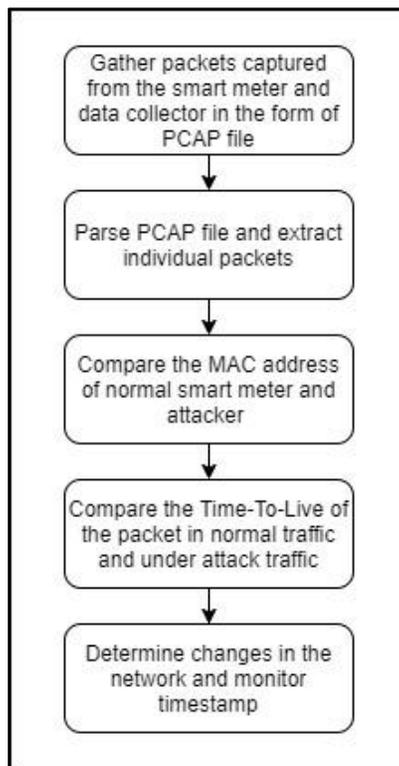


Fig. 14. Forensic Analysis Flow Chart

```
Wireshark - Packet 371 - underattackDB18_12.pcap
Address Resolution Protocol (request)
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0000)
  Hardware size: 6
  Protocol size: 4
  Opcode: request (1)
  Sender MAC address: Raspberr_bc:06:f9 (dc:a6:32:bc:06:f9)
  Sender IP address: 192.168.1.13
  Target MAC address: 00:00:00:00:00:00 (00:00:00:00:00:00)
  Target IP address: 192.168.1.1
  Duplicate IP address detected for 192.168.1.13 (dc:a6:32:bc:06:f9) - also in use by dc:a6:32:bc:06:27 (frame 366)
    [Frame showing earlier use of IP address: 366]
    [Expert Info (Warning/Sequence): Duplicate IP address configured (192.168.1.13)]
    [Duplicate IP address configured (192.168.1.13)]
    [Severity level: Warning]
    [Group: Sequence]
    [Seconds since earlier frame seen: 1]
```

Fig. 15. Use of Duplicate IP Address in MAC-IP Address Binding.

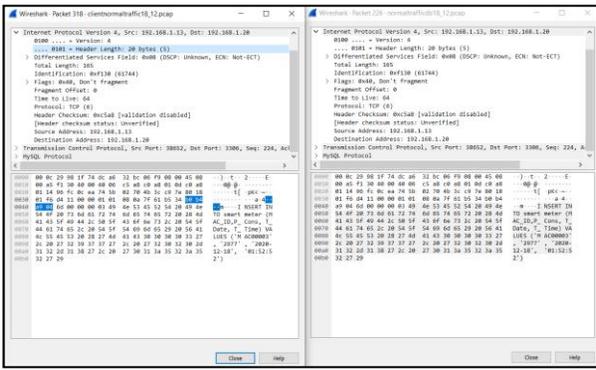


Fig. 16. TTL of the Packet during Normal Traffic from the Smart Meter (Left) and the Data Collector (Right).

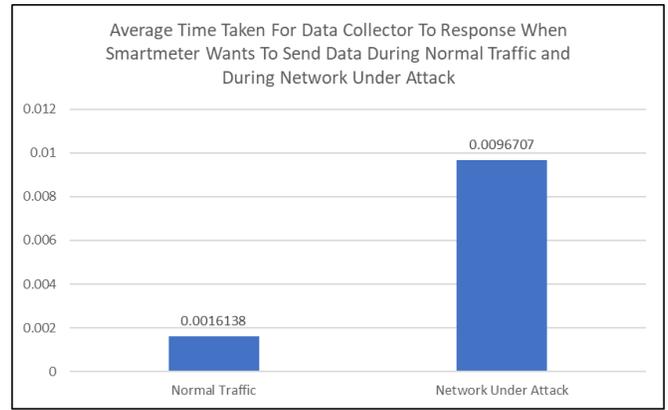


Fig. 19. The Average Data Collector Response Time.

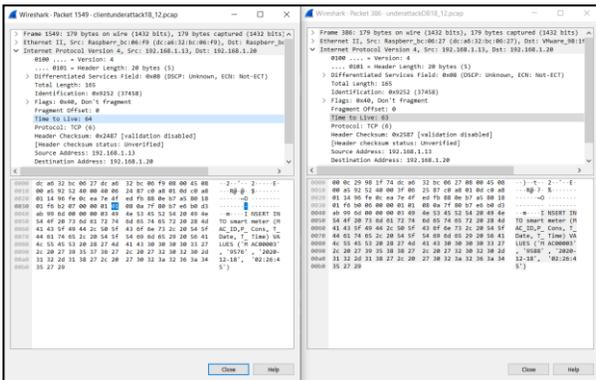


Fig. 17. TTL of the Packet during under Attack from the Smart Meter (Left) and the Data Collector (Right).

TABLE I shows a list of attributes that forensic investigators can use as references on what attributes of data to be collected to perform forensic analysis in tracing FDIA. The list can be used as a reference for forensic investigators to perform evidence collection during FDIA investigations.

TABLE I. TABLE OF ATTRIBUTES

Attributes	Description
SrcIp	Source IP address
SrcPort	Source port address
DstIp	Destination IP address
DstPort	Destination port address
SrcMac	Source MAC address
DstMac	Destination MAC address
TTL	Time to live of the packets
ARPreq	ARP request traffic
ARPRep	ARP reply traffic
TimeDelay	Time delay for the client to receive a reply from the server

As displayed in Fig. 18, the time taken for the data collector to respond to the smart meter when the smart meter wants to send data is much lower than when under attack. Fig. 19 shows the average time taken by the data collector to respond when the smart meter wants to send data. This shows a huge gap of time taken for the data collector to reply during normal traffic, and the network was under attack. It can be concluded that the delay that occurred during the network was under attack is caused by the path and process that happened on the data to reach the destination. The data went through a longer path and was processed by the attacker first before the data was forwarded back to the destination.

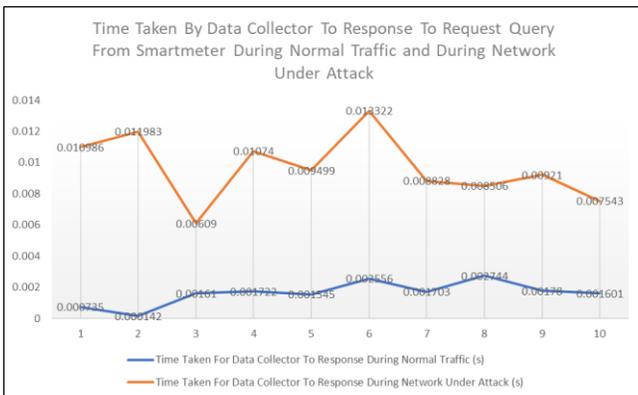


Fig. 18. Comparison of the Time Taken for the Data Collector to Respond to the Request Query from the Smart Meter during Normal Traffic and under Attack.

## V. CONCLUSION

This study's primary motivation was to study FDIA impact in the IoT environment and perform forensics analysis on digital traces from data obtained. Based on the data obtained from the experiments, the proposed list of attributes for forensic analysis could be useful to trace FDIA. In future works, there is a need to explore different types of attacks, such as buffer overflow payloads that may result in a system crash, creating a path for the hackers to initiate their malicious actions. Future studies may also focus on the integration of forensic-by-design principles in the design of any critical system because it will be quite difficult to know what has happened if there is no log or no proof. If the system is able to produce a series of events, it would be very helpful for the

forensic investigator to reconstruct the events in order to identify available sources and different types of potential evidence in such cases. Therefore, another potential study could explore how to integrate forensic-by-design principles in the design of such systems.

#### ACKNOWLEDGMENT

This study was funded by Tenaga Nasional Berhad Seed Fund (U-TD-RD-19-24) in collaboration with TNB Asset Management Department. This research team would like to thank UNITEN R&D Sdn. Bhd. for fund management.

#### REFERENCES

- [1] P. Brous, M. Janssen, and P. Herder, "The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations," *Int. J. Inf. Manage.*, vol. 51, no. May 2019, p. 101952, 2020, doi: 10.1016/j.ijinfomgt.2019.05.008.
- [2] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus. Horiz.*, vol. 58, no. 4, pp. 431–440, 2015, doi: 10.1016/j.bushor.2015.03.008.
- [3] P. Alto, "Impacts of Cyberattacks on IoT Devices," *Impacts Cyberattacks IoT Devices*, 2019.
- [4] S. Sharma, M. Manuja, and K. Kishore, "Vulnerabilities, attacks and their mitigation: An implementation on internet of things (IoT)," *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 10, pp. 146–150, 2019, doi: 10.35940/ijitee.F3761.0881019.
- [5] M. Kuzlu, C. Fair, and O. Guler, "Role of Artificial Intelligence in the Internet of Things (IoT) cybersecurity," *Discov. Internet Things*, vol. 1, no. 1, 2021, doi: 10.1007/s43926-020-00001-4.
- [6] W. A. Dimitrov and G. S. Panayotova, "The impacts of dns protocol security weaknesses," *J. Commun.*, vol. 15, no. 10, pp. 722–728, 2020, doi: 10.12720/jcm.15.10.722-728.
- [7] M. Ahmed and A. S. K. Pathan, "False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure," *Complex Adapt. Syst. Model.*, vol. 8, no. 1, 2020, doi: 10.1186/s40294-020-00070-w.
- [8] D. B. Rawat and C. Bajracharya, "Detection of false data injection attacks in smart grid communication systems," *IEEE Signal Process. Lett.*, vol. 22, no. 10, pp. 1652–1656, 2015, doi: 10.1109/LSP.2015.2421935.
- [9] D. Allison, P. Smith, K. Mclaughlin, F. Zhang, J. Coble, and R. Busquim, "PLC-Based Cyber-Attack Detection: A Last Line of Defence," *Int. Conf. Nucl. Secur. Sustain. Strength. Efforts*, pp. 1–10, 2020.
- [10] S. Bhattacharjee, A. Thakur, S. Silvestri, and S. K. Das, "Statistical security incident forensics against data falsification in smart grid advanced metering infrastructure," *CODASPY 2017 - Proc. 7th ACM Conf. Data Appl. Secur. Priv.*, pp. 35–45, 2017, doi: 10.1145/3029806.3029833.
- [11] O. Abu Waraga, "Design and Implementation of an Automated IoT security testbed." 2019.
- [12] V. Sachidananda, J. Toh, S. Siboni, S. Bhairav, A. Shabtai, and Y. Elovici, "Let the cat out of the bag: A holistic approach towards security analysis of the internet of things," *IoTPTS 2017 - Proc. 3rd ACM Int. Work. IoT Privacy, Trust. Secur. co-located with ASIA CCS 2017*, pp. 3–10, 2017, doi: 10.1145/3055245.3055251.
- [13] M. L. Hale, K. Lotfy, R. F. Gamble, C. Walter, and J. Lin, "Developing a platform to evaluate and assess the security of wearable devices," *Digit. Commun. Networks*, vol. 5, no. 3, pp. 147–159, 2019, doi: 10.1016/j.dcan.2018.10.009.

# Design of Decentralized Application for Telemedicine Image Record System with Smart Contract on Ethereum

Darrell Yonathan<sup>1</sup>, Diyanatul Husna<sup>2</sup>, Fransiskus  
Astha Ekadiyanto<sup>3</sup>, Anak Agung Putri Ratna<sup>10</sup>  
Computer Engineering Department of Electrical  
Engineering, University of Indonesia, Depok, Indonesia

I Ketut Eddy Purnama<sup>4</sup>, Mauridhi Hery Purnomo<sup>6</sup>,  
Supeno Mardi Susiki Nugroho<sup>7</sup>, Reza Fuad Rachmadi<sup>8</sup>  
Faculty of Engineering Department of Computer  
Engineering, Sepuluh November Institute of Technology  
Surabaya, Indonesia

Afif Nurul Hidayati<sup>5</sup>  
Faculty of Medicine Department of Dermatology and  
Venereology, Airlangga University  
Surabaya, Indonesia

Ingrid Nurtanio<sup>9</sup>  
Faculty of Engineering Department of Informatics  
Hassanudin University  
Makassar, Indonesia

**Abstract**—This paper discusses the implementation of smart contracts on the Ethereum blockchain system for telemedicine data storage. Telemedicine is one of the currently developing digital technologies in the health and medical sectors. Telemedicine can be more efficient when seeking treatment because patients do not need to see a doctor face to face. When using blockchain technology, the stored data becomes more transparent for each node in the blockchain network but has verification on every transaction which takes time and gas costs. However, telemedicine has several risks and problems, one of which is long data storage process time because there must be a verification process first to ensure data security. Another problem faced is the issue of the gas fee of the blockchain telemedicine system which is billed in every data storage transaction. In this study, a blockchain system was introduced for managing and securing databases on telemedicine. The implementation of this blockchain system was carried out on a website page that can add data to and retrieve data from the blockchain system. The results of this study showed that blockchain was successfully implemented to store telemedicine data with Ethereum. The analysis in this paper refers to the set and gets functions. The set function is used to send data to the blockchain, and the get function is used to retrieve data from the blockchain. From testing, the Get function has a much faster execution time than the Set function because the Get function does not require verification to retrieve its data. In the iterations carried out—namely 1, 10, and 100—the longest time on average was at 100 iterations when compared to the other iterations. In the tests carried out, the more characters that were stored, the more gas costs must be paid. In the tests, the percentage increase in costs was 0.34% per character.

**Keywords**—Blockchain; Ethereum; smart contract; telemedicine

## I. INTRODUCTION

Health is one of the most important components in life. By being healthy, one's productivity will be good and one can work optimally. The health of a person can be more easily

analyzed using data. However, a person's health information is confidential. One example of confidential medical information is an image of a medical record from a hospital. For that, we need a system mechanism to protect confidential data or information because this confidential information should not be known to just anyone. Blockchain technology can protect confidential information [1].

The blockchain system will make data storage decentralized. In general, information data are stored in a server such that the data are in one place only. This makes information or data on the server easy to hack because the data are centralized. Therefore, blockchain technology is reliable because this system decentralizes information data [1]. Thus, the use of blockchain is not managed centrally but is instead managed by each user in the network.

Blockchain has several frameworks that can be implemented, such as Hyperledger Fabric and Ethereum. These two types of blockchain have different functionalities. The difference seen is in the type of consensus. This consensus is built to build user trust in the blockchain network. A certain algorithm will be created for approval on all nodes in the network. All approved algorithms are code-based. Consensus has several types, such as Proof of Work (PoW), Proof of Authority (PoA), and Proof of Stake (PoS) [2]. Ethereum is a decentralized blockchain system. Ethereum is open source so that anyone can use it. On the Ethereum platform, the cryptocurrency unit used is Ether (ETH).

Smart contracts on Ethereum can manage transactions from every node on the blockchain network [1]. This managed transaction will become a record that will be propagated to all nodes. In telemedicine, patient data collected by the telemedicine center are a node because of the party who has the disease data or complaints at the time of treatment. The data from these patients will be decentralized with the blockchain network so that the data are much more secure and are in hashed form.

An image data management system for telemedicine transactions was developed by implementing blockchain technology to create transparency in the transaction. This transparency can improve the data integrity of telemedicine transactions through a decentralized system so that transaction activities in telemedicine can gain the trust of consumers. In the system created, image data on patients can be uploaded to the blockchain network, and medical parties can see these data in the network [1]. This makes the data much more secure because in the blockchain network there is a separate authentication and verification process. Image data can be accessed on nodes that have been confirmed and registered as valid. Therefore, the researcher designed a medical image recording application with blockchain using Ethereum.

There are various frameworks on the blockchain that can be used to develop a system, such as Hyperledger and Ethereum. The Hyperledger framework is described in the paper "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains" [3]. From paper "Design and Implementation of Storage System for Real-time Blockchain Network Monitoring System" This paper describes how to monitor the blockchain network using an apache engine that analyzes the block size of each block on the blockchain [4]. For data management, the paper "Analysis of Data Management in Blockchain-based Systems" describes how data management can be implemented on a blockchain network and the quality of the data [5]. The implementation of Blockchain technology using Ethereum in healthcare has been described in the paper "Decentralized Telemedicine Framework for a Smart Healthcare Ecosystem" but in this paper there is no data other than String data that can be stored (images that are converted to other forms also do not exist) [1]. The healthcare flow mechanism that uses Blockchain is discussed in the paper "A Blockchain-Based Smart Contract System for Healthcare Management", the analysis of the costs required for the analysis of each parameter is mentioned in the paper [6]. To develop a user interface for interaction with users the paper "The Implementation of Blockchain in Banking System using Ethereum" discusses using react.js with development using Ethereum [7].

The purpose of this research was to design and develop a blockchain system for use in telemedicine image data storage. A smart contract function on Ethereum was designed to send and retrieve telemedicine image data to and from the blockchain network. The flow of data on the implemented blockchain system in telemedicine was examined, and the performance of this blockchain system was analyzed. In this study, the implementation is limited to analyzing the system from the blockchain only. For the telemedicine process, this research only implements uploading and downloading images through a simple website page. So the analysis used is to analyze the upload time, download images, and analyze the cost of each transaction.

## II. BASIC CONCEPT OF TELEMEDICINE SYSTEM USING SMART CONTRACT ETHEREUM

### A. Blockchain

Blockchain is a digital data storage system that contains data and records that are connected to a cryptographic system

[8]. Currently, the best-known blockchain technology is cryptocurrency transactions, one of which is Bitcoin. Blockchain technology takes the form of recording digital transactions that exist on many servers.

Blockchain has many sets of blocks that contain information. Each of these blocks will have a hash component. This hash is the character set that composes the information in the block. The character hash is entered sequentially for each piece of new information. Thus, the information from each block from blockchain will continue to add the new hash value to be recorded so that all data are not lost.

Each block on the blockchain will form a blockchain network. Any data will be replicated to all networks. Every computer that exists and is connected to this network will execute the program at the same time. Therefore, blockchain is arguably a computer on a large scale formed from communication between several computers. If it is implemented in a database, then blockchain makes the database a decentralized system.

Blockchain has characteristics that can benefit some systems, including a chain-like structure that stores and updates a chain of transaction data. Each block will store transaction data through one consensus rule to validate. Other characteristics of the blockchain system include:

- **Decentralization:** The main advantage of blockchain systems is the decentralization of data. As data centralization has many vulnerabilities, blockchain can be a solution. The consensus mechanism will validate the transaction. The decentralization of data on the blockchain will make the data in the network well verified so that security is much better than that in centralized data.
- **Transparency:** The blockchain network is data decentralized such that every node on the network can see the transactions. The principle of the blockchain network will also record every transaction and distribute it to all nodes on the blockchain network. Private and public keys in blockchain can also help data security such that even though they are transparent, blockchain still maintains data security.

Blockchain technology can be implemented in several ways in the expected conditions. There are three types of blockchain:

- **Public Blockchain:** A public blockchain is a blockchain that anyone can access and use. Public blockchains are not controlled by any individual or organization. The ledger on the blockchain is open and transparent. However, there are drawbacks to public blockchains, namely high operating and maintenance costs, and slow transaction speeds. Examples of its use are in Bitcoin, Ethereum, and Hyperledger.
- **Private Blockchain or Permissioned Blockchain:** Private blockchains are formed to facilitate the private exchange of data among a group of individuals or organizations. Unknown users cannot access this blockchain network without a special invitation. An example of its use is on the R3 Corda.

- **Blockchain Consortium:** The blockchain consortium is a combination of public and private blockchains where there is no single organization that is responsible for controlling the network; instead, the network is controlled by several predetermined nodes. These nodes can decide who can be part of the network and who can be miners. For block validation, a multi-signature scheme is used in which a block is considered valid only if it is signed by some of these nodes. An example of its use is on Fabric.

A consensus algorithm is an algorithm used to validate the data. The algorithm have hash value for each block that has been formed in the blockchain. This hash value can be formed by converting inputs, reference hashes, and random numbers using the SHA-256 hash algorithm, which produces a hash value with a certain pattern [9]. However, on Ethereum, the hash used in general is Keccak-256. This hash is used on Ethereum addresses derived from public keys or contracts. Ethereum addresses are hexadecimal numbers, with the identifier derived from the last 20 bytes of the Keccak-256 hash of the public key. Unlike Bitcoin addresses, which are coded in the client's user interface or displayed to include a built-in checksum to protect against typos, Ethereum addresses are written as raw hexadecimal without any checksums.

The PoW mining process is carried out with dependence on computing power; while in PoS, the validation capacity depends on the stakes on the network. Prizes in the form of cryptographic money are given to miners when they can solve cryptographic puzzles on PoW and transaction fees on PoS. Attacks that may occur in each consensus are also different. In PoW, it takes a large computation about 51% larger than the existing blockchain network. On the other hand, PoS can be attacked if 51% of cryptocurrencies are already in the hands of hackers, but this is impossible.

Another consensus that can be used is the Proof-of-Authority (PoA) consensus. The PoA usually used in the Ethereum private network. This consensus has good performance as well [10]. The PoA consensus have different system because everyone can be a node in blockchain network. As such, it is different from the type of blockchain that uses permissions on each node. The PoA consensus is used in test networks, one of which is Rinkeby, which can be used to develop a system.

In PoA, to generate a new block is granted to a node that has proven its authority operate. Such nodes are referred to as "Validators," and they run software that allows them to place transactions in blocks. The process is automated and does not require validators to continuously monitor their computers but require good computer maintenance. PoA is suitable for both private and public networks.

There are several advantages to using PoA. It has a fairly large risk tolerance, the block creation time is predictable, and it can be used more sustainably because it does not require large computations such as PoW. But, on the other hand, PoA has a drawback, namely that the validator can be seen so that there can be manipulation from third parties.

## B. Telemedicine

Telemedicine is an information technology-based health service that allows patients to consult with doctors or other health experts without having to meet [11]. This innovation in health services with the internet can help patients use their time more efficiently because they do not have to come to a hospital or health facility for a consultation. During the remote consultation, the doctor helps the patient to get information regarding the suspected diagnosis, treatment, or first treatment for illness or injury, as well as tips to improve body health.

However, telemedicine also has a limitation in that doctors cannot detect where the patient is sick. This makes the diagnosis less accurate [12]. But if it is developed further, then telemedicine can be a breakthrough. Doctors and patients alike will be able to rest more and maintain health. Some implementations of telemedicine are being developed, one of which is the detection of skin diseases through images and disease consultations through doctors. This innovation in health services with the internet can help patients use their time more efficiently because they do not have to come to a hospital or health facility for a consultation. During the remote consultation, the doctor helps the patient to get information regarding the suspected diagnosis, treatment, or first treatment for illness or injury, as well as tips to improve body health.

Telemedicine has various types, three of which are as follows [13]:

- **Real-time Interactive Medicine:** This type allows communication between patients and doctors in realtime when there is a complaint from the patient.
- **Store and Forward:** This type allows owners of patient data to share their data with other practitioners.
- **Remote Patient Monitoring:** This type allows a medical professional to monitor patients remotely using a mobile medical device to collect data, such as blood pressure and blood sugar levels.

The use of blockchain in telemedicine has many benefits. It was mentioned in another paper that there are 6 properties of blockchain that can be useful in implementing telemedicine[14]. The first is its decentralized nature which allows data records to be accessible and managed in multiple locations. Then there is the immutability nature of the blockchain which makes patient data records cannot be changed once the data has been entered into the blockchain system, then there is asymmetric key cryptography that supports immutability. Next is data transparency which makes data exchange always traceable. Furthermore, there is also an important feature, which is open source so that patients can see the doctor's profile first. The nature of auditability and anonymity is also important to trace and hide the identity of user data.

The implementation of a simple application for telemedicine interaction using blockchain can also be applied to remote monitoring. For the selected storage, using several tools such as Filecoin, Storj.io, Napster, and IPFS [14]. The storage is usually intended to store documents that have a large enough size such as images or videos. In this section,

blockchain will play an important role in every data storage process that will be connected to the main system, users, and doctors.

### C. Ethereum

Ethereum is an open-source blockchain platform [15]. Ethereum uses PoS as its consensus algorithm, but several test networks use PoA as well. To run transactions, Ethereum uses smart contracts with the Solidity programming language. The type of cryptocurrency used in Ethereum is ether (ETH).

Solidity is a high-level programming language that is better known as being contract-based. The syntax of this programming language is similar to the Javascript programming language. This programming language is used to improve the performance of virtual machines on Ethereum. Solidity is a scripting language that is statically created for verification and compile-time constraints. In addition to the time of compilation, this programming language will also help check at runtime. The Solidity programming language also supports object-oriented programming, such as object inheritance.

Solidity is a programming language created specifically for smart contracts on Ethereum [16]. Solidity is written in the .sol storage format. Solidity is not an executable language on a blockchain virtual machine but rather a language that aims to make it easier for developers to create smart contracts. When compiling or deploying smart contracts, a Solidity Compiler is needed. Through the Solidity Compiler, the smart contract is compiled into bytecode, which is then executed by the virtual machine.

In the Solidity programming language, several data types can be used, namely strings, integers, and Booleans, and others. Strings are generally a variable from a set of characters. Integers are used for data types in the form of positive or negative numbers. Boolean is a data type with a Boolean variable (true or false). Solidity includes new resources or new languages so that the code documentation of this programming language is not too excessive.

A smart contract is a script that is stored in a blockchain system. This smart contract has a unique address and consists of executable functions and state variables [17]. The user launches the smart contract by addressing the transaction to the contract. Once launched, the code of the smart contract cannot be changed.

The workings of this smart contract correspond to the basic function of Ethereum. Because Ethereum will work based on the exchange of information on an account owned by its users, when a smart contract is created, there must be an identification for each actor entity involved in the network. Then, in the existing smart contract, certain functions are added according to the design. This function will manage the exchange of information on the existing blockchain network.

To execute this smart contract, a function is triggered. This function depends on the code used along with the programming logic that has been made previously. There are two types of accounts in Ethereum; the first is Externally Owned Accounts (EOA) and the second is contract accounts [17]. EOA is

controlled by the private key assigned to the user and the public address used to send and receive ETH from other accounts and send transactions to smart contracts. The contract account, on the other hand, does not have a private key and can only be activated by EOA. The contract account is where the smart contract resides in Ethereum.

Smart contracts are written in the Solidity programming language, which is a high-level programming language [18]. Users use EOA to make transactions on a contract account. This account is encrypted with a private key to be able to send transactions to other nodes. After that, other users verify the integrity of the transaction. This happens until a consensus is reached that has been agreed upon previously. The transaction will then be added to the block and will be recorded. The status of the network will also be updated as the smart contract has been successfully executed. The presence of this smart contract allows developers to send transactions with specific data and can check transactions between servers and inputs entered [19]. The checks performed are almost the same as the checks performed on the database. However, the specific difference is that there is an address for each data stored in the blockchain network.

In implementing the blockchain system for telemedicine, the Ethereum framework is used. Ethereum is a cryptocurrency-based blockchain like Bitcoin and is based on a public network, but it can also be used to implement a permissioned blockchain. Like Bitcoin, Ethereum also implements the PoW protocol [20]. In this implementation, a blockchain network is used which is a test network and coins from fees for each transaction that are executed can be obtained from a faucet on a website. So for every transaction that will be executed, a fee will be obtained from a faucet. Because it uses a test network, the consensus of the blockchain will change to Proof of Authority (PoA). The most important feature of Ethereum is that it supports the execution of a smart contract, which allows decentralized applications to build on top of it [20]. This is one of the considerations for choosing a framework. With the smart contract, the data that will be stored in the blockchain can be structured. So the implementation is generally not too different from the database implementation. When compared to other frameworks such as bitcoin, Ethereum has advantages such as private transactions and has higher transactions per second. When compared to Hyperledger Fabric, Ethereum has limitations, one of which is that it has a smaller throughput compared to other papers [20]. From the implementation using Ethereum, it can be investigated whether Ethereum can still be implemented to store image data with low transaction throughput.

### D. Node.js

Node.js is an open-source, cross-platform platform for developing server- and network-side applications [21]. Node.js applications are written in JavaScript and can be run in the Node.js runtime on OS X, Microsoft Windows, and Linux.

Node.js is a platform built on top of the Chrome JavaScript runtime to easily build fast and scalable network applications. Node.js uses an event-driven and non-blocking I/O model that makes it lightweight and efficient. The use of this platform is

suitable for data-intensive real-time applications running across distributed devices.

The features of Node.js are as follows:

- It is asynchronous; all API libraries in Node.js are asynchronous, which means that Node.js-based servers never wait for the API to return data.
- The speed is good; the execution speed is quite fast because it uses the Google Chrome V8 JavaScript Engine.
- It is a single thread but still scalable; Node.js uses a single-threaded program, and the same program can provide services to a much larger number of requests than traditional servers like the Apache HTTP Server.

In Node.js there is Web3, which is a collection of JavaScript Libraries (GNU Lesser General Public License version 3) that possess functionality for interacting with the Ethereum ecosystem. Web3 is built by the Ethereum Foundation and includes functionality to communicate with Ethereum nodes via Object Notation - Remote Procedure Call (JSON-RPC). Web3 allows users to interact with other Ethereum nodes using the HTTP, IPC, or WebSocket protocols [21]. Communication involves reading and writing data from the blockchain via smart contracts. Web3 providers can be set up on the frontend and backend to send transactions and listen for events happening on the blockchain network. With this, Node.js can be used because it has a library.

### III. TELEMEDICINE SYSTEM DESIGN USING BLOCKCHAIN

In this study, the design of a blockchain model for a telemedicine system used hardware and software with the following specifications. The hardware specifications used in this study are as follows:

- Manufacturer
- Asus ROG GL553VD
- Processor
- Intel® Core™ i7-7700HQ
- Graphics adapter
- NVIDIA GeForce GTX 1050 (Laptop) - 4096 MB; Core: 1354 MHz; Memory: 7000 MHz, NVIDIA GeForce GTX 1050 21.21.13.7654, Optimus
- Memory
- 16384 MB, DDR4-2400
- Storage
- Travelstar 7K1000 HGST HTS721010A9E630, 1000 GB, 7200 rpm, 1 TB HDD, 7200 RPM, 930 GB free
- Operating System
- Windows 10 (64-bit)

The following software specifications were used in this study:

- Node.js : version 14.15.4
- Solidity : version 0.4.25 - 0.7.0
- Metamask : version 9.5.4
- Truffle : version 5.3.1
- Git : version 2.24.1.windows.2
- NPM : version 6.14.10
- Solidity compiler : version 0.6.12

#### A. System Design

Smart contracts on Ethereum can be leveraged to ensure the integrity of transactions from patient care to the doctors involved. This can reduce the risk of scattered data and increase the scalability and transparency of a transaction. More specifically, this smart contract permits participating entities, especially doctors, to monitor and track all transactions on the network. In this way, both doctors and patients can feel more secure because their personal health data details are stored securely.

The blockchain technology design implemented in this telemedicine system has the advantage of being immutable. This makes the data that has been stored on the blockchain immutable as well, i.e., the data can no longer be changed. This feature can support data security from telemedicine data in the form of images represented as hash values. Access to stored data is also secured by smart contracts so that only interested parties can access the data.

The system applied in this study used a simple web page to upload the required medical images. There are two entities, namely doctors and specialists. Doctors upload images that are analyzed by specialists. The implementation is done using Node.js to run Web3, a metamask for the wallet system on transaction fees, and Infura.io to run smart contracts.

To ensure secure telemedicine and blockchain-based healthcare data transactions, in this scenario, the researcher designed a framework for patients to provide data to doctors for analysis. This agreement was carried out at the telemedicine center by approving health care data with the health organization as shown in Fig. 1. After that, the patient made an appointment with a doctor for consultation, after which the doctor gave a consultation and medication, and then updated the patient's data. The hash value was stored as a transaction when the patient was consulted. The physician could then provide access to the patient's health care data to medical research organizations to conduct trials and clinical trials. After providing a diagnosis according to the patient's illness, the data were sent back to the puskesmas through the same process, after which the puskesmas sent the data to the telemedicine center.

The problem faced today in a telemedicine system is the use of a database system that uses one server. The idea of this paper is to improve data security using a storage system on a blockchain network. But, the difference in the network used for data storage can make a difference in the speed of data storage. In this paper, we discuss how the speed of data storage to the blockchain network is discussed. A variation of the

implemented implementation is the amount of data sent to the blockchain (String). This paper involves image data that has been converted into a hash because it has a more efficient value compared to uploading the full image to the blockchain system, and the blockchain system also has a limitation on the size of the uploaded file to produce data in the form of a String which is sent to save gas usage on Ethereum.

In the sequence diagram in Fig. 2, we can see the sequence of the blockchain system for telemedicine. First, the doctor uploads pictures to send information. If the patient agrees, then the treatment process is complete. After that, the central telemedicine system in the form of a website sends image data to the blockchain system in the form of a hash value of the IPFS value. Next, the specialist who analyzes the image data continues to the center so that the hash can be known, and the image can be retrieved for analysis.

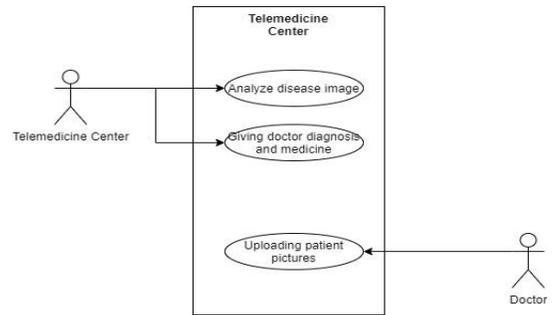


Fig. 3. Use Case Diagram for Blockchain Implementation.

In the use case diagram in Fig. 3, the telemedicine center analyzes the existing images and also provides a diagnosis of the disease from which the patient may be suffering. Meanwhile, the doctor only uploads pictures of the patient, which are then analyzed by specialist doctors at the telemedicine center.

**B. System Design**

The implementation scenario on this system was programmed in the Solidity programming language with web browser-based Remix. Entities participating in the framework were identified using their Ethereum addresses within the blockchain network. Communication between entities was possible by calling functions in smart contracts. Doctors uploaded notes in the form of images in an entity that recorded all patient care documents stored in smart contracts. Consequently, there was a flow-on of each doctor entity until the data were stored in the blockchain network using smart contracts. These stored data were in the form of a hash value generated by the IPFS system.

In Fig. 4, the implementation of scenarios that can be combined into steps can be seen.

- The doctor opens a website to upload patient data.
- Image data are telemedicine data that have been encrypted using Frenzel's thesis.
- The smart contract contains input data in the form of ID, name, description, and IPFS hash, which is generated when the image is uploaded to the IPFS system.
- The state contract is idle until there is a transaction.
- The state contract is ready to be submitted after a transaction occurs at the telemedicine center in the form of parameters set by the smart contract in the form of strings and image uploads that are converted into hash values.
- After being successfully verified, the ID appears automatically through an alert.
- Image (IPFS hash) and data are entered into the blockchain database using IPFS and smart contracts.
- To retrieve the data, the ID is needed. This Get process returns the value of the parameter that was sent previously on the blockchain network.

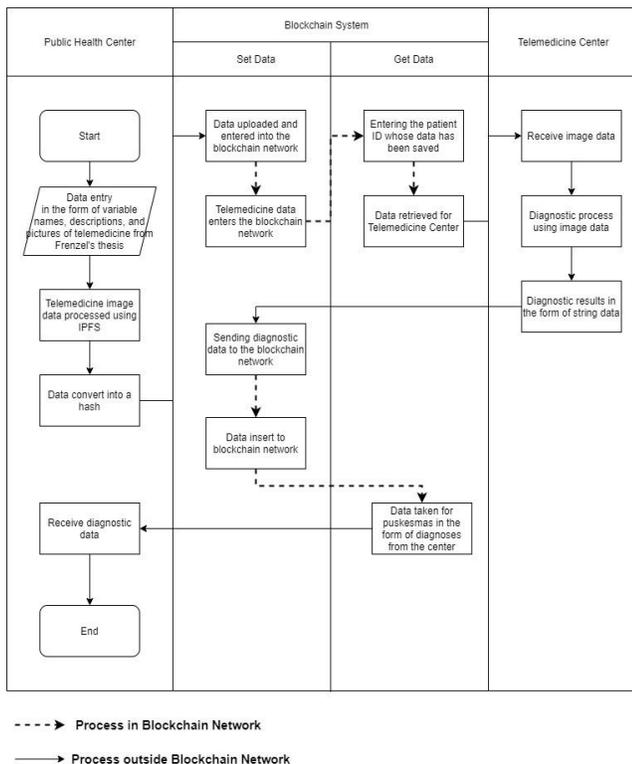


Fig. 1. Activity Diagram for Blockchain Implementation.

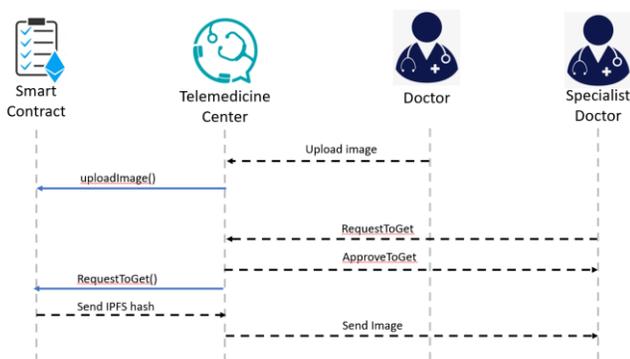


Fig. 2. Sequence Diagram for Blockchain Implementation.

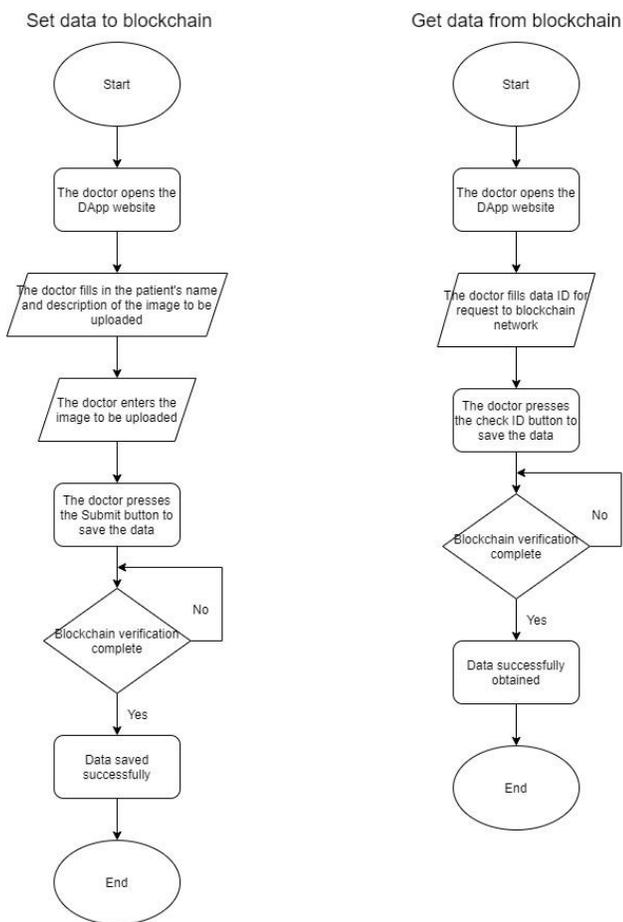


Fig. 4. Get and Set Function Scenario.

### C. Collecting Data Scenario

In Fig. 5, data retrieval is done by taking the execution time of the Get and Set functions on the blockchain system. This data retrieval uses a testing function from Truffle with the Chai library. The program that runs this test is Upload.test.js, which contains tests for the Get and Set methods on the blockchain network. The test is carried out with the same data declared at the beginning of the code, which is iterated for 1, 10, and 100 transactions, respectively. The following parameters are measured in this scenario:

- The time of each Get transaction and Set transaction in milliseconds is taken on average for each iteration.
- The difference in the amount of gas fee used by the transaction is based on the number of strings entered in the description.

The system test scenario, especially the Get and Set functions, is executed with a Javascript file called Upload-test.js. This file is in the test folder in the project documents using the React framework. This document will integrate with the scripts installed in the module package from Node.js that are run using Truffle.

Fig. 6 is a flowchart of the Upload-test.js. This document contains instructions that one wants to perform in the test. There are two important functions in this document, namely

the describe() function and the assert() function. The describe() function is tested using the Mocha library. Another library that can be used is from Truffle using the contract() function; but in this test, the Mocha function was used. The assert() function is used to create a condition that must be met—for example, there is a condition for sending data. However, in this test, the testing scenario was directed to focus more on the describe() function to get the test results in the form of time.

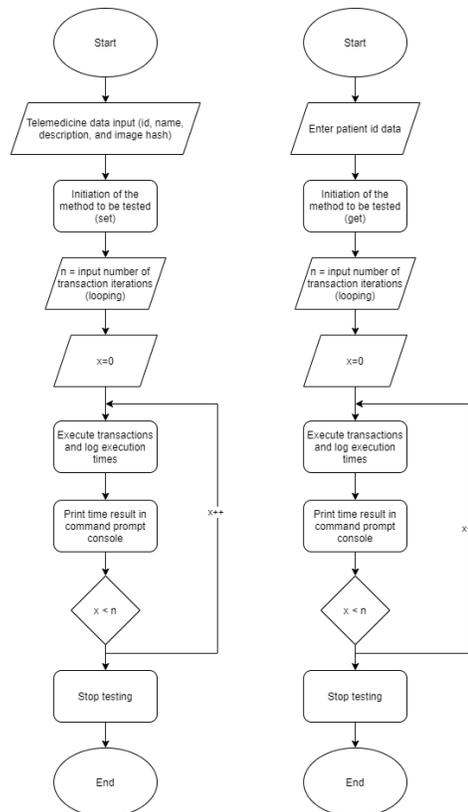


Fig. 5. Collecting Data Diagram Scenario.

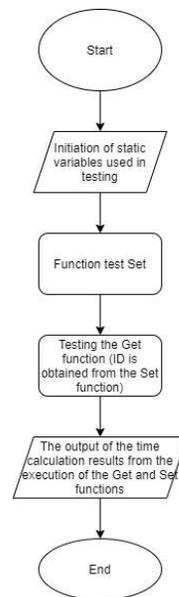


Fig. 6. Process Testing Set and Get Function Diagram.

#### IV. TEST RESULTS AND ANALYSIS

The test was carried out to determine system performance based on the duration needed to send and retrieve data on the blockchain system. This time was measured using a Javascript document that was run using Truffle. The measurement time was based on the execution time of the Set and Get functions on the telemedicine data. This time measurement was performed because the blockchain network system was run on Infura.io, which uses the Rinkeby test network such that the performance of the blockchain can be known to add new blocks to the network. This performance test was performed using a Javascript document that was executed using Truffle.

The test was distinguished by iterations and the number of strings that filled the description variable. Iterations or repetitions were varied into three, namely 1, 10, and 100 iterations. This iteration was performed as a burst value that was used to load which is referred to this test performed on the blockchain test network. Iteration variations were carried out to determine the rate of three repetition variations with the previously mentioned number. As for the number of strings, these were divided into three as well, namely:

- string1 (contains 39 characters, 6 words, and 5 spaces)
- string2 (contains 96 characters, 16 words, and 15 spaces)
- string3 (contains 161 characters, 28 words, and 27 spaces)

Test implementation is using only string not image from telemedicine data to reduce gas cost from a transaction. It is possible to store image data directly to blockchain but small image. Ethereum network has an 8M gas block limit. Every new 32 bytes of storage uses 20k gas, because the cost of data storage is 640K gas per kilobyte of data and the current gas price is approximately 15 GWEI [22]. So the system can't store data that sum to more than 12.8 kb. The solution is to use IPFS to convert images as IPFS hash so only string data will store at blockchain network and will also reduce gas costs as a whole. Due to the limitations of sending data on each transaction on the blockchain network, the variation in the number of strings is not too large. This is done because the test does not test limitations and only examines the effect of variations on the time and gas costs charged for each transaction.

From each of these tests, the average time was taken to be able to represent the calculation of the time of each iteration and each string difference. This time corresponded to the time needed to make transactions, apart from the time needed for miners to mine because the time for mining blocks was 15 seconds, which, in all transactions, was the same value because it used the Rinkeby test network.

##### A. Comparison and Analysis of Time in the Set Function and Get Function

In Table I, a comparison between the average times based on the number of iterations performed on each string can be seen. Comparisons were made by comparing the average time obtained in each iteration. For this reason, in this comparison, the 1x iteration as compared to the average time of the Set and

Get functions that applied to all iterations. Thus, the results of the comparison of the amount of time taken to perform the two functions are as follows.

- 1x iteration =  $12663.3 / 576.3 = 21.97$  times faster
- 10x iteration =  $15180.2 / 589.5 = 25.75$  times faster
- 100x iteration =  $15321.3 / 594.2 = 25.78$  times faster

From the average amount of time taken to obtain each iteration, it can be seen that in the 1x iteration the execution speed was 21.97 times faster in the Get function than in the Set function. For speed, the biggest difference between the Set and Get functions was in 100x iterations, which was 25.78 times faster than the Set function than in the Get function. The significant difference was in the 1x iteration, where the average iteration obtained tended to be small. This happened because the initial initiation and lack of repetition made the blockchain network not load transactions at almost the same time. The absence of this transaction burden made the time required for verification of the Set function faster, in contrast to string data that have repetitions or iterations greater than one time.

Time parameter in this implementation is important. The time parameter in this implementation will compare the time it takes to send and retrieve data because there are verification differences. At the time of sending data, a new transaction will be made that requires gas fees and will take time to verify. While in the data collection process there is no verification process at all. Verification on this test network sometimes takes a long time, resulting in data that is much longer than the average time.

##### B. Comparison and Analysis of Gas Fee Results with String Variations

This test was intended to determine how much it costs to store data on a blockchain network. Keep in mind that the blockchain network used was the Rinkeby testing network. However, this test can be used as a reference for the number of fees that must be paid when storing data in the blockchain network. The test was varied using the number of letters, words, and spaces in the "description" variable in the form of a string. In detail, the cost of each string was as follows:

- string1 : 0.000205 ETH
- string2 : 0.00025 ETH
- string3 : 0.000296 ETH

TABLE I. AVERAGE TIME COMPARISON BETWEEN SET AND GET FUNCTIONS

String / Iteration	Function					
	Set			Get		
	1x	10x	100x	1x	10x	100x
String1	12027	14857.9	14881.3	571	546.7	593.3
String2	12962	15687.4	15465.7	552	558.6	592.1
String3	13001	14995.3	15616.8	606	663.3	597.3
Average	12663.3	15180.2	15321.3	576.3	589.5	594.2

When string1 was compared to string2, an additional cost of 0.000045 ETH, or 21.95%, occurred for storing string2 when compared to the cost required to store string1. This means that there were additional costs when data were added. It can be concluded that the addition of special characters from string1 to string2 involved 57 characters. The addition of these 57 characters required an additional fee of 0.00045 ETH. In this test, spaces were ignored because they did not affect the amount of data stored. From the comparison test of string1 and string2, it can be concluded that the average additional gas cost is 0.38% per character.

In the next test, we compared the transaction gas costs using string2 and string3. The difference in gas costs between the two was 0.000046 ETH. Then, concerning the number of characters, string2 had 96 characters and string3 had 161 characters. If these two variables are separated, it produces 65 characters. For the cost of gas required from string2 to string3, there was an increase of 18.4%. If the average value per character is taken, an increase of 0.28% is obtained for each character.

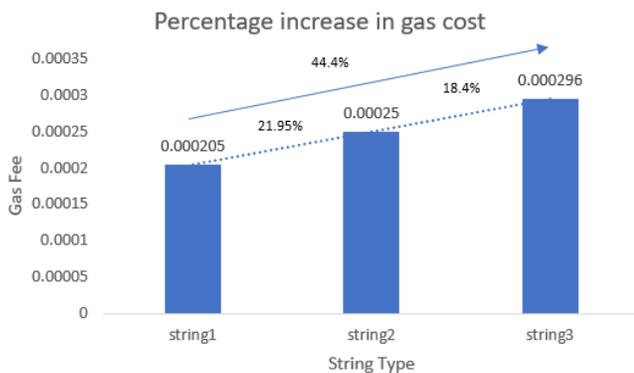


Fig. 7. Average Time Comparison between Set and Get Functions.

Fig. 7 depicts a graph of the percentage increase in the number of gas costs. The rising line has a linear tendency. Therefore, it can be concluded that the amount of string data is directly proportional to the number of gas costs that must be paid. However, in the tests carried out, the percentage increase in gas costs was slightly inappropriate. This discrepancy can be seen in Fig. 9, where the percentage increase from string1 to string3 is not the same as the sum of the percentage increase from string1 to string2 plus string2 to string3. This could be because the number of spaces was not taken into account or was ignored in this test. Thus, the percentage increase in costs had an error of 4.05% in this test.

## V. CONCLUSION

In the tests carried out in this work, several conclusions from the implementation can be made. First, we can conclude that the implementation of smart contracts on Ethereum as a blockchain system for application to telemedicine data repositories was successfully achieved. Thus, telemedicine treatment can improve the effectiveness of a person's time and can secure data. In addition, the performance of the blockchain was determined by the cost of the gas used. Using PoA, the validator block was limited in number to make the network

more scalable and faster in the transaction process. From the tests carried out, the performance for retrieving data from the blockchain was 24.4 times faster than adding data to the blockchain system. This is because the addition of data first requires a transaction verification such that the number of required time increases. Additionally, the more data one wants to store (in this study, in the form of string data), the more average time is required to make a transaction. The additional fee is as previously mentioned, the cost of each verified transaction will be following the amount of data that will be stored in the blockchain network. At the time of the experiment, the success rate of data transmission and retrieval was 100%, but there were some time spikes from time testing, especially in the Get function at 100 iterations. This was due to pending transactions at the time of verification. The gas fee that must be paid to add data to the blockchain system or for transaction validation fees to the validator was directly proportional to the amount of data stored in the blockchain. Therefore, from the experiment, it was shown that the larger the amount of data stored in the system, the higher the gas costs incurred. In this test, an additional cost of 0.34% per character string was added. The error obtained from the gas cost comparison experiment was 4.05%.

## ACKNOWLEDGMENT

This research is supported and funded by the Directorate of Research and Community Service, Deputy for Strengthening Research and Development, Ministry of Research, Technology / National Research and Innovation Agency of the Republic of Indonesia under the grant of Penelitian Konsorsium Riset Unggulan Perguruan Tinggi, contract number: 1056/PKS/ITS/2021 between researchers and Direktorat Riset dan Pengabdian kepada Masyarakat, Institut Teknologi Sepuluh Nopember.

## REFERENCES

- [1] A. Abugabah, N. Nizamuddin and A. A. Alzubi, "Decentralized Telemedicine Framework for a Smart Healthcare Ecosystem," in *IEEE Access*, vol. 8, pp. 166575-166588, 2020, doi: 10.1109/ACCESS.2020.3021823.
- [2] "Analysis of PoW, PoS and PoA," [Online]. Available: <https://www.programmersought.com/article/2017130150/>. [Accessed 21 July 2021].
- [3] Androulaki, Elli & Barger, Artem & Bortnikov, Vita & Cachin, Christian & Christidis, Konstantinos & Caro, Angelo & Enyeart, David & Ferris, Christopher & Laventman, Gennady & Manevich, Yacov & Muralidharan, Srinivasan & Murthy, Chet & Nguyen, Binh & Sethi, Manish & Singh, Gari & Smith, Keith & Sorniotti, Alessandro & Stathakopoulou, Chrysoula & Vukolic, Marko & Yellick, Jason. (2018). *Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains*.
- [4] J. Bang and M. Choi, "Design and Implementation of Storage System for Real-time Blockchain Network Monitoring System," 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2019, pp. 1-4, doi: 10.23919/APNOMS.2019.8892967.
- [5] H. Paik, X. Xu, H. M. N. D. Bandara, S. U. Lee and S. K. Lo, "Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance," in *IEEE Access*, vol. 7, pp. 186091-186107, 2019, doi: 10.1109/ACCESS.2019.2961404.
- [6] Khatoon, A. A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics* 2020, 9, 94. <https://doi.org/10.3390/electronics9010094>.
- [7] Bakaul, Masum & Das, Nipa & Moni, Madhabi Akter. (2020). *The Implementation of Blockchain in Banking System using Ethereum*.

- International Journal of Computer Applications. 177. 50-54. 10.5120/ijca2020919895.
- [8] T. Annisa, "Mudah, ini penjelasan dasar blockchain untuk pemula," Ekirut Media, [Online]. Available: <https://www.ekrut.com/media/blockchain-adalah>. [Accessed 20 December 2020].
- [9] J. Bang and M. Choi, "Design and Implementation of Storage System for Real-time Blockchain Network Monitoring System," 2019 20th Asia-Pacific Network Operations and Management Symposium (APNOMS), 2019, pp. 1-4, doi: 10.23919/APNOMS.2019.8892967.
- [10] "Proof of authority consensus," [Online]. Available: <https://www.geeksforgeeks.org/proof-of-authority-consensus/>. [Accessed 25 May 2021].
- [11] R. W. Ahmad, S. Khaled, R. Jayaraman, I. Yaqoob, S. Ellahham and M. Omar, "The Role of Blockchain Technology in Telehealth and Telemedicine," International Journal of Medical Informatics, vol. 148, no. 18:104399, p. 1, 2020.
- [12] A. Efendi, "Mengenal Telemedicine Beserta Kelebihan dan Kekurangannya," 13 May 2020. [Online]. Available: <https://tirto.id/mengenal-telemedicine-beserta-kelebihan-dan-kekurangannya-fsnL>. [Accessed 21 December 2020].
- [13] V. Kamani, "3 Telemedicine Types for Every Healthcare Organization," arkenea, [Online]. Available: <https://arkenea.com/blog/types-of-telemedicine/>. [Accessed 21 December 2020].
- [14] Ahmad, Raja & Salah, Khaled & Jayaraman, Raja & Yaqoob, Ibrar & Ellahham, Samer & Omar, Mohammed. (2021). The Role of Blockchain Technology in Telehealth and Telemedicine. International Journal of Medical Informatics. 148. 104399. 10.1016/j.ijmedinf.2021.104399.
- [15] J. Golosova and A. Romanovs, "The Advantages and Disadvantages of the Blockchain Technology," IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), pp. 1-6, 2018.
- [16] "What is Solidity Programming, its Data Types, Smart Contracts, and EVM in Ethereum?" Simplilearn, [Online]. Available: <https://www.simplilearn.com/tutorials/blockchain-tutorial/what-is-solidity-programming>. [Accessed 23 October 2021].
- [17] A. Pinna, S. Ibba, G. Baralla, R. Tonelli and M. Marchesi, "A Massive Analysis of Ethereum Smart Contracts Empirical Study and Code Metrics," in IEEE Access, vol. 7, pp. 78194-78213, 2019, doi: 10.1109/ACCESS.2019.2921936.
- [18] R. Ghods, "web3.js - Ethereum JavaScript API," 24 June 2020. [Online]. Available: <https://web3js.readthedocs.io/en/v1.3.4/>. [Accessed 18 April 2021].
- [19] Yu, Hongru & Sun, Haiyang & Wu, Danyi & Kuo, Tsung-Ting. (2020). Comparison of Smart Contract Blockchains for Healthcare Applications. AMIA ... Annual Symposium proceedings. AMIA Symposium. 2019. 1266-1275.
- [20] Agbo, Cc & Mahmoud, Qusay. (2019). Comparison of Blockchain Frameworks for Healthcare Applications. Internet Technology Letters. 2. e122. 10.1002/itl2.122.
- [21] "About Node.js," OpenJS Foundation, [Online]. Available: <https://nodejs.org/en/about/>. [Accessed 13 April 2021].
- [22] "Is it possible to store images on the Ethereum blockchain?, [Online], Available: <https://stackoverflow.com/questions/52994467/is-it-possible-to-store-images-on-the-ethereum-blockchain/52994971> [Accessed 21 October 2021].

# Multi-lane LBP-Gabor Capsule Network with K-means Routing for Medical Image Analysis

Patrick Kwabena Mensah<sup>1</sup>, Anokye Acheampong  
Amponsah<sup>2</sup>, Kwame Baffour Agyemang<sup>3</sup>, Mighty  
Abra Ayidzoe<sup>5</sup>, Faiza Umar Bawah<sup>6</sup>, Adebayor Felix  
Adekoya<sup>7</sup>, Benjamin Asubam Weyori<sup>8</sup>, Mark Amo-  
Boateng<sup>9</sup>

Department of Computer Science & Informatics  
University of Energy and Natural Resources  
Sunyani, Ghana

Gabriel Kofi Armah<sup>4</sup>

Department of Business Computing  
Faculty of Computing and Information Sciences (FCIS)  
University of Technology and Applied Sciences, Navrongo,  
Ghana

**Abstract**—Medical images naturally occur in smaller quantities and are not balanced. Some medical domains such as radiomics involve the analysis of images to diagnose a patient's condition. Often, images of sick inaccessible parts of the body are taken for analysis by experts. However, medical experts are scarce, and the manual analysis of the images is time-consuming, costly, and prone to errors. Machine learning has been adopted to automate this task, but it is tedious, time-consuming, and requires experienced annotators to extract features. Deep learning alleviates this problem, but the threat of overfitting on smaller datasets and the existence of the “black box” still lingers. This paper proposes a capsule network that uses Local Binary Pattern (LBP), Gabor layers, and K-Means routing in an attempt to alleviate these drawbacks. Experimental results show that the model produces state-of-the-art accuracy for the three datasets (KVASIR, COVID-19, and ROCT), does not overfit on smaller and imbalanced datasets, and has reduced complexity due to fewer parameters. Layer activation maps, a cluster of features, predictions, and reconstruction of the input images, show that our model is interpretable and has the credibility and trust required to gain the confidence of practitioners for deployment in critical areas such as health.

**Keywords**—Convolutional neural networks; deep learning; Gabor filters; k-means routing; local binary pattern; power squash introduction

## I. INTRODUCTION

Health is among the top critical areas that affect human life. For instance, 50,000 people die each year from pneumonia in the United States whereas colorectal polyps are projected to increase by 60% in 2030 which is likely to increase the number of causalities [1]. Images, videos, and text are the commonly generated and analyzed data used for the evaluation of most medical conditions. The analysis of these data requires the expertise of professionals which is rare and expensive in some regions and additionally susceptible to human errors [2], less effective [3], and falls below recommended levels in clinical procedures [4]. This calls for computer vision-assisted diagnosis. Machine learning-based methods such as support vector machines have been employed to assist in the effective diagnosis of medical diseases [5]. However, the performance of these methods was below the standard practices and the feature extraction procedure is time-consuming. To address

these issues, deep learning models such as convolutional neural networks (CNNs) were adopted to improve feature extraction. Interestingly, CNNs achieved performance rivaling human experts. For example, a CNN model made up of 121 layers (termed CheXNet), was trained on 100,000 frontal view chest X-rays and performed far better than 4 radiologists [6].

Regardless of CNN's good performance, the research identified certain limitations such as being translationally invariant [7], requiring large datasets, being computationally expensive [8], and following certain criteria for effective feature selection [9]. In health, the availability of a large dataset is a major challenge coupled with the lack of unavailability of qualified annotators [8]. Therefore, to prevent CNNs from overfitting on these small datasets, data augmentation techniques are employed. These data augmentation techniques are time-consuming and laborious.

To address these challenges, Capsule Network (CapsNet) [7] was introduced, and unlike CNNs, they do not require large datasets making them suitable for health applications. Notwithstanding, CapsNets also have their limitations. They perform poorly on complex images and images with varied backgrounds, have complex routing processes, poor learning of lower-level description [10], and polarization.

The contributions of this paper, therefore, are a) architectural innovation: we propose a Local binary pattern (LBP) – Gabor Capsule Network to address the weak feature extraction problem and the inability of CapsNets to learn lower-level descriptions of a complex image, b) algorithmic innovation: we adopt K-means routing, power squash, and sigmoid functions to complement the feature extraction abilities of the LBP-Gabor layers, c) explainable artificial intelligence (XAI): we provide extensive visualizations of the outputs of our network in an attempt to “open” the “black box” in deep learning models for enhanced credibility and understandability.

The rest of the paper is organized as follows: Section 2 presents the related work leading to Section 3 where the proposed methods are outlined. The experiments and experimental results are presented in Section 4 and the work concluded in Section 5.

## II. RELATED WORK

The limitations of human-centered diagnosis led to the adoption of algorithms for predicting medical conditions found in domains such as “radiomics”. Radiomics involves the use of data-characterization algorithms to extract features from radiographic images. Studies in the literature, such as Saif et al. [5] proposed a Capsule Network algorithm for the recognition of musculoskeletal conditions from radiographic images. The proposed model outperformed a 169-layer DenseNet in recognizing abnormality in musculoskeletal radiography. To address the inability of CNNs in encoding part-whole relationships, Mobiny et al. [11] proposed an efficient bi-directional long short-term recurrent capsule network for the recognition of apoptosis (cell death). The proposed model achieved competitive performance and outperformed CNNs especially when the number of training samples is small.

One of the deadliest medical conditions is brain tumors. Detection of the correct type of brain tumor at an early stage is vital to enable early treatment and reduce mortality in both children and adults. Consequently, there has been a surge of interest in developing efficient brain tumor detection algorithms. Afshar et al. [12] proposed a capsule network algorithm for the detection of a brain tumor on segmented images generated from the training images. The segmentation was done to avoid the negative effect of miscellaneous background objects on the model’s performance. Afshar et al. [13] proposed a focus-oriented capsule network algorithm that takes coarse boundaries of brain tumor images as extra inputs to diagnose brain tumors. The proposed model achieved overall recognition accuracy of 90.89%.

Given the challenges encountered during human-centered diagnosis of other lung infections and COVID computed tomography (CT) scan and X-ray images, Afshar et al. [14] proposed a capsule network termed COVID-Caps. The proposed model achieved an accuracy of 95.7%, sensitivity of 90%, and specificity of 90% on small datasets of COVID-19. This study is more related to the works in [15, 16] and [17] where transfer learning and custom-built CNNs are designed to diagnose diseases such as COVID-19 and retinal diseases from Chest X-ray and retinal optical coherence tomography (ROCT) images respectively. However, we leverage on CapsNet’s ability to avoid overfitting and identify the pose and deformation of objects and object parts to diagnose medical conditions from challenging medical images. Furthermore, the aforementioned works did extensive data preprocessing, augmentation, segmentation, and balancing of datasets (especially [15]) before fitting their models. We, however, used the raw datasets without augmentation and preprocessing to understand the model’s performance on the natural data since it may not be feasible to perform augmentation or segmentation during a medical emergency. Although the work in [15] provided images of the regions recognized by the model, we provide elaborate visualizations of image regions that attract the attention of parts of our model, clusters of features at the class capsule layer to measure the performance of the routing algorithm, performance on imbalanced datasets in the form of Precision-Recall (PR) curves, and reconstruction of input images as a way to enhance model transparency and understandability.

## III. PROPOSED METHODS

In this section, we present the model modifications and the methodology adopted to achieve our objective of designing a capsule network with superior feature extraction capabilities compared to the original CapsNet. We avoid shallowness and at the same time strive to reduce the number of parameters by using layers that generate no or less trainable parameters.

### A. K-Means Routing

We adopt the K-means routing in [18] with Sigmoid normalization, Power squash  $v_j = \|v_j\|^n \frac{v_j}{\|v_j\|}$ , and a modified logit updates procedure, instead of dynamic routing [7] in an attempt to minimize the problem of polarization [19] leading to improved performance on difficult medical images. Instead of using dot product and initializing  $b_{ij}$  with zero and adding the old logits to perform updates, our method respectfully uses the  $\ell_2$  distance measure, initializes  $b_{ij}$  as  $b_j^{(0)} \leftarrow \sum_{i=1}^n \|W_{ij}u_i - v_j^{(0)}\|^2$  and does not add old logits to new logits during updates. Algorithm 1 shows the K-means routing procedure.

**Algorithm 1** K-Means Routing for image classification [18]

1. **procedure** ROUTING ( $u_i, r$ )
2.     **Initialize**  $v_j^{(0)} \leftarrow \frac{1}{k} \sum_{i=1}^k W_{ij}u_i$
3.      $b_j^{(0)} \leftarrow \sum_{i=1}^n \|W_{ij}u_i - v_j^{(0)}\|^2$
4.     **for**  $r$  iterations **do**
5.          $b_{ij} \leftarrow \sum_{i=1}^n \|W_{ij}u_i - v_j\|^2$
6.          $c_{ij} \leftarrow \text{Sigmoid}(b_{ij})$
7.          $v_j \leftarrow \sum_{i=1}^n c_{ij}W_{ij}u_i$
8.     **return**  $power_r(v_j)$

### B. Feature Extraction with LBP and Gabor

Both LBP [20] and Gabor filters [21] have each been shown to be superior edge and texture feature extractors [22, 23] than convolutional layers [18, 24, 25].

Gabor filters belong to a special class of bandpass filters with frequency and orientation representation mimicking those of the mammalian cortex. They are made up of real and imaginary parts. It is the real part shown in equation 1 that is used to extract image features.

$$g(x,y;\lambda,\theta,\psi,\sigma,\gamma)=\exp\left(-\frac{x^2+y^2}{2\sigma^2}\right)\cos\left(2\pi\frac{x}{\lambda}+\psi\right) \quad (1)$$

where  $x' = x\cos\theta + y\sin\theta$ ,  $y = -x\sin\theta + y\cos\theta$  with  $(x, y)$  being the pixel position in the spatial domain.  $\lambda$  controls the width of the Gabor function strips,  $\theta$  represents the orientation to the normal,  $\psi$  is the phase offset,  $\gamma$  is the spatial aspect ratio, and  $\sigma$  is the standard deviation of the Gaussian envelope. To extract features with Gabor filters, five frequencies  $f$  and eight orientations  $\theta$  are adopted. These parameters are defined in equations 3 and 4.

$$= \frac{\pi}{2} \sqrt{2}^{(n-1)} \quad (2)$$

$$\theta = \frac{\pi}{2} (m-1) \quad (3)$$

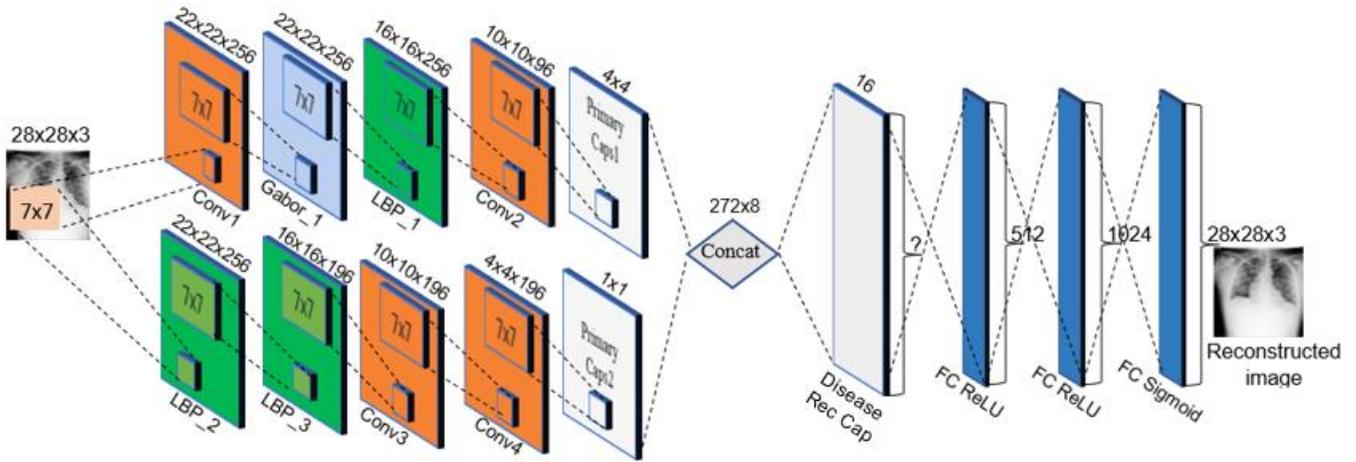


Fig. 1. The Gabor-LBP Capsule Network Architecture.

where  $n = 1, 2, \dots, 5$ ,  $m = 1, 2, \dots, 8$ , and  $\sigma = \frac{\pi}{f}$ .

The Local Binary Pattern (LBP) [20] is a powerful feature extractor that adds no trainable parameters to a model when used to extract contrast and spatial patterns of an image. It accomplishes this by thresholding  $n$  neighbouring pixels and computing its equivalent binary number based on equation 4.

$$LBP(n,r) = \sum_{n=0}^{n-1} f(i_n - i_c) 2^n \quad (4)$$

where  $i_n$  = neighboring pixels' intensity,  $i_c$  = current pixels' intensity,  $n$  = number of selected neighboring pixels at radius  $r$ , and a sign function defined as  $f = \begin{cases} 1, & \text{if } x \geq 0 \\ 0, & \text{otherwise} \end{cases}$ .

### C. LBP-Gabor CapsNet Architecture

The proposed model is a combination of Conv-LBP-Gabor layers placed in a multi-lane fashion (see Fig. 1). The input images are resized to 28x28x3 and fed to both lanes simultaneously. The first lane (upper lane) has a conv1 layer made up of 256, 7x7 kernels with ReLU non-linear activation at a stride of 1 to produce 256, 22x22 feature maps. These feature maps serve as input to the Gabor\_1 layer made up of 256, 22x22 feature maps for subsequent layers. The feature maps are processed in this manner as they pass through each layer in lane one until they reach the Primary Caps 1 layer which is a convolutional capsule layer made up of 7x7 kernels with a stride of 2. It is a 16-component capsule each with 4x4 capsules in an 8-dimensional vector.

LBP\_2 extracts the features directly from the input image to feed lane two (bottom lane). It is made up of 256, 7x7 kernels with stride 1 to produce 256, 22x22 feature maps. The features are refined as they pass through the rest of the layers to Primary Capsule 2 which has 3x3 kernels at a stride of 2. This too is a 16-component convolutional capsule each with a 1x1 capsule in an 8-dimensional vector.

The outputs of the two PCs are concatenated via axis 1 to produce a 272x8 dimensional tensor. It is the features of this tensor that are used for routing with the Disease recognition cap layer. The latter is 16-dimensional while the number of capsules is varied according to the number of classes in the

dataset. We have used (?) to indicate that the number of capsules will vary from 8, 4, 4 for KVASIR, COVID-19, and ROCT datasets respectively. Reconstruction of the input image is carried out by the decoder. The quality of the reconstructed images (see Fig. A1 in Appendix A) depends on the performance of the classification.

## IV. EXPERIMENTS

In this section, we present the experiments conducted on each dataset as well as their respective results. Three publicly available datasets were used to evaluate the performance of the model's ability to generalize on unseen data.

### A. Dataset Description

The Kvasir [24] is a dataset consisting of images from inside of the gastrointestinal (GI) tract. It consists of eight different classes made up of images from 720x576 to 1920x1072 pixels. The dataset can be used for multiclass classification [24] as the images can be categorized under three important anatomical landmarks. For a detailed description of this dataset, readers are encouraged to look at the work in [24]. This dataset is not balanced.

The COVID-19 dataset [16, 17] was collected by a team of doctors from 4 countries, and it is made up of chest X-ray images of COVID-19 positive cases plus some Normal and Viral Pneumonia images. Categories such as COVID, Lung Opacity, Normal, and Viral Pneumonia form the class in this dataset. This dataset is also imbalanced and details can be found in [16, 17].

The Retinal Optical coherence tomography (ROCT) dataset [15] contains high-resolution cross-sectional images of the retina. The dataset was collected from adult patients at the Shiley Eye Institute of the University of California San Diego, the California Retinal Research Foundation, Medical Center Ophthalmology Associates, the Shanghai First People's Hospital, and Beijing Tongren Eye Center [25]. It has four classes and is originally organized such that each test set has 250 images while the training set has 20,135 (i.e. approximately 95% to 5% train-test split). We, however, split all the three datasets into 80% training and 20% test. Additionally, we did not perform data augmentation to any of

our datasets as a means to measure the ability of the proposed model to decode the spatial orientation of the images. A summary of the datasets used in this study is provided in Table A1 in Appendix A.

### B. Experimental Setup

We performed all the experiments using the following tools and software; Keras with TensorFlow backend, one 64-bit Windows machine with NVIDIA GeForce GTX 1060 Graphic Processing Unit (GPU), 8GB GPU memory, 16GB system memory, and CUDA 10.1 toolkit. Hyperparameters such as the number of epochs, batch size range, learning rate, learning rate decay, and early stopping were respectively set to 100, 50-100, 0.001, 0.9, and 15. We varied the number of routing iterations from 2 to 7 (see Section 4.5) to test the ability of the model to scale up. To calculate the loss, we adopted the margin loss from [7]. This loss is given by:

$$L_k = T_k \max(0, m^+ - \|v_k\|)^2 + \lambda(1 - T_k) \max(0, \|v_k\| - m^-)^2$$

where  $T_k = \begin{cases} 1 & \text{if class } k \text{ is active} \\ 0 & \text{otherwise} \end{cases}$ ,  $\lambda = 0.5$ ,  $m^+ = 0.9$ , and  $m^- = 0.1$

We adopted, customized, and modified the code from <https://github.com/XifengGuo/CapsNet-Keras> for this study.

### C. Experimental Results

We present the experimental results in this Section and show that the model performed well when evaluated on the three datasets. To enhance confidence and reliability in the model's results, several evaluation methods were adopted and carefully conducted. Metrics such as the number of parameters, classification loss, and accuracy, the Area Under the Curve (AUC) for both the Receiver Operating Characteristic Curve (ROC) and Precision-Recall (PR) curves were used for the performance evaluation. Additionally, the model's robustness, ability to scale-up, fail-safe, extract only relevant features and the performance of the routing process were also evaluated. The traditional capsule network was also trained with the datasets and the results compared to our model based on the aforementioned performance metrics.

### D. Accuracy

We used the multi-class confusion matrix to summarize the performance of the model on the datasets. This method includes powerful per-class metrics such as true positive (TP), true negative (TN), false positive (FP), and false-negative (FN). The values in the principal diagonals of the confusion matrices are the TP values representing the level of correct identification of the true classes from the respective datasets. Few FNs as seen from Fig. A2 in Appendix A. indicates a good performance considering the field of application (i.e. health). In other words, the high TP values indicate good performance for a disease recognition model since it is not fatal for a healthy medical image (and by extension a healthy person) to be categorized as sick compared to when a sick person is classified as healthy.

From the confusion matrices, the accuracy of the model can be computed based on equation 5.

$$\text{Accuracy} = \frac{\text{TP} + \text{TN}}{\text{TP} + \text{FP} + \text{TN} + \text{FN}} \quad (5)$$

It is worth noting that accuracy, even though very popular [26] at evaluating classification algorithms, is not appropriate for medical images since they tend to be small and highly imbalanced [27]. Despite its drawback, it can provide a snapshot of the entire system performance, especially when the datasets are balanced..

The performance of the model in terms of accuracy during training and validation can be monitored via the training and validation curves. These curves for the three datasets are depicted in Fig. 2, with (c) and (d) depicting that the model had some difficulty in extracting the relevant features from the COVID-19 dataset. This is indicated by the zig-zag nature of the curves. Consistently, the proposed GLC model outperformed the traditional capsule network on the respective datasets in terms of training and validation accuracy/loss. A comparison of the accuracies of the proposed model, the traditional CapsNet, and other models in the literature on the same datasets are shown in Table A2 in Appendix A. The 93.40% accuracy of [15] on the ROCT dataset was obtained on the original 95%-5% train-test split. However, we split the data into 80%-20% for training and testing respectively. Unavailable values in Table A2 in Appendix A are indicated by (?).

To further probe the superiority of the proposed model, we performed additional experiments to determine the accuracy of the model as it is subjected to architectural damages in what is known as ablation studies (see Section 4.6). Additionally, we performed more experiments to explore the effect of increasing the capacity of the model on accuracy by increasing the number of routing iterations from 2 to 7 (see Section 4.5).

### E. Model's Ability to Scale

Dynamic routing has an inner loop [28] [18] which contributes to hindering the algorithm to scale on complex data and increases the threat of overfitting when the network capacity is increased through an increase in the number of routing iterations. To test the models on this score, we varied the number of routing iterations and the results of these experiments are depicted in Fig. A3 in Appendix A. It is observed that the proposed GLC maintains a marginal loss in accuracy for both KVASIR (Fig. A3 (a)) and COVID-19 (Fig. A3 (b)) as the number of routing iterations increases from 2 to 7. On the contrary, the traditional model begins to overfit after the third routing iteration (Fig. A3 (a)), probable because the number of classes is comparatively higher than the other datasets while at the same time the number of images in the dataset is relatively smaller. As the traditional model scales up, it becomes "hungrier" for data and tends to depend on the number of classes, consequently increasing the number of interrelationships to a level likely to cause overfitting.

We also observe from Fig. A3 (Appendix) that at 3 iterations, the traditional CapsNet achieved optimal performance as established in [7], however, this varies for the proposed model. For instance, GLC's accuracy for KVASIR and ROCT are highest at 2 and 4 routing iterations respectively.

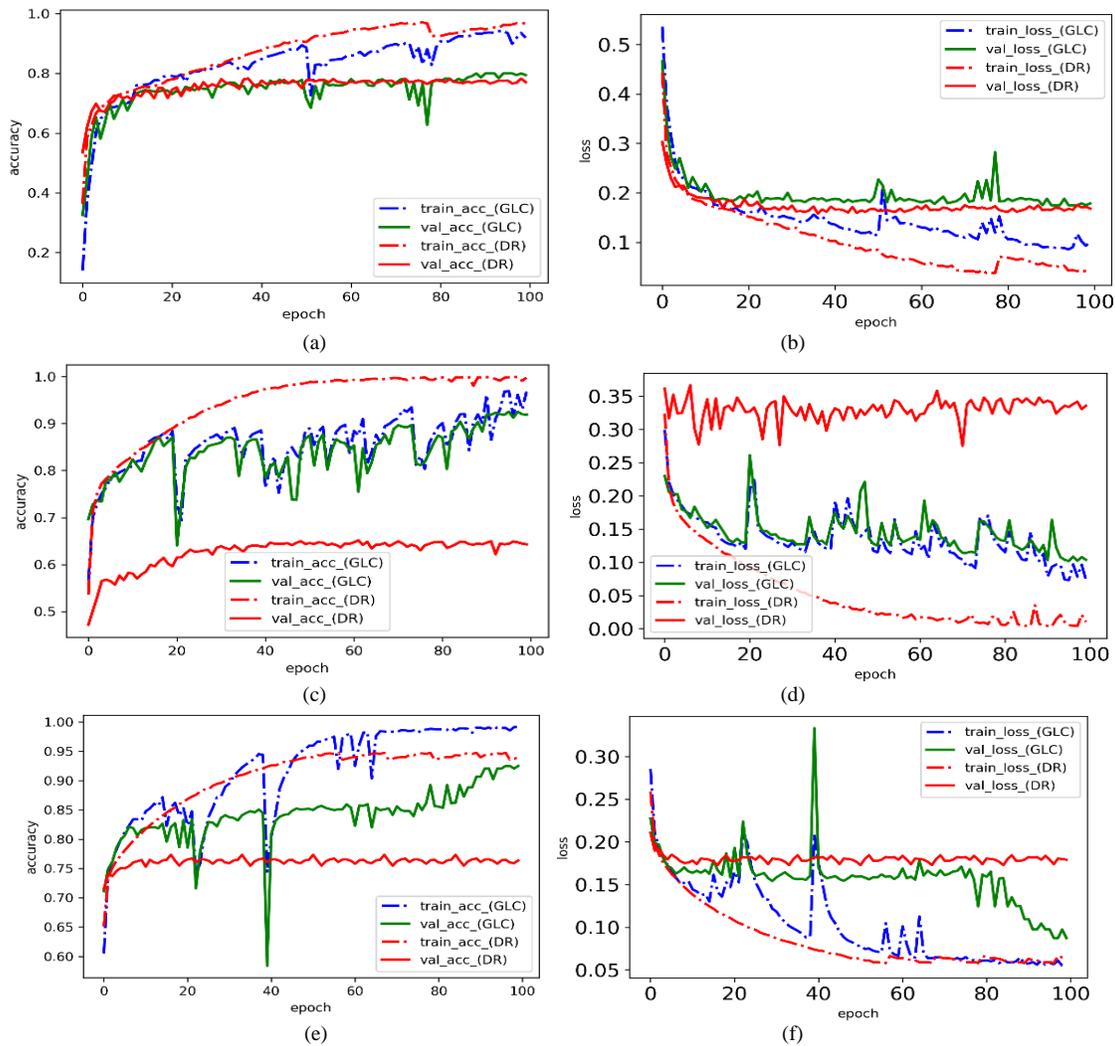


Fig. 2. Training and Validation Curves (a) Accuracy for KVASIR, (b) Loss for KVASIR (c) Accuracy for COVID-19, (d) Loss for COVID-19, (e) Accuracy for ROCT, and (f) Loss for ROCT Dataset.

#### F. Model's Robustness and Ability to Fail-Safe

Setting the number of routing iterations to 3, we performed additional experiments to determine parts and configurations of the model that made significant contributions to its high performance. We removed layers at a time and trained the network to measure the effect of their presence/absence in the network. Also, hyperparameters such as the squash and normalizer were varied and several pieces of training were carried out. This technique is called ablation study [29], and it can determine the ability of a network to fail-safe or undergo graceful degradation. Graceful degradation is a required property for critical applications. It is also a means to enhance confidence in the model since network components with the ability to stand in for failed parts can be identified and to also test for the robustness of the model to architectural changes.

From Table 1, Conv1 (row 1) and LBP2 (row 7) are very crucial in the network due to their positions as lower-layer (primary) feature extractors. Their removal causes a drop in accuracy across all the datasets. However, the removal of any of the rest of the conv layers causes a slight drop in accuracy, an indication that we could comfortably remove any one of them in situations where our objective is to reduce model parameters/size. Again, removing all the conv layers (row13) seems to have little effect on the performance compared to removing all LBP (row 11) and all LBP plus Gabor (row 12) layers. Rows 16 and 17 indicate the use of all layers in the network. We observe that the combination of the original squash and SoftMax underperformed relative to that of the Power squash and Sigmoid normalization consistent with what was reported in [18].

TABLE I. RESULTS OF ABLATION STUDY ON THE GLC MODEL

No	Layer(s) removed	Squash	Normalizer	Validation Accuracy (%)		
				KVASIR	COVID-19	ROCT
1	Conv1	Power	Sigmoid	79.11	90.02	90.13
2	Conv2	Power	Sigmoid	79.43	90.76	91.01
3	Conv3	Power	Sigmoid	79.51	90.62	90.35
4	Conv4	Power	Sigmoid	79.60	90.71	90.32
5	Gabor	Power	Sigmoid	77.07	80.23	81.56
6	LBP1	Power	Sigmoid	72.97	81.66	82.97
7	LBP2	Power	Sigmoid	70.94	79.52	80.50
8	LBP3	Power	Sigmoid	73.43	81.05	82.03
9	Gabor+LBP1	Power	Sigmoid	76.02	79.81	81.43
10	Conv1+Conv2	Power	Sigmoid	79.55	89.05	90.17
11	LBP1+LBP2+LBP3	Power	Sigmoid	66.91	70.12	75.57
12	Gabor+LBP1+...+LBP3	Power	Sigmoid	65.43	70.63	77.09
13	Conv1+...+Conv4	Power	Sigmoid	79.11	88.95	89.98
14	Lane 1 (top lane)	Power	Sigmoid	75.29	79.85	81.00
15	Lane 2 (bottom lane)	Power	Sigmoid	76.71	80.32	84.21
16	None	Original	SoftMax	78.54	88.70	89.01
17	None	Power	Sigmoid	80.91	91.96	91.30

### G. Performance on Smaller and Imbalanced Datasets

Medical images are usually smaller and highly imbalanced [33]. Class imbalance, on the other hand, contributes to a problem called the “accuracy paradox” [31] which causes the larger classes to overshadow the smaller classes during accuracy computations. In other words, accuracy under these conditions is influenced or biased towards the class with the highest number of samples. Besides, the asymmetric misclassification costs and probability estimates of the classification are not taken into consideration during accuracy computations under class imbalance. The AUCs for the ROC and PR curves become handy when fitting a model with balanced and imbalanced classes respectively [36, 37]. The AUC is invariant to the a priori likelihoods of the classes as well as being independent of the decision threshold [34]. Large AUCs are preferred over their smaller counterparts.

Fig. 3. shows the ROC and PR curves for the GLC model. We observe that the ROC curves have relatively larger areas separating them from the diagonal. The impression is that the model performed very well in all the classes, however, the PR curves depict that the model did not perform equally well in all the classes. This is so because ROC tends to be overly optimistic with insufficient data [35] as well as when there is a large skew in the dataset class distribution [32]. A medical practitioner ultimately needs to see the PR curves of a model (not only accuracy) before taking critical decisions on a patient’s condition. Compared to the ROC and PR curves of the DR model (shown in Fig. 3), the GLC model outperformed the traditional CapsNet model under class imbalanced

conditions. The respective AUC values are; ROC -KVASIR (0.96), PR-KVASIR (0.71), ROC-COVID-19 (0.97), PR-COVID-19 (0.95), ROC-ROCT (0.93), and PR-ROCT (0.87).

On smaller datasets, CapsNets are known to outperform convolutional neural networks due to the ability of CapsNets to encode pose and orientation. This reason, plus our superior feature extractors explain why our model performed well on the KVASIR dataset (see Fig. 2(a)) without any data augmentation.

### H. Prediction and Reconstruction

During prediction, the capsule outputs the class with the longest vector as the correct class. It is compared with the ground truth (GT) image to measure how well the trained model can classify an unseen image. This aspect of the model is very crucial for health applications since it quantifies the confidence the model has in its prediction. To introduce variability in the testing set, 1% of each dataset was reserved for prediction, and as such was not used as part of the training set. Sample prediction results on the unseen images are shown in Fig. A1 in Appendix A. The KVASIR dataset (Fig. A1 (a)) has eight classes, each of which is assigned a likelihood of being the correct class. The class with the highest probability is the predicted class. For both KVASIR and COVID-19 predictions, the model misclassified 0.5% of the unseen images (e.g. Fig. A1 (a) row 5 and Fig. A1 (b) row 4). We observe that the model imposed huge confidence (83%) in predicting class 2 of the KVASIR dataset as the correct class (Fig. A1 (a) row 3) while at the same time predicting class 1 with the confidence of 82% for the COVID dataset (Fig. A1 (b) row 5).

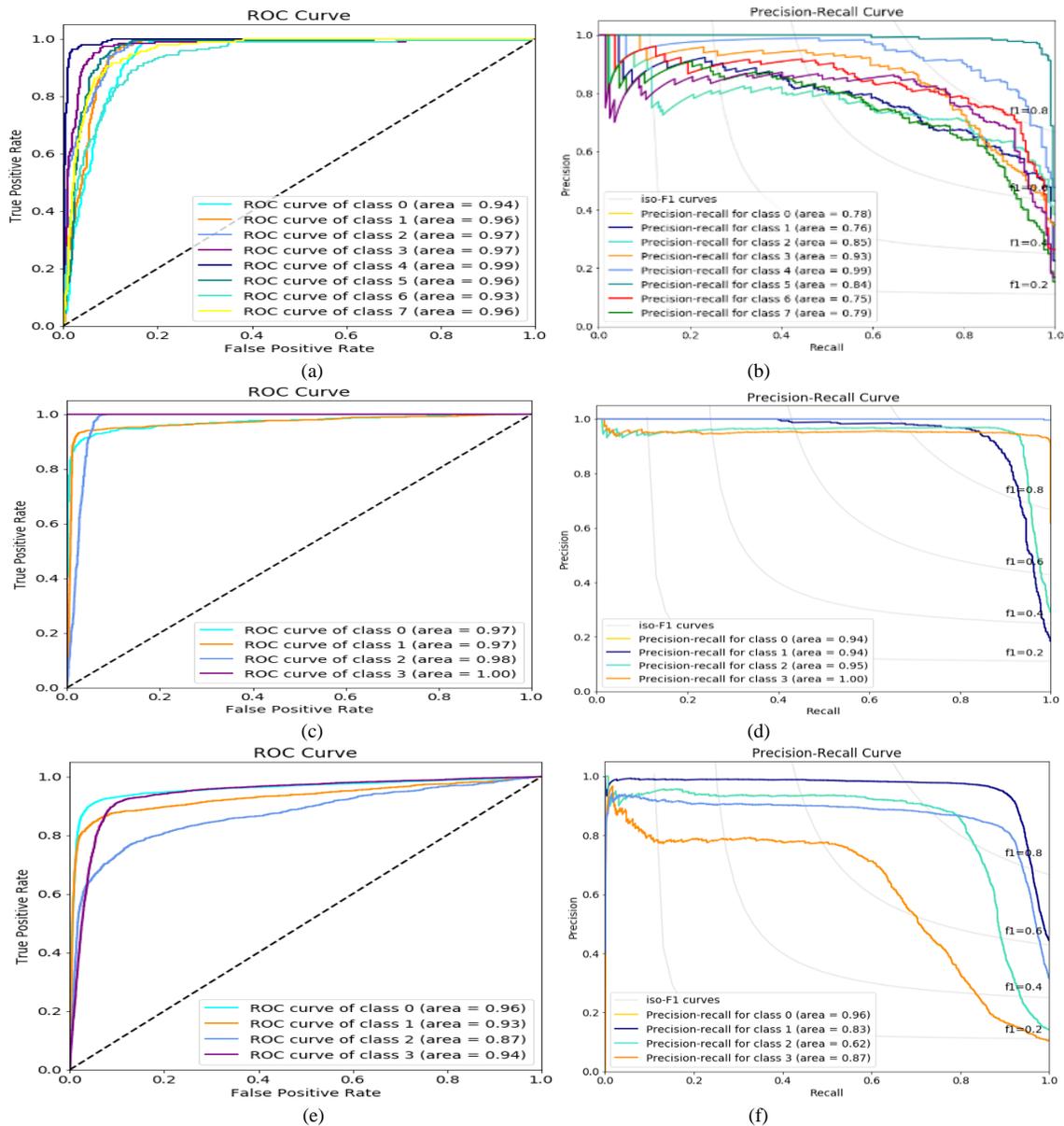


Fig. 3. ROC and PR Curves for the GLC Model. (a) ROC -KVASIR, (b) PR-KVASIR, (c) ROC-COVID-19, (d) PR- COVID-19, (e) ROC-ROCT, and (f) PR-ROCT.

Reconstruction allows visual verification of the model’s output/performance and also works as a regularizer. The reconstructed images in Fig. A1 in Appendix A. are clearly showing that the network layers effectively used the instantiating parameters to reconstruct the input mages (GT). We also carried out predictions and reconstruction on the ROCT dataset as well as using the DR model to predict and reconstruct unseen images from the three datasets. The DR model misclassified 1% of the unseen images across the 3 datasets. These results, however, are omitted for brevity.

### I. Model Complexity

Smaller deep learning models are required for efficient implementation on embedded devices such as FPGAs and

mobile phones with limited memory [36]. Such models are also important for reducing overhead to make distributed online training and inference possible. The smaller the number of a model’s trainable parameters, the less computationally complex the model is. This reduces the number of resources required by the model and also helps to prevent overfitting by ensuring that an 1-layer capsule model has  $\ln+k$  parameters required to exactly fit a  $d$ -dimensional dataset with  $n$  samples [37]. Our proposed model (see Fig. 1.) is deeper than the traditional CapsNet, but with a comparatively fewer number of parameters as shown in Table A3 in Appendix A. The values in Table A3 (Appendix) confirm that relatively smaller CapsNet models can represent complex real-life functions to outperform models with huge parameters [43, 18].

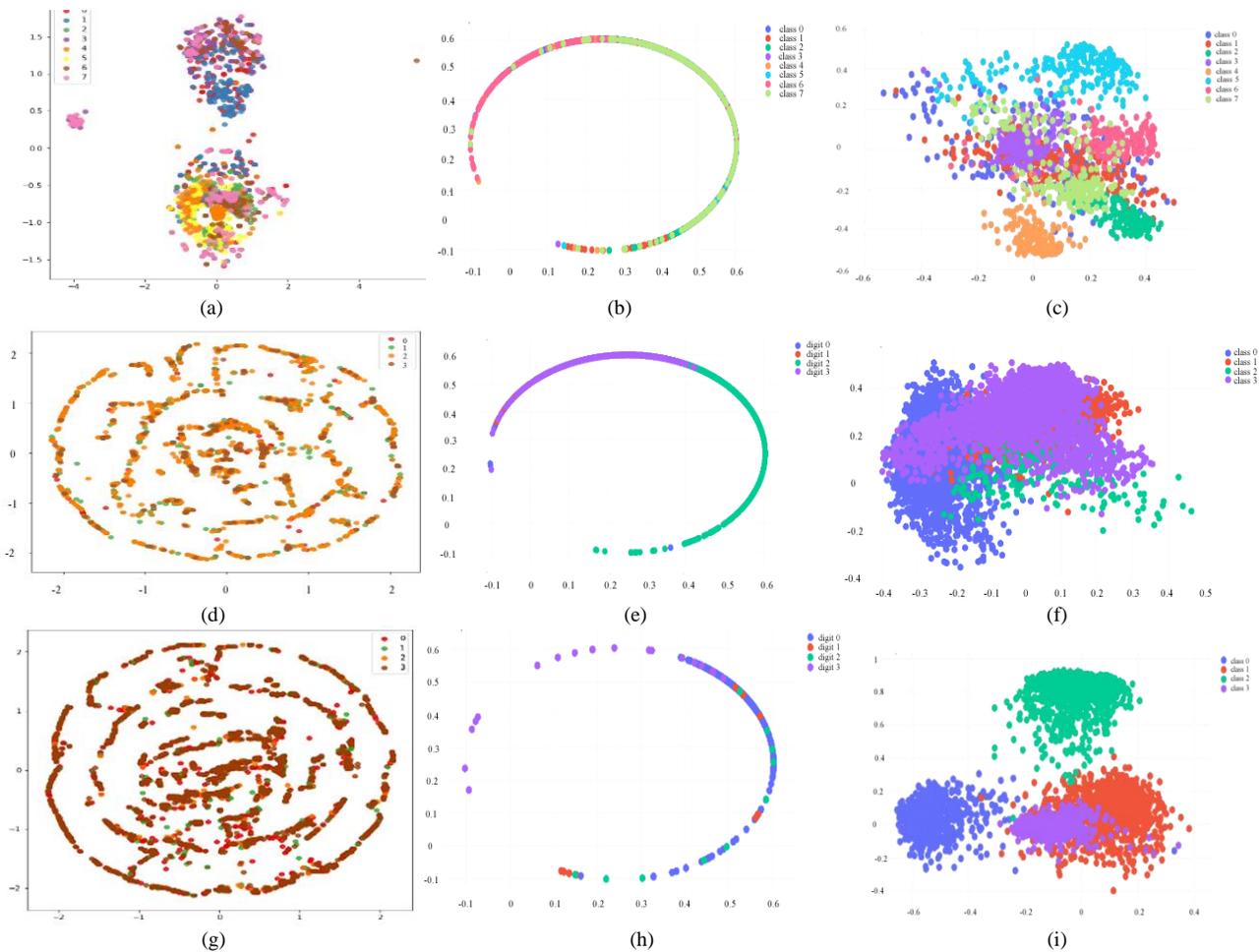


Fig. 4. *Tsne* Visualization of the Network’s Raw and Learned Features at the Class Capsule Layer, (a) KVASIR Raw Test Set, (b) GLC clusters of KVASIR, (c) DR Clusters of KVASIR, (d) COVID-19 Raw Test Set, (e) GLC Clusters of COVID-19, (f) DR Clusters of COVID-19, (g) ROCT Raw Test Set, (h) GLC clusters of ROCT, and (i) DR Clusters of ROCT.

### J. Performance of the Routing Process

We use the t-distributed stochastic neighbor embedding (TSNE) to visualize the network learned features at the class capsule layer. This method helps us to visually determine the level to which the network can differentiate between the different classes. Since primary capsules are coupled with secondary capsules with which there is a high agreement  $a_{ij}$  during routing, the features involved can be modeled as clusters. The compactness and separability of these clusters in the feature space indicate the performance of the routing algorithm at effectively making a distinction between the various classes. From Fig. 4., we observe that the clusters formed by the GLC model (second column); even though overlapping, are separable and some compact compared to those formed by the DR model (third column). These properties are linearly related to the performance of the routing algorithm and may be essential for further decision-making in case-by-case-based health applications.

We note that the reason for the GLC model forming circular clusters is that the routing algorithm is driven by K-means whose clusters are naturally circular from its use of the  $l_2$  norm [39].

### K. Feature Extraction

To uncover the network layers with good texture, edge, and shape feature extraction capabilities, we performed experiments to visualize the activation maps of the layers. This method is useful as it provides the opportunity to identify regions in the input image responsible for the activation of parts of the network. It also contributes to investigating whether a model is robust and can avoid failure through the inspection of the presence of layers with redundant features. Aside from the threat of overfitting resulting from model complexity, redundant layers are major contributors to a model’s robustness and fault tolerance capabilities. On the other hand, through this method, redundant layers can be eliminated to improve the model’s feature extraction to consequently reduce excessive oscillations and prolonged convergence during training [18]. This is a vital step for medical applications since it contributes significantly to the explainability and understandability of the “black box” [40] required to enhance confidence in model outputs for critical applications.



Fig. 5. Comparison of the Activation Maps of the Proposed GLC and the DR Models. (a) the First and Second Rows Show the Activation Maps for GLC and DR respectively on KVASIR, (b) Row One Shows the Activation Maps of GLC while Row Two Shows the Activation Maps of the DR Model for COVID-19, and (c) First and Second Rows are respectively the Activation Maps of GLC and DR Models for ROCT Dataset.

The feature maps in Fig. 5. show that the Gabor and LBP layers in the GLC have superior feature extraction capabilities than the convolutional layers. The Conv1 layer of the GLC network extracts some quality features since it is a higher-level layer with the ability to sample features from the lower-level layers (Gabor and LBP1) to represent advanced parts of the GT image. On the contrary, the Conv1 layer of the DR model is a lower-level layer, and with the difficulty of CNNs to extract quality features [18], it is not able to extract relevant features as required.

#### V. CONCLUSION AND FUTURE WORK

In this paper, we propose a capsule network architecture with superior feature extraction capabilities for the recognition of medical conditions in medical images. The adoption of

Local Binary Pattern (LBP), Gabor layers, and K-Means routing in an innovative architecture has dramatically improved the model's feature extraction capabilities leading to an appreciable performance while scaling up, preventing overfitting under class imbalance, and obtaining competitive validation and test accuracies. We further subjected the model through extensive visualization of layer activation maps, cluster of features, and ablation studies to enhance model interpretability and confidence for practical adoption. The results indicate that, it is possible to develop deep models to have smaller number of parameters (hence lower complexity) with huge potential for implementation on embedded devices with lower memories.

In the future, we will perform extensive experiments on these medical datasets for purposes of explainable artificial

intelligence (XAI). The aim will be to eliminate every ambiguity on model outputs to pave the way for its practical adoption in health.

REFERENCES

- [1] P. Wieszczy, J. Regula, and M. F. Kaminski, "Adenoma detection rate and risk of colorectal cancer," *Best Pract. Res. Clin. Gastroenterol.*, vol. 31, no. 4, pp. 441–446, 2017, doi: 10.1016/j.bpg.2017.07.002.
- [2] M. Akbari et al., "Polyp Segmentation in Colonoscopy Images Using Fully Convolutional Network," *Proc. Annu. Int. Conf. IEEE Eng. Med. Biol. Soc. EMBS*, vol. 2018-July, pp. 69–72, 2018, doi: 10.1109/EMBC.2018.8512197.
- [3] M. Arnold, M. S. Sierra, M. Laversanne, I. Soerjomataram, A. Jemal, and F. Bray, "Global patterns and trends in colorectal cancer incidence and mortality," *Gut*, vol. 66, no. 4, pp. 683–691, 2017, doi: 10.1136/gutjnl-2015-310912.
- [4] R. Lalonde, P. Kandel, C. Spampinato, M. B. Wallace, and U. Bagci, "Diagnosing Colorectal Polyps in the Wild with Capsule Networks," *Proc. - Int. Symp. Biomed. Imaging*, vol. 2020-April, pp. 1086–1090, 2020, doi: 10.1109/ISBI45749.2020.9098411.
- [5] A. F. M. Saif, C. Shahnaz, W. P. Zhu, and M. O. Ahmad, "Abnormality Detection in Musculoskeletal Radiographs Using Capsule Network," *IEEE Access*, vol. 7, pp. 81494–81503, 2019, doi: 10.1109/ACCESS.2019.2923008.
- [6] P. Rajpurkar et al., "CheXNet: Radiologist-level pneumonia detection on chest X-rays with deep learning," *arXiv:1711.05225v3 [cs.CV]*, pp. 3–9, 2017.
- [7] S. Sabour, N. Frosst, and G. E. Hinton, "Dynamic routing between capsules," in *31st Conference on Neural Information Processing Systems (NIPS 2017)*, 2017, vol. 2017-Decem, no. NIPS 2017, pp. 3857–3867.
- [8] N. Tajbakhsh et al., "Convolutional Neural Networks for Medical Image Analysis: Full Training or Fine Tuning?," *IEEE Trans. Med. Imaging*, vol. 35, no. 5, pp. 1299–1312, 2016, doi: 10.1109/TMI.2016.2535302.
- [9] X. Zhang et al., "Real-time gastric polyp detection using convolutional neural networks," *PLoS One*, vol. 14, no. 3, pp. 1–16, 2019, doi: 10.1371/journal.pone.0214133.t005.
- [10] S. Sabour, A. Tagliasacchi, S. Yazdani, G. E. Hinton, and D. J. Fleet, "Unsupervised part representation by flow capsules," *arXiv:2011.13920v2 [cs.CV]*, 2021.
- [11] A. Mobiny, H. Lu, H. V. Nguyen, B. Roysam, and N. Varadarajan, "Automated Classification of Apoptosis in Phase Contrast Microscopy Using Capsule Network," *IEEE Trans. Med. Imaging*, vol. 39, no. 1, pp. 1–10, 2020, doi: 10.1109/TMI.2019.2918181.
- [12] P. Afshary, A. Mohammadi, and K. N. Plataniotis, "BRAIN TUMOR TYPE CLASSIFICATION VIA CAPSULE NETWORKS," *arXiv:1802.10200v2 [cs.CV]*, 2018.
- [13] P. Afshar, K. N. Plataniotis, and A. Mohammadi, "Capsule Networks for Brain Tumor Classification Based on MRI Images and Coarse Tumor Boundaries," *ICASSP, IEEE Int. Conf. Acoust. Speech Signal Process. - Proc.*, vol. 2019-May, pp. 1368–1372, 2019, doi: 10.1109/ICASSP.2019.8683759.
- [14] P. Afshar, S. Heidarian, F. Naderkhani, A. Oikonomou, K. N. Plataniotis, and A. Mohammadi, "COVID-CAPS: A capsule network-based framework for identification of COVID-19 cases from X-ray images," *Pattern Recognit. Lett.*, vol. 138, pp. 638–643, 2020, doi: 10.1016/j.patrec.2020.09.010.
- [15] D. S. Kermany et al., "Identifying Medical Diagnoses and Treatable Diseases by Image-Based Deep Learning," *Cell*, vol. 172, no. 5, pp. 1122–1131.e9, 2018, doi: 10.1016/j.cell.2018.02.010.
- [16] M. E. H. Chowdhury et al., "Can AI Help in Screening Viral and COVID-19 Pneumonia?," *IEEE Access*, vol. 8, pp. 132665–132676, 2020, doi: 10.1109/ACCESS.2020.3010287.
- [17] T. Rahman et al., "Exploring the effect of image enhancement techniques on COVID-19 detection using chest X-rays images," *Comput. Biol. Med.*, vol. 132, no. November 2020, p. 104319, 2020, doi: 10.1016/j.compbiomed.2021.104319.
- [18] P. Mensah Kwabena, B. A. Weyori, and A. Abra Mighty, "Exploring the performance of LBP-capsule networks with K-Means routing on complex images," *J. King Saud Univ. - Comput. Inf. Sci.*, pp. 1–15, 2020, doi: https://doi.org/10.1016/j.jksuci.2020.10.006.
- [19] H. Ren and H. Lu, "Compositional Coding Capsule Network with K-Means Routing for Text Classification," *arXiv:1810.09177v3 [cs.LG]*, 2018.
- [20] T. Ojala, M. Pietikainen, and T. Maenpaa, "Multiresolution Gray-Scale and Rotation Invariant Texture Classification with Local Binary Patterns," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 24, no. 7, pp. 971–987, 2002.
- [21] D. Gabor, "Theory of communication. Part 1: The analysis of information," *J. Inst. Electr. Eng. - Part III Radio Commun. Eng.*, vol. 93, no. 26, pp. 429–441, 1946, doi: 10.1049/ji-3-2.1946.0074.
- [22] P. K. Mensah, B. A. Weyori, and A. A. Mighty, "Max-Pooled Fast Learning Gabor Capsule Network," in *IEEE International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD)*, 2020.
- [23] P. K. Mensah, B. A. Weyori, and A. A. Mighty, "Gabor Capsule Network for Plant Disease Detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 10, pp. 388–395, 2020.
- [24] K. Pogorelov et al., "Kvasir: A multi-class image dataset for computer aided gastrointestinal disease detection," *Proc. 8th ACM Multimed. Syst. Conf. MMSys 2017*, pp. 164–169, 2017, doi: 10.1145/3083187.3083212.
- [25] P. Mooney, "Retinal OCT Images (optical coherence tomography)," *Kaggle*, 2018. [Online]. Available: https://www.kaggle.com/paultimothymooney/kermany2018. [Accessed: 19-Apr-2021].
- [26] N. Japkowicz and M. Shah, *Evaluating Learning Algorithms- A Classification Perspective*, vol. 5, no. 1. New York: Cambridge University Press, 2011.
- [27] F. Provost, T. Fawcett, and R. Kohavi, "The Case Against Accuracy Estimation for Comparing Induction Algorithms," in *Proceedings of the Fifteenth International Conference on Machine Learning*, 1998, pp. 445–453.
- [28] B. Mandal, S. Ghosh, R. Sarkhel, N. Das, and M. Nasipuri, "Using dynamic routing to extract intermediate features for developing scalable capsule networks," in *2nd International Conference on Advanced Computational and Communication Paradigms, ICACCP 2019*, 2019, pp. 1–6, doi: 10.1109/ICACCP.2019.8883020.
- [29] R. Meyes, M. Lu, C. W. De Puiseau, and T. Meisen, "Ablation Studies in Artificial Neural Networks," *arXiv:1901.08644v2 [cs.NE]*, pp. 1–19, 2019.
- [30] A. S. Lundervold and A. Lundervold, "An overview of deep learning in medical imaging focusing on," *Z MedPhys*, vol. 29, no. 2, pp. 102–127, 2019, doi: 10.1016/j.zemedi.2018.11.002.
- [31] F. J. Valverde-Albacete and C. Peláez-Moreno, "100% classification accuracy considered harmful: The normalized information transfer factor explains the accuracy paradox," *PLoS One*, vol. 9, no. 1, 2014, doi: 10.1371/journal.pone.0084217.
- [32] J. Davis and M. Goadrich, "The Relationship Between Precision-Recall and ROC Curves," in *Proceedings of the 23rd International Conference on Machine Learning*, 2006, pp. 546–559, doi: 10.4135/9780857021113.n29.
- [33] P. Domingos and P. Singla, "Discriminative training of Markov logic networks," *Proc. 20th Natl. Conf. Artificial Intelligence*, vol. 20, p. 868{873, 2005.
- [34] C. X. Ling, J. Huang, and H. Zhang, "AUC: A Better Measure than Accuracy in Comparing Learning Algorithms," *Adv. Artif. Intell. Can. AI 2003. Lect. Notes Comput. Sci. (Lecture Notes Artif. Intell.)*, vol. 2671, pp. 329–330, 2003, doi: https://doi.org/10.1007/3-540-44886-1\_25.
- [35] M. Sokolova, N. Japkowicz, and S. Szpakowicz, "Beyond Accuracy, F-Score and ROC: A Family of Discriminant Measures for Performance Evaluation," *LNAI 4304*, pp. 1015–1021, 2006.

[36] F. N. Iandola, S. Han, M. W. Moskewicz, K. Ashraf, W. J. Dally, and K. Keutzer, "SQUEEZENET: ALEXNET-LEVEL ACCURACY WITH 50 X FEWER PARAMETERS AND < 0.5 MB MODEL SIZE," *arXiv1602.07360v4 [cs.CV]*, pp. 1–13, 2017.

[37] C. Zhang, B. Recht, S. Bengio, M. Hardt, and O. Vinyals, "Understanding deep learning requires rethinking generalization," in *5th International Conference on Learning Representations, ICLR 2017 - Conference Track Proceedings*, 2017.

[38] C. W. Wu, "ProdSumNet: reducing model parameters in deep neural networks via product-of-sums matrix decompositions," *arXiv:1809.02209v2 [cs.LG]*, no. 1, pp. 1–10, 2018.

[39] B. Ojeda-Magaina, R. Ruelas, M. A. Corona-Nakamura, and D. Andina, "An Improvement to the Possibilistic Fuzzy C-Means Clustering Algorithm," in *World Automation Congress (WAC)*, 2006.

[40] A. Barredo Arrieta *et al.*, "Explainable Artificial Intelligence (XAI): Concepts, taxonomies, opportunities and challenges toward responsible AI," *Inf. Fusion*, vol. 58, no. October 2019, pp. 82–115, 2020, doi: 10.1016/j.inffus.2019.12.012.

APPENDIX A

TABLE A1. NUMBER OF IMAGES AND THE DIVISIONS PER 80% TRAINING, 20% TEST FOR EACH DATASET

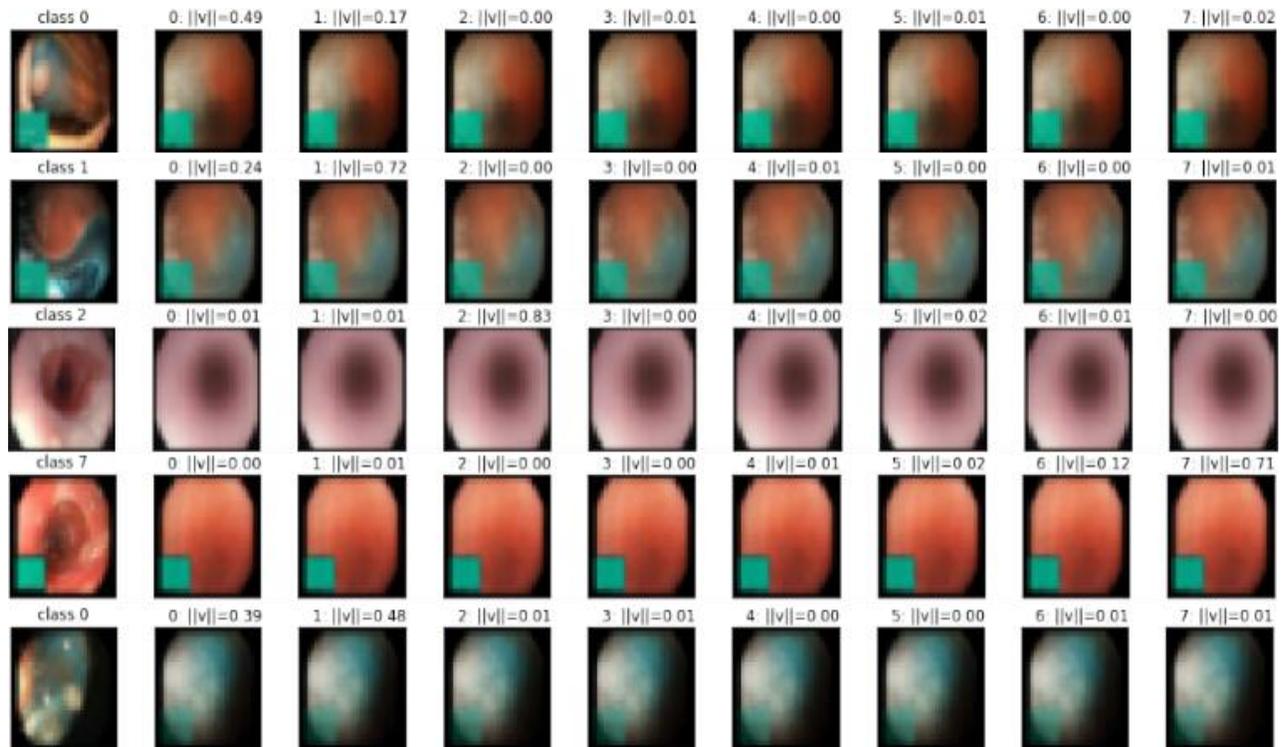
Dataset	Total Number of Images	Training Set	Validation Set	Test Set
KVASIR-2	8,095	6,476	1,619	100
COVID-19	82,570	66,056	16,514	100
ROCT	21,135	16,908	4,227	100

TABLE A2. COMPARISON OF MODEL ACCURACY TO THE TRADITIONAL CAPSNET. UNREPORTED VALUES ARE REPRESENTED BY (?)

Model	KVASIR	COVID-19	ROCT
CNN [17]	?	91.30%	?
Transfer Learning [15]	?	?	93.40%
DR [7]	78.54%	65.15%	77.35%
<b>GLC (ours)</b>	<b>80.91%</b>	<b>91.96%</b>	<b>91.30%</b>

TABLE A3. COMPARISON OF MODEL PARAMETERS

Model	KVASIR		COVID-19		ROCT	
	Trainable	Non-Trainable	Trainable	Non-Trainable	Trainable	Non-Trainable
Traditional capsule (DR)	9,552,944	0	9,552,441	0	9,552,441	0
<b>GLC (ours)</b>	<b>8,323,640</b>	<b>0</b>	<b>8,302,136</b>	<b>0</b>	<b>8,302,136</b>	<b>0</b>
Difference	1,229,304	0	1,250,305	0	1,250,305	0



(a)

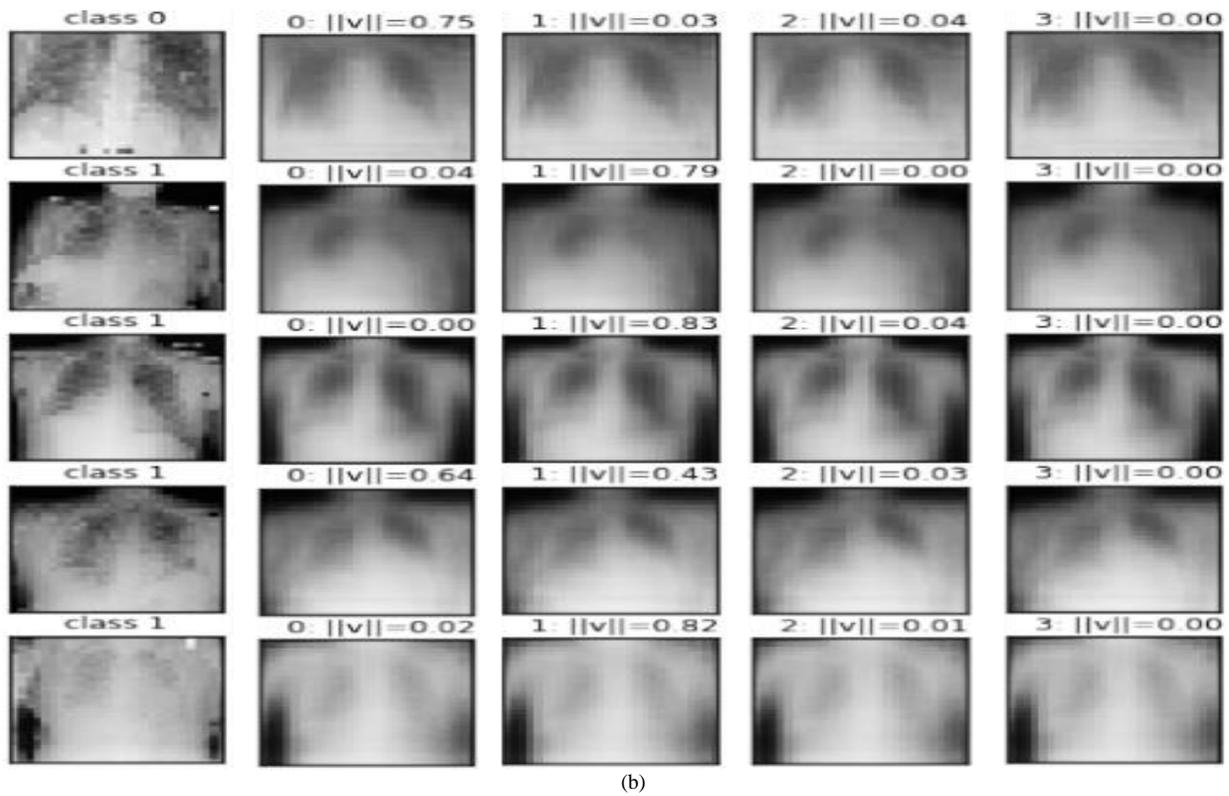


Fig. A1. The Reconstructed Images of the Proposed Model on (A) KVASIR and (B) COVID-19 Datasets.

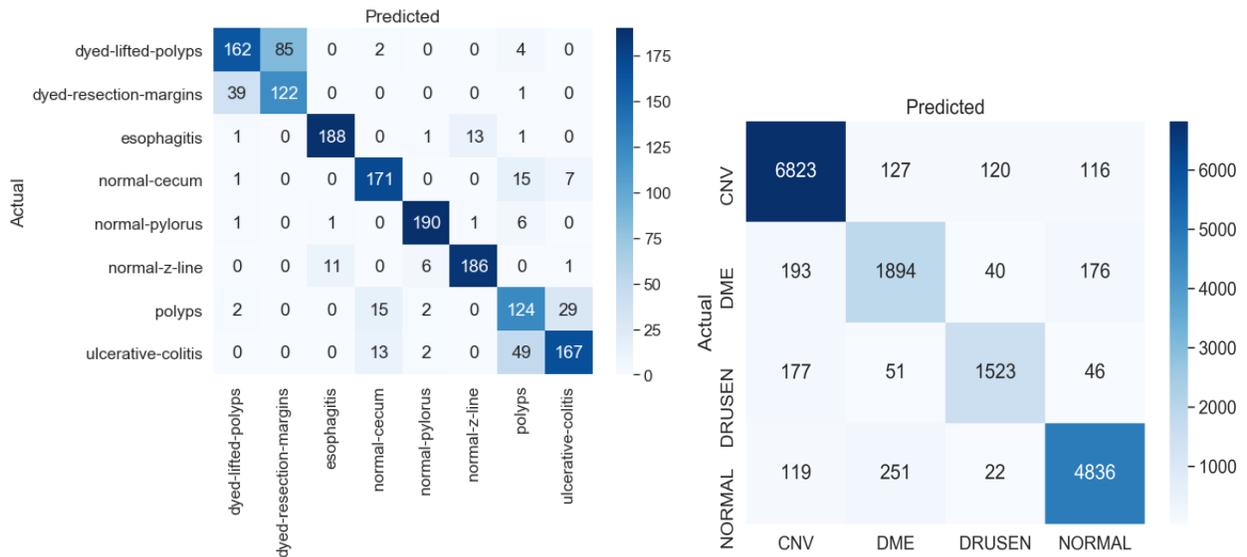


Fig. A2. Confusion Matrices of the Proposed Model on the KVASIR and COVID-19 Datasets.

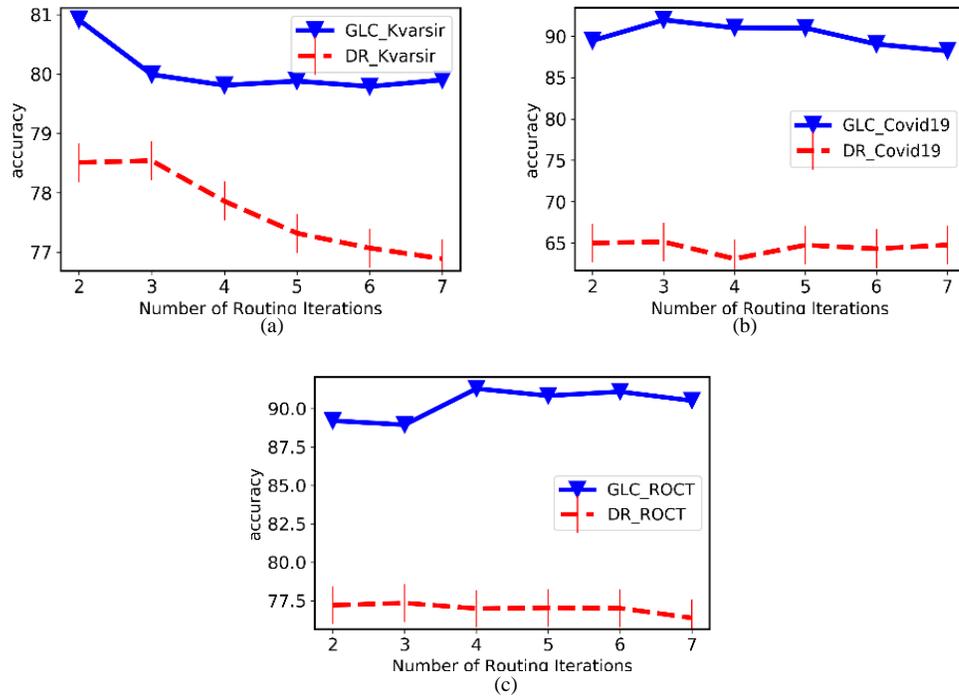


Fig. A3. Comparison of the Models' Ability to Scale on (a) KVASIR, (b) COVID-19, and (c) ROCT Datasets.

# Healthcare Misinformation Detection and Fact-Checking: A Novel Approach

Yashoda Barve<sup>1</sup>, Jatinderkumar R. Saini<sup>2\*</sup>

Suryadatta College of Management Information Research and Technology, Pune, India<sup>1</sup>

Symbiosis Institute of Computer Studies and Research, Symbiosis International (Deemed University), Pune, India<sup>2</sup>

**Abstract**—Information gets spread rapidly in the world of the internet. The internet has become the first choice of people for medication tips related to their health problems. However, this ever-growing usage of the internet has also led to the spread of misinformation. The misinformation in healthcare has severe effects on the life of people, thus efforts are required to detect the misinformation as well as fact-check the information before using it. In this paper, the authors proposed a model to detect and fact-check the misinformation in the healthcare domain. The model extracts the healthcare-related URLs from the web, pre-processes it, computes Term-Frequency, extracts sentimental and grammatical features to detect misinformation, and computes distance measures viz. Euclidean, Jaccard, and Cosine similarity to fact-check the URLs as True or False based on the manually generated dataset with expert's opinions. The model was evaluated using five state-of-the-art machine learning classifiers Logistic Regression, Support Vector Machine, Naïve Bayes, Decision Tree, and Random forest. The experimental results showed that the sentimental features are crucial while detecting misinformation as more negative words are found in URLs containing misinformation compared to the URLs having true information. It was observed that Naïve Bayes outperformed all other models in terms of accuracy showing 98.7% accuracy whereas the decision tree classifier showed less accuracy compared to all other models showing an accuracy of 92.88%. Also, the Jaccard Distance measure was found to be the best distance measure algorithm in terms of accuracy compared to Euclidean distance and Cosine similarity measures.

**Keywords**—Misinformation detection; sentiment analysis; document similarity; fact-check; healthcare

## I. INTRODUCTION

Online social media and the web as a whole have become the spring of information to users all around the world. Due to its convenience, feasibility, unrestricted access, and reasonable cost the internet have become popular amongst the community [1], [2]. The people read, share, write, and view the articles, blogs, news, videos, audios, etc., all over the internet. The rate of sharing articles, blogs, news, etc., has been accelerated dramatically. However, the users not only share immaculate information but also try to spread wrong or incorrect information either knowingly or unknowingly in a moment. This widespread misinformation has relentless consequences on individuals, commercial, health, government, and all other facets of society. The ramification of the misinformation is catastrophic and may lead to extermination. For example, the political disinformation spread during the 2016 USA presidential elections led to public shootings. These enduring

consequences of misinformation contribute towards ferocious conflicts that are preventable otherwise [3], [4].

The internet has become the most popular and the first choice of the public to investigate health problems. However, people get misinformed with wrongly populated content. A famous and perfect example is the misconception among the public about the measles, mumps, and rubella (MMS) vaccine causing autism. Health misinformation is defined as "A health-related claim of fact that is currently false due to a lack of scientific evidence" [5]. The promulgated experiences of people over the internet or articles were written about certain diseases without knowing or verifying the fact or having a lack of evidence can cause health ruination of readers and thus can lead to complete desolation [6], [7]. The misinformation related to health can have hazardous effects on people's life directly, thus detecting misinformation in healthcare is a need of time [8]–[10].

Misinformation detection has become the topic of interest amongst researchers in the literature. The researchers have studied different types of false information. The first category is termed misinformation, which is the inaccurate or incorrect information that is confirmed with existing evidence [11]. The other categories include the fake news [12], [13], rumor [6], satire news [14], hoaxes [15], misinformation [16], [17], disinformation [18] and opinion spam [19]. To detect each of these categories of false information the authors have used several features like sentiment analysis, user-specific features, syntactical features, grammatical features, image or message specific features, etc. Also, there are readily available datasets for false information detection in various domains viz. politics, news, business, and healthcare. Few examples of these datasets are LIAR, FakeNewsNet, BSDetector, etc. With the help of features and datasets, machine learning and deep learning techniques are applied to detect false information [11]. However, detecting misinformation is an exhaustive task. This is due to two main reasons: first, is the availability of dataset in a certain domain and second is fact-checking of the data [11], [20], [21]. It is difficult to get the benchmark and gold-standard datasets in a specific domain. Also, manual fact-checking of data is time-consuming, requires expert guidance, and involves laborious tasks. Thus, automatic fact-checking of data is a need of time to endure with the speed of the newly arriving and changing data.

Document Similarity is a measure of the distance between the two documents (DS). There are several distance measures available in the literature to compute the similarity between the

\*Corresponding Author.

documents like Euclidian Distance, Cosine Similarity, Jaccard Distance, etc. The concept of document similarity can be used to fact-check the information with the existing verified documents and thus can help to detect misinformation. Document Similarity is a measure of the distance between the two documents (DS). There are several distance measures available in the literature to compute the similarity between the documents like Euclidian Distance, Cosine Similarity, Jaccard Distance, etc. The concept of document similarity can be used to fact-check the information with the existing verified documents and thus can help to detect misinformation.

Sentiment Analysis (SA) techniques to detect the polarity of data into positive, negative, and neutral have been widely used in the literature to detect misinformation, fake news, rumors, etc. The process of knowing the opinion of the people about the products, services, movie reviews, etc. can be easily captured using sentiment analysis [20], [22]–[26]. The literature related to misinformation detection or finding the credibility of information using sentiment analysis has marked that the articles or blogs containing more positive words are tend to be spreading true information while the articles having negative information contain more negative information [27], [28].

Thus, to detect misinformation and perform fact-checking automatically the authors have proposed a hybrid approach of sentiment analysis and document similarity. In this research paper, the authors have created a sentiment-based Bag-of-Words (BoW) as a dataset related to the healthcare domain. Further, features like sentiment analysis, grammatical and lexical features are used to detect misinformation and document similarity measures viz. Euclidian distance, Cosine similarity, and Jaccard distance are used to perform fact-checking.

The remaining sections of the paper are structured as follows: Section II provides the literature survey describing the techniques of using sentiment-based features to detect misinformation in the healthcare domain and also the document similarity-based approaches used to fact-check the documents which could help to detect misinformation in the healthcare domain. Section III describes the proposed model architecture, dataset collection and cleaning process, and methodology used in the proposed model. Section IV discusses the results generated based on the proposed model of a hybrid approach of sentiment analysis and document similarity and section V describes the conclusion and future enhancements.

## II. RELATED WORK

### A. Sentiment Analysis in Healthcare

In terms of web articles, the sentiment analysis is an expression that measures the attitude of the author in terms of positive, negative or neutral towards the article topic. Especially, when talked about healthcare-related articles, people like to express and share their opinions about their

experiences about the disease which they have suffered from. Therefore the readers get biased towards the opinion of the author and believe the article without verifying the facts or evidence. Due to the rich contents of health information available online, the web has become the first choice of patients or users to know about the cure of disease and related remedies. Thus, understanding the sentiment of the article contents is much needed when it comes to misinformation detection. In the state-of-the-art techniques, the authors have analyzed the moods of cancer patients from tweets. Long Short Term Memory (LSTM) techniques were used to find the sentiments from the tweets [29]. In another research, authors collected 1,000 text comments of medical experts through various medical animation videos of the Youtube repository, and applied sentiment analysis to these comments to enhance the reputation of telemedicine education across the globe [30]. To study the effectiveness or popularity of a medicine, authors have performed sentiment analysis on public reviews using weighted word representation techniques and added linguistic constraints to model the contextually similar words [31]. Also, sentiment analysis techniques were used to detect misinformation in herbal treatments of diabetes in Arabic comments of YouTube videos [32]. The sentiment analysis is widely used in the healthcare sector to understand the sentiment polarity of the text and thus it can act as a major feature for misinformation detection. Table I displays the recent techniques of sentiment analysis in the healthcare domain in comparison with the proposed model techniques.

### B. Document Similarity in Healthcare

Document similarity measures the distance between two documents in a numeric value. The document similarity measures are used to find the similarity between healthcare documents. For example, to detect medical codes of the documents the authors have used an attention mechanism which targets the most informative parts of the documents [33]. In another research, Jaccard distance measure was used to compute the similarity between medical documents using a Non-negative matrix factorization algorithm [34]. In another research, the Term Frequency-Inverse Document Frequency (TF-IDF) of a document is computed and document similarity is measure using cosine similarity, further k-means is used to cluster the documents of similar types. The authors have also used the Unified Medical Language System (UMLS) to extract domain-specific features and select the required features using Principal Component Analysis (PCA). Further, the authors have used expected maximization techniques to cluster the similar documents together [35]. The document similarity is extensively applied in the healthcare domain to group similar documents together. This technique along with sentimental features will be useful for detecting misinformation in the healthcare domain. Table II displays the recent techniques of document similarity in the healthcare domain concerning the proposed model.

TABLE I. RECENT TECHNIQUES OF SENTIMENT ANALYSIS IN HEALTHCARE DOMAIN AND THE PROPOSED MODEL TECHNIQUES

Sr. No.	Reference	Technique	Dataset	Features	Sentiment Classification
1	[29]	LSTM	821,483 public tweets	N-gram, TF-IDF,LDA, PCA	Cancer Tweets
2	[30]	Classifiers used like SVM, kNN	1,010 comments	Sentiment	Medical Videos
3	[31]	Classifiers used like SVM, kNN	2,15,063 patient reviews	TF-IDF	Patient Reviews
4	<b>Proposed Model</b>	<b>Classifiers used like LR, SVM, NB, DT, RF</b>	<b>1000 Healthcare Web URLs</b>	<b>TF-IDF, Sentiment Polarity, Grammatical Features</b>	<b>Healthcare web URLs as True or False</b>

TABLE II. RECENT TECHNIQUES OF DOCUMENT SIMILARITY IN HEALTHCARE DOMAIN AND THE PROPOSED MODEL TECHNIQUES

Sr. No.	Reference	Technique	Dataset	Distance Measure	Similarity
1	[33]	RNN, CNN, LR, RNNatt	59652 discharge summary notes, 344 Wikipedia pages	KSI (Knowledge Source Integration)	Clinical Notes
2	[34]	Classifiers used like SVM, CRF_based, Rule-Based and Aggregator	889 records of medication, 1237 of Obesity, 871 records of VA (each record is a medical document)	Jaccard Distance	Medical Documents
3	[35]	K-means	2673 medical prescriptions	Cosine Similarity	Clinical Notes
4	<b>Proposed Model</b>	<b>Classifiers used like LR, SVM, NB, DT, RF</b>	<b>1000 Healthcare Web URLs</b>	<b>Jaccard Distance, Euclidean Distance, Cosine Similarity</b>	<b>Fact-Check Healthcare Web URLs</b>

### C. Sentiment Analysis and Document Similarity Approaches

The document classification can be best achieved using document similarity measures. The amalgamation of sentiment analysis and document similarity is effective in terms of document classification as found in the literature. The deep learning techniques along with cosine similarity measures are used to successfully classify documents related to stock news based on the sentiments in literature, resulting in the merging of most relevant documents together [36]. In another approach, One-Class Support Vector Machine (OCSVM) and Latent Semantic Indexing (LSI) were used to classify text documents into positive and negative [37]. In another approach, NET-LDA model was proposed to find the semantic similarity between documents using sentiment polarity and cosine similarity approaches [38]. There are three different types of measures followed in the literature for document similarity measurement viz. Jaccard Distance, Cosine Similarity, and Euclidean Distance. However, the authors didn't find any articles with document similarity measures used along with sentiment analysis to classify documents based on their similarity. Thus, the hybrid combination of document similarity and sentiment analysis is a novel approach and can be used to detect and fact-check healthcare related misinformation. Table III displays the recent techniques of document similarity and sentiment analysis and the proposed model techniques

### D. Document Similarity and Fact-Checking

The major challenge faced in detecting misinformation is performing the fact-checking of data as there fewer benchmark datasets available specific to a certain domain like healthcare. With the enormous amount of information generated online, it is a highly challenging task to perform manual fact-checking of individual articles or blogs available online. Therefore the recent tools and techniques are automated using features from the text like sentimental features, user-specific features, grammatical features, etc. In the literature, authors have used techniques like Term Frequency Inverse Document Frequency (TF-IDF), and cosine similarity measures with k-means, Support Vector Machine, and Multilayer Perceptron to detect credibility of Indonesian news. Also, in another research, Latent Dirichlet Allocation (LDA) and Jaccard distance measures are used to detect fake news on the Buzzfeed dataset. In research to collect evidence for fake news detection word embeddings were used followed by Word Mover's distance measure to measure the similarity between the documents. However, it was observed that Word Mover's distance is very expensive for a large amount of data [39]-[42]. Table IV displays the recent techniques of detecting misinformation using document similarity and sentiment analysis. Though there are few studies handling fact-checking using document similarity measures, not major work is carried out in this field. Thus, in this paper, the authors propose a model with a hybrid combination of sentiment analysis and document similarity approach to detect and fact-check the misinformation.

TABLE III. RECENT TECHNIQUES OF DOCUMENT SIMILARITY AND SENTIMENT ANALYSIS AND THE PROPOSED MODEL TECHNIQUES

Sr. No.	Reference	Technique	Dataset	Features	Distance Measure	Application
1	[36]	Deep Neural Network	62,478 articles related to stock	Sentiment Polarity	Cosine Similarity	Stock Market News Similarity Estimation
2	[38]	NET-LDA	1518 Turkish reviews and 1K from amazon	Sentiment Polarity	Cosine Similarity	Merge semantically similar documents
3	<b>Proposed Model</b>	<b>Classifiers used like LR, SVM, NB, DT, RF</b>	<b>1000 Healthcare Web URLs</b>	<b>Sentiment Polarity and Grammatical Features</b>	<b>Jaccard Distance, Euclidean Distance, Cosine Similarity</b>	<b>Detect and Fact-Check Healthcare Web URLs</b>

TABLE IV. RECENT TECHNIQUES OF DETECTING MISINFORMATION USING DOCUMENT SIMILARITY AND SENTIMENT ANALYSIS

Sr. No.	Reference	Technique	Dataset	Features	Distance Measure	Application
1	[39]	K-Means, SVM, Multilayer Perceptron	9038 Fake news titles & 1069 Fact titles	TF-IDF	Cosine Similarity	Credibility Measurement of Indonesian News
2	[40]	Nil	Buzzfeed News	LDA	Jaccard Distance	Detect Fake News
3	[41]	Nil	Self-curated dataset	Word Embeddings	Word2Vec and Word Mover's Distance	Evidence Retrieval for Fake News
4	<b>Proposed Model</b>	<b>Classifiers used like LR, SVM, NB, DT, RF</b>	<b>1000 Healthcare Web URLs</b>	<b>Sentiment Polarity and Grammatical Features</b>	<b>Jaccard Distance, Euclidean Distance, Cosine Similarity</b>	<b>Detect and Fact-Check Healthcare Web URLs</b>

### III. PROPOSED MODEL

#### A. Model Architecture

The proposed model architecture for misinformation detection in the healthcare domain and performing fact-checking automatically is shown in Fig. 1. Sections B, C, and D describe in detail the architecture building. Section B talks about the data collection method, section C describes the features extracted and used for model building in detail, and section D explains the process of working model.

#### B. Dataset Creation

The authors have crawled 60 URLs from the web on the healthcare domain and classified them as True and False with the help of expert opinion. This dataset is used to verify and classify other URLs from the healthcare domain. Further, authors have crawled 898 web URLs related to the healthcare domain. Out of which, 280 URLs are used for training the model and 618 URLs are used for testing purposes. These 1000 URLs are the combination of true and false URLs in the healthcare domain and are classified with the help of document similarity measures, sentimental features, and grammatical features along with machine learning techniques.

#### C. Feature Extraction

There are mainly three different types of features extracted from the URLs datasets. First, the authors focus on sentimental features which include a number of positive word count, number of negative word count, percentage of positive and negative word counts, and the total number of words. In a research to find sentiments of people in a covid-19 pandemic, authors have created a large benchmark dataset based on tweets generated on the twitter [43]. Thus sentimental features are crucial in healthcare domain. In grammatical features, authors have extracted noun, pronoun, verb, and adjectives from the URL text. The third type of feature is document similarity measure. There are three measures used in this paper to fact-check the URLs with manually classified web URLs related to

healthcare. The first is Euclidean Distance, which measures the straight line distance between two points in Euclidean space. Equation1 depicts the Pythagorean formula to compute the Euclidean distance between two points x and y [44].

$$d(x, y) = d(y, x) = \sqrt{(X_1 - Y_1)^2 + (X_2 - Y_2)^2 + \dots + (X_n - Y_n)^2} = \sqrt{\sum_{i=1}^n (X_i - Y_i)^2} \quad (1)$$

In this paper, the authors have used Euclidean Distance (ED) measure as a feature computed separately for true and false URLs. The other distance measure used is Jaccard Distance (JD) measures the similarity between two documents by finding the ratio of the size of the intersection and size of the union. Equation2 shows the formula to compute Jaccard Distance between two documents to find the similarity between the documents [44].

$$J(A, B) = \frac{|A \cap B|}{|A \cup B|} = \frac{|A \cap B|}{|A| + |B| - |A \cap B|} \quad (2)$$

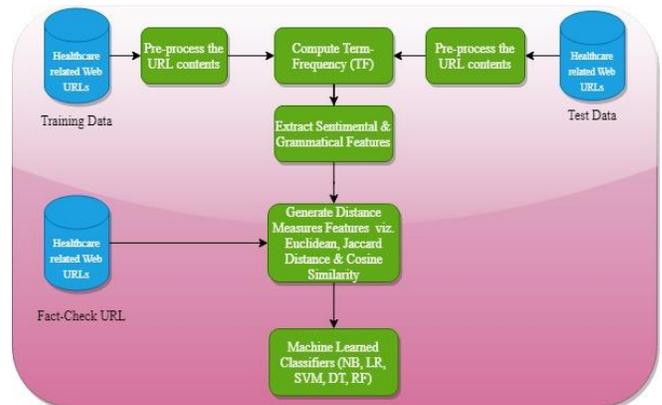


Fig. 1. Proposed Model Architecture for Misinformation Detection and Fact-Checking.

Another document similarity measure is the cosine similarity measure. Cosine similarity computes the cosine angle between the vectors. It is represented by the dot product and a magnitude between the vectors. Equation 3 shows the formula to compute the cosine similarity between two documents A and B [44].

$$\cos(\theta) = \frac{A \cdot B}{\|A\| \|B\|} \quad (3)$$

In this paper, authors have used Euclidean, Jaccard, and Cosine similarity measures as features to perform fact-checking of the URLs and thus detect misinformation in the healthcare domain. Table V lists the final set of features used in the proposed model.

TABLE V. LIST OF ALL THE FEATURES USED IN THE MODEL

Sr. No	Feature Name	Description
1	Pos_count	Positive count
2	Neg_count	Negative count
3	Per_pos_count	Percentage of a positive count
4	Per_neg_count	Percentage of a negative count
5	Total_count	Total number of words
6	Noun	Noun
7	Pro-noun	Pro-noun
8	Verb	Verb
9	Adjective	Adjective
10	ED_T	Euclidean Distance for True URLs
11	ED_F	Euclidean Distance for False URLs
12	JD_T	Jaccard Distance for True URLs
13	JD_F	Jaccard Distance for False URLs
14	C_T	Cosine Similarity for True URLs
15	C_F	Cosine Similarity for False URLs

#### D. Working Model of Misinformation Detection and Fact-Checking

In the proposed model, the training dataset is first pre-processed to remove punctuations, stop-words, numeric data, duplicate data, etc. This is required to get the cleaned data for the execution of the model. After pre-processing the URL contents, Term-Frequency (TF) is computed to find the count of terms from the URL textual contents. This term-frequency is stored in the CSV file for future use. The next step is to generate features. The first type of features is sentimental feature that focus mainly on the polarity in terms of positive and negative words of the textual contents from the URL. This is computed to the TF generated in the previous step. Along with sentimental features, grammatical features are also retrieved like noun, pronoun, verb, and adjectives. In misinformation detection, sentimental features play a significant role. It was detected that a text containing misinformation generates more negative words compared to positive words and vice-versa. Thus, more negative sentiments can lead to misinformation [17]. Thus, sentimental features and grammatical features together help to detect misinformation in this proposed model. The next aim is to perform automatic fact-checking of newly arriving URLs from the test dataset. For this reason, a fact-check URL dataset is generated. Fact-

Check URL dataset contains manually fact-checked URLs from healthcare-domain classified into True and False. To perform fact-checking of URLs from the test dataset, the authors have used standard distance measures like Euclidean Distance, Cosine Similarity, and Jaccard Distance as features. Therefore, every URL from the test dataset is first pre-processed to clean the data, term-frequency, and sentimental features are generated and finally, distance measure features are created using the standard formulas explained in section C. To compute the distance measures URL from test dataset is matched with URL from the fact-checked dataset of URLs which gives two numeric values viz. numeric value for distance between true URL from the fact-checked dataset and second numeric value with False URL from the fact-check dataset. These two values are compared and the minimum value is considered as a final feature value. This process is repeated with every URL from the test dataset and for every distance measure. When all the features are generated, machine learning classifiers are applied to test the accuracy of the model. Authors have used five machine learning state-of-the-art classifiers from the literature viz. Logistic Regression (LR), Support Vector Machine (SVM), Naïve Bayes (NB), Decision Tree (DT), and Random Forest (RF).

#### IV. RESULTS AND DISCUSSION

This section explains the experimental results carried out to evaluate the performance of the model. The proposed methodology is evaluated on five different state-of-the-art classifiers namely LR, SVM, NB, DT, and RF. Section A displays the performance matrix of the model in terms of Accuracy, Precision, Recall, and F1-Score based on the three different parameters viz. Jaccard distance, Euclidean distance, and Cosine similarity distance measures and contains the confusion matrix for the NB classifier. Section B explains the word clouds generated to show the words related to true information and false information from the URLs and Section C explains the analysis of misinformation detection.

##### A. Performance Matrix

The performance matrix is measured in terms of accuracy, precision, recall, and F1-score. Fig. 2 shows the accuracy of the proposed model based on 5 different classifiers. It was observed that NB outperformed all other models in terms of accuracy showing 98.7% accuracy whereas the decision tree classifier showed less accuracy compared to all other models showing an accuracy of 92.88%.

Fig. 3, Fig. 4 and Fig. 5 display the precision matrix, recall, and F1-score of the proposed model on various classifiers using three parameters viz. Jaccard Distance, Euclidean Distance, and Cosine Similarity measures. Table VI, Table VII and Table VIII display the performance of the distance measure technique used in terms of accuracy, precision, recall, and F1-Score per machine learning classifier. It is observed that the Jaccard Distance Measure showed maximum accuracy compared to other distance measures with maximum accuracy of 98.71% for the Naïve Bayes classifier whereas the Cosine similarity measure showed minimum accuracy of 88.19% with the Decision Tree classifier model. Euclidean Distance measure showed average accuracy in comparison with other distance measures.

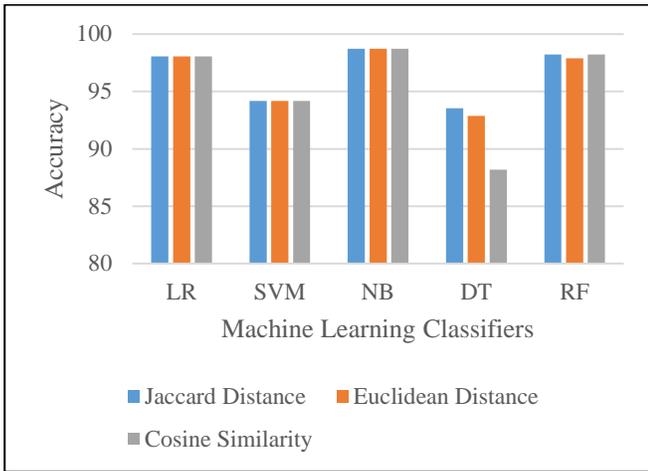


Fig. 2. Performance Matrix in Terms of Accuracy (in Percentage).

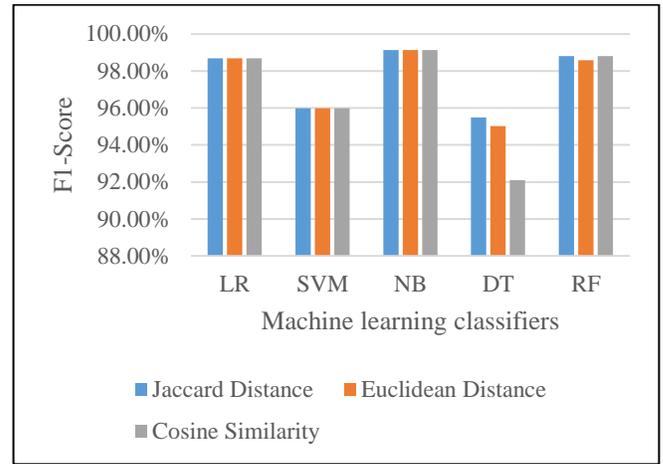


Fig. 5. Performance Matrix in Terms of F1-score (in Percentage) of the Proposed Model.

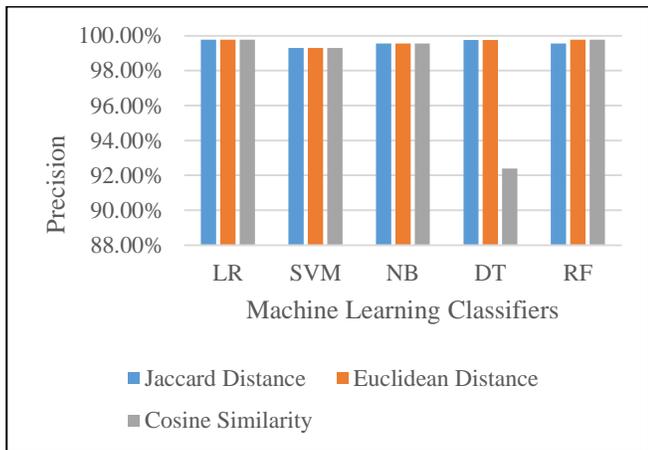


Fig. 3. Performance Matrix in Terms of Precision (in Percentage) of the Proposed Model.

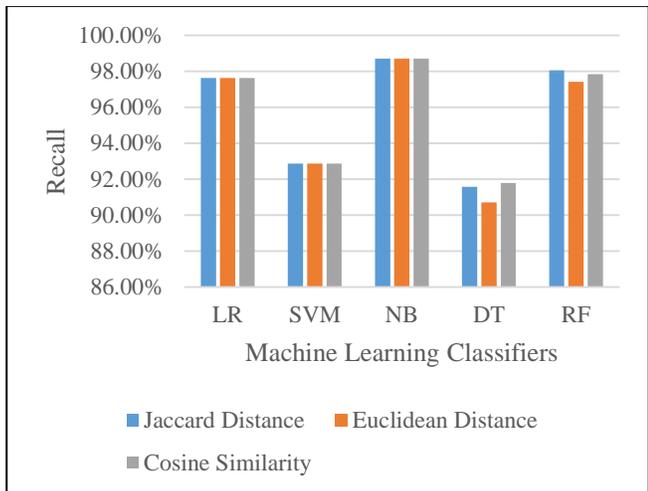


Fig. 4. Performance Matrix in Terms of Recall (in Percentage) of the Proposed Model.

TABLE VI. PERFORMANCE MATRIX OF JACCARD DISTANCE MEASURE (IN PERCENTAGE) OF THE PROPOSED MODEL

Jaccard Distance				
	Accuracy	Precision	Recall	F1-Score
LR	98.06%	99.78%	97.62%	98.69%
SVM	94.17%	99.31%	92.87%	95.98%
NB	98.71%	99.56%	98.70%	99.13%
DT	93.53%	99.76%	91.58%	95.50%
RF	98.22%	99.56%	98.06%	98.80%

TABLE VII. PERFORMANCE MATRIX OF EUCLIDEAN DISTANCE MEASURE (IN PERCENTAGE) OF THE PROPOSED MODEL

Euclidean Distance				
	Accuracy	Precision	Recall	F1-Score
LR	98.06%	99.78%	97.62%	98.69%
SVM	94.17%	99.31%	92.87%	95.98%
NB	98.71%	99.56%	98.70%	99.13%
DT	92.88%	99.76%	90.71%	95.02%
RF	97.90%	99.78%	97.41%	98.58%

TABLE VIII. PERFORMANCE MATRIX OF COSINE SIMILARITY MEASURE (IN PERCENTAGE) OF THE PROPOSED MODEL

Cosine Similarity				
	Accuracy	Precision	Recall	F1-Score
LR	98.06%	99.78%	97.62%	98.69%
SVM	94.17%	99.31%	92.87%	95.98%
NB	98.71%	99.56%	98.70%	99.13%
DT	88.19%	92.39%	91.79%	92.09%
RF	98.22%	99.78%	97.84%	98.80%

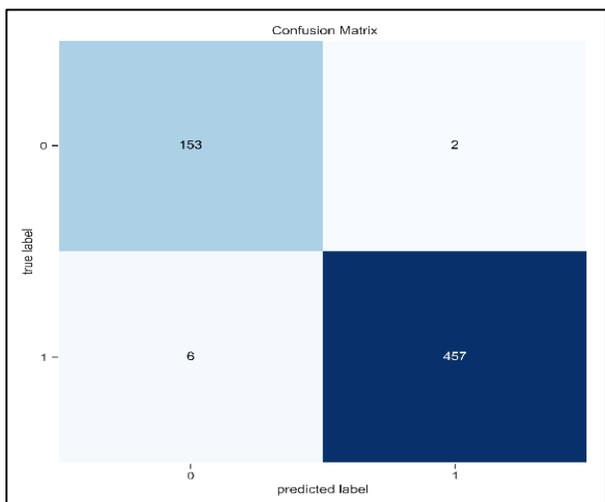


Fig. 6. Confusion Matrix for Naïve Bayes Classifier using Parameters as Euclidean Distance, Jaccard Distance & Cosine Similarity Measure.

Fig. 6 shows the confusion matrix for Naive Bayes classifier. It can be seen from the confusion matrix that 457 samples are correctly classified as true positive, whereas 153 samples are classified as true negative. False-positive and false-negative sample values are 2 and 6, respectively.

**B. Word Clouds**

Fig. 7 and Fig. 8 displays word clouds of URLs having misinformation and legitimate information respectively. It can be seen that the URLs having misinformation contain more negative words like death, false, etc. whereas URLs with true information contain more positive words like well, symptom, increase, etc. This shows that sentiment analysis can play a vital role in detecting misinformation.

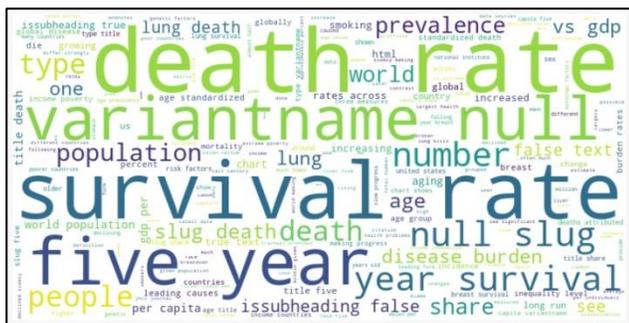


Fig. 7. Word cloud for URLs having Misinformation.



Fig. 8. Word Cloud for URLs having True Information.

**C. Analysis of Misinformation Detected**

Fig. 9 displays the average percentage of misinformation and true information in the web URLs. It can be seen from Fig. 9 that for around 200 URLs the percentage of misinformation is high compared to true information and it is at a peak for URLs ranging from 200 to 300. Fig. 10 displays the average count of positive and negative words in the URLs classified as True. It is been observed that the average positive count of words is 71% in True URLs and the negative count is 29%. Fig. 11 displays the average count of positive and negative words in the URLs classified as False. It is been observed that the average negative count of words is 62% in False URLs and the positive count of words is 38%. Thus, the authors found that for URLs with misinformation the average count of negative words is more and positive words are less. Therefore, sentiment analysis is an important feature to detect misinformation in web URLs.

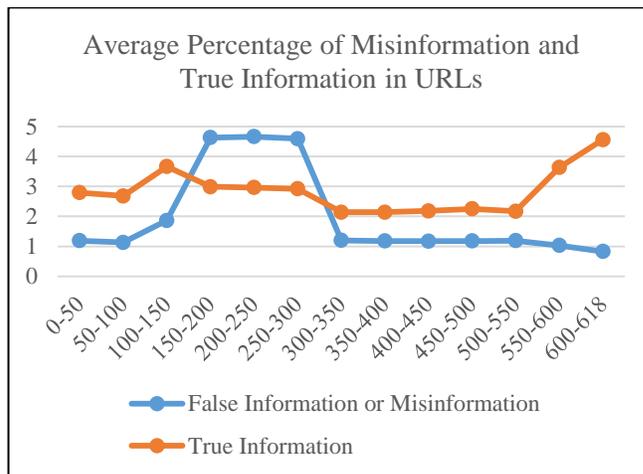


Fig. 9. A Graph showing the Average Percentage of Misinformation and true Information in URLs.

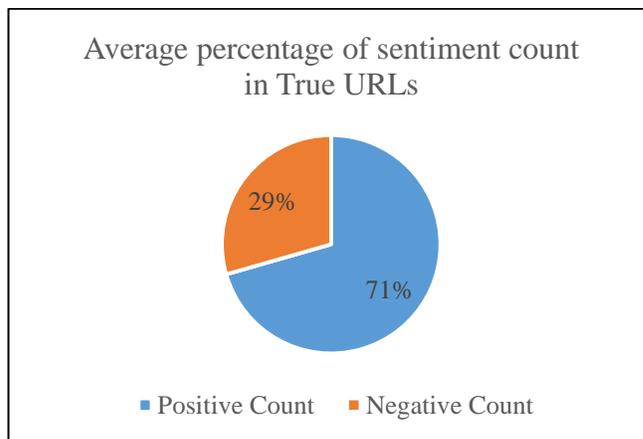


Fig. 10. A Graph showing the Average Percentage of Positive and Negative Counts in True URLs.

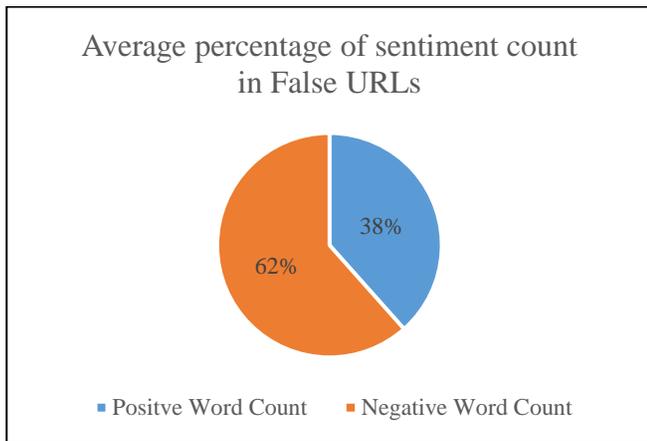


Fig. 11. A Graph Showing the Average Percentage of Positive and Negative Counts in False URLs.

## V. CONCLUSION AND FUTURE WORK

In this research, authors have proposed a model to detect and fact-check misinformation in the healthcare domain. The fact-checking of URLs using distance measures improves the performance of the model than standard techniques of manual fact-checking of data. It was observed that the sentimental features are crucial while detecting misinformation as more negative words is found in URLs containing misinformation compared to the URLs having true information. It was observed that NB outperformed all other models in terms of accuracy showing 98.7% accuracy whereas the decision tree classifier showed less accuracy compared to all other models showing an accuracy of 92.88%. Also, the Jaccard Distance measure was found to be the best in terms of accuracy compared to Euclidean distance and Cosine similarity measures. In the future, authors want to collect more URLs and observe the difference in the accuracy of the model. Also, the authors want to identify the spreaders of misinformation by keeping track of the percentage of misinformation containing in the text published by these authors.

### REFERENCES

- [1] X. Zhou and R. Zafarani, "A Survey of Fake News: Fundamental Theories, Detection Methods, and Opportunities," *ACM Comput. Surv.*, vol. 53, no. 5, 2018, doi: 10.1145/3395046.
- [2] K. Shu, D. Mahudeswaran, S. Wang, D. Lee, and H. Liu, "FakeNewsNet: A Data Repository with News Content, Social Context, and Spatiotemporal Information for Studying Fake News on Social Media," *Big Data*, vol. 8, no. 3, pp. 171–188, 2020, doi: 10.1089/big.2020.0062.
- [3] C. Carvalho, N. Klage, and E. Moench, "The persistent effects of a false news shock," *J. Empir. Financ.*, vol. 18, no. 4, pp. 597–615, 2011, doi: 10.1016/j.jempfin.2011.03.003.
- [4] S. Lewandowsky, U. K. H. Ecker, C. M. Seifert, N. Schwarz, and J. Cook, "Misinformation and Its Correction: Continued Influence and Successful Debiasing," *Psychol. Sci. Public Interes. Suppl.*, vol. 13, no. 3, pp. 106–131, 2012, doi: 10.1177/1529100612451018.
- [5] Y. Zhao, J. Da, and J. Yan, "Detecting health misinformation in online health communities: Incorporating behavioral features into machine learning based approaches," *Inf. Process. Manag.*, vol. 58, no. 1, 2021, doi: 10.1016/j.ipm.2020.102390.
- [6] P. Meel and D. K. Vishwakarma, "Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities," *Expert Syst. Appl.*, vol. 153, 2020, doi: 10.1016/j.eswa.2019.112986.

- [7] Y. Wang, M. McKee, A. Torbica, and D. Stuckler, "Systematic Literature Review on the Spread of Health-related Misinformation on Social Media," *Soc. Sci. Med.*, vol. 240, 2019, doi: 10.1016/j.socscimed.2019.112552.
- [8] I. Secosan, D. Virga, Z. P. Crainiceanu, L. M. Bratu, and T. Bratu, "Infodemia: Another enemy for romanian frontline healthcare workers to fight during the covid-19 outbreak," *Med.*, vol. 56, no. 12, pp. 1–9, 2020, doi: 10.3390/medicina56120679.
- [9] S. Tejedor, A. Pérez-Escoda, A. Ventín, F. Tusa, and F. Martínez, "Tracking websites' digital communication strategies in latin american hospitals during the COVID-19 pandemic," *Int. J. Environ. Res. Public Health*, vol. 17, no. 23, pp. 1–19, 2020, doi: 10.3390/ijerph17239145.
- [10] A. P. Worrall et al., "Readability of online COVID-19 health information: a comparison between four English speaking countries," *BMC Public Health*, vol. 20, no. 1, 2020, doi: 10.1186/s12889-020-09710-5.
- [11] A. Habib, M. Z. Asghar, A. Khan, A. Habib, and A. Khan, "False information detection in online content and its role in decision making: a systematic literature review," *Soc. Netw. Anal. Min.*, vol. 9, no. 1, 2019, doi: 10.1007/s13278-019-0595-5.
- [12] P. Kaur, R. S. Boparai, and D. Singh, "Hybrid text classification method for fake news detection," *Int. J. Eng. Adv. Technol.*, vol. 8, no. 5, pp. 2388–2392, 2019, [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85069445671&partnerID=40&md5=67b1d4b3b93f226a348b7859e1eaeff6>.
- [13] F. A. Ozbay and B. Alatas, "Fake news detection within online social media using supervised artificial intelligence algorithms," *Phys. A Stat. Mech. its Appl.*, vol. 540, p. 123174, 2020.
- [14] J. I. De Moraes, H. Q. Abonizio, G. M. Tavares, A. A. Da Fonseca, and S. Barbon, "Deciding among fake, satirical, objective and legitimate news: A multi-label classification system," in *ACM International Conference Proceeding Series*, 2019, doi: 10.1145/3330204.3330231.
- [15] K. Popat, S. Mukherjee, J. Strötgen, and G. Weikum, "Credibility assessment of textual claims on the web," in *International Conference on Information and Knowledge Management, Proceedings*, 2016, vol. 24-28-Octo, pp. 2173–2178, doi: 10.1145/2983323.2983661.
- [16] C. S. de Britto Almeida and D. A. Santos, "Text similarity using word embeddings to classify misinformation," in *CEUR Workshop Proceedings*, 2020, vol. 2607, pp. 63–68, [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-85085651452&partnerID=40&md5=dfe87346ce88014b2c2fe83b25bd1737>.
- [17] Z. Xu and H. Guo, "Using Text Mining to Compare Online Pro- and Anti-Vaccine Headlines: Word Usage, Sentiments, and Online Popularity," *Commun. Stud.*, vol. 69, no. 1, pp. 103–122, 2018, doi: 10.1080/10510974.2017.1414068.
- [18] A. Benamira, B. Devillers, E. Lesot, A. K. Ray, M. Saadi, and F. D. Malliaros, "Semi-supervised learning and graph neural networks for fake news detection," in *Proceedings of the 2019 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining, ASONAM 2019*, 2019, pp. 568–569, doi: 10.1145/3341161.3342958.
- [19] E.-S. M. El-Alfy and S. Al-Azani, "Statistical comparison of opinion spam detectors in social media with imbalanced datasets," *Commun. Comput. Inf. Sci.*, vol. 969, pp. 157–167, 2019, doi: 10.1007/978-981-13-5826-5\_12.
- [20] I. Ahmad, M. Yousaf, S. Yousaf, and M. O. Ahmad, "Fake News Detection Using Machine Learning Ensemble Methods," *Complexity*, vol. 2020, 2020, doi: 10.1155/2020/8885861.
- [21] G. L. Ciampaglia, P. Shiralkar, L. M. Rocha, J. Bollen, F. Menczer, and A. Flammini, "Computational fact checking from knowledge networks," *PLoS One*, vol. 10, no. 6, 2015, doi: 10.1371/journal.pone.0128193.
- [22] I. Agarwal and D. P. Rana, "Credibility of misinformation and the science of sentiments," *J. Adv. Res. Dyn. Control Syst.*, vol. 12, no. 7 Special Issue, pp. 1738–1745, 2020, doi: 10.5373/JARDCS/V12SP7/20202283.
- [23] M. A. Alonso, D. Vilares, C. Gómez-Rodríguez, and J. Vilares, "Sentiment analysis for fake news detection," *Electron.*, vol. 10, no. 11, 2021, doi: 10.3390/electronics10111348.
- [24] R. Asha, R. Jain, G. Das, and P. Bharadwaj, "Sentimental analysis and detection of rumours for social media data using logistic regression," *Int.*

- J. Innov. Technol. Explor. Eng., vol. 9, no. 1, pp. 2123–2126, 2019, doi: 10.35940/ijitee.A4670.119119.
- [25] B. R. Prathap, A. K. Sujatha, C. B. S. Yadav, and M. Mounika, “Polarity detection on real-time news data using opinion mining,” *Adv. Parallel Comput.*, vol. 37, pp. 90–97, 2020, doi: 10.3233/APC200124.
- [26] V. Raghupathi, J. Ren, and W. Raghupathi, “Studying public perception about vaccination: A sentiment analysis of tweets,” *Int. J. Environ. Res. Public Health*, vol. 17, no. 10, 2020, doi: 10.3390/ijerph17103464.
- [27] Y. Yang, L. Zheng, J. Zhang, Q. Cui, Z. Li, and P. S. Yu, “TI-CNN: Convolutional Neural Networks for Fake News Detection,” 2018, [Online]. Available: <http://arxiv.org/abs/1806.00749>.
- [28] C. Castillo, M. Mendoza, and B. Poblete, “Information credibility on Twitter,” *Proc. 20th Int. Conf. Companion World Wide Web, WWW 2011*, no. January, pp. 675–684, 2011, doi: 10.1145/1963405.1963500.
- [29] D. C. Edara, L. P. Vanukuri, V. Sistla, and V. K. K. Kolli, “Sentiment analysis and text categorization of cancer medical records with LSTM,” *J. Ambient Intell. Humaniz. Comput.*, 2019, doi: 10.1007/s12652-019-01399-8.
- [30] P. M. Arunkumar, S. Chandramathi, and S. Kannimuthu, “Sentiment analysis-based framework for assessing internet telemedicine videos,” *Int. J. Data Anal. Tech. Strateg.*, vol. 11, no. 4, pp. 328–336, 2019, doi: 10.1504/IJDATS.2019.103755.
- [31] A. Yadav and D. K. Vishwakarma, “A Weighted Text Representation framework for Sentiment Analysis of Medical Drug Reviews,” in *Proceedings - 2020 IEEE 6th International Conference on Multimedia Big Data, BigMM 2020*, 2020, pp. 326–332, doi: 10.1109/BigMM50055.2020.00057.
- [32] W. M. S. Yafooz and A. Alsaeedi, “Sentimental Analysis on Health-Related Information with Improving Model Performance using Machine Learning,” *J. Comput. Sci.*, vol. 17, no. 2, pp. 112–122, 2021, doi: 10.3844/jcssp.2021.112.122.
- [33] T. Bai and S. Vucetic, “Improving medical code prediction from clinical text via incorporating online knowledge sources,” in *The Web Conference 2019 - Proceedings of the World Wide Web Conference, WWW 2019*, 2019, pp. 72–82, doi: 10.1145/3308558.3313485.
- [34] X.-B. Li and J. Qin, “Anonymizing and sharing medical text records,” *Inf. Syst. Res.*, vol. 28, no. 2, pp. 332–352, 2017, doi: 10.1287/isre.2016.0676.
- [35] E. Naaz, D. Sharma, D. Sirisha, and M. Venkatesan, “Enhanced K-means clustering approach for health care analysis using clinical documents,” *Int. J. Pharm. Clin. Res.*, vol. 8, no. 1, pp. 60–64, 2016, [Online]. Available: <https://www.scopus.com/inward/record.uri?eid=2-s2.0-84965097226&partnerID=40&md5=e406b59b8e4787d8d0c5083a31862c2a>.
- [36] H. Yanagimoto, M. Shimada, and A. Yoshimura, “Document similarity estimation for sentiment analysis using neural network,” in *2013 IEEE/ACIS 12th International Conference on Computer and Information Science, ICIS 2013 - Proceedings*, 2013, pp. 105–110, doi: 10.1109/ICIS.2013.6607825.
- [37] B. Shrahan Kumar and V. Ravi, “One-class text document classification with OCSVM and LSI,” *Adv. Intell. Syst. Comput.*, vol. 517, pp. 597–606, 2017, doi: 10.1007/978-981-10-3174-8\_50.
- [38] E. Ekinci and S. I. OMURCA, “NET-LDA: A novel topic modeling method based on semantic document similarity,” *Turkish J. Electr. Eng. Comput. Sci.*, vol. 28, no. 4, pp. 2244–2260, 2020, doi: 10.3906/ELK-1912-62.
- [39] R. Arianto, S. Warnars, H. Leslie, and Y. Heryadi, “FAKE NEWS DETECTION MODEL BASED ON CREDIBILITY MEASUREMENT FOR INDONESIAN ONLINE,” vol. 99, no. 7, pp. 1571–1593, 2021.
- [40] K. Xu, F. Wang, H. Wang, and B. Yang, “Detecting fake news over online social media via domain reputations and content understanding,” *Tsinghua Sci. Technol.*, vol. 25, no. 1, pp. 20–27, 2020, doi: 10.26599/TST.2018.9010139.
- [41] H. Gong, T. Sakakini, S. Bhat, and J. Xiong, “Document similarity for texts of varying lengths via hidden topics,” *ACL 2018 - 56th Annu. Meet. Assoc. Comput. Linguist. Proc. Conf. (Long Pap.)*, vol. 1, pp. 2341–2351, 2018, doi: 10.18653/v1/p18-1218.
- [42] V. Gupta, K. Beckh, S. Giesselbach, and D. Wegener, “Supporting verification of news articles with automated search for semantically similar articles,” pp. 1–13, 2021.
- [43] U. Naseem, I. Razzak, M. Khushi, P. W. Eklund, and J. Kim, “COVIDSenti: A Large-Scale Benchmark Twitter Data Set for COVID-19 Sentiment Analysis,” *IEEE Trans. Comput. Soc. Syst.*, vol. 8, no. 4, pp. 976–988, 2021, doi: 10.1109/TCSS.2021.3051189.
- [44] P. Marjai, P. Lehotay-Kéry, and A. Kiss, “Document similarity for error prediction,” *J. Inf. Telecommun.*, 2021, doi: 10.1080/24751839.2021.1893496.

# Evaluating Deep and Statistical Machine Learning Models in the Classification of Breast Cancer from Digital Mammograms

Amel A. Alhussan<sup>1</sup>, Nagwan M. Abdel Samee<sup>2\*</sup>, Vidan F. Ghoneim<sup>3</sup>, Yasser M. Kadah<sup>4</sup>

Computer Science Department, College of Computer & Information Sciences<sup>1</sup>  
Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia<sup>1</sup>

Information Technology Department, College of Computer & Information Sciences<sup>2</sup>  
Princess Nourah bint Abdulrahman University, Riyadh, Saudi Arabia<sup>2</sup>

Computer Engineering Department, Misr University for Science and Technology, Giza, Egypt<sup>2</sup>

Biomedical Engineering Department, Helwan University, Cairo, Egypt<sup>3</sup>

Electrical and Computer Engineering Department, King Abdulaziz University, Jeddah, Saudi Arabia<sup>4</sup>

Biomedical Engineering Department, Cairo University, Giza, Egypt<sup>4</sup>

**Abstract**—The application of artificial intelligence techniques in computer aided detection and diagnosis problems has been among the most promising areas with interest from the scientific community and healthcare industry. Recently, deep learning has become the prime tool for such application with many studies focusing on developing variants that optimize diagnostic performance. Despite the widely accepted success of this class of techniques in this application by the scientific community, it is not prudent to consider it as the only tool available for such purpose. In particular, statistical machine learning offers a variety of techniques that can also be applied at a much lower computational cost. Unfortunately, the results from both strategies cannot be directly compared due to the differences in experimental setups and datasets used in available research studies. Therefore, we focus in this study on this direct comparison using the same dataset and similar data preprocessing as the input to both. We compare statistical machine learning to deep learning in the context of computer-aided detection of breast cancer from mammographic images. The results are compared using diagnostic performance metrics and suggest that simpler statistical machine learning techniques may provide better performance with simpler architectures that allow explanation of results.

**Keywords**—Computer-aided detection; computer-aided diagnosis; statistical machine learning; deep learning

## I. INTRODUCTION

Breast cancer is the most frequently diagnosed cancer and accounts for a significant portion of the total cancer related deaths among women[1]. The early detection of cancer in general, and particularly in breast cancer, is crucial to patient survival. Therefore, periodic screening was recommended for women above a certain age or before that for those women with a family history of the disease. The primary imaging modality for such screening is x-ray mammography where two images in cranio-caudal and mediolateral oblique directions are taken and examined carefully by a radiologist for early signs of abnormalities including microcalcifications [2]. The resultant images in their digital form have very high resolution and quantization level (for example, 5k resolution is common at

12-16 bits of grayscale). As a result, the process for reading such images is tiring, lengthy, costly, and prone to errors. Moreover, the shortage of radiologists compounded by increase in volume of image data due to better awareness and introduction of 3D techniques such as tomosynthesis poses a challenge for healthcare services in this area. Therefore, computer-aided diagnosis is now pursued as a possible solution to this problem. Even though many such systems were proposed early on as applications of the growing artificial intelligent systems, the digital transition of radiology departments made the utilization of such assisting tools more readily available in many applications including mammography.

Computer-aided diagnosis (CAD) is generally defined as a diagnosis made by a radiologist who uses the output of a computer analysis of the images when making his/her interpretation. CAD systems can play different roles in the diagnostic process. For example, it can be used for as pre-screening where the CAD system is utilized as the first reader then the radiologist verifies such reading and makes the final diagnosis. Alternatively, concurrent reading of images between the radiologist and the CAD system, which in this case serves as a second independent reader. Also, another approach is to make the diagnosis interactively using the CAD system where the radiologist marks suspicious areas on image and uses analysis from the CAD system to confirm the likely diagnosis. Therefore, this approach improves diagnostic performance, reduces performance intra- and inter-observer variability of radiologists, improves radiologist productivity and hence serves as a mitigation of global shortage of radiologists.

The early CAD systems relied on statistical machine learning techniques (e.g., [3]), while most recent scientific studies targeting this field were overwhelmingly using deep learning techniques (e.g., [4] [5] [6]). This is a natural consequence of the usual technology hype cycle (sometimes called Gartner hype curve) of deep learning technologies where this area is within the peak of inflated expectations. In order to speed up the process of reaching the plateau of productivity of

\*Corresponding Author

such curve with its associated wide adoption of the technology, it is important to consider comparisons with earlier technologies in order to better assess potential and realize limitations.

In this study, we address the direct comparison of statistical machine learning and deep learning techniques in the context of computer-aided detection of breast cancer from mammographic images. The same dataset and similar data preprocessing are used as the input to several techniques that represent both categories. The details of all steps of implementation are provided to allow reproducibility of results and the performance is compared using statistical diagnostic performance metrics to allow objective comparison.

Performance evaluation rests at the heart of any machine learning model[7]. It is necessary in selecting the input features and it decides which model is appropriate for each data set. This is a fact that should be considered when we select an algorithm for cancer detection, classical or deep learning-based method, for a CAD system. Currently, there are a huge number of researches[5] [8] [9] that have utilized the deep learning approaches and recommending them as they have yielded higher accuracies, above 97%. However, a comparable accuracy, 96%, has been attained using the conventional machine learning paradigms as surveyed in [10]. Therefore, a comparison of deep learning techniques with the earlier artificial intelligence techniques based on statistical machine learning would provide a valuable insight in this regard. Unfortunately, there are no studies that targeted such direct comparison with common datasets and classification tasks and hence, addressing this comparison would be a useful addition to guide researchers in this field.

This paper is organized as follows. Section II includes the literature review. Section III gives detailed description about the data set employed in this work. The methodologies used in statistical machine learning models and deep learning techniques are presented in Section IV. Sections V and VI presents the results and discussion of both statistical and deep learning methods and the comparison between them. Finally, the conclusions in Section VII summarize this work and its significant results.

## II. RELATED WORK

Pretrained CNN models such as Alex net [11], VGG[12], and Googlenet[13] are the most popular pre-trained models for image classification. A survey of 83 research studies is presented by Abdelhafiz *et al.* [14] which demonstrate the significant results gained by CNN models in breast cancer detection and classification. They discuss the datasets used and all limitations and challenges that affect the results. They show the significant results in the latest research of breast cancer classification and emphasize on the significant effects of image preprocessing techniques. They also highlighted the effects of some important customized parameters such as validation techniques, activation function, and learning rates. They found that many studies depend on pretrained models, data augmentation, batch normalization, and dropout techniques to improve their results. Shen *et al.* [15] designed CAD system based on VGG and ResNet pretrained CNN networks. The datasets used to train their machine were DDSM and INbreast

datasets. They designed batch classifier and whole image classifier to detect and classify breast cancer. The networks have been adapted by adjusting the number of layers, learning rate and number of epochs. Different techniques such as batch normalization, and data augmentation have been employed to improve the model. The achieved results surpassed the results of previous studies. Also, the CAD system that proposed by Al-antari *et al.*[16] based on Deep belief network (DBN) to automatically detect and classify breast cancer. They used two techniques for mass diagnosis, the whole mass ROIs, and Randomly extracted ROI with size 32x32, then they classify the detected masses using their proposed DBN system. The results of their proposed system outperformed other conventional classifiers. Al-masni *et al.* [17] CAD system based on CNN model that is called You Only Look Once (YOLO) technique [18] for automatic detection and classification of breast cancer. In their system, DDSM dataset is used to train and test their system, in addition to the augmented data produced by different techniques such as rotation, translation, and scaling to avoid overfitting. They also utilized number of preprocessing techniques to eliminate irrelevant characteristics of the mammograms. Their CAD system achieved 99.7% for mass detection and 97% for classification. Several studies show that the pretrained CNN models such as Resnet [19], Alexnet [20], [21] and GoogleNet [30] demonstrate higher results using unaugmented patches and more enhanced results with augmented ones. Different CNN models [22][23] show different detection and classification accuracies and performance depending on the application, techniques and datasets used. On other hand, the state-of-the-art methods in building CAD system have been compared to the deep learning-based methods in few studies such as the work done in [24] that have evaluated some of the classical methods against the CNN based system. However, the complexity of the incredible performance of the pretrained CNN networks has not been yet fairly assessed and compared to the simple conventional machine learning methods.

## III. DATA PREPARATION

In The data used in this work were obtained from the popular Mammography Image Analysis Society (MIAS) database [25]. This database was prepared from x-ray films carefully selected from the United Kingdom National Breast Screening Program and digitized with to a resolution of 50 microns using a device with a linear optical density mapping range from 0 to 3.2 and quantization of 8-bits per pixel. Then, the images were reduced to 200-micron resolution and clipped/padded to maintain size of all images at 1024x1024 pixels in the mini-MIAS version of this database, which was used in this study [26]. The database contains left and right breast images for 161 patients with a total of 322 images. The images represent samples from normal, benign and malignant cases with 208, 63 and 51 images respectively. The database provided the ground truth diagnoses for all images and exact locations of abnormalities that may be present within each image given as the center and radius of the surrounding circle for each lesion. A square region of interest (ROI) of size 32x32 was selected inside the lesion. The size of the ROI was selected this way to ensure adequate statistical representation of the lesion while keeping the size as small as possible to

subsequently allow better lesion localization ability for the developed system [3]. A database of 144 ROIs was built with equal number of normal and abnormal regions (72 each). The abnormal regions were selected from the available lesions with 41 benign and 31 malignant samples such that each of them was obtained from a different case to avoid bias in testing. Also, the samples represented the various abnormality subclasses having lesion or cluster sizes that are large enough to contain the selected ROI size. The database of labelled ROIs was then used as the input to both statistical machine learning and deep learning techniques.

#### IV. METHODS

##### A. Statistical Machine Learning Methods

In this study, several statistical machine learning techniques representing the spectrum of methods in this area are implemented and their parameters are optimized to allow proper performance comparison to be conducted. The general block diagram for all statistical machine learning systems is shown in Fig. 1.

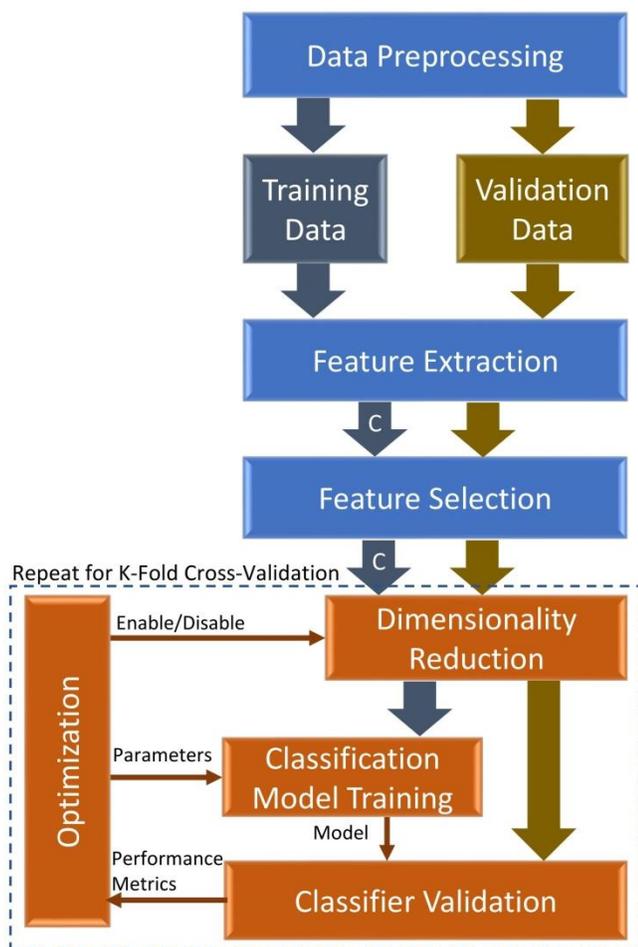


Fig. 1. Block Diagram of the Statistical Machine Learning System.

The learning system in this class of techniques is based on multiple-fold cross-validation to obtain reliable results and minimize the problem of overfitting. In particular, the data for normal and abnormal cases are randomly divided into training

and validation sets where the validation set is equal to the number of cases divided by the number of folds and the rest are assigned to the training set. In our system, the number of folds was selected to be 5 such that in each fold, 14 images from each of the normal and abnormal data are used for validation while 58 images from each are used to train the classifier. This is repeated 5 times (same as number of folds) and the results from all folds are averaged together to provide the overall system performance.

A critical part of all statistical machine learning systems is feature extraction. This is the main difference between statistical machine learning and deep learning techniques where features are implicitly learned from the data in the training process. Here, a set of 175 statistical textural features were calculated including 25 first-order features (e.g., mean, standard deviation, percentiles) [27] and 150 higher-order statistical textural features utilizing different textural analysis methods with different attributes including features from the gray-level co-occurrence matrix (GLCM) (also known as spatial gray level dependence method or SGLDM) [28], neighborhood gray tone difference matrix (NGTDM) [29] [30], spatial frequency-based method (SFM) [31], texture energy transform [32][33], fractal analysis [34], and Fourier power spectrum [35].

In order to select the best features that show statistically significant changes between normal and abnormal cases, two-sample t-test was performed between the normal and abnormal training samples in the first fold of the cross-validation process. This avoids any bias from including the validation samples in this process directly in the first fold or indirectly through their inclusion in other folds. The significance level was set at a p-value of 0.05 whereby features showing p-values lower than that are indicated as good features, while the others are deemed indiscriminate and discarded in subsequent steps. This resulted in a total of 43 selected features with 17 first-order and 26 higher-order features.

The next step in the processing pipeline is responsible for dimensionality reduction to minimize the feature space by combining features into major directions that are orthogonal to each other and spanning the directions of most variance in the data. This is done using principal component analysis (PCA) where the features are reduced to only 7 combined features or principal components that explain 95% of the variance of the data. This helps remove redundancies from multiple correlated features. Since the subsequent classification step may include techniques that rely on distance measurements, the dimensionality reduction may not always be needed. In fact, the small amount of variance that was not explained by the output of PCA may contribute to the accuracy of the classification. Therefore, the optimization of different classifiers was allowed to enable or disable such dimensionality reduction in its search for the best performance for each classifier.

The statistical machine learning system of this study included the implementation of six different families of traditional classifiers that included parametric and nonparametric classification methods. Such methods are decision trees, discriminant analysis, ensemble, k-nearest

neighbor (KNN), naïve Bayes, and support vector machines (SVM) [36]. The different parameters and variants for each classifier were optimized to reach the best performance using 5-fold cross-validation to obtain reliable estimation of the performance. The performance was measured using the accuracy (Acc), sensitivity (Sens), specificity (Spec), positive predictive value (PPV), and negative predictive value (NPV) [36]. While the accuracy is an important performance metric since it gives the percentage of correct outcomes to the total number of cases, it does not differentiate between false-positive and false-negative errors. This is problematic in the context of a computer-aided detection system where a false-negative diagnosis could have much more severe consequences than a false-positive one. The sensitivity metric addresses that where it gives the percentage of abnormal cases that were correctly diagnosed. On the other hand, the specificity gives the percentage of normal cases that were correctly diagnosed. Together they give the complete picture that allows an observer to compare different systems. For example, if two systems have the same accuracy, a system with a better sensitivity is preferred in a computer-aided detection system. The two other metrics of PPV and NPV address the post examination questions of the reliability of the results. For example, given a particular positive diagnosis outcome from a classifier, a question can be posed as how reliable such result is. Such metrics depend on disease prevalence in the patient population, unlike the sensitivity and specificity metrics.

Given the higher risk of false-negative outcomes of classification, a custom cost function that makes the cost of such errors twice that of false-positives was included in the optimization process. That is, for each classifier, the optimization process that searches through different parameter values and classifier variants is also allowed to add such custom cost function to compare the outcomes of different selections and choose the technique that minimizes this new cost function rather than the one with uniform cost for all types of error.

The results from different classifiers are reported as the cross-validation performance metrics for the best variant of optimal parameters for each classifier family. Also, to investigate the effects of dimensionality reduction and custom cost function, the best results are reported for three cases including using no dimensionality reduction or custom cost function, using custom cost function, and using both dimensionality reduction and custom cost function.

### B. Deep Learning Methods

Three deep learning networks were considered in this study. These networks are AlexNet [11][37], GoogLeNet [38], and VGG-16 [12] networks that represent different architectures with different levels of complexity as represented by the number of parameters (weights and biases). In particular, the numbers of parameters for these networks are approximately 61 million for AlexNet, 7 million for GoogLeNet, and 138 million for VGG-16. Even with the least complex of them, the huge number of parameters suggests that it is not possible to properly train such networks with the limited data set available in this study. In fact, it is difficult to collect sufficiently large data sets for such purpose for most

medical diagnosis problems given the difficulty of such collection in a standardized manner, privacy issues that prevent access without consent, as well as the severe data imbalance usually encountered in medical data with much less abnormal cases than normal cases. Therefore, two strategies are commonly utilized to mitigate this problem. The first is to use data augmentation whereby each image in the original dataset is used to generate multiple images that include the same diagnostic characteristics as the original [39]. The idea behind this approach is that changing the orientation of the abnormality in the image does not affect the diagnosis by a doctor. Therefore, using rotated or flipped versions of the image would present the network with different images that still represent the diagnostic classification of the original one. In this work, 8-fold data augmentation is used whereby each ROI in the dataset is augmented using flipping (left-right and up-down), rotation (90 and 270 degrees), image matrix transposition, in addition to their combinations of flipping left-right of 90 degrees rotated images and flipping left-right of up-down flipped images. This augmentation results in increasing the size of the dataset to 1152 samples representing 576 normal and 576 abnormal ROIs. An illustration of such augmentation is shown in Fig. 2.

Although the size of the dataset is significantly larger after augmentation, this size is still much smaller than the number of network parameters, which means that it cannot be used as is for training the network without compromising the performance due to the certain overfitting problem. Therefore, the second strategy relies on transfer learning to start from pre-trained networks and fine tune such networks to address the classification task at hand. The idea behind this strategy is that the early stages of deep learning networks are trained to extract low-level image features, which is common and similar between different image classification problems, while the rest of the network are intended to learn the specific classes for each application. Therefore, keeping such early stages intact and replacing only the application-specific final stages would make the training requirements much less demanding without sacrificing the overall performance. This is the essence of network-based transfer learning [40]. In this study, this strategy is applied using the selected networks pre-trained using ImageNet database with more than 14 million images [41]. A block diagram of the transfer learning process is shown in Fig. 3.

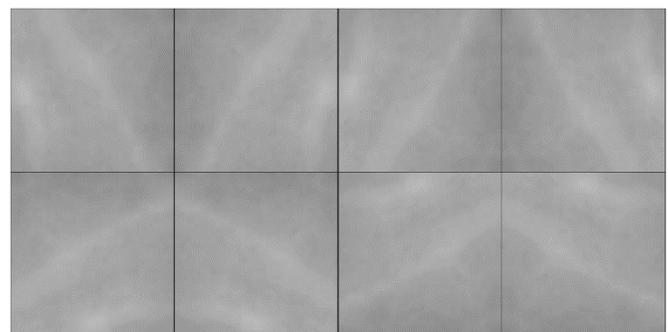


Fig. 2. Illustration of Augmentation Applied to a Sample Abnormal ROI. The Original Image is shown at the Top Left Corner with its Seven Orthogonal Transformations.

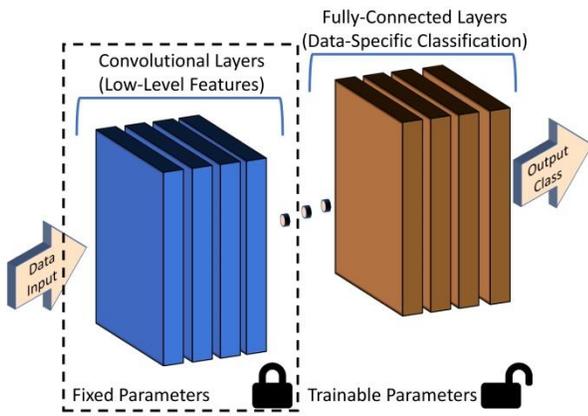


Fig. 3. Illustration of Network-based Transfer Learning.

Given that the input layer must not be altered as a part of the transfer learning strategy, the s ROIs in the dataset were resized to the respective size of each network (227×227 for AlexNet and 224×224 for the others) using bilinear interpolation with an anti-aliasing filter to meet network requirements and maintain the quality of the images and keep them free of aliasing artifacts. All networks require color images rather than grayscale images. This was dealt with by using the same grayscale image for each of the three color components of the network input. Then, the available resized dataset was divided into 3 independent sets at the beginning of the process with 60% designated as training, 20% for validation and 20% for testing. The training data are used to train the parameters of the trainable part of the network to minimize the error in the diagnostic task classification outcome using a suitable optimization technique. On the other hand, the validation data can be used to optimize the hyperparameters of the network including the optimization technique selection and parameters to optimize the performance metrics. Therefore, given that they are both utilized, even in different ways, in the optimization process, it is important to keep an independent set for testing to avoid bias and to be able to assess the presence of overfitting.

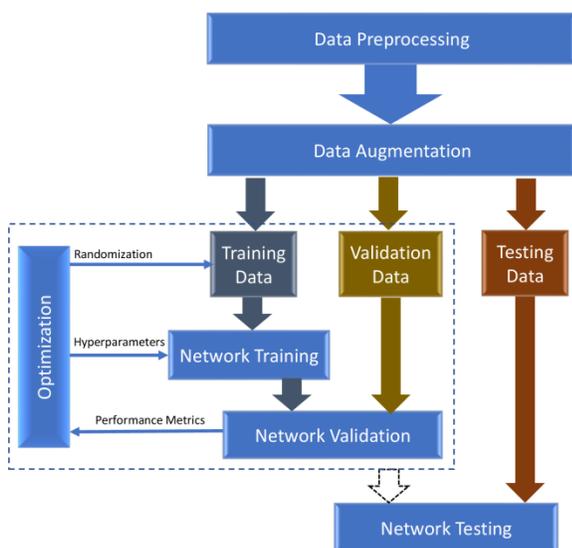


Fig. 4. Block Diagram of the Deep Learning System.

The process of estimating the optimal parameters for each network to give the best performance is a challenging optimization problem because of its high dimensionality and non-convex objective function. Therefore, stochastic optimization techniques are conventionally utilized. In this study, stochastic gradient descent with momentum (SGDM) optimizer is used with a learning rate: 0.0001, momentum term factor of 0.9,  $L_2$ -Regularization: 0.0005, and gradient threshold method of  $L_2$ -norm. The selected mini-batch size was 16 images, and the maximum number of training epochs was set to 100. Such settings were selected by observing validation results through experimentation and were used for all networks in order to allow direct comparison of their results and computational costs. A diagram representing the deep learning systems used is shown in Fig. 4.

## V. RESULTS

The statistical machine learning and deep learning systems were implemented on an academic license of Matlab 2020b (Mathworks, Inc.) with Statistics and Machine Learning and Deep Learning toolboxes. The computer system uses a quad-core Intel® Core™ i7-6700HQ CPU running at 2.60GHz and 16 GB of RAM and NVIDIA GeForce GTX 950M graphics card with 4 GB of memory and CUDA-supported graphics processing units (GPUs). The operating system is Windows 10 Home Edition (version 20H2). Due to the differences in machine configurations and software development environments, the reported computational time measurements of the conducted experiments may be specific to the machine and environment used but the findings derived from their relative values can still be useful to compare different techniques.

The results for the statistical machine learning techniques are presented in Table I. As can be observed, the best accuracy of 99.3% was obtained using a support vector machine classifier with a linear kernel with no feature standardization, uniform cost function, and no PCA feature dimensionality reduction. The second-best accuracy of 98.6% was obtained from a KNN classifier with a Minkowski distance metric, an exponent of 3, a number of neighbors (K) of 5, an inverse distance weight, standardized features, custom cost function that penalizes false negatives double that of false positives, and no PCA feature dimensionality reduction. From the point of view of computer-aided detection, the most important performance metric is the sensitivity. The best sensitivity of 100% was obtained from multiple classifiers including both classifiers with best accuracy, in addition to the other variants of the support vector machine classifier with custom cost function and PCA feature dimensionality reduction. The best specificity of 98.6%, best positive predictive value of 98.6% and best negative predictive value of 100% were also obtained by the same support vector machine classifier variant that provided the best accuracy and sensitivity results. This indicates that this particular classifier has the best overall performance among statistical classification techniques.

The results for the deep learning techniques from pretrained networks using transfer learning are shown in Table II. The results from AlexNet and GoogLeNet networks showed similar results that are consistent in all performance metrics with a

value of 98.3% each. On the other hand, the best results were obtained from the VGG-16 network with an accuracy of 98.7%, sensitivity of 99.1%, specificity of 98.3%, positive predictive value of 98.3%, and a negative predictive value of 99.1%. The training hyperparameters for all networks were the same where the optimization algorithm was stochastic gradient descent with momentum with a rate of 0.0001 and L2-regularization of 0.0005, and 8x data augmentation (total of

1152 images) divided as 60% for training, 20% for validation and 20 for testing. The training was done only to the fully-connected layers of all networks whereby the convolutional layers were kept the same as a part of the transfer learning strategy used. The training was performed on GPU with 100 training epochs and a mini-batch size of 16 with a total time of 25 minutes for AlexNet, 53 minutes for GoogLeNet, and 279 minutes for VGG-16 networks.

TABLE I. PERFORMANCE METRICS OF STATISTICAL LEARNING TECHNIQUES

Method	PCA	Cost	Accuracy	Sensitivity	Specificity	PPV	NPV
Decision Tree <sup>1</sup>	-	Custom	97.20%	97.22%	97.22%	97.22%	97.22%
Decision Tree <sup>2</sup>	-	Equal	94.40%	97.22%	91.67%	92.11%	97.06%
Decision Tree <sup>3</sup>	95%	Custom	94.40%	95.83%	93.06%	93.24%	95.71%
Discriminant Analysis <sup>4</sup>	-	Custom	96.50%	95.83%	97.22%	97.18%	95.89%
Discriminant Analysis <sup>4</sup>	-	Equal	95.10%	93.06%	97.22%	97.10%	93.33%
Discriminant Analysis <sup>4</sup>	95%	Custom	97.90%	98.61%	97.22%	97.26%	98.59%
Ensemble <sup>5</sup>	-	Custom	96.50%	97.22%	95.83%	95.89%	97.18%
Ensemble <sup>6</sup>	-	Equal	95.10%	97.22%	93.06%	93.33%	97.10%
Ensemble <sup>7</sup>	95%	Custom	95.10%	97.22%	93.06%	93.33%	97.10%
KNN <sup>8</sup>	-	Custom	98.60%	100.00%	97.22%	97.30%	100.00%
KNN <sup>9</sup>	-	Equal	97.90%	97.22%	98.61%	98.59%	97.26%
KNN <sup>10</sup>	95%	Custom	97.20%	98.61%	95.83%	95.95%	98.57%
Naïve Bayes <sup>11</sup>	-	Custom	92.40%	90.28%	94.44%	94.20%	90.67%
Naïve Bayes <sup>11</sup>	-	Equal	93.10%	88.89%	97.22%	96.97%	89.74%
Naïve Bayes <sup>12</sup>	95%	Custom	96.50%	98.61%	94.44%	94.67%	98.55%
SVM <sup>13</sup>	-	Custom	97.20%	100.00%	94.44%	94.74%	100.00%
SVM <sup>14</sup>	-	Equal	99.30%	100.00%	98.61%	98.63%	100.00%
SVM <sup>14</sup>	95%	Custom	97.90%	100.00%	95.83%	96.00%	100.00%

<sup>1</sup>Maximum number of splits: 4

<sup>2</sup>Maximum number of splits: 13

<sup>3</sup>Maximum number of splits: 12

<sup>4</sup>Linear discriminant

<sup>5</sup>Method: Bag, Number of learning cycles: 13

<sup>6</sup>Method: Bag, Number of learning cycles:119

<sup>7</sup>Method: LogitBoost, Number of learning cycles: 11

<sup>8</sup>Minkowski distance, Number of neighbors: 5, Distance weight: Inverse, Standardized data

<sup>9</sup>Cosine distance, Number of neighbors: 3, Distance weight: Inverse, Standardized data

<sup>10</sup>City block distance, Number of neighbors: 5, Distance weight: Squared inverse

<sup>11</sup>Normal kernel

<sup>12</sup>Triangle kernel

<sup>13</sup>Linear kernel, Standardized data

<sup>14</sup>Linear kernel

TABLE II. PERFORMANCE METRICS OF DEEP LEARNING TECHNIQUES\*

Network	Training Time (minutes)	Accuracy	Sensitivity	Specificity	PPV	NPV
AlexNet	25	98.26%	98.26%	98.26%	98.26%	98.26%
GoogLeNet	53	98.26%	98.26%	98.26%	98.26%	98.26%
VGG-16	279	98.70%	99.13%	98.26%	98.28%	99.12%

\*Training options: Stochastic Gradient Descent with Momentum (SGDM) optimizer, Mini-Batch Size: 16, Maximum number of training epochs: 100, Learning rate: 0.0001, Data shuffling: every epoch, Validation frequency: 10 steps, Validation Patience: infinity, L2-Regularization: 0.0005, Execution environment: GPU.

In order to better visualize the results and allow direct comparison between all techniques from both statistical and deep learning approaches, the results from all methods are shown in a graphical form in Fig. 5 and Fig. 6. In Fig. 5, the accuracy for all methods is shown as a square marker that varies in color for different variants. On the other hand, to distinguish the sensitivity and specificity values on the plot, the sensitivity is marked with an upward-pointing triangle, while the specificity is marked as a downward-pointing triangle. This provides an easy visual comparison of the accuracy, sensitivity and specificity values from all techniques. This also allows

direct visualization of those techniques where specificity values are higher than those of the sensitivity. In Fig. 6, a similar strategy was used to mark the results of positive predictive values as circles, while those of negative predictive values as asterisks. It is clear that deep learning techniques provide better results than several statistical learning techniques, but they are comparable to several other techniques. Furthermore, the results indicate that deep learning techniques are outperformed by a support vector machine classifier variant in all performance metrics and by several classifiers when the sensitivity metric is emphasized.

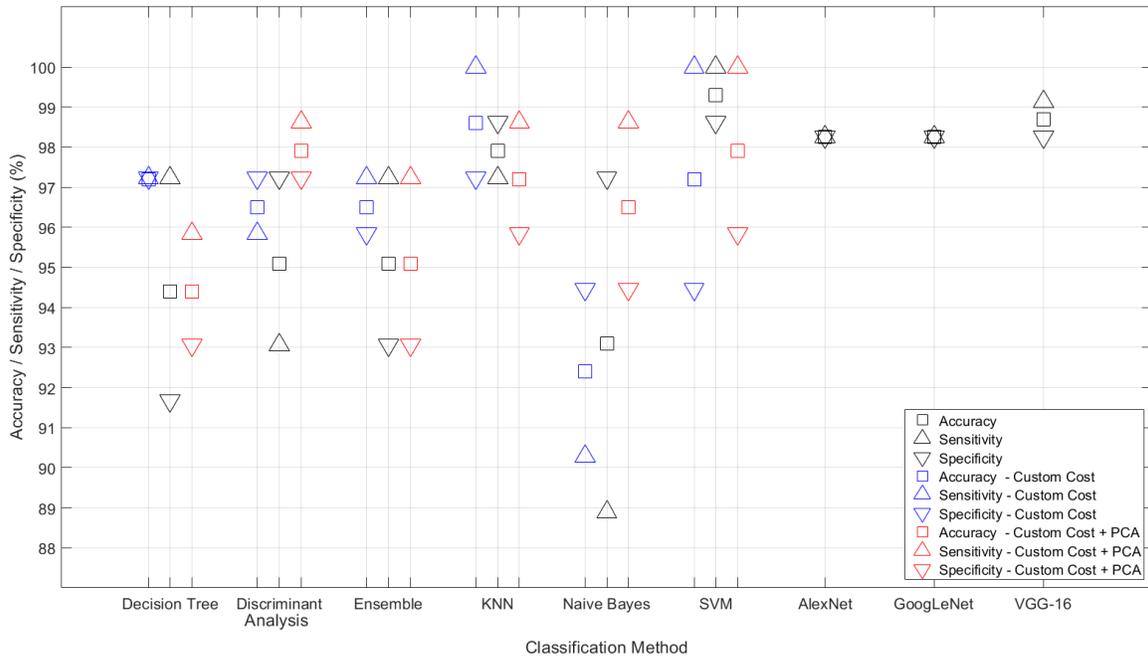


Fig. 5. Comparison of the Results of all Techniques with respect to Accuracy, Sensitivity, and Specificity (or Pretest) Performance Metrics.

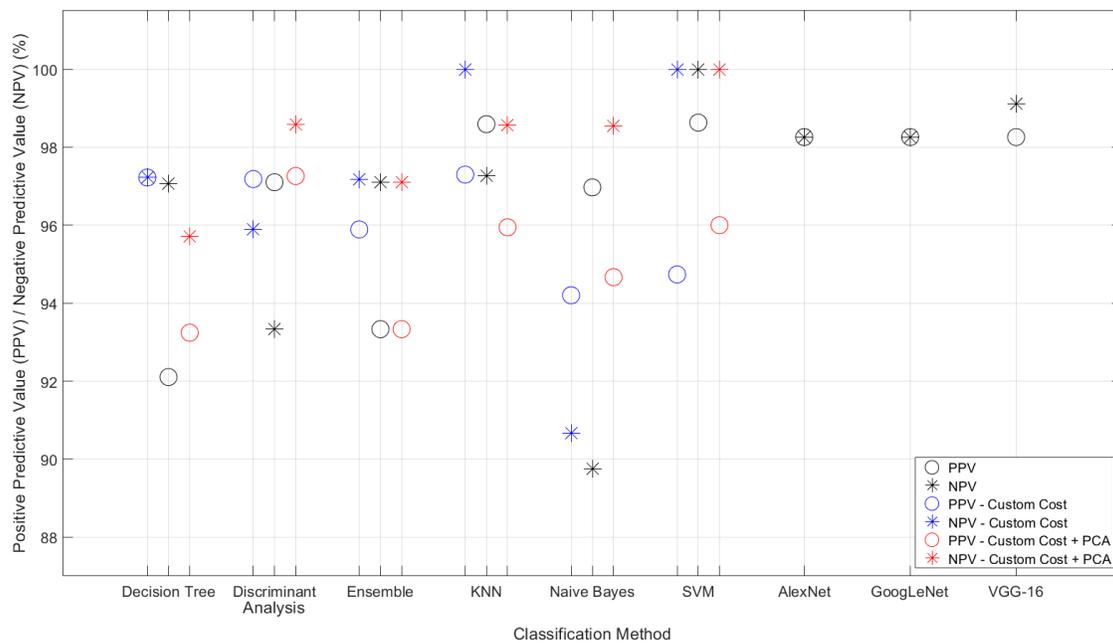


Fig. 6. Comparison of the Results of all Techniques with respect to Positive Predictive Value and Negative Predictive Value (or Post-Test) Performance Metrics.

## VI. DISCUSSION

The results suggest that the performance of statistical classification and deep learning methods are both generally acceptable with performance metrics mostly well above 90%. The best result was obtained with a statistical classification technique, which is clearly a simpler, faster alternative to the deep learning methods. While all statistical learning techniques took less than a minute to train, the computational requirements of training deep learning networks were much more demanding with training times up to 279 minutes even though transfer learning was used to keep the convolutional weights the same. Even though deep learning has been heavily emphasized in most recent research studies in the field of computer-aided diagnosis, the results of this work provide an objective comparison that suggests that simpler traditional approaches may yield comparable if not better results.

The results of all techniques showed sensitivity and specificity values that are generally close as they should be in clinical practice. Given that the data used were balanced with equal numbers of normal and abnormal cases, the accuracy values are the average of those of the sensitivity and specificity where the accuracy is exactly in the middle. It should be noted that the results for several classifiers showed higher values for specificity than sensitivity such as all variants of discriminant analysis, one variant of KNN, and two variants of Naïve Bayes classifiers. Even though some of these classifiers provide good overall accuracy, they are not suitable for computer-aided detection especially in screening studies.

The results of statistical classifier variants indicate that effect of using a custom cost function varied across different variants, but the sensitivity was improved or remained the same in all variants after applying such customization. This was particularly evident in the KNN classifier where the application of such customization provided significant improvement becoming the second-best statistical classifier and showing better accuracy than two deep learning networks with a sensitivity that is better than all of them. Therefore, it is suggested that this customization is considered in experimental evaluation of different statistical classification techniques. On the other hand, the results of using PCA for dimensionality reduction along with custom cost function showed a desirable effect of making the sensitivity values go above those of the specificity for the same classifier. This is evident in discriminant analysis and Naïve Bayes classifiers in particular. This allows the use of such classifier variants in computer-aided detection rather than discarding them as suggested above. Therefore, it is suggested that such dimensionality reduction is considered in such cases when sensitivity is lower than specificity. It should be noted that the explicability of the results of the system given that the features used and their weights are explicitly defined in the eigenvectors (principal components) of PCA outcomes.

As a part of the ongoing efforts to develop regulatory standards to govern the artificial intelligence solutions, an emphasis on explicability, or the ability to explain the outcomes, is a requirement that clinical systems must be able to

meet. This is clearly an advantage for such traditional methods where simpler equations can be used to do that. On the other hand, this is largely not possible with deep learning methods due to the complexity of the networks structure and its huge number of parameters that make it difficult to understand the decision-making process inside the network and also render such networks prone to such issues as data gaps and overfitting. This is particularly evident in medical systems because of the much less data sizes available and also the data imbalance where several abnormal classes can be significantly underrepresented in the training and testing processes.

The yielded results in this research using the AlexNet have surpassed the recent results achieved in the literature. The overall accuracy of the AlexNet, GoogLeNet on the MIAS Dataset achieved in [42], and [9] was 95.70%, 91.58% respectively. And as depicted in Table I, the conventional machine learning approached has yielded an extraordinary result that is greater than the results achieved the pretrained CNN networks. It also surpasses the current results achieved in the literature. The retrieved accuracy in the work done in [43] using SVM, and KNN on the MIAS database was 87.69%, and 88.54% respectively. The higher performance of the state-of-art classification methods retrieved here in this work has been achieved by the employed image augmentation paradigm. The data augmentation has helped in increasing the size of the training and testing data. The augmented images have been shuffled before being submitted to the classification models. In addition, the data has been split into three totally independent subsets for training, validation, and testing subset to minimize the problem of overfitting. For statistical machine learning methods, the use of K-fold cross-validation explained in the Methods section also addresses the overfitting problem. The variations across different experiments were found to be less than 1% indicating that the proposed framework does not suffer from overfitting.

## VII. CONCLUSION

In this study, direct comparison between the performances of statistical machine learning to deep learning in the context of computer-aided detection of breast cancer from mammographic images was performed. The results are compared using diagnostic performance metrics and suggest that simpler statistical machine learning techniques may provide better performance with simpler architectures that require much fewer demanding computations while allowing explanation of results. In particular, a support vector machine classifier variant provided a better performance overall, while other statistical machine learning techniques such as KNN classifier variants provided comparable results to those of three widely used deep learning networks. The obtained accuracies above 98% using both classical and deep learning models surpassed reported results in the literature. Furthermore, the present study suggests that statistical machine learning based methods might be closer to meeting regulatory approval requirements for clinical use. This also emphasizes the importance of addressing such issues as data gaps and explicability of outcomes in deep learning techniques to boost their transition to clinical use.

#### ACKNOWLEDGMENT

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Ab-dulrahman University through the Research Funding Program (Grant No# FRP-1440-30).

#### REFERENCES

- [1] U. Bick and F. Diekmann, "Mammographic Signs of Malignancy," in *Digital Mammography*, Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 175–185.
- [2] M. P. Sampat, M. K. Markey, and A. C. Bovik, "Computer-Aided Detection and Diagnosis in Mammography," in *Handbook of Image and Video Processing*, Elsevier Inc., 2005, pp. 1195–1217.
- [3] Y. M. Kadah, A. A. Farag, J. M. Zurada, A. M. Badawi, and A. B. M. Youssef, "Classification algorithms for quantitative tissue characterization of diffuse liver disease from ultrasound images," *IEEE Trans. on Med. Imaging.*, vol. 15, no. 4, pp. 466–478, 1996.
- [4] M. A. Al-Antari, M. A. Al-Masni, S. U. Park, J. Park, M. K. Metwally, Y. M. Kadah, S. M. Han, and T. S. Kim, "An Automatic Computer-Aided Diagnosis System for Breast Cancer in Digital Mammograms via Deep Belief Network," *J. Med. Biol. Eng.*, vol. 38, no. 3, pp. 443–456, Jun. 2018.
- [5] M. A. Al-antari, S. M. Han, and T. S. Kim, "Evaluation of deep learning detection and classification towards computer-aided diagnosis of breast lesions in digital X-ray mammograms," *Comput. Methods Programs Biomed.*, vol. 196, p. 105584, Nov. 2020.
- [6] W. E. Fathy and A. S. Ghoneim, "A deep learning approach for breast cancer mass detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 1, pp. 175–182, 2019.
- [7] D. J. Hand, "Evaluating Statistical and Machine Learning Supervised Classification Methods," in *Statistical Data Science*, pp. 37–53, Jul. 2018.
- [8] F. Mohanty, S. Rup, B. Dash, B. Majhi, and M. N. S. Swamy, "An improved scheme for digital mammogram classification using weighted chaotic salp swarm algorithm-based kernel extreme learning machine," *Appl. Soft Comput.*, vol. 91, p. 106266, Jun. 2020.
- [9] S. A. Hassan, M. S. Sayed, M. I. Abdalla, and M. A. Rashwan, "Breast cancer masses classification using deep convolutional neural networks and transfer learning," *Multimed. Tools. and Appl.*, vol. 79, no. 41, pp. 30735–30768, Aug. 2020.
- [10] G. Meenalochini and S. Ramkumar, "Survey of machine learning algorithms for breast cancer detection using mammogram images," *Proc. Mater. Today*, vol. 37, no. Part 2, pp. 2738–2743, Jan. 2021.
- [11] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," *Commun. ACM.*, vol. 60, no. 6, pp. 84–90, Jun. 2017.
- [12] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," [Online]. Available: <http://arXiv:1409.1556>.
- [13] C. Szegedy, S. Ioffe, V. Vanhoucke, and A. A. Alemi, "Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning," [Online]. Available: <http://arXiv:1602.07261>.
- [14] D. Abdelhafiz, C. Yang, R. Ammar, and S. Nabavi, "Deep convolutional neural networks for mammography: advances, challenges and applications," *BMC bioinform.*, vol. 20, no. Suppl 11, Jun. 2019.
- [15] L. Shen, L. R. Margolies, J. H. Rothstein, E. Fluder, R. McBride, and W. Sieh, "Deep Learning to Improve Breast Cancer Detection on Screening Mammography," *Sci. Rep.*, vol. 9, no. 1, pp. 1–12, 2019.
- [16] Al-Antari M.A., M. A. Al-Masni, and T. S. Kim, "Deep Learning Computer-Aided Diagnosis for Breast Lesion in Digital Mammogram," *Adv Exp Med Biol.*, vol 1213. Springer, 2020.
- [17] M. A. Al-Masni M. A. Al-Antari, J. M. Park, G. Gi, T. Y. Kim, P. Rivera, E. Valarezo, M.T. Choi, S.M. Han, and T. S. Kim, "Simultaneous detection and classification of breast masses in digital mammograms via a deep learning YOLO-based CAD system," *Comput. Methods. Programs. Biomed.*, vol. 157, pp. 85–94, Apr. 2018.
- [18] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, vol. 2016-December, pp. 779–788, 2016.
- [19] N. Ismail and C. Sovuthy, "Breast Cancer Detection Based on Deep Learning Technique," *Proc. 2019 Int. UNIMAS STEM 12th Eng. Conf. (EnCon)*, pp. 89–92, 2019.
- [20] E. L. Omonigho, M. David, A. Adejo, and S. Aliyu, "Breast Cancer:Tumor Detection in Mammogram Images Using Modified AlexNet Deep Convolution Neural Network," *Proc. 2020 Int. Conf. Math. Comput. Eng. Comput. Sci. (ICMCECS)*, pp. 1–6, 2020.
- [21] A. Marchesi et al., "The Effect of Mammogram Preprocessing on Microcalcification Detection with Convolutional Neural Networks," *Proc. 2017 IEEE 30th Int. Symp. Comput.-Based Med. Sys. (CBMS)*, vol. 2017-June, pp. 207–212, Jun. 2017.
- [22] S. A. Agnes, J. Anitha, S. I. A. Pandian, and J. D. Peter, "Classification of Mammogram Images Using Multiscale all Convolutional Neural Network (MA-CNN)," *J. Med. Sys.*, vol. 44, no. 1, pp. 1–9, Dec. 2019.
- [23] R. S. Patil and N. Biradar, "Automated mammogram breast cancer detection using the optimized combination of convolutional and recurrent neural network," *Evol. Intell.*, pp. 1–16, Apr. 2020.
- [24] T. Kooi, G. Litjens, B. Van Ginneken, A. Gubern-Mérida, C. I. Sánchez, R. Mann, A. den Heeten, and N. Karssemeijer, "Large scale deep learning for computer aided detection of mammographic lesions," *Med. Image Anal.*, vol. 35, pp. 303–312, Jan. 2017.
- [25] J. Suckling, J. Parker, D. Dance, S. Astley, I. Hutt, and et al., « Mammographic Image Analysis Society (MIAS) database v1.21 », [Online]. Available: <https://www.repository.cam.ac.uk/handle/1810/250394>.
- [26] J. Suckling, S. Astley, D. Betal, N. Cerneaz, D. Dance, et al, "The Mammographic Image Analysis Society Digital Mammogram Database, Int. Congr. Ser. - Excerpta Med., Vol. 1069, pp375-378. [Online]. Available: <http://peipa.essex.ac.uk/info/mias.html>
- [27] Z. Abduh, M. A. Wahed, and Y. M. Kadah, "Robust computer-Aided detection of pulmonary nodules from chest computed tomography," *J. Med. Imaging. Health. Inform.*, vol. 6, no. 3, pp. 693–699, Jun. 2016.
- [28] R. M. Haralick, I. Dinstein, and K. Shanmugam, "Textural Features for Image Classification," *IEEE Trans. Syst. Man Cybern.: Syst.*, vol. SMC-3, no. 6, pp. 610–621, 1973.
- [29] J. S. Weszka, C. R. Dyer, and A. Rosenfeld, "A Comparative Study of Texture Measures for Terrain Classification," *IEEE Trans. Syst. Man Cybern.: Syst.*, vol. SMC-6, no. 4, pp. 269–285, 1976.
- [30] M. Amadasun and R. King, "Textural Features Corresponding to Textural Properties," *IEEE Trans. Syst. Man Cybern.: Syst.*, vol. 19, no. 5, pp. 1264–1274, 1989.
- [31] C. M. Wu and Y. C. Chen, "Statistical feature matrix for texture analysis," *CVGIP-GRAPH. MODEL. IM.*, vol. 54, no. 5, pp. 407–419, Sep. 1992.
- [32] K. I. Laws, "Rapid Texture Identification," *Proc. SPIE 0238, Image Proc. Missile Guid.*, Dec. 1980, vol. 0238, pp. 376–381.
- [33] R. M. Haralick, "Image texture survey," in *Handbook of Statistics*, vol. 2. Elsevier, pp. 399–415, 1982.
- [34] P. Shanmugavadivu and V. Sivakumar, "Fractal dimension based texture analysis of digital images," *Procedia Eng.*, vol. 38, pp. 2981–2986, 2012.
- [35] M. I. Owis, A. B. M. Youssef, and Y. M. Kadah, "Characterisation of electrocardiogram signals based on blind source separation," *Med. Biol. Eng. Comput.*, vol. 40, no. 5, pp. 557–564, 2002.
- [36] M. Sugiyama, *Introduction to Statistical Machine Learning*, Morgan Kaufmann, Elsevier, 2016.
- [37] O. Russakovsky, J. Deng, H. Su, J. Krause S. Satheesh S. Ma, Z. Huang, A. Karpathy, A. Khosla, M. Bernstein, and A.C. Berg, "ImageNet Large Scale Visual Recognition Challenge," *Int. J. Comput. Vis.*, vol. 115, no. 3, pp. 211–252, Dec. 2015.
- [38] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Oct. 2015, pp. 1–9.

- [39] C. Shorten and T. M. Khoshgoftaar, "A survey on Image Data Augmentation for Deep Learning," *J. Big Data*, vol. 6, no. 1, pp. 1-48, Dec. 2019.
- [40] C. Tan, F. Sun, T. Kong, W. Zhang, C. Yang, and C. Liu, "A survey on deep transfer learning," *Lect. Notes Comput. Sci.*, Oct. 2018, vol. 11141 LNCS, pp. 270–279.
- [41] J. Deng, W. Dong, R. Socher, L.-J. Li, Kai Li, and Li Fei-Fei, "ImageNet: A large-scale hierarchical image database," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, pp. 248–255, 2010.
- [42] E. L. Omonigho, M. David, A. Adejo, and S. Aliyu, "Breast Cancer:Tumor Detection in Mammogram Images Using Modified AlexNet Deep Convolution Neural Network," *Proc. Int. Conf. Math. Comput. Eng. Comput. Sci. (ICMCECS 2020)*, pp. 1-6, 2020.
- [43] V. Devakumari, "A Hybrid Algorithm with Modified SVM and KNN for Classification of Mammogram Images using Medical Image Processing with Data Mining Techniques," *Eur. J. Mol. Clin. Med.*, vol. 7, no. 10, pp. 2956–2964, 2021.

# Arabic Document Classification by Deep Learning

Taghreed Alghamdi<sup>1</sup>

Department of Computer Science  
College of Computer Science and  
Engineering, University of Jeddah  
Jeddah, Saudi Arabia

Samia Snoussi<sup>2</sup>

Department of Computer Science  
and Intelligence, College of  
Computer Science and Engineering  
University of Jeddah, Jeddah,  
Saudi Arabia

Lobna Hsairi<sup>3</sup>

Data Science Department  
University of Jeddah and Tunis  
ElManar University  
Saudi Arabia, Tunisia

**Abstract**—In this paper, we show how to classify Arabic document images using a convolutional neural network, which is one of the most common supervised deep learning algorithms. The main goal of using deep learning is its ability to automatically extract useful features from images, which eliminates the need for a manual feature extraction process. Convolutional neural networks can extract features from images through a convolution process involving various filters. We collected a variety of Arabic document images from various sources and passed them into a convolutional neural network classifier. We adopt a VGG16 pre-trained network trained on ImageNet to classify the dataset of four classes as handwritten, historical, printed, and signboard. For the document image classification, we used VGG16 convolutional layers, ran the dataset through them, and then trained a classifier on top of it. We extract features by fixing the pre-trained network's convolutional layers, then adding the fully connected layers and training them on the dataset. We update the network with the addition of dropout by adding after each max-pooling layer and to the fourteen and the seventeenth layers which are the fully connected layers. The proposed approach achieved a classification accuracy of 92%.

**Keywords**—Arabic document; document classification; deep learning; convolutional neural network (CNN); pre-trained network

## I. INTRODUCTION

Documents classification is traditionally considered an important task and the first step in several document image processing pipelines, including document retrieval, information extraction, and text recognition. The initial classification of documents into various predefined classes not only makes various document processing activities easier but also saves time. It's also possible to enhance document processing systems' overall efficiency [1]. A wide range of classification problems can be solved using the deep learning technique. The ability and flexibility for changeability in the deep learning model with a wide spectrum of datasets make the deep learning algorithm the most important method for the classification task [2]. Several approaches for document image classification have been proposed. There are three approaches to consider. The first category makes use of the document images' layout/structural similarity. Extracting the basic document components and then using them for classification is time-consuming. The creation of local and/or global image descriptors is the focus of the second category of work. These descriptors are then used to categorize documents. Extracting

local and global features takes a long time. Finally, the third category of methods employs CNN to automatically learn and extract features from document images, which are then categorized. With CNN's improved success in recent years, it's become easier to distinguish images without having to extract hand-crafted elements. It's the most commonly used neural network model for image classification [6]. Deep learning is preferred in image processing applications because it produces fast and significant results. Several problems in image processing and understanding have been solved using deep learning methods, including document image classification, handwriting recognition, and blind image quality assessment. Previously, various shallow-structure learning methods and handcrafted features were used to solve these issues [7].

We use supervised deep learning algorithms to identify Arabic document images in this paper. Because Arabic is a very rich language with complicated morphology, it has a very different and challenging structure than other languages. Hundreds of millions of people utilize it, and its internet presence is continually expanding. Furthermore, Arabic has several distinct characteristics that render automated handling and understanding of the Arabic language difficult and interesting [3]. As a result, it's critical to create an Arabic text classifier to deal with this difficult language. The importance of document classification stems from the vast number of Arabic document images distributed through many sources from different classes, the majority of which contain a significant amount of important knowledge. Manually classifying Arabic document images takes a long time and is extremely difficult. However, it has become possible to classify Arabic document images into their appropriate classes without requiring human intervention. This paper aims to use deep learning to introduce a model for classifying Arabic documents. The proposed deep learning model is trained using several different Arabic document image classes. It can differentiate between different classes, so it operates as multiple classifiers. The model can then be used to classify an Arabic document image that has been supplied after training. This paper is organized as follows. The current section provides a quick overview of the paper's topic and structure. The second section discusses related document classification studies. The third section discusses image recognition using deep learning. The CNN classification system is defined briefly in the fourth section. The fifth section summarizes the evaluation and its results. The final section summarizes the paper and suggests future work.

## II. RELATED WORK

The proliferation and subsequent usefulness of deep learning techniques in a wide range of machine learning tasks have been extensively discussed in the literature over the last decade. Deep neural networks have shown outstanding results in a variety of fields, including document image classification [3].

The classification of document images for the Arabic language is a subject that has received little attention.

Abdulmunim et al. [4] proposed a header-words-based printed Arabic document image classification and retrieval system based on a decision tree classifier enhanced by the bagging technique. This document's Arabic header words are detected by the proposed system. In addition, sets of discriminative features are extracted from detected header words to correctly classify them to the appropriate class. Several structural and statistical features specific to Arabic scripts can be observed. On the official printed Arabic document dataset, the experimental tests score 97.35 % for precision. This dataset contains images of various types of official printed Arabic documents collected from a variety of official websites, including ministries, universities, government departments, and other official states. The dataset includes letters, records, books, forms, notices, administrative instructions, and other official Arabic documents.

Al-Khurabi et al. [5] applied this work to Arabic documents, proposing an Arabic document Image Classification system based on Artificial Neural Networks on a set of 120 captured document images types such as text, geometric, and photographic images. This system was divided into two parts, the first of which was image processing. The second part uses an Artificial Neural Network to classify document images based on the contents into the appropriate class. It received an overall recognition rate of 86%.

On the other hand, many works in the literature in various languages, including English, have addressed the topic of document image classification.

In the field of document classification, Afzal et al. [1] used the deep Convolutional Neural Networks model (CNN). They created a network (except for the last fully connected layer) using weights from AlexNet, which was trained on images from ImageNet, in this study. The proposed network has five convolutional layers, which give the fully connected layer a lot more features for classification. On the Tobacco-3428 Legislation dataset, with 100 samples per class used for training and validation, the proposed method achieved an accuracy of 77.6%.

Kölsch et al. [6] propose a two-stage approach that combines automated deep CNN feature learning with efficient training using Extreme Learning Machines (ELM). As compared to a previous Convolutional Neural Network (CNN) method in [1] accuracy was achieved at 83.24% on the Tobacco-3428 Legislation dataset, resulting in a relative error reduction of 25%.

It's important to highlight the following crucial differences between the proposed approach and previous approaches: Though deep CNN-based approaches have made considerable progress in recent years and are now the current state-of-the-art, training these networks takes a long time. For the classification of Arabic document images, we propose a convolutional neural network supervised deep learning algorithm. To identify the dataset of four classes as handwritten, historical, typed, and signboard, we use VGG16 pertained weights that were trained on ImageNet. We used a convolutional neural network classifier to classify different classes of Arabic document images obtained from various sources. We used VGG16 convolutional layers, ran the dataset through convolutional layers, and then trained a classifier on top of that for Arabic document image classification. We extract features from the pre-trained network's convolutional layers by freezing them, then adding the fully connected layers and training them on the dataset. We added dropout after each max-pooling layer and to the fourteenth and seventeenth layers, which are the fully connected layers, to update the network. The proposed approach had a classification rate of 92%.

TABLE I. COMPARISON BETWEEN THE PROPOSED APPROACH AND PREVIOUS APPROACHES

Authors	Approach	dataset	Language of Dataset	Classification rate
Abdulmunim et al. [4]	Decision Tree Classifier and Bagging Technique to improve the performance of classification.	Official Arabic printed document images were collected from different authorized websites.	Document images in the Arabic language.	97.35%
al-Khurabi et al. [5]	The proposed system used Artificial Neural Network(NN)	Set of 120 captured document images types.	Document images in the Arabic language.	86%
Afzal et al. [1]	The proposed CNN model used pertained weights from a network (AlexNet)	Tobacco-3428 Legislation	Document images in the English language.	77.6%
Kölsch et al. [6]	The proposed CNN model used pertained weights from a network (AlexNet) and Extreme Learning Machines (ELM)s which provide real-time training	Tobacco-3428 Legislation dataset	Document images in the English language.	83.24%
The proposed work	The proposed approach is based on a convolutional neural network supervised deep learning algorithm. the CNN model uses pertained weights from a network (VGG16) with the addition of the dropout layer applied after each VGG block.	Arabic document images were collected from different sources.	Document images in the Arabic language.	92%

It should be noted that the pre-training in the proposed method did not previously apply to the classification of Arabic document images. The [1] is the first attempt to classify document images using a pre-trained model. Table I compares the proposed approach to previous methods in terms of the method used, type and language of datasets used in the experiment, and the accuracy achieved.

### III. DEEP LEARNING FOR DOCUMENT IMAGE PROCESSING

DL has opened the door to a new era of AI applications where is a subset of machine learning. It depends on artificial neural networks and representation learning as it is capable of imitating the way the human brain operates by creating patterns and processing data [8][9].

#### A. Deep Learning for Document Classification

DL contains multilayered neural networks. Its commonly applied to document and image processing. Recurrent Neural Networks (RNN) and convolutional neural networks are two of the most common supervised deep learning architectures (CNN). A recurrent Neural Network (RNN) is suitable for modeling sequential data such as texts, audio, and time series. It has been widely used in machine translation, speech recognition. A convolutional neural network (CNN) is suitable for modeling static data such as images. It has been proved to be a very powerful tool in image processing. Indeed, in the areas of computer vision such as handwriting recognition, image classification. It has become a much better tool compared to previous tools [10], [11].

We are employing deep learning because of its ability to learn useful features from raw data, which makes it extremely useful when working with unstructured data. We realize that one of the most supervised deep learning techniques is the Convolutional Neural Network (CNN). CNN is widely employed in image processing because it performs in image classification and recognition and has significantly improved the efficiency of a number of machine learning tasks. It has since developed into a powerful and widely used deep learning model. The CNN architecture enables it to extract features from images automatically, eliminating the need for manual feature extraction. Different filters are used in the convolutional layer to convolve through images to create complex features that are then passed on to the next layer. This process continues until it reaches the last feature. This makes CNN highly accurate for image classification.

Convolutional Neural Networks (CNN) have shown their efficacy in the classification of document images. In the field of document image classification, Convolutional Neural Networks (CNN) are efficient. Different classification techniques are compared by Lecun et al. [27]. The results reveal that CNN outperformed all other methods when it came to dealing with the range of 2D shapes. As a result, we consider CNN as the model for the challenging tasks of Arabic document image classification [12], [13].

Our contribution is to use CNN to classify Arabic document images and extract information. The proposed model aims to understand CNN and apply it to Arabic document image recognition filters, a CNN extracts feature maps from 2D images.

#### B. Convolution Neural Network (CNN) Architecture

We use CNN as a model for categorizing Arabic document images. With minimal preprocessing, we built a Convolutional Neural Network to recognize Arabic scripts directly from pixel images. A CNN's central building block is the convolutional layer. The parameters of the layer are made up of a collection of learnable filters (or kernels) for recognizing features (like edges) that span the whole depth of the input image. Each filter convolves over the width and height of the input image during the forward transfer. Produce a features map by computing the dot product of the kernel and the input field. As a result, the network gains an understanding of the filters. When the filter detects a particular type of feature at a specific spatial location in the input, it activates. The function maps are then fed into a pooling layer, where identical convolutions are added one patch at a time. CNN also has a completely connected layer that categorizes performance into one of four classes. Almost all CNN architectures follow the same general design principles: sequentially adding convolutional layers to the input, regular spatial downsampling (Max pooling), and increasing the number of feature maps. Layers that are fully connected, activation, and loss functions are also provided. As a result, before introducing the proposed model, we'll quickly go through these layers. The first layer where it can remove features from images is the convolutional layer. Convolution is the process of reducing the size of an image while maintaining the relationship between pixels by filtering it with a smaller pixel filter. Filter (kernel) is simply a weighted matrix of values that has been trained to detect unique features. The basic concept behind CNNs is to spatially convolve the kernel on an input image to see if the function it's supposed to detect is present. Convolution is performed by computing the kernel's dot product with the input field and then generating a features map [14]. The convolution operation is shown in Fig. 1.

After each convolution process, the ReLU (Rectified-Linear Unit) was used. It replaces all negative pixel values in the function map with zero and is added per pixel. The rectifier function is used to increase non-linearity in the CNN and convert the linear model we train into a network with more expressive capabilities, which aids in faster and more efficient training [17], [18].

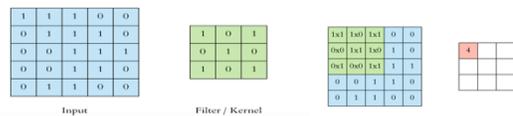


Fig. 1. Convolution Operation [13].

The pooling layer is usually inserted after each convolutional layer in a CNN, and it entails selecting a pooling operation, similar to a filter applied to feature maps, to reduce the representation's spatial size. This layer reduces the computational complexity of each map by minimizing its dimensionality while preserving important data. Overfitting can also be mitigated by pooling layers. The function map typically takes up more space than the pooling or filtering operation. As a result, we pick the maximum, average, or total values within these pixels as a pooling size to reduce the number of parameters. Fig. 2 depicts the maximum pooling

operation. In CNN, the max-pooling approach is widely used, which involves placing a 2x2 matrix on the feature map and choosing the largest value in that box. The 2x2 matrix is passed around the function map from left to right, picking the largest value in each pass. These values are then combined to form a pooled feature map, which is a new matrix. It preserves the image's main features while reducing its scale. We'll use dropout to prevent overfitting, which happens when the proposed model is unable to predict new data labels. The dropout layer reduces the random set of activations in that layer to zero as data passes through it, effectively eliminating them from the layer [9].

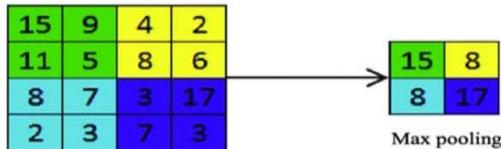


Fig. 2. Max Pooling Operation [14].

A fully connected layer takes the outputs of the convolution and pooling processes and converts them into labels with categories. Convolution and pooling output is flattened into a single vector of values, each representing a probability that defines a specific feature of the class. In the end, we can create a fully connected network to classify the dataset [14]. The fully connected layer is shown in Fig. 3.

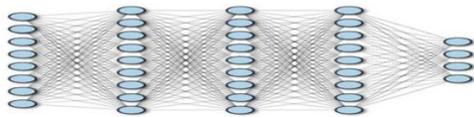


Fig. 3. Fully Connected Layer [14].

Fig. 4 shows the overview look of the proposed convolutional neural network. We can divide the model into seven sequences of layers.

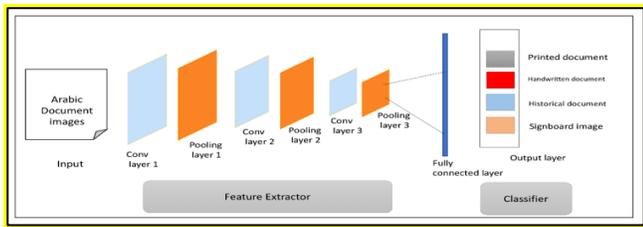


Fig. 4. General Architecture of the Proposed CNN Model.

### C. CNN and Feature Extraction

In image processing, we can extract features from images using a variety of convolutional filters in the convolutional layer. Canny filters, for example, can detect edges. Canny normally takes a grayscale image as input and outputs an image that shows where strength discontinuities are located (i.e. edges). Filters aren't described in CNN. During the training phase, the value of each filter is learned. CNN can extract additional meaning from images that humans and human-designed filters might not be able to find. We can get more abstract and in-depth information from a CNN by stacking layers of convolutions on top of each other. Convolution may also be capable of performing hierarchical

feature learning, which is thought to be how to brains identify objects. CNN is very effective in image recognition because of its ability to discover abstract and complex features [15], [16].

## IV. CNN CLASSIFICATION SYSTEM

The general architecture of the proposed Convolutional Neural Network (CNN) model is designed for the recognition of Arabic document images, as shown in Fig. 4. We need to do some pre-processing on the document images first, such as resizing them because CNN uses a fixed-size input image So, resize the document images that we'll be experimenting with.

The first step in the proposed approach is to prepare the data. We need to set up training and testing data and reshape it into the right size before we can create the network. The original dataset folder had four subfolders, each containing four different types of Arabic document images. Arabic handwritten documents, Arabic printed documents, Arabic historical documents, and Arabic signboard images are the four main classes. We divided the original dataset folder into training and validation dataset folders using the split-folder python package, with the same four classes in each folder. For the training dataset, we used 80% of document images and 30% for the validation dataset. The training dataset was used to train the model, and the validation dataset was used to fine-tune it.

### A. Data pre-processing and Data Augmentation

We'll use Keras, an open-source python library for developing and testing deep learning models, to preprocess the document images. It includes the ImageDataGenerator class, which defines the image data preparation and augmentation configuration and is a powerful tool for image augmentation and feeding these images into the proposed model. All data in the Arabic handwritten document folder will be automatically labeled as Arabic handwritten documents by the ImageDataGenerator. It's the same for the rest of the folders. Data is effectively ready to be transferred to the neural network in this way. The names of the classes will be created automatically from the names of the sub-directories, so we won't have to identify them explicitly. The dataset directory structure is shown in Fig. 5.

Image augmentation, on the other hand, helps to minimize overfitting and improves model generalization by generating more training data based on existing training data. It takes place in memory, and the generators make it simple to set up data for training and testing. It has a lot of resizing, rotating, zooming, and flipping options. Before providing images as input to a deep learning model for training or evaluation, the pixel values in the images must be scaled. The ImageDataGenerator class will rescale pixel values from 0-255 to the preferred range of 0-1 for neural network models [19], [20].

### B. Dataset and CNN Training

We have a dataset directory where we will store all of the document image data, as shown in Fig. 5. We'll have subdirectories for each class under each dataset directory, where the actual image files will be stored.

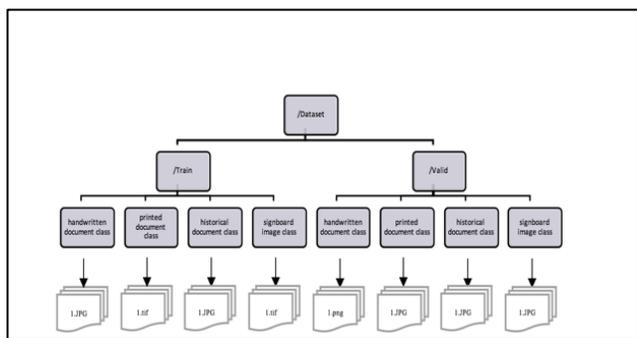


Fig. 5. Dataset Directory Structure.

The training dataset will be stored in the dataset/train/ directory. During training, we may also have a dataset /validate/ for a validation dataset. The document images were categorized into four classes in the train folder. For example, the handwritten document subfolder contains all document images related to the Arabic handwritten document, and so on.

Data is ready to be fed into the model after the required pre-processing. Below, we'll go over the information in greater depth.

Transfer learning is a deep learning technique that involves training a neural network model on a problem that is close to the one being solved. The initial blocks of CNN in the computer vision domain extract low-level features such as edges, shapes, corners, and so on. We transfer the information (features, weights) from a pre-trained network and use them to identify new images since we know that initial blocks use more computational resources. Since the final blocks in CNN are more focused on image data, we freeze the top layers and use the bottom layers as needed. For feature extraction, we use all of the convolution layers. The completely connected and dense layer is then replaced with the layers to identify the document images as (handwritten, historical, printed, and signboard).

We'll use the VGG16 architecture, which is based on ImageNet, a research project that aims to build a broad database of images and labels. There are over 14 million images in this dataset, divided into 1000 categories. VGG16 model architecture for image classification consists of 13 convolutional layers with 3\*3 filters, max-pooling, two fully connected layers, and one SoftMax classifier based on the ImageNet database. The feature extractor, which is made up of VGG blocks, and the classifier, which is made up of fully connected layers and the output layer [17], [22], [23], are the two main components of VGG16. We can use the model's feature extraction section and add a new classifier section that is specific to our Arabic document images. Specifically, during training, we may keep the weights of all convolutional layers set and only train new fully connected layers that will learn to understand the features extracted from the model and create a document image classification.

We'll load the dataset and classes, and then begin the training process by learning ImageNet's prior weights. The network was also updated with the addition of dropout. In this case, a 30% dropout is applied after each max-pooling layer, as well as to the fourteenth and seventeenth layers, which are

fully connected. We also changed the final layers of the network to identify the classes. Fig. 6 depicts a summary of the model's proposed architecture. One of the reasons we chose the VGG16 model as the base classifier model for the classification of Arabic documents since it has been shown in [3] to be one of the most effective models for dealing with document classification tasks.

### C. CNN Implementation

Fig. 7 shows that there are five blocks in total: the first two have two convolutional layers, followed by ReLU and max-pooling layers, while the last three have three convolutional layers, followed by ReLU and max-pooling layers. The first and second convolutional layers are made up of 64 feature kernel filters, each of which is 3\*3 in size. The dimensions of the input image (RGB image with depth 3) changed to 500x750x64 as it moved through the first and second convolutional layers. The output is then sent to the max-pooling layer.

The third and fourth convolutional layers are made up of 128 feature kernel filters that are 3\*3 in size. The output will be reduced to 250x375x128 after these two layers are accompanied by a max-pooling layer. Convolutional layers with kernel size 3\*3 make up the fifth, sixth, and seventh layers. 256 function maps are used for all three. A max-pooling layer comes after these layers.

Two sets of convolutional layers, each with a kernel size of 3\*3, are used in the eighth to thirteenth layers. 512 kernel filters are used in each series of convolutional layers. The max-pooling layer comes after these two. The fourteenth through seventeenth layers are fully connected hidden layers with 256, 64, 32, and 8 units, respectively, followed by a four-unit SoftMax output layer (eighth layer). The dropout layer is added after each max-pooling layer, as well as the fourteenth and seventeenth fully connected layers, to prevent overfitting. The actual number of classes is represented by the eighth sheet.

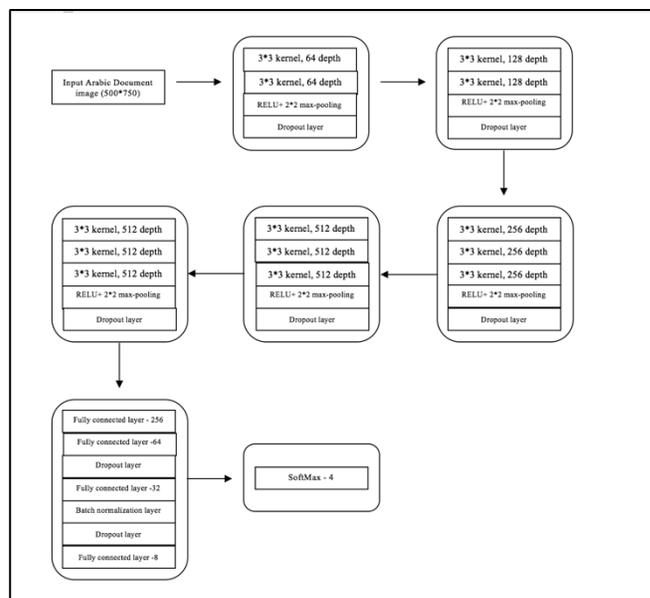


Fig. 6. The Proposed Architecture of the Model.

In this way, as in Fig. 7, CNN transforms the pixel values in the original document image to the final class, layer by layer. While some layers contain parameters, some don't. The convolution and fully connected layers, in particular, perform transformations that are dependent on both the activations in the input volume and the parameters (the weights and biases of the neurons). The Relu/pooling layers, on the other hand, will follow a fixed function. In the convolutional and fully connected layers, we train the parameters. The trained model will be prepared to recognize the document image in the test data. As a result, we can classify document images into four main categories: handwritten, historical, printed, and signboard. Training and testing the model is the third step. Finding kernels in convolution layers and weights in fully connected layers to reduce the gaps between output predictions and given actual classes on a training dataset is the method of training a network. The backpropagation algorithm is a method for training neural networks that involve the use of a loss function and a gradient descent optimization algorithm. A loss function calculates a model's performance under specific kernels and weights using forwarding propagation on a training dataset, and learnable parameters, including kernels and weights, are modified according to the loss value using optimization algorithms which include backpropagation and gradient descent [21]. The adaptive learning rate (Adam) optimization algorithm was used to construct the model and perform random gradient descent training. We used the Adam optimization algorithm to change the weight of the relation between neurons so that the loss is reduced to a minimum or stops after several epochs. Adam is defined as one of the most popular optimization algorithms for optimizing neural networks in deep learning, based on an adaptive learning rate algorithm [25], [26]. Finally, we can start CNN training by providing the training data, the built model, and the current batch of data. Only the data specified for training play a significant role in reducing CNN error. For both the forward and backward passes, we feed the training data into the network. The validation data is only used to see how the CNN reacts to new data that is close to it. The validation data isn't used to train the network. After that, we save the CNN that has been trained and prepare for the testing process. Finally, we can evaluate the model using the testing data.

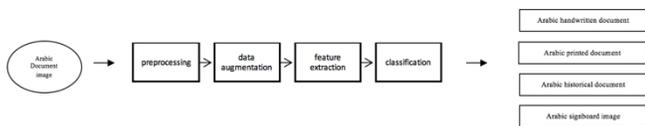


Fig. 7. CNN Implementation Steps.

### V. EVALUATION AND RESULT

The proposed document collection contains 2373 documents regarding Arabic script, all of which are divided into four classes: handwritten, historical, printed, and signboard in Arabic script. These documents were collected from various sources. We must evaluate the model's performance and estimate the model prediction accuracy, which is how effective the model is at predicting the outcome of a new test dataset that has not been used to train the model, by comparing the

expected result values to the actual result values. We use a Confusion Matrix, Accuracy, Recall, Precision, and F1- Score as the most common classification evaluation metrics. In the handwritten document image class, for example, we feed the handwritten document image into the trained model before the model prediction. We compare the prediction to the correct class after the model predicts that this is a handwritten document. As compared to the class of "handwritten document," the prediction is accurate. However, if it predicts that this image is a printed document, the comparison to the correct class will be incorrect. This process is repeated for each of the document images in the test data. We'll eventually get a count of how many test records the model correctly predicted and how many it incorrectly predicted. The Confusion Matrix is a tabular architecture of prediction results that includes counts of test records correctly and incorrectly predicted by the model. It provides information about the types of errors produced by the classifier. Table II displays a confusion matrix of four classes and 20 handwritten document images that have been misclassified as printed documents. The correct classifications are represented by the yellow cells on the diagonal, while the incorrect classifications are represented by the white cells. As can be shown, this provides a much more detailed view of the proposed model's efficiency.

Table III shows the classification accuracy, recall, precision, and f1-score are all factors to consider. The following Table III will clarify everything, shows the classification accuracy, precision, recall, and f1-score for each document type in the dataset. Accuracy is a common metric used by many researchers to evaluate the efficacy of classifiers. It is defined as the percentage of correct predictions for test data. It is easy to calculate by dividing the number of correct predictions by the total number of predictions. The proposed model demonstrates that it is capable of accurately recognizing various documents. Using this dataset to run the model, we were able to achieve a 92% accuracy rate.

Precision is expressed as a percentage of (true positives) correctly predicted out of the total number of positive results predicted by the model. The recall is calculated by dividing the number of positive results correctly classified by the total number of positive examples that should have been found.

TABLE II. CONFUSION MATRIX

Truth		Arabic handwritten document	Arabic historical document	Arabic printed document	Arabic signboard image
Predicted	Arabic handwritten document	136	0	0	0
	Arabic historical document	0	134	0	0
	Arabic printed document	20	0	109	0
	Arabic signboard image	0	3	13	62

TABLE III. CLASSIFICATION REPORT

Classification report				
	Precision	Recall	F1-score	Support
Arabic handwritten document	87%	100%	93%	136
Arabic historical document	98%	100%	99%	134
Arabic printed document	89%	84%	87%	129
Arabic signboard image	100%	79%	89%	78
Accuracy			92%	477
Macro avg	94%	91%	92%	477
Weighted avg	93%	92%	92%	477

The f1-score is computed by applying the harmonic mean of precision and recall [23], [24]. All the metrics formulae are shown in the equation (1), (2), (3), and (4).

$$Accuracy (acc) = \frac{TP+TN}{TP+FP+TN+FN} \quad (1)$$

$$Recall (R) = \frac{TP}{TP+FN} \quad (2)$$

$$Precision (P) = \frac{TP}{TP+FP} \quad (3)$$

$$F - Measure = \frac{2 \times P \times R}{P+R} \quad (4)$$

The classification report, shown in Table III, provides an overview of the proposed model's performance. The handwritten class results are shown in the third row. The 'support' column indicates how many class handwritten document images were included in the test data. The model performance for the historical class is shown in the fourth row. Tables II and III show how we can describe precision and recall for each of the classes. The precision for the handwritten class, for example, is calculated as the number of correctly predicted handwritten documents (136) out of all predicted handwritten documents (136+20=156), which amounts to 136/156=87%. The recall for the handwritten document, on the other hand, is the number of correctly predicted handwritten documents (136) divided by the number of real handwritten documents (136+0+0=136), which amounts to 136/136=100%. We can measure the precision and recall for the other three classes in the same way. On the other hand, the f1-score for a handwritten document is 93% because it is harmonic between accuracy and recall (2\*0.87\*1.00)/ (.87+1.00). The three classes are all computed in the same way. The proposed model has proven its effectiveness in classifying Arabic document images by achieving higher accuracy of 92%, as shown in Table III.

## VI. CONCLUSION AND FUTURE WORK

The proposed Arabic document collection includes 2373 documents, which are divided into four categories: handwritten, historical, printed, and signboard in Arabic script. These documents were obtained from different sources, the majority of which contain a significant amount of knowledge. As a result, document classification is crucial. It takes a long

time and is extremely difficult to manually identify Arabic document images. However, it is now possible to categorize Arabic document images into their appropriate classes. In this paper, we develop a system for classifying Arabic document images into four classes: handwritten, historical, typed, and signboard. The CNN supervised deep learning algorithm was used to create the proposed approach. The pre-trained model VGG16, which was trained on ImageNet, was used in the CNN model. We used the model's feature extraction part and added a new classifier part that is specific to the Arabic document images. Specifically, we may keep the weights of all convolutional layers fixed throughout training and only train new fully connected layers that will learn to understand the features extracted from the model and classify document images. We changed the network by adding dropout after each max-pooling layer and to the fourteenth and seventeenth fully connected layers. The proposed model has proven its effectiveness in classifying Arabic document images by achieving higher accuracy of 92%. We plan to work on big data Arabic document images in the future, and the final data is to apply the same techniques to keyword searches in deep learning classified documents.

## ACKNOWLEDGMENT

This work was funded by the University of Jeddah, Jeddah, Saudi Arabia, under grant No. {UJ-20-018-DR}. The authors, therefore, acknowledge with thanks the University of Jeddah technical and financial support.

## REFERENCES

- [1] Afzal, M. Z., Capobianco, S., Malik, M. I., Marinai, S., Breuel, T. M., Dengel, A., & Liwicki, M. (2015, August). Deepdocclassifier: Document classification with a deep convolutional neural network. In 2015 13th international conference on document analysis and recognition (ICDAR) (pp. 1111-1115). IEEE.
- [2] Ezat, W. A., Dessouky, M. M., & Ismail, N. A. (2020). Multi-class Image Classification Using Deep Learning Algorithm. In Journal of Physics: Conference Series (Vol. 1447, No. 1, p. 012021). IOP Publishing.
- [3] Das, A., Roy, S., Bhattacharya, U., & Parui, S. K. (2018, August). Document image classification with intra-domain transfer learning and stacked generalization of deep convolutional neural networks. In 2018 24th International Conference on Pattern Recognition (ICPR) (pp. 3180-3185). IEEE.
- [4] Abdulmunim, M. E., & Abass, H. K. (2019). Classification and Retrieving Printed Arabic Document Images Based on Bagged Decision Tree Classifier. AL-MANSOUR JOURNAL, (32).
- [5] al-Khurabi, Abd Allah Ali& Mansur, Muhammad Abd Allah. 2004. Arabic document image classification using neural networks. Mansoura Engineering Journal·Vol. 29, no. 1, pp.1-8.
- [6] Kölsch, A., Afzal, M. Z., Ebbecke, M., & Liwicki, M. (2017, November). Real-time document image classification using deep CNN and extreme learning machines. In 2017 14th IAPR International Conference on Document Analysis and Recognition (ICDAR) (Vol. 1, pp. 1318-1323). IEEE.
- [7] AL-Saffar, A., Awang, S., Al-Saiagh, W., Tiun, S., & S Al-khaleefa, A. (2018). Deep learning algorithms for Arabic handwriting recognition: A review. International Journal of Engineering & Technology, 7(3.20).
- [8] What Is Deep Learning? | How It Works, Techniques & Applications. <https://in.mathworks.com/discovery/deep-learning.html>.
- [9] Deep Learning in Keras - Building a Deep Learning Model. <https://stackabuse.com/deep-learning-in-keras-building-a-deep-learning-model/>.
- [10] Mu, R. (2018). A survey of recommender systems based on deep learning. Ieee Access, 6, 69009-69022.

- [11] Demystifying AI, Machine Learning and Deep Learning, from <https://developer.hpe.com/blog/demystifying-ai-machine-learning-and-deep-learning/>.
- [12] Shaheen, F., Verma, B., & Asafuddoula, M. (2016, November). Impact of automatic feature extraction in deep learning architecture. In 2016, International conference on digital image computing: techniques and applications (DICTA) (pp. 1-8). IEEE.
- [13] O'Mahony, N., Campbell, S., Carvalho, A., Harapanahalli, S., Hernandez, G. V., Krpalkova, L., ... & Walsh, J. (2019, April). Deep learning vs. traditional computer vision. In Science and Information Conference (pp. 128-144). Springer, Cham.
- [14] Hossain, M. A., & Sajib, M. S. A. (2019). Classification of the image using a convolutional neural network (CNN). Global Journal of Computer Science and Technology.
- [15] Different Kinds of Convolutional Filters. <https://www.saama.com/different-kinds-convolutional-filters/>.
- [16] Digital Filters. <https://homepages.inf.ed.ac.uk/rbf/HIPR2/filtops.htm>.
- [17] Krishna, S. T., & Kalluri, H. K. (2019). Deep learning and transfer learning approaches for image classification. International Journal of Recent Technology and Engineering (IJRTE), 7(5S4), 427-432.
- [18] Sun, X., Li, Y., Kang, H., & Shen, Y. (2019, March). Automatic Document Classification Using Convolutional Neural Network. In Journal of Physics: Conference Series (Vol. 1176, No. 3, p. 032029). IOP Publishing.
- [19] Brownlee, J. (2021). Your First Deep Learning Project in Python with Keras Step-By-Step, from <https://machinelearningmastery.com/tutorial-first-neural-network-python-keras/>.
- [20] Brownlee, J. (2021). Image Augmentation for Deep Learning With Keras, from <https://machinelearningmastery.com/image-augmentation-deep-learning-keras/>.
- [21] Yamashita, R., Nishio, M., Do, R. K. G., & Togashi, K. (2018). Convolutional neural networks: an overview and application in radiology. Insights into Imaging, 9(4), 611-629.
- [22] Tammina, S. (2019). Transfer learning using VGG-16 with a deep convolutional neural network for classifying images. International Journal of Scientific and Research Publications, 9(10), 143-150.
- [23] Burugupalli, M. (2020). Image Classification Using Transfer Learning and Convolution Neural Networks.
- [24] Hossin, M., & Sulaiman, M. N. (2015). A review on evaluation metrics for data classification evaluations. International Journal of Data Mining & Knowledge Management Process, 5(2), 1.
- [25] Soydaner, D. (2020). A comparison of optimization algorithms for deep learning. arXiv preprint arXiv:2007.14166.
- [26] Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. arXiv preprint arXiv:1412.6980.
- [27] LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. nature, 521(7553), 436-444.

# Comparative Analysis of Data Mining Algorithms for Cancer Gene Expression Data

Preeti Thareja, Rajender Singh Chhillar  
Department of Computer Science and Applications  
Maharshi Dayanand University, Rohtak, India

**Abstract**—Cancer is amongst the most challenging disorders to diagnose nowadays, and experts are still struggling to detect it on early stage. Gene selection is significant for identifying cancer-causing different parameters. The two deadliest cancers namely, colorectal cancer and breast malignant, is found in male and female, respectively. This study aims at predicting the cancer at an early stage with the help of cancer bioinformatics. According to the complexity of illness metabolic rates, signaling, and interaction, cancer bioinformatics is among strategies to focus bioinformatics technologies like data mining in cancer detection. The goal of the proposed study is to make a comparison between support vector machine, random forest, decision tree, artificial neural network, and logistic regression for the prediction of cancer malignant gene expression data. For analyzing data against algorithms, WEKA is used. The findings show that smart computational data mining techniques could be used to detect cancer recurrence in patients. Finally, the strategies that yielded the best results were identified.

**Keywords**—Colorectal cancer; breast cancer; bioinformatics; data mining; WEKA; machine learning

## I. INTRODUCTION

Non - communicable diseases (NCDs) responsible for 71 percent of all fatalities worldwide. Non-communicable diseases (NCDs) are illnesses which are never spread by pathogens. They are long-term illnesses with a sluggish course that are caused by a mix of biological, physiologic, ecological, and behavioral variables. Malignant is a non-communicable disorder in wherein some tissues grow out of control and extend to many other areas of the organism. Malignant is another name used for cancer that can begin practically at any place in the trillions of cells that make up the human body. Cancer is among the top contributors of death rate in India, accounting for 63 percent of all fatalities (9 percent). According to the National Cancer Registry Programme Report 2020, males will have a tumor incidence of 679,421 in 2020 and 763,575 in 2025, while women will have a tumor incidence of 712,758 in 2020 and 806,218 in 2025 [1]. As per research, oral, lung, and colorectal are the most frequent malignancies among men while breast and cervix uteri malignancies are most frequent amongst women. Cancer researchers require access to selected data from multiple sources in order to make advances. In medicine, data analysis has a remarkable ability to uncover hidden patterns in disease prediction [2,3].

As an emerging technique, cancer bioinformatics is one of the most important and valuable ways to facilities biochemical engineering for medical advancements, as well as improving

the outcomes of cancer victims. Bioinformatics is focused on building an infrastructure to assist researchers in storing, analyzing, integrating, accessing, and visualizing large biological datasets and supporting information [4]. Bioinformatics is a computing platform that focuses on extracting information from biology content. It entails the creation of analysis tools and techniques to obtain, store, retrieve, manipulate, model databases, visualization, and estimation. As a result, custom analytics tools have become extremely important in bioinformatics, and they help to speed up the research process [5]. Sequencing and annotating an individual's entire collection of DNAs, for instance, are two common tasks in biotechnology. Led to the creation of machine learning techniques, bioinformatics models had to be manually configured, which is extremely challenging for problems like proteomics. Massive amounts of health data are gathered and made accessible to medical researchers because of the usage of computers employing automated technologies. As a matter of fact, Knowledge Discovery in Databases, which involves machine learning techniques, has now become a successful learning tool for health investigators to locate and manipulate correlations among a huge set of samples allowing them to foresee disease outcomes using specific instances stored in databases [6].

This study discusses recent research methodologies as well as an examination of predictive approaches, with a focus on classifying co-regulated genes according to their biological function. The work, basically, aims to find the foremost learning models for predicting cancer malignant gene expression data through study of related research work. Further, this study finds out the outperforming learning model by comparing them on certain performance metrics. The work has been divided into several sections. Section 2 talks about the recent advances in the field of cancer bioinformatics and most commonly used techniques for predicting cancer data. Section 3 presents the methodology employed in this research to analyze various algorithms on cancer datasets, as well as the measures used for evaluating their performances. Section 4 discusses the findings, which is preceded by the conclusion in Section 5.

## II. RELATED RESEARCH WORK

This section will provide an overview of many cancers gene expression data-related research publications from a variety of databases, including IEEE Xplore, Google Scholar, Scopus, and Springer. Mostly, the publications are from year 2019-2021. This will aid in the discovery of techniques that have recently been used in the cancer detection. A list of

prominent algorithms and performance metrics used in publications are produced in Tables I and II, respectively. These techniques will also be used to analyze performance.

Keerthika et al. [7] used information-mining strategy for proposing the cancer prediction model. This algorithm helps to find the amount of breast malignant that will occur in the near future. The main objective of this strategy is to safeguard users while also making it cheaper for them to use. Physical injury prevention and diagnosis will be aided by a prediction model. This discovery aids in detecting a person's risk of cancer at such an initial phase of treatment.

Changhee et al. [8] developed a better prognosis model based on machine learning named Survival Quilts. This model is being developed on the 10-year data of US prostate cancer patients to predict their mortality rate. Survival Quilts was compared with 9 prognosis models that are in clinical use and it showed a better decision curve.

T. Jayasankar et al. [9] used OGH0 for optimal feature selection and kernel SVM (Support Vector Machine) in conjunction with gray wolf optimization algorithm to predict the breast cancer on the Wisconsin Breast Cancer dataset from UCI.

Heydari et al. [10] took a survey of leading data mining used for cancer detection in early phases. The author compared the top techniques of data mining and listed their advantages and disadvantages.

Byra et al. [11] proposed 2 CNN (convolutional neural network) techniques for breast malignant prediction. This method combines transfer learning with pre-trained CNN to produce excellent results of prediction.

M.A.Fahami et al. [12] clustered the colon cancer patients into 2 important categories and as a result they found out top 20 genes that are effective in both the categories.

Alireza et al. [13] applied novel and traditional data mining methods viz, linear vector quantization (LVQ) neural network (NN), multi-layer perceptron (MLP), Bayesian NN, Decision Tree (DT-C5.0), kernel principal component analysis with support vector machine (KPCA-SVM), and random forest (RF). The author clearly demonstrates the impact of machine learning technology on breast cancer recur classification. In compared to other approaches, the C5.0 and the KPCA-SVM have demonstrated to perform better in terms of accuracy. C5.0, on the other hand, had the finest sensitivity result.

Mostafa et al. [14] examined the results of different classification algorithms for identifying Colorectal Cancer (CRC), namely, J-48, Bayesian NN, RF, and MLP. All methods were found to be suitable and capable of providing reasonable results. J-48, on the other hand, performed best across the board.

Yanke et al. [15] mined 7 colorectal cancer related datasets using their new technique that combined NB (Naïve Bayes), RF and DT. After analysis the final result are optimized using an appropriate optimization technique. It was found that the proposed algorithm is superior than the SVM. This helps in better discovery of the genuine possibility of colorectal cancer

target genes, and provides suggestions for its medical trials and promoting gene extraction.

Md. Rejaul et al. [16] created a technique for detecting the danger of stomach cancer beforehand. To acquire the feature score in a range of 0 to 1, the authors employed 5 distinct features extraction strategies along with ranker algorithms. The average rating was then used to provide a one exact score of each attribute. Then, apply predictive apriori algorithm to find the data's hidden pattern. The experiment had 300 patients, 150 of them were sick and the remaining 150 were not. Out of the 32 risk variables, they found 18 major risk factors for stomach cancer.

Ahmed et al. [17] proposed a Radial Basis Function NN (RBFNN) for diagnosing chronic diseases like breast cancer. The author has also compared his proposed method with other state of the art methods and found out that proposed method accuracy is the highest among all. Also, the author compared his method with learning classifier like RF, SVM, NB, ANN and many others. The result showed that his method is more accurate than other predefined classifiers.

Hooda et al. [18] employed a prediction model Bagoost to predict the breast cancer risk. The framework showed the accuracy of around 98%. The author states that it has better accuracy as compared to SVM, RF and adaboost.

Shanjida et al. [19] compared NB, k-nearest neighbor (kNN) and J48 data mining techniques on nine different types of cancer datasets. It was found that all the three algorithms were performing well but kNN outperforms the other two by a difference of around 0.4 percent in accuracy.

TABLE I. LIST OF ALGORITHMS USED IN RELATED RESEARCH WORK

Data Mining Techniques	References	Count
SVM	[9], [13], [15], [16], [18]	5
ANN	[11], [13], [14], [16]	4
NB	[13]-[16]	4
RF	[13]-[16], [18], [20]	6
DT	[7], [13]-[16], [19]-[21]	8
kNN	[19]-[21]	3
Bayesian NN	[13], [14]	2
LVQ-NN	[13]	1

TABLE II. LIST OF PERFORMANCE METRICS USED IN RELATED RESEARCH WORK

Performance Metrics	References	Count
Accuracy	[10]-[13], [17]-[19], [21]	8
Sensitivity	[11]-[14], [19]-[21]	7
Specificity	[11]-[14], [19]-[21]	7
ROC	[11], [14], [15], [18]	4
AUC	[11], [13], [15], [18]	4
F-Measure	[13], [14], [18], [19]	4
F1-Score	[20]	1
Decision Curve	[8]	1

Ray et al. [20] explored different classification methods (Gaussian NB, kNN, DT, RF) for detecting breast cancer involving both numeric and image datasets. It was found that the accuracy of RF was better in both numeric and image datasets.

Harikumar et al. [21] presented model that uses two machine learning (ML) techniques to categorize Breast Cancer (BC), viz. DT and kNN algorithms. Following feature selection with principal component analysis (PCA), these two techniques are tested on the BC dataset. The typical performance measures like accuracy, specificity, sensitivity, precision and Matthew's correlation are used to compare them. The findings show that the kNN classifier outperforms the DT classifier in the BC classification.

### III. METHODOLOGY

The mathematical aspects of the problem are presented in this section of the paper. It all begins by outlining the key features of each of the data mining algorithms applied, with an emphasis on the description of the adjustable hyper-parameters. Fig. 1 highlights the methodology of this paper.

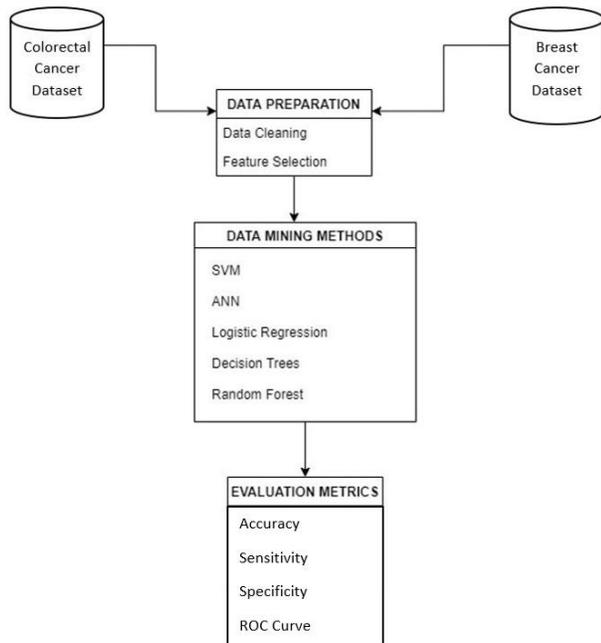


Fig. 1. Methodology for Cancer Gene Expression Data Prediction

#### A. Data Understanding and Preparation

The information was gathered from a public genomic database Gene Expression Omnibus (GEO) [22]. Two gene expressions namely, GSE45827 (Breast Cancer) and GSE41328(Colorectal Cancer). These are microarray datasets. Microarray data analysis is one of the most significant advances in statistical data and biology in the recent two decades. Microarray data may be examined using a number of methods and technologies. This section outlines a typical strategy for processing microarray data with Weka. The two most common cancers, Colorectal and Breast, will be studied here. The dataset for colorectal cancer contains 22284 attributes to be classified into four classes adenoma, carcinoma,

metastasis and normal. The dataset for breast cancer contains 54676 attributes to be classified into six classes basal, HER, cell line, normal, luminal A and luminal B. Table III lists some properties of datasets.

TABLE III. PROPERTIES OF DATASETS

Properties	Colorectal Cancer Dataset	Breast Cancer Dataset
Number of Attributes	22284	54676
Number of Instances	55	151
Missing Values	No	No
Attribute Data Type	Numeric	Numeric
Target Attribute	Class	Class

#### B. Data Mining Methods

This section discusses a brief introduction of the selected data mining techniques to be applied on the selected dataset. The motive behind selecting these techniques is that they are widely used methods for analyzing bioinformatics dataset in state-of-the-art techniques.

1) SVM: SVM stands for Support Vector Machine and is a guided technique in data mining that may be used for regression and classification. SVMs are based on the concept of determining the optimal decision boundary for dividing a sample into two groups. SVM method discovers the points from both classes that are nearest to the boundary, which are called as support vectors. The separation seen between boundary and the support vectors is termed as margin. The main objective is to increase this margin. The optimum hyperplane is the one for which the margin is the greatest. As a result, SVM seeks to create a decision boundary with as much split into two different classes as feasible. The SVM method is depicted in Fig. 2.

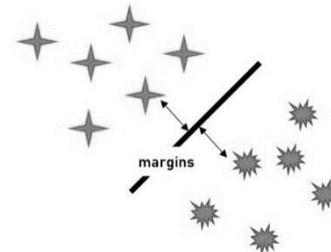


Fig. 2. SVM Method.

2) ANN: An Artificial Neural Network (ANN) is a system built on neurons that is motivated by biology neuron for the creation of artificial brains. It is built to evaluate and interpret data in the same way as beings do. Since more information becomes accessible, the algorithm may self-learn and provide superior outcomes. The inputs will be pushed into an aggregate of layers by an algorithm. A loss function must be used to measure the network's efficiency. The network may use the loss function to figure out which direction it wants to enforce to acquire the knowledge, as shown in Fig. 3. With the aid of an optimization, the net intends to promote its

knowledge. For predictive analytics, ANN is hardly applied. The reason behind this is that ANN tend to over-fit the correlation in most instances. In most situations, ANN is employed when something that happened in the past is replicated almost identically in the same way.

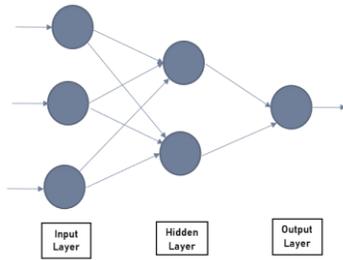


Fig. 3. ANN Method.

3) *Logistic regression*: Logistic Regression (LR) is analytical tool that is guided. This is a parametric regression models, meaning they employ numerical methods to make forecasts. The categorization issues are solved using logistic regression. The output is discrete value. The linear parameters are fitted to the sigmoid curve using logistic regression, as depicted in Fig. 4. Maximum likelihood estimation is the technique used to devise the loss function.

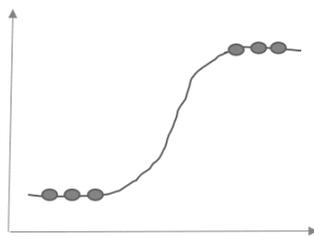


Fig. 4. LR Method.

4) *Decision trees*: A decision tree (DT) is a flowchart that aids in the decision-making process or displays statistical probabilities. A probable option, consequence, or response is represented by each node of the DT, as shown in Fig. 5. The tree's farthest branch reflects the outcomes of a particular choice route. DTs are a non-parametric ensemble learning approach. The aim is to understand basic rule base from extracted features to construct a system that anticipates the performance of the model. DTs are a prominent technique in neural networks and are widely used in business analytics to identify the best method for achieving a goal.

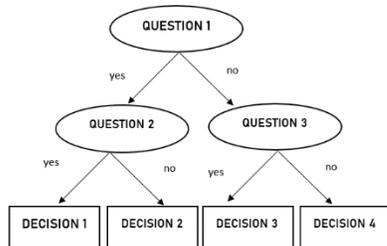


Fig. 5. DT Method.

5) *Random forest*: Random forest (RF) is a supervised learning algorithm that is commonly used to for classification and regression. It creates tree structure from several samples, using "majority vote" for classification and "average" for regression. RF collects data at random, creates a tree structure, and averages the results. It does not rely on any formulae. To create a RF, three important steps are there to follow. Firstly, randomly select slice of the whole dataset set for training particular trees separately. This is known as Bootstrapping or Sampling with Replacement. If these particular trees lack in connection, this RF Ensemble Learning performs well. Secondly, picking arbitrary features to examine at every node to accomplish connection. Lastly, Hundreds of times these steps are repeated to create a huge forest with a diverse range of trees. This variation is what distinguishes a RF from a single DT, as can be seen from Fig. 6.

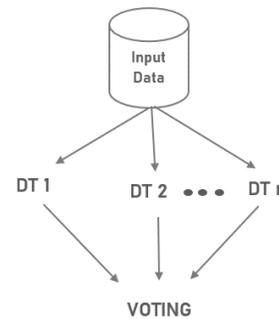


Fig. 6. RF Method.

C. Performance Metrics

In terms of performance, each prediction could be one of four kinds: True Positive, True Negative, False Positive, or False Negative. These entries are a part of confusion matrix which tells how well the classifier has performed. True Positive test is expected to be positive like saying the person is predicted to get sick but the label is really positive in terms of saying the person will get the sickness in actual. True Negative test is anticipated to be negative like saying the person is not predicted to get sick and the label is also predicted to be negative in terms of saying the person will not get the sickness in actual. False Positive occurs when a test is anticipated to be positive like saying the person is predicted to get sick) but the label is really negative in terms of saying the person will not get sick in actual. The test is “falsely” forecasted as positive in this scenario. False Negative test is expected to be negative like saying the person is predicted to not get sick but the label is really positive in terms of saying the person will get sick in actual. The test is “falsely” forecasted as negative in this situation. These values will help in determining the model’s accuracy, sensitivity, specificity, and receiver operating characteristic curve.

1) *Accuracy*: The number of properly categorised points (forecasts) divided by the total range of forecasts is Accuracy. Its value varies from 0 to 1. Accuracy is basically measured as shown in equation 1.

$$Acc = \frac{True\ Positive + True\ Negative}{True\ Positive + True\ Negative + False\ Positive + False\ Negative} \quad (1)$$

2) *Sensitivity*: Among all of the algorithms, the one with the higher sensitivity should be picked. Sensitivity determines what percentage of true positives was accurately recognised as depicted in equation 2.

$$Sensitivity = \frac{True\ Positive}{True\ Negative + False\ Negative} \quad (2)$$

3) *Specificity*: The goal of specificity is to determine what percentage of real negatives were properly recognised. How many of the genuine negative cases were identified as such is the job performed by specificity. Specificity is calculated using equation 3.

$$Specificity = \frac{True\ Negative}{False\ Positive + True\ Negative} \quad (3)$$

4) *Receiver operating characteristic*: The trade-off between sensitivity and specificity is depicted by the ROC curve. Classifiers with curves that are closer to the top-left side perform better, as can be seen in Fig. 7. A random classifier is anticipated to give values that are falling diagonally mostly as baseline. The test becomes less accurate when the curve approaches the ROC space's 45° diagonally.

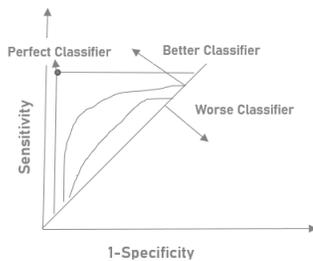


Fig. 7. ROC Curve.

D. *K-fold Cross Validation*

When there isn't enough data to utilize other more efficient approaches like the three - way division of training, validating and testing, then cross-validation is commonly used in deep learning to improve prediction performance. Initially dataset is scrambled such that the sequence of the inputs and outputs is totally arbitrary. This step is performed to ensure that our inputs are not skewed in any manner. The dataset then is divided into k equal portions. In this analysis, stratified 3-fold cross-validation is used. When cross-validation is used with the stratified sampling approach, the training and test sets contain the same fraction of the interested feature as the original dataset. When this is done with the class label, the cross-validation score is a close estimate of the generalization error.

E. *Software Used*

Weka – Waikato Environment for Knowledge Analysis is a machine learning package created by the University of Waikato in New Zealand [23]. The software is built in the Java programming language. It comes with a graphical interface and a variety of visualization tools and techniques for large - scale data processing. Data pre-processing, grouping, categorization, regressing, visualization, and dimensionality reduction are just a few of the common analysis methods that Weka offers. Weka v3.8.5 is used for the experiments on 11th Gen Intel® Core™

i5 @ 2.40 GHz with 8 GB RAM, windows 10 and 64-bit operating system.

IV. EXPERIMENTAL RESULTS AND DISCUSSION

This research is intended to classify the selected datasets according to the class labels. The datasets are normalized and processed to reduce the unwanted features. Then, the data is passed through stratified 3-fold cross validation to separate it for training and testing purpose. The comparison of the two datasets, Colorectal and Breast, is done by applying algorithms, namely SVM, ANN, LR, DT and RF. The basis of comparison are the metrics, namely, Accuracy, Sensitivity, Specificity and Execution Time. Table IV shows the results of the performance metrics of Colorectal Cancer dataset and Table V shows the results of the performance metrics of Breast Cancer dataset.

The results for the algorithms with comparison on performance metrics is also depicted through graphs as shown in Fig. 8 and 9, respectively.

TABLE IV. PERFORMANCE METRICS OF ALGORITHMS AGAINST COLORECTAL CANCER DATASET

Algorithms	Performance Metrics			
	Accuracy	Sensitivity	Specificity	ROC Curve
SVM	0.709	0.793	0.709	0.977
ANN	<u>0.945</u>	<u>0.946</u>	<u>0.945</u>	<u>0.997</u>
LR	0.891	0.901	0.891	0.960
DT	0.691	0.693	0.691	0.723
RF	0.873	0.874	0.873	0.963

TABLE V. PERFORMANCE METRICS OF ALGORITHMS AGAINST BREAST CANCER DATASET

Algorithms	Performance Metrics			
	Accuracy	Sensitivity	Specificity	ROC Curve
SVM	<u>0.947</u>	0.948	<u>0.947</u>	0.984
ANN	0.583	NA	0.583	0.876
LR	<u>0.947</u>	<u>0.950</u>	<u>0.947</u>	<u>0.992</u>
DT	0.808	0.805	0.808	0.882
RF	0.934	0.934	0.934	0.990

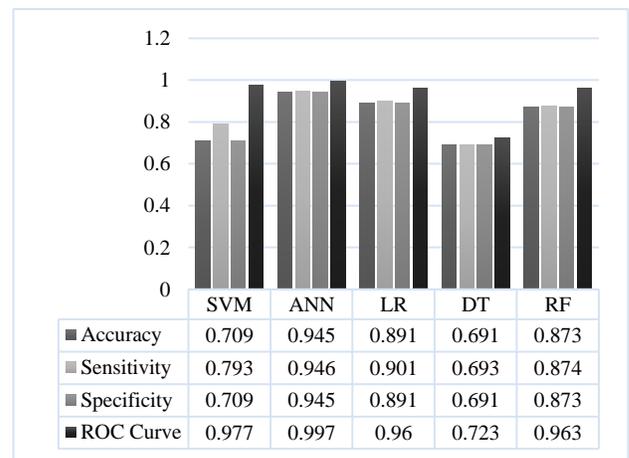


Fig. 8. Comparison of Performance Metrics against Colorectal Cancer Dataset.

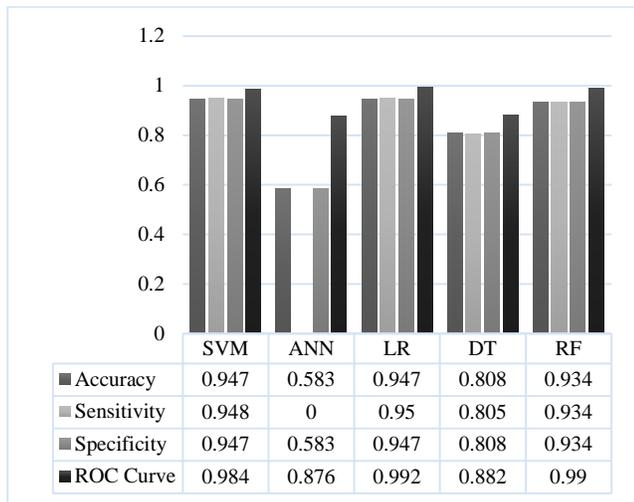


Fig. 9. Comparison of Performance Metrics against Breast Cancer Dataset.

As per the results of applying algorithms on Colorectal dataset, ANN shows the highest accuracy of around 95% with same level of sensitivity and specificity. The lowest level of accuracy, sensitivity and specificity is shown by decision trees. According to the results of applying algorithms on Breast dataset, SVM and logistic regression beats all others in accuracy of around 95%.

## V. CONCLUSION

This work is carried to provide a brief outline of the state of art techniques SVM, ANN, Logistic Regression, Decision Tree and Random Forest applied on datasets for classification. These are applied on two most common problems prevailing in India, namely, Colorectal Cancer and Breast Cancer, in men and women, respectively. The experiment is carried out in Weka and the results are compared on certain metrics like accuracy, sensitivity, specificity and ROC. The experimental test shows an accuracy of 94.5% in colorectal cancer data with ANN outperforms all other algorithms. Similarly, an accuracy of 94.7% is found in breast malignant data with SVM and logistic regression beating all other algorithms. The input dataset has a significant impact on the limitations of an algorithm analysis. Like in breast dataset the ANN model is unable to recollect the results of sensitivity; it shows a question mark for it. This work can be improved by taking more folds in cross validation and also implying hybrid models for better analysis and results. Further, it can be compared for other datasets that include cancer patients of varying types of cancer.

## REFERENCES

[1] P. Mathur et al., "Cancer Statistics, 2020: Report From National Cancer Registry Programme, India," *JCO Glob. Oncol.*, no. 6, pp. 1063–1075, 2020, doi: 10.1200/go.20.00122.

[2] Aman and R. S. Chhillar, "Disease predictive models for healthcare by using data mining techniques: State of the art," *Int. J. Eng. Trends Technol.*, vol. 68, no. 10, pp. 52–57, 2020, doi: 10.14445/22315381/IJETT-V68I10P209.

[3] Aman and R. S. Chhillar, "Analyzing Predictive Algorithms in Data Mining for Cardiovascular Disease using WEKA Tool," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 8, p. 2021, Oct. 2021.z.

[4] "Bioinformatics, Big Data, and Cancer," *Cancer Research Infrastructure*, 2020.

[5] P. Thareja and R. S. Chhillar, "A review of data mining optimization techniques for bioinformatics applications," *Int. J. Eng. Trends Technol.*, vol. 68, no. 10, pp. 58–62, 2020, doi: 10.14445/22315381/IJETT-V68I10P210.

[6] V. Krishnaiah, D. Narsimha, and D. Chandra, "Diagnosis of lung cancer prediction system using data mining classification techniques," *Int. J. Comput. Sci. Inf. Technol.*, vol. 4, no. 1, pp. 39–45, 2013.

[7] J. ; D. S. D. S. S. S. R. V. Keerthika, "Diagnosis of Breast Cancer using Decision Tree Data Mining Technique," in *2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS)*, 2021, pp. 1530–1535.

[8] C. Lee, A. Light, A. Alaa, D. Thurtle, M. van der Schaar, and V. J. Gnanaprasagam, "Application of a novel machine learning framework for predicting non-metastatic prostate cancer-specific mortality in men using the Surveillance, Epidemiology, and End Results (SEER) database," *Lancet Digit. Heal.*, vol. 3, no. 3, pp. e158–e165, 2021, doi: 10.1016/S2589-7500(20)30314-9.

[9] T. Jayasankar, N. B. Prakash, and G. R. Hemalakshmi, "Big Data based breast cancer prediction using kernel support vector machine with the Gray Wolf Optimization algorithm," in *Applications of Big Data in Healthcare*, Elsevier, 2021, pp. 173–194.

[10] H. Farzad; Rafsanjani, Marjan K, "A Review on Lung Cancer Diagnosis Using Data Mining Algorithms," *Curr. Med. Imaging*, vol. Volume 17, no. 1, pp. 16–26, 2021.

[11] M. Byra, K. Dobruch-Sobczak, Z. Klimonda, H. Piotrkowska-Wroblewska, and J. Litniewski, "Early Prediction of Response to Neoadjuvant Chemotherapy in Breast Cancer Sonography Using Siamese Convolutional Neural Networks," *IEEE J. Biomed. Heal. Informatics*, vol. 25, no. 3, pp. 797–805, 2021, doi: 10.1109/JBHI.2020.3008040.

[12] M. A. Fahami, M. Roshanzamir, N. H. Izadi, V. Keyvani, and R. Alizadehsani, "Detection of effective genes in colon cancer: A machine learning approach," *Informatics Med. Unlocked*, vol. 24, no. May, p. 100605, 2021, doi: 10.1016/j.imu.2021.100605.

[13] A. Mosayebi, B. Mojaradi, A. B. Naeini, and S. H. K. Hosseini, "Modeling and comparing data mining algorithms for prediction of recurrence of breast cancer," *PLoS One*, vol. 15, no. 10 October, pp. 1–23, 2020, doi: 10.1371/journal.pone.0237658.

[14] M. Shanbehzadeh, R. Nopour, and H. Kazemi-Arpanahi, "Comparison of four data mining algorithms for predicting colorectal cancer risk," *J. Adv. Med. Biomed. Res.*, vol. 29, no. 133, pp. 100–108, 2021, doi: 10.30699/jams.29.133.100.

[15] Y. Li, F. Zhang, and C. Xing, "Screening of Pathogenic Genes for Colorectal Cancer and Deep Learning in the Diagnosis of Colorectal Cancer," *IEEE Access*, vol. 8, pp. 114916–114929, 2020, doi: 10.1109/ACCESS.2020.3003999.

[16] M. Rejaul Islam Royel, M. Ajmanur Jaman, F. Al Masud, A. Ahmed, A. Mueyed, and K. Ahmed, "Machine learning and data mining methods in early detection of stomach cancer risk," *J. Appl. Sci. Eng.*, vol. 24, no. 1, pp. 1–8, 2021, doi: 10.6180/jase.202102\_24(1).0001.

[17] A. H. Osman and H. M. A. Aljahdali, "An Effective of Ensemble Boosting Learning Method for Breast Cancer Virtual Screening Using Neural Network Model," *IEEE Access*, vol. 8, pp. 39165–39174, 2020, doi: 10.1109/ACCESS.2020.2976149.

[18] N. Hooda, R. Gupta, and N. R. Gupta, "Prediction of Malignant Breast Cancer Cases using Ensemble Machine Learning: A Case Study of Pesticides Prone Area," *IEEE/ACM Trans. Comput. Biol. Bioinforma.*, vol. 5963, no. c, pp. 1–1, 2020, doi: 10.1109/tccb.2020.3033214.

[19] S. K. Maliha, R. R. Ema, S. K. Ghosh, H. Ahmed, M. R. J. Mollick, and T. Islam, "Cancer Disease Prediction Using Naive Bayes, K-Nearest Neighbor and J48 algorithm," *2019 10th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2019*, pp. 1–7, 2019, doi: 10.1109/ICCCNT45670.2019.8944686.

[20] R. Ray, A. A. Abdullah, D. K. Mallick, and S. Ranjan Dash, "Classification of Benign and Malignant Breast Cancer using Supervised Machine Learning Algorithms Based on Image and Numeric Datasets," *J. Phys. Conf. Ser.*, vol. 1372, no. 1, 2019, doi: 10.1088/1742-6596/1372/1/012062.

- [21] H. Rajaguru and S. R. Sannasi Chakravarthy, "Analysis of decision tree and k-nearest neighbor algorithm in the classification of breast cancer," *Asian Pacific J. Cancer Prev.*, vol. 20, no. 12, pp. 3777–3781, 2019, doi: 10.31557/APJCP.2019.20.12.3777.
- [22] "GEO Dataset," <https://www.ncbi.nlm.nih.gov/gds/>, 2021.
- [23] "Weka-Data Mining with Open Source Machine Learning Software in Java," <https://www.cs.waikato.ac.nz/ml/weka/>, 2021.

# Proactive Virtual Machine Scheduling to Optimize the Energy Consumption of Computational Cloud

Shailesh Saxena<sup>1</sup>

Research Scholar, Department of CS and IT  
MJP Rohilkhand University, Bareilly, India

Dr. Mohammad Zubair Khan<sup>2</sup>

Department of CS  
Taibah University, Medina, KSA

Dr. Ravendra Singh<sup>3</sup>

Department of CS and IT  
MJP Rohilkhand University, Bareilly, India

Abdulfattah Noorwali<sup>4</sup>

Department of Electrical Engineering  
Umm Al-Qura University, Makkah, Saudi Arabia

**Abstract**—The rapid expansion of communication and computational technology provides us the opportunity to deal with the bulk nature of dynamic data. The classical computing style is not much effective for such mission-critical data analysis and processing. Therefore, cloud computing is become popular for addressing and dealing with data. Cloud computing involves a large computational and network infrastructure that requires a significant amount of power and generates carbon footprints (CO<sub>2</sub>). In this context, we can minimize the cloud's energy consumption by controlling and switching off ideal machines. Therefore, in this paper, we propose a proactive virtual machine (VM) scheduling technique that can deal with frequent migration of VMs and minimize the energy consumption of the cloud using unsupervised learning techniques. The main objective of the proposed work is to reduce the energy consumption of cloud datacenters through effective utilization of cloud resources by predicting the future demand of resources. In this context four different clustering algorithms, namely K-Means, SOM (Self Organizing Map), FCM (Fuzzy C Means), and K-Mediod are used to develop the proposed proactive VM scheduling and find which type of clustering algorithm is best suitable for reducing the energy uses through proactive VM scheduling. This predictive load-aware VM scheduling technique is evaluated and simulated using the Cloud-Sim simulator. In order to demonstrate the effectiveness of the proposed scheduling technique, the workload trace of 29 days released by Google in 2019 is used. The experimental outcomes are summarized in different performance matrices, such as the energy consumed and the average processing time. Finally, by concluding the efforts made, we also suggest future research directions.

**Keywords**—Cloud computing; CO<sub>2</sub>; proactive scheduling; unsupervised learning; clustering; energy; prediction; cloud-sim; performance assessment

## I. INTRODUCTION

“Go Green” is the key theme of the proposed investigation. However, a significant amount of digital data is generated and consumed every day. This demand for computation leads to develop such infrastructure that can deal with such a huge load. One such technology is cloud computing which provides computational resources on demand. The proposed work is keenly focused on offering the techniques that improve the

VM workload scheduling to reduce environmental loss and preserve the energy for achieving green computing.

Green is the way of life and it teaches us how to live a sustainable and luxurious life. To support the new generation types of equipment and technologies, we depend on cloud computing to deal with bulky data. Cloud servers are an effective solution because a rich amount of data is generated using these devices and processing such big data. The cloud can scale the computational ability according to demand. On the other hand, to perform computation, we need a huge power supply and cooling system that increases the power consumption and emission of harmful gases. Thus, need to achieve green computing by reducing the power consumption of the computational cloud. In this context, in recent literature [1][2][3], we found VM (virtual machine) workload scheduling can be a good strategy to efficiently utilize the computational resources and reducing power consumption of cloud servers.

The physical machines contain several virtual machines. These VMs are used to deal with the workload that appeared for processing. If we better utilize the resources, we can process a large number of jobs in fewer VMs. Additionally, we can also turn off the ideal machines to reduce power consumption [4]. In this context, the proposed work is motivated to work with VM scheduling techniques to achieve green computing. In recent literature, we identify there are two kinds of VM scheduling approaches active and proactive. The proactive technique is more effective than the active approach due to prior knowledge of VM workload. Thus, this approach can be more beneficial for the proposed investigation.

### A. Motivation

VM scheduling provides many benefits in different scenarios of the cloud and relevant technologies. Those facts are validated by using identifying some noteworthy contributions related to the proposed domain of study. Some essential of them are discussed in this section.

Proficient VM management is extremely critical for expanding benefit, energy-saving, and forestalling SLA infringement. VM placement plans can be characterized as reactive and proactive to improve VM arrangement by

determining future workloads expectations. M. Masdari et al. [5] advances a review of the proactive VM placement and classifies them. They depict how techniques have been applied to lead viable and low overhead. Also, factors like assessment boundaries, simulators, workload, energy-saving, and predictions are analyzed. Finally, the issues and future opportunities are featured.

Fault-aware scheduling is significant for the cloud and identified with the reception of dynamic workload. R. Kaur et al. [6] proposes a pattern similarity-based scheduling for the cloud. To approve the solution, they performed two investigations with conventional technique and with the fault aware technique. The outcomes show the viability of the plan.

The server burns a tremendous measure of energy to fulfill the expanding need of computational assets. Computing and Cooling are the two frameworks that are enormous energy-devouring. Dynamic VM consolidation is a procedure to lessen energy utilization. Forceful union prompts the production of areas of interest that affects energy utilization. S. Ilager et al. [7] propose an Energy and Thermal-Aware Scheduling (ETAS) that merges VMs to limit energy utilization. The ETAS tends to compromise between time and cost-saving and can be tuned dependent on the prerequisite. They perform tests by utilizing real traces. The outcomes show that ETAS decreasing energy.

In a Virtual Symmetric Multiprocessing (VSMP) climate, the conduct of the scheduler can impact I/O responsiveness. The hinder remapping component can use different virtual CPUs. W. Zhang et al. [8] recognized an "Interfere with capacity Holder Pre-emption" (IHP) issue. The IHP presents that a virtual CPU handicapping the interferes with the capacity of the visitor's organization gadget is de-booked by a scheduler. In this manner, the creator proposes CoINT, a gasket organizer dwelling in the hypervisor, to improve the organization I/O execution. CoINT wipes out the IHP issue and lessens I/O intrudes on delay. They execute CoINT in the KVM hypervisor and assess its proficiency utilizing benchmarks. The outcomes show that CoINT can work on the netperf throughput up to 3x.

Cloud research has needed data on the qualities of the creation of VM workloads. A comprehension of these qualities can illuminate the resource management frameworks. E. Cortez et al. [9] present an interpretation of Microsoft Azure's VM workloads, including VMs' lifetime, size, and resource utilization. Then, show that specific VM is genuinely reliable. In light of this perception, present Resource Central (RC) gathers VM telemetry, learns practices, and gives predictions to administrators. They change the VM scheduler to use predictions in oversubscribing servers. Utilizing real traces show that the aware prediction schedules increment use and actual resource fatigue.

Conventional virtualization frameworks can't viably detach shared micro-architectural assets. Processors and memory-concentrated VMs fighting for assets will prompt genuine execution interference. Y. Cheng et al. [10] propose a contention-aware prediction model on the virtualized multi-core frameworks. Start with recognizing performance interference factors and plan benchmarks to get VM's

contention affectability and intensity features. Second, based on the features, fabricate a VM performance forecast model utilizing ML. The model can be utilized to streamline VM execution. The outcomes show that the model accomplishes high accuracy, and the MAE is 2.83%.

### B. Objectives

This paper investigates the energy-efficient Cloud resources scheduling for reducing the power utilization of datacenters. We focused on energy-aware VM consolidation schemes to reduce the number of running hosts to preserve energy.

We deal with this issue of selecting a power-efficient configuration that may also be suitable for mapping the client request through available VMs. The framework also considers the selection of optimal pair of the server. To scale the solution, considering client requests as time-varying, the framework enables us to virtualize the system to react to workload variations and adapt relevant configurations. The dynamic configuration improves leveraging predictions about upcoming resource demand and availability. The system takes advantage of the correlation between the historical workload and future workload demands in predictions [11].

An increasing number of datacenters are being deployed to support different applications and services. In a cloud, the applications are hosted on physical servers. These servers have great processing capabilities and can fulfill the performance demands, incurring high energy costs and increasing CO<sub>2</sub> generation and environmental losses [12].

The energy utilization for keep servers running became an important issue, which requires major investigation and immediate steps to improve energy efficiency. According to [13] the datacenters contribute to 30% of the world's CO<sub>2</sub> emissions. Thus, energy-efficient servers are a fundamental concern. To allow hosting multiple independent applications, platforms rely on virtualization to better utilize server resources. Virtualization has been adopted for resource usage efficiency; by VM consolidation and on-demand resource allocation and migration [14]. The dynamic workloads consolidation using migration of VMs, helps to increase the server utilization, reducing the use of resources and power. The ability to move workloads enables PMs to be turned off during low requirements. This offers an efficient way of running a data center in terms of energy saving. However, the data center workload often stays around 30%, and the part of under loaded servers can be as high as 70% [15].

The workloads vary with time, and prior knowledge about future demand may help to handle different critical conditions. So, we proposed a clustering scheme to predict the requests and resource requirements with network and traffic. This method improves the decisional accuracy and guaranteeing high quality of service. The aim is to provide a power aware performance management system in a virtualized environment.

Thus, we proposed a prediction approach based on ML clustering to predict the workload regarding the resource demand of requests. We also incorporate improvements that make the tunable parameters in real-time. Using this technique, we are minimizing the power utilization to meeting the

performance expectations. In order to implement, we investigate the use of dynamic configuration techniques, such as voltage scaling, the server on/off switching, and migration. We also collect evidence to verify feasibility and effects through simulations. The solution supports different types of virtualization techniques to enable resource provisioning. The framework has three major components: Data clustering, workload prediction, and power management, as shown in Fig. 1.

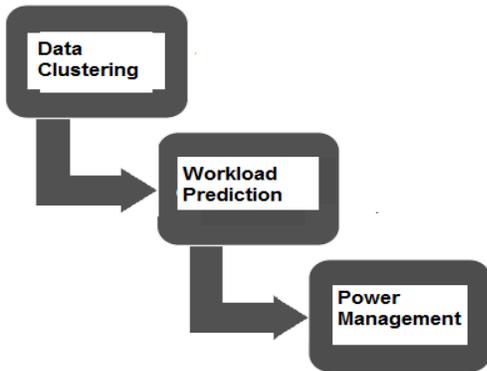


Fig. 1. Life Cycle of Proposed Framework.

1) *Data clustering*: The approach relies on historical workload dynamics for a time period referred to as the observation window. A VM request consists of multiple cloud resources (e.g., CPU, bandwidth etc.). This poses unique challenges to developing prediction techniques. Also, different clients may request different amount and type of the resource. Therefore, it is difficult to predict the demand for each type of resource. To address this issue of maintaining the personalized QoS requirements, we divide requests into several categories and then apply prediction for each category.

2) *Workload prediction*: We rely on the traces as training data samples to calculate the weights. One of the problems in implementation is that we will also need to train the model to adjust these weights according to the workload dynamics, which may vary over time. We refer to these predictive models as to be needed training from time to time. We will use a predictive model that increases the accuracy over time and avoids storing large traces. The model predicts a number of requests based on the learned weights. Next, the model observes requests received in each category. The algorithm uses these observations to update the weights. Therefore, we will find the optimal weights. The predictor has an overhead after observing the actual workload to update the weights. These updates increase the accuracy with time and make it dynamic to adopt the latest variations.

3) *Power management*: The predictions are passed to the Power Management module, which uses this prediction to decide when a PMs go to in ideal state and when become alive. This component is updated with the information of all PMs and maintains their utilizations and states. It uses a heuristic to predict requests and determine how many PMs are alive. The algorithm tries to map requests with live PMs. To

do that, it sorts PMs according to the best fit to the least fit. The conventional algorithm could not be used directly. Thus, a modification is made to the algorithm. This limitation has been addressed by mapping these multiple dimensions into a single metric. Furthermore, heuristic considers the energy when sorting the PMs by the following criteria:

- a) PMs that are in a working state
- b) PMs that have higher utilizations. The utilization is defined as the product of the utilization.
- c) PMs that have higher capacities. The capacity is defined as the product of the capacities of an individual resource.

The aim behind sorting conditions is to use the available PMs already being used, so live PMs are ranked first. Then use the utilization metric, since increasing the utilization of the PMs makes the cluster more efficient. Thus model allows for sleeping more PMs. Finally, based on capacities, we can fit more VMs in a PM.

## II. LITERATURE REVIEW

In this section we are exploring the recent research work carried out to improve the performance of cloud infrastructure and also contribute for VM scheduling and green computing aspects.

### A. Related Work

Cloud Computing (CC) is a multi-tenant framework used by multiple users' concurrently, each exhibiting different and varied behaviour. This heterogeneity shapes highly fluctuating load and creates new usage patterns. VMs interference plays a big part in changes at load. Server load prediction is crucial to ensure efficient resource usage.

### B. Literature Summary

The investigation of green computing is being essential for reducing the carbon footprints and for long-term sustainable computing. To understand the effect of green computing in this paper, a survey is performed on green cloud computing techniques. The key focus is paid on proactive techniques of cloud power management, which involve the predictive strategies for regulating the QoS (quality of service) requirements of applications. According to the collected literature, we found that the VM consolidation by improving the scheduling techniques can significantly preserve datacenters power demands. Additionally, proactive methodologies improve the performance on step ahead. In this context, we also summarize the recent VM scheduling approaches in Table I. These tables include the summary of recent contributions in terms of research work for achieving power efficiency. This summary includes the solutions developed for improve the virtual machine scheduling performance to reduce brown energy and those algorithms which are utilized to derive the required power optimization technique. There are two main key findings as a conclusion of this survey. First, the prediction based VM management in the cloud for consolidating the scattered future requests in multiple machines can reduce the power demand of the datacenters in effective manners. And second, the available

solutions have a lack of adjustment about the uncertainty of users' demand.

the uncertain future demands of users to maintain the effective consumption of power in cloud datacenters.

So here the proposed proactive VM scheduling focused on prediction using unsupervised learning algorithms to handle

TABLE I. REVIEW SUMMARY

Ref. No	Direction	Solution	Significance
[16]	Virtual Machines (VMs) interference	A real-time server load prediction system based on incoming task classification and VM interference.	An improved HAT, with ensemble drift detectors. Able to dealing with changes and good accuracy with less time and memory
[17]	Concerned with balancing servers load	Utilize resource and job response time, enhance scalability, and user satisfaction.	Dynamic resource allocation using EANN to predict VM load and get better performance.
[18]	Prediction of server load	Improving the resource utilization, reducing energy consumption and guaranteeing the QoS.	Integrates the cloud and Markov chain to realize CM-MC algorithm. Results show that algorithm is high accuracy and reduce energy consumption.
[19]	Host load prediction	Proposed a host load prediction method based on Bidirectional Long Short-Term Memory (BiLSTM)	BiLSTM improve the memory capability and nonlinear modeling. 1-month trace of 12K machines is used to validate accuracy.
[20]	Focusing on the issue of host load estimating in mobile cloud	LSTM, for the intricate and long-term arrangement of the cloud condition and dependent on GSO LSTM neural system.	Cloud load forecasting model using LSTM, and GSO to search optimal parameters. And compared with similar algorithms. Results show that the algorithms are offers higher accuracy.
[21]	Performance of dynamic clouds depends on efficiency of its load balancing and resource allocation	A study on the predictive approach for dynamic resource distribution. And a rule-based workload-balancing based on predictions.	Simulation of cloud using CloudSim and used an algorithm with lower computational demand and a faster balancing. The result will show a predictive workload balancing is an effective solution.
[22]	Cloud DBMS load balancing	Distribution of transactions between replicas, load balancing to improve the resources utilization.	A predictive load balancing service for replicated cloud databases.
[23]	a predictive and elastic load balancing service for replicated cloud databases	The distribution of transactions among replicas, load balancing can improve the resources utilization.	Showed that the use of prediction can help to predict possible SLA violations that represent workloads of cloud-replicated databases.
[28]	Datacenter consuming a high amount of energy and increasing carbon emissions.	VM need to be allocated to minimize resource and energy wastage.	Solution for datacenters named E-FPA. Aim is to provide energy-oriented VM allocation using Switching Probability. It enhances energy consumption, Migration, and First Fit Decreasing.
[29]	Green Computing to reduce, power and water consumption, hardware and carbon emission.	Presents an analysis report about green computing and its characteristics.	Discusses about green computing, trending concepts and future challenges. This analysis helps researchers to understand green cloud.
[30]	Economic and environmental costs of data centre and equipped for peak processing.	Idle servers and components of the network consume a significant amount of resources.	Describe the green data centre and metrics. And discuss energy-saving solutions for servers, network, and other green solutions.
[31]	Efficient VM management for energy saving, increasing profit, and preventing SLA violations.	This survey on the proactive VM placement approaches and categorizes them.	Factors such as evaluation parameters, simulation software, workload, power management, and prediction are compared to illuminate VM placement. Issues and future studies are provided.
[32]	VoIP have face a crisis: 1. Lack of resources and, overload; 2. Redundancy of resources and, energy loss.	The SDN can provide a view of the network for resource management. NFV can be used to implement a variety of devices and functions.	GreenVoIP to manage the resources of cloud VoIP centers. It not only prevents overload but also supports green computing. That framework can minimize active devices.
[33]	Communication traffic have imposed a heavy burden on data centers and resulted in high energy consumption.	Edge computing is explored to provision the latency-sensitive applications.	Geo-distribution of edge devices is leverage green computing. It is desirable to maximize utilization of green energy. Investigate cost minimization problem of VM migration, task allocation and scheduling using heuristic algorithm.
[34]	Provisioning Edge computing QoS mainly delay guarantee for delay-sensitive applications. energy consumption in edge servers may be higher	Energy-efficient and delay-guaranteed workload allocation problem in an IoT-edge-cloud computing system are investigated	Offloading workloads to servers, and computation experience, e.g., delay and energy consumption. Delay is un-negligible in a intensive environment. The workload allocations among local, neighbour, minimal energy and delay using algorithm.
[35]	Promote ecosystem services, including mitigation of storm water flooding and water quality degradation	Goals include increasing carbon sequestration, songbird habitat, reducing urban heat effects, and improving the landscape.	GI is improving water and the ecosystem by reducing storm water runoff. Provide design to enable better communication among designers and groups. Demonstrates workflows to facilitate the creation of GI, incorporated models using web applications.
[36]	VM placement	Vector Bin-Packing (VBP) problem to minimize the number of PMs used	FFD variant, Aggregated Rank in FFD is proposed. Experiments using two datasets: based on Amazon and a synthetic dataset. The efficiency of FFD-AR is better.

### III. PROPOSED PROACTIVE VM SCHEDULING

This section explains the proposed proactive virtual machine scheduling technique for optimizing the cloud datacenter performance in terms of power consumption. In this context, this section provides a discussion about the different algorithms and the data analytics steps to explain the work of the required model.

#### A. System Overview

The increasing demand for computational and storage resources motivates us to design sustainable and prolong computing technologies. In this direction, one of the most crucial development is green cloud computing. Green computing technology is providing a way to minimize the cost and consumption of infrastructural assets. Therefore, green cloud computing has become one of the most essential and trending areas of research and development. The key idea is to employ various techniques to switch off the additional computational and network devices that are unused or in an ideal state to preserve the power consumption. Additionally, when the load again appeared on datacenters, machines became alive to deal with the workload.

In this context, we are proposing an unsupervised learning technique for designing the physical machine consolidation scheme. The unsupervised learning techniques are suitable for time-critical applications and also for parameter enhancement and optimization. Therefore, to improve the capability of power management the clustering algorithms are adopted. Therefore, first implemented four popular clustering approaches (namely K-Means, SOM (Self Organizing Map), FCM (Fuzzy C-Means), and K-Medoid) that categorize the cloud datacenters workload into three categories, i.e., low, medium, and high workload groups.

Further, these trained machine learning models are being used for efficient VM allocation and making power on and off decisions based on the predicted outcomes. In this context, a modified VM scheduling algorithm has been proposed. That makes use of one step ahead predicted workload and evaluates the current wearability of data center resources. Based on this decision function, we decide the required resources which fulfill the demand. In this way, we are reducing the migration of processes and maintain less traffic overhead. In addition, by using the predictive method, we estimate the future possible resource demand. Suppose demand is higher than the available one step ahead workload. In that case, we restart the physical machines, or if the future trend shows a low demand, we turn off the machines to utilize the minimum resources.

#### B. Clustering of Workload

To utilize the proactive VM scheduling for improving the performance of cloud datacenters in terms of energy efficiency, we are intended to use the unsupervised learning techniques for predictions.

In this context, Fig. 2 demonstrates the model for learning with the historical workload patterns. Therefore, the Google workload trace dataset is being used for performing the clustering. The dataset consists of parent ID, Task ID, job type, nrmlTaskCores, nrmlTaskMem, and time. Among them,

parent ID and Task ID provide the identification of the process. Thus, we remove one of them, so here we eliminate parent ID for the dataset. The remaining attributes are utilized further for clustering of the tasks. To create clusters, we need to provide a number of clusters here; use  $k=3$  for preparing clusters of three types, to categorize and belong in low, medium and high groups.

Further, we have implemented a provision that will be used to select the clustering algorithm for training. The algorithms are discussed in the previous section. The selected algorithm is used with the trace file and clusters the data. The employed clustering algorithms result in two key outcomes, i.e., validation performance of the clustering algorithm and the centroids identified from the data. These centroids are further being used for predicting the trends of the upcoming workload.

#### C. Predictive VM Scheduling

The VM scheduling in energy efficient manner need to include the following phases:

1) *Predicting the future workload:* To demonstrate the effective VM scheduling and consolidation technique, using the proactive manner. First of all, we need to have workload trends. Therefore, to prepare future trends for each one-minute interval, we have trained machine learning algorithms. These algorithms use the cluster centroids and simple linear regression technique to compute the future trends of the host workload. In this context, let we have a set of centroids (C) such that:

$$C = [C_L, C_M, C_H] \quad (1)$$

Where,  $C_L$  = centroid for small workload,  $C_M$  = centroid for medium workload,  $C_H$  = High workload.

Each centroid  $C_L$ ,  $C_M$ , and  $C_H$  consists of memory and CPU properties of demand. Thus, when talking about the centroids, then we also considering each element of these subsets or centroids. Now, we need to predict a pattern relevant to the upcoming future workload. In this context, first, consider one hour for predicting the workload values. Thus, we extract the last one hour per minute values and keep them in a list  $L_N$  where  $N$  are minutes.

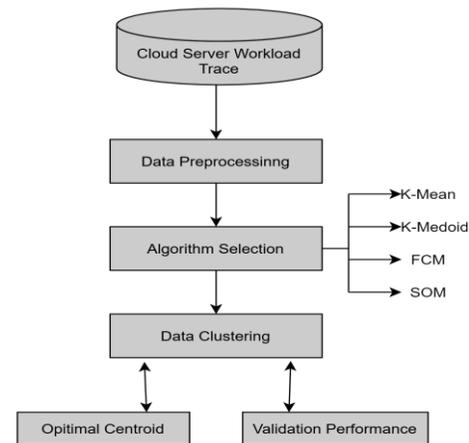


Fig. 2. Workload Clustering.

---

**Algorithm 1: Proposed load Encoding**

---

**Input:** last recent workload list  $L_N$ , list of centroids

$$C = [C_L, C_M, C_H]$$

**Output:** Encoded list  $E_n$

---

**Process:**

1. for ( $i = 1; i < n; i++$ )
    - 1)  $temp = L_i$
    - 2) for ( $j = 1; j < m; j++$ )
      - I.  $tempC = C_j$
      - II.  $d_j = temp - tempC$
    - 3) end for
    - 4)  $S = getShortest(d)$
    - 5)  $e = getlabel(S)$
    - 6)  $E.Add(e)$
  2. End for
- 

Let considering the one-hour forecast, then  $N=60$ . Now we encode the values available in the list with three symbols L, M, and H. The encoding process is demonstrated in algorithm 1. According to the given algorithm 1, we accept a list of likelihood workload list  $L_N$  and prepared centroids  $C = [C_L, C_M, C_H]$ . The algorithm processes both the inputs and prepares a list of encoded patterns of the list. The algorithm extracted each element of the list  $L_N$  and compared it with all the centroids. The most minimum distance centroid is labelled as the encoding value of  $L_N$ . After assigning a label to the load value, we get a new list E of encoded n values in terms of L, M and H.

The next step proposes to utilize the Encoded list  $E_N$  as the initial prediction of the next one-hour workload pattern. Now we need to enhance the prediction. Therefore first, we calculate or difference between the actual extracted value as well as encoded values using the following equation:

$$D_N = L_N - E_N \quad (2)$$

Where  $D_N$  is the difference between the last observed value and reference or actual value.

2) *VM consolidation*: This section explains how the prediction is used in real-time to predict and reduce power utilization by on and off the physical machines. Therefore, let at actual time  $t_a$ , we have a basic prediction taken from the list  $E_N$  for the given time  $t_a$ . That workload is denoted here as  $P_{t_a}$ . Additionally, at that time, we also get the actual workload appeared and denoted as  $W_a$ . Further, at the next time movement  $t_b$ , we need to adjust the initial prediction. Thus, the new predicted value is:

$$P_{t_b} = E_{t_b} + E_r \quad (3)$$

where,

$$E_r = W_a - P_{t_a} \quad (4)$$

Here,  $E_r$  it can be positive or negative.  $E_{t_b}$  is the basic prediction at the time  $t_b$ . Further, we make use of a difference list  $D_N$  to impure the prediction.

$$F = D_{t_a} - E_r \quad (5)$$

The measured different F is demonstrating the influence in prediction error; therefore, the system needs to adjust this for making the final prediction by restructuring the prediction equation using the following equation:

$$P_{t_b} = E_{t_b} + E_r + F \quad (6)$$

Now, the system utilizing the predicted resource demand and the available resources of the datacenter to decide to switch ON and OFF, the physical machine. In this context, we prepare an algorithm for making decisions regarding the same, steps are described as algorithm 2.

---

**Algorithm 2: Predictive VM Scheduling Technique**

---

**Input:** list of datacenters host list  $H_m$ , P predicted workload, T consolidated resource available

---

**Process:**

1. For each next time event
  2. if ( $P < T * 0.66$ )
    - a.  $S = m * 0.2$
    - b. For ( $i = 1; i < m; i++$ )
      - 1) if ( $m < S$ )
        1. *MigrateProcessofHost*( $H_i$ )
        2.  $HID = H_i$ . Sleep
      - 2) End if
    - c. end for
  3. Else
    - 1)  $HID.Start(Top,1)$
    - 2)  $H_m.Add(HID)$
  4. End if
  5. End for
- 

According to the discussed algorithm 2, we have the host lists  $H_m$  with m elements; on the other hand, we compute the total consolidated resources available as T. the algorithm starts with the analysis of each time increment. To compute the predicted demand of resources P. if the P is less than 66% of available resources in the consolidated resource T, we compute the capacity of 20% of machines available, which the existing resources will handle; thus, we turn off one physical machine at a time. These two thresholds depend on the designer and the application's quality of service requirements. Otherwise, each time we turn on one physical machine available in the sleep list of the host.

#### IV. RESULTS ANALYSIS

This section provides the experimental analysis of the proposed VM scheduling approach. Thus, first the clustering algorithms are applied on the dataset. The predictive performance of ML techniques is measured. Additionally, the performance of cloud infrastructure has also been evaluated and simulated in this section.

##### A. Experimental Scenarios

The experimental simulation of proposed proactive VM scheduling is done through Cloud-Sim simulator with a datacenter of 5 servers [Host1, Host2, Host3, Host4, Host5] having 20, 5,10 20, and 10 VMs respectively. The

computational setup of the simulated datacenter can be elaborate through Table II.

TABLE II. SIMULATION SETUP OF PROPOSED PROACTIVE VM SCHEDULING

Datcenters	Host1	Host2	Host3	Host4	Host5
CPU per VM (MIPS)	250	250	250	500	250
RAM per VM (MB)	2048	2048	2048	2048	2048
Total Storage (GB)	1M	1M	1M	1M	1M
Bandwidth (Gbits/sec)	1000	1000	1000	1000	1000
VMs	20	5	10	20	10

The VM scheduling ensures the optimal VM resource utilization and reduction in power consumption. The aim is to investigate the proactive VM scheduling techniques using ML techniques to understand the demand of resources and prepare the plan to better schedule the cloud VM for reducing the power consumption and enhancing the running cost of the cloud. Therefore, first, some unsupervised learning approaches are compared to identify the best-performing clustering approach. Further, an algorithm will be proposed to design a proactive resource scheduling technique to achieve Green Computing, reduce power consumption, and reduce carbon emission. Thus, the given experiment includes two experimental scenarios:

1) *Comparing different clustering algorithms:* Clustering is an unsupervised learning task. It automatically discovers grouping the data. Clustering only interpret the data and find natural groups. In this scenario, we compare four clustering algorithms, namely, K-Means, SOM (Self Organizing Map), FCM (Fuzzy C Means), and K-Mediod over different performance parameters and different data sizes.

2) *Comparing simulation performance of cloud for VM scheduling:* This simulation scenario implements proactive VM scheduling techniques using the above-discussed algorithms. Thus, using all the algorithms, the prepared VM Scheduling techniques are compared to investigate energy consumption.

### B. Experiments Comparing Clustering Algorithms

In this section, a comparative performance study is carried out among different unsupervised learning algorithms. The aim is to obtain an efficient and accurate algorithm for predicting the accurate future VM resource demand and can optimize the scheduling to better resource allocation. The comparative outcomes of the algorithm’s performance are reported in this section.

We are investigating the efficiency of the algorithms, so it needs to compute the models’ performance in terms of memory and time required to process the workload of different sizes. The memory usage of the algorithms is measured based on java function and using the following formula:

$$M_{Used} = M_{Assigned} - M_{Free} \tag{7}$$

Similarly, the time consumption of the implemented algorithms is given as the amount of time consumed for processing the data using the algorithms is given as the time consumption of the algorithm. That can be calculated using the following formula:

$$Time_{Consumed} = Time_{End} - Time_{Start} \tag{8}$$

The memory and time consumption of the implemented clustering algorithms are described using Fig. 3(A) and (B). Additionally, the observed values are given in Table III. In both the line graphs, the X-axis demonstrate the size of experimental dataset size in terms of instances, additionally, in Fig. 3(A) the Y-axis shows the memory used in terms of kilobytes (KB) and in Fig. 3(B), the Y-axis shows the time consumed in processing the data in terms of seconds (Sec). According to the obtained performance, the SOM and FCM are producing a higher amount of time and memory overhead during the computation. Therefore, these algorithms are also producing a significant delay during the cloud VM allocation. Therefore, according to all the obtained performance parameters, we can say the K-Means and K-Mediod are time and memory efficient. Thus, we recommend being using the K-Means and K-Mediod algorithms to reduce the delay in scheduling.

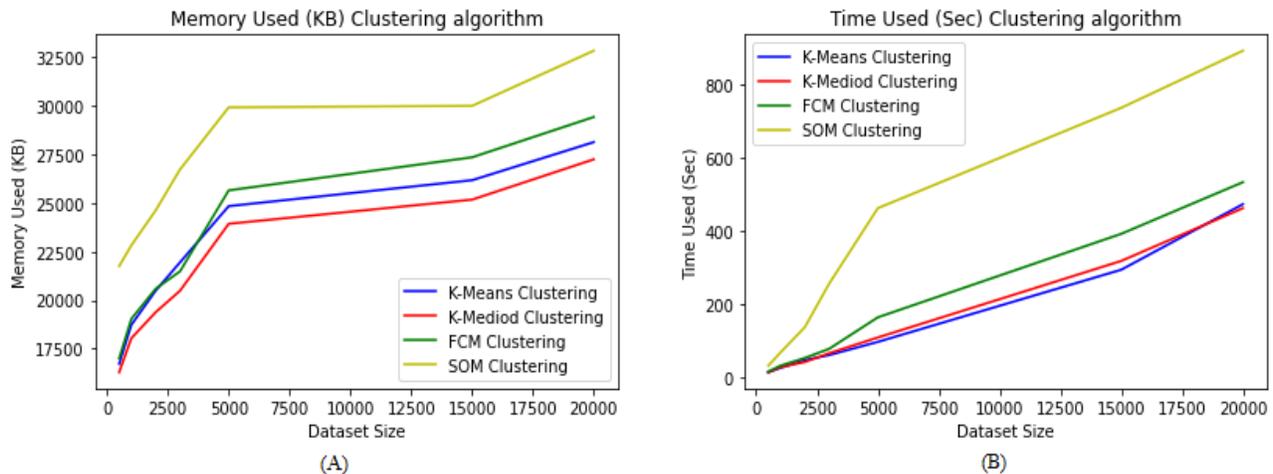


Fig. 3. Comparative Performance of Clustering Algorithms in (A) Memory used (B) Time Consumed.

TABLE III. PERFORMANCE OF CLUSTERING ALGORITHMS IN MEMORY USAGE AND TIME CONSUMED

Dataset Size	Memory Usage				Time Consumed			
	K-Mean	K-Medioid	FCM	SOM	K-Mean	K-Medioid	FCM	SOM
500	16712	16279	16992	21746	14	14	16	32
1000	18718	18028	19028	22817	26	28	32	68
2000	20484	19372	20582	24617	47	42	53	137
3000	21942	20478	21477	26725	61	66	78	256
5000	24837	23927	25649	29927	97	109	164	462
15000	26173	25173	27352	30002	294	318	392	736
20000	28134	27248	29428	32846	473	462	533	892

C. Proactive VM Scheduling for Green Computing

The VM scheduling by proactive techniques are demonstrated using different clustering algorithms, namely K-Mean, K-Medioid, FCM (Fuzzy C Mean), and SOM (Self Organizing Map). The aim is to find the impact on scheduling using these ML techniques over different parameters. The simulation consists of two major goals:

- a) Compare the Impact of four different clustering based proactive scheduling over average processing time ( $Pt_{AVG}$ ).
- b) Compare the impact of four different clustering based proactive scheduling over efficient power consumption (PC).

1) *Average processing time*: The process time is the amount of time for which a central processing unit (CPU) was used for processing instructions. The processing time is a combination of the total time a process resides in the processor and the time required to wait for the resource. Processing time ( $Pt$ ) is generally calculated in MS (Milliseconds).

$$Pt_{AVG} = \frac{1}{N} \sum_{i=1}^N Pt_i \tag{9}$$

Where, N number of processes to be scheduled, and  $Pt_i$  is the processing time of the  $i^{th}$  process.

Table IV have the simulation results of average processing time for proposed proactive VM scheduling based on four different clustering to evaluate which one take minimum time in VM scheduling.

The comparative evaluation of four different clustering based proactive VM scheduling using average processing time ( $Pt_{AVG}$ ) is also shown in Fig. 4. That is a bar graph that is prepared using the observations collected from the simulation. The processing time of the implemented simulation is measured here in terms of Minutes. In order to show the performance, the X-axis contains the number of VMs, and in the Y axis, the average processing time in minutes is reported. According to the system's performance, K-Medioid clustering algorithm requires less processing time than other similar algorithms.

2) *Power consumption*: The entire VM scheduling optimization techniques are works to enhance the profitability of cloud service providers. In this context, the low energy or power consumption is tried to reduce by optimal resource allocation of the cloud. Table V is used to show the simulation results of power usage during proactive VM scheduling based

on four different clustering to evaluate which one gives the efficient usage of power during VM scheduling.

TABLE IV. SIMULATION RESULT OF AVG. PROCESSING TIME

Dataset Size	K-Mean	K-Medioid	FCM	SOM
1000	10.2	9.3	11.2	9.3
2500	21.5	18.7	23.5	20.9
5000	43.3	39.1	46.3	29.5
7500	60.4	55.9	68.4	56.8
10000	80.3	73.2	90.3	76.3
15000	115.9	101.2	126.9	108.1
20000	173.3	158.8	182.3	163.2

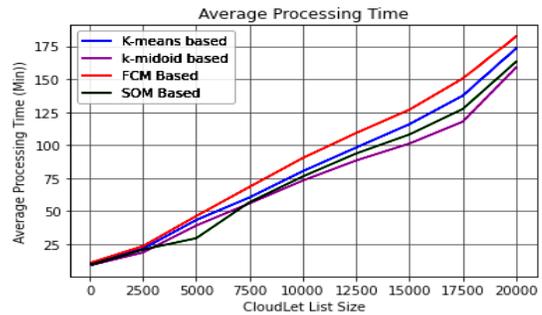


Fig. 4. Performance of Proactive VM Scheduling's on Average Processing Time.

TABLE V. SIMULATION RESULTS OF POWER CONSUMPTION

Dataset Size	K-Mean	K-Medioid	FCM	SOM
1000	60.3	54.8	58.9	53.8
2500	98.3	108.2	94.1	86.6
5000	124.5	128.7	119.2	109.5
7500	160.3	155.5	153.1	136.9
10000	198.3	201.3	183.7	166.3
15000	225.9	241.2	216.4	201.9
20000	263.3	266.2	252.3	245.4

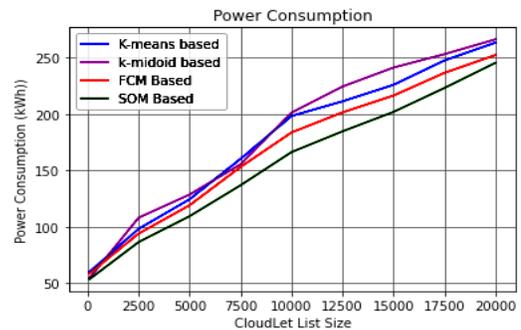


Fig. 5. Performance of Proactive VM Scheduling's on Power Consumption.

The Power Consumption is measured here in terms of KW/h. The recorded power consumption for all clustering based proactive VM scheduling's is shown in Fig. 5. To show the performance, the X axis shows the number of VMs, and the Y-axis shows the cloud's power consumption. According to the performance of the system, the FCM and SOM-based models report the lowest consumption.

## V. CONCLUSION

The proposed work is implementing a simulation-based experimental study for designing an effective and efficient proactive VM scheduling approach to minimize the energy consumption of the cloud infrastructure. The scheduling techniques are essential for allocating the resources to the users' request to limit the unwanted resource utilization of cloud datacenters. That also increases the energy consumption, maintenance cost, and running cost of the datacenters. Therefore, we need some effective resource allocation strategy that can deal with the dynamic nature of workload. In addition, by implementing the host switch ON and OFF technique, we can also control the power consumption and running cost of datacenters.

Therefore, the proposed work is motivated to design and develop a proactive VM scheduling model which utilizes four different unsupervised learning techniques to predict the future demand of the cloud. Additionally, based on the predicted demand trend, the proposed algorithm plans to keep switching OFF the resources when the model predicts the less resource demand trend. In this way, by replacing, we prepared four resource scheduling techniques by using the reported clustering algorithms. Based on the experimental analysis and obtained findings, we can see the model successfully preserves the energy by making inactive hosts in datacenters to minimize energy consumption. Additionally, the obtained performance of the models also justifies our argument for the proposed proactive VM scheduling model.

## VI. FUTURE SCOPE

In near future we are motivated to perform more extensive experiments on the given resource provisioning model, additionally we also compare the technique with the classical resource scheduling model to find how the proposed technique can improve the productivity of the model. Finally, in near future we also work for involving the deep learning models for making the accurate future resource demand prediction.

### REFERENCES

- [1] J. M. T. I. Jayalath, E. J. A. P. C. Chathumali, K. R.M . Kothalawala, N. Kuruwitaarachchi, "Green Cloud Computing: A Review on Adoption of Green-Computing attributes and Vendor-Specific Implementations", Smart Computing and Systems Engineering, 2019, Paper No: SC 24.
- [2] Q. Zhang, X. Lin, Y. Hao, J. Cao, "Energy-Aware Scheduling in Edge Computing Based on Energy Internet", IEEE access VOLUME 8, 2020.
- [3] N. Gholipour, E. Arianyan, R. k. Buyya, "A novel energy-aware resource management technique using joint VM and container consolidation approach for green computing in cloud data centers", Simulation Modelling Practice and Theory 104 (2020) 102127.
- [4] M. A. Alsaih, R. Latip, A. Abdullah, S. K. Subramaniam, K. A. Alezabi, "Dynamic Job Scheduling Strategy Using Jobs Characteristics in Cloud Computing", Symmetry 2020, 12, 1638; doi:10.3390/sym12101638.
- [5] M. Masdari, M. Zangakani, "Green Cloud Computing Using Proactive Virtual Machine Placement: Challenges and Issues", J Grid Computing, <https://doi.org/10.1007/s10723-019-09489-9>.
- [6] R. Kaur, G. Kaur, "Proactive Scheduling in Cloud Computing", Bulletin of Electrical Engineering and Informatics ISSN: 2302-9285 Vol. 6, No. 2, June 2017, pp. 174~180, DOI: 10.11591/eei.v6i2.649.
- [7] S. Ilager, K. Ramamohanarao, R. K. Buyya, "ETAS: Energy and thermal-aware dynamic virtual machine consolidation in cloud data center with proactive hotspot mitigation", Concurrency Computat Pract Exper. 2019;31:5221. 2019 John Wiley & Sons, Ltd. 1 of 15.
- [8] W. Zhang, X. Hu, J. Li, H. Guan, "CoINT: Proactive Coordinator for Avoiding Interruptability Holder Preemption Problem in VSMF Environment", IEEE INFOCOM 2018 - IEEE Conference on Computer Communications, 978-1-5386-4128-6/18/\$31.00.
- [9] E. Cortez, A. Bonde, A. Muzio, M. Russinovich, M. Fontoura, R. Bianchini, "Resource Central: Understanding and Predicting Workloads for Improved Resource Management in Large Cloud Platforms", SOSP'17, October 28, 2017, Shanghai, China © 2017 Association for Computing Machinery, ACM ISBN 978-1-4503-5085-3/17/10.
- [10] Y. Cheng, W. Chen, Z. Wang, Y. Xiang, "Precise contention-aware performance prediction on virtualized multi-core system", Journal of Systems Architecture 72 (2017) 42–50.
- [11] L. He, D. Zou, Z. Zhang, K. Yang, H. Jin, S. Jarvis, "Optimizing Resource Consumption in Clouds", in Proc. of the 12th IEEE/ACM International Conference on Grid Computing(Grid 2011), 2011, PP.42-49.
- [12] Maarten van Steen, Andrew S. Tanenbaum, "A brief introduction to distributed systems", Computing (2016) 98:967–1009, DOI 10.1007/s00607-016-0508-7.
- [13] Auday Al-Dulaimy, Wassim Itani, Ahmed Zekri1, and Rached Zantout, "Power management in virtualized datacenters: state of the art", Journal of Cloud Computing: Advances, Systems and Applications (2016) 5:6 DOI 10.1186/s13677-016-0055-y.
- [14] Leila Helali, Mohamed Nazih Omri, "A survey of data center consolidation in cloud computing systems", Computer Science Review 39 (2021) 100366.
- [15] Dzmityr Kliazovich, Pascal Bouvry, Samee Ullah Khan, "DENS: data center energy-efficient network-aware scheduling", Cluster Comput, DOI 10.1007/s10586-011-0177-4.
- [16] H. Toumi, Z. Brahmi, M. M. Gammoudi, "Real time server load prediction system for the ever-changing cloud computing environment", ScienceDirect – 2019.
- [17] K. S. Qaddoum , N. N. El Emam , M. A. Abualhaj, "Elastic neural network method for load prediction in cloud computing grid", International Journal of Electrical and Computer Engineering (IJECE)-April 2019.
- [18] X. Xiaolong, Z. Qitong, M. Yiqi, L. Xinyuan, "Server load prediction algorithm based on CM-MC for cloud systems", IEEE - Journal of Systems Engineering and Electronics Vol. 29, No. 5, October 2018.
- [19] H. Shen, X. Hong, "Host Load Prediction with Bi-directional Long Short-Term Memory in Cloud Computing", arXiv – 2020.
- [20] P. Sudhakaran, S. Swaminathan, D. Yuvaraj, S. S. Priya, "Load Predicting Model of Mobile Cloud Computing Based on Glowworm Swarm Optimization LSTM Network". IJIM – 2020.
- [21] M. Jodayreea, M. Abazab, Q. Tan, "A Predictive Workload Balancing Algorithm in Cloud Services", ScienceDirect -2019.
- [22] C. S. S. Marinho, E. F. Coutinho, J. S. C. Filho , L. O. Moreira, F. R. C. Sousa, J. C. Machado, "A Predictive Load Balancing Service for Cloud-Replicated Databases", IEEE – 2017.
- [23] C. S. S. Marinho, L. O. Moreira, E. F. Coutinho, J. S. C. Filho, F. R. C. Sousa, J. C. Machado, "LABAREDA: A Predictive and Elastic Load Balancing Service for Cloud-Replicated Databases", Journal of Information and Data Management, Vol. 9, No. 1, June 2018.
- [24] H. Moradi, W. Wang, A. Fernandez, D. Zhu, "uPredict: A User-Level Profiler-Based Predictive Framework for Single VM Applications in Multi-Tenant Clouds", arXiv – 2019.

- [25] S. Mittal, Prof. M. Dubey, "AMO Based Load Balancing Approach in Cloud Computing", IOSR Journal of Computer Engineering (IOSR-JCE) – 2017.
- [26] S. Manaseer, M. Alzghoul, M. Mohmad, "An Advanced Algorithm for Load Balancing in Cloud Computing using MEMA Technique", International Journal of Innovative Technology and Exploring Engineering (IJITEE) January 2019.
- [27] X. Zhou, F. Lin, L. Yang, J. Nie, Q. Tan, W. Zeng, N. Zhang, "Load balancing prediction method of cloud storage based on analytic hierarchy process and hybrid hierarchical genetic algorithm", SpringerPlus (2016).
- [28] U. M. Joda, A. S. Ismail, H. Chizari, G. A. Salaam, A. M. Usman, A. Y. Gital, O. Kaiwartya, A. Aliyu, "Virtualization oriented Green Computing in Cloud Datacenter: Flower Pollination Approach", Springer – 2018.
- [29] A. Patil, R. Patil, "An Analysis Report on Green Cloud Computing Current Trends and Future Research Challenges". Elsevier SSRN – 2019.
- [30] P. A. Naidu, P. Chadha, V. Nalina, "Efficient Strategies for Green Cloud Computing", Journal of Network Communications and Emerging Technologies (JNCET) Volume 10, Issue 6, June (2020).
- [31] M. Masdari, M. Zangakani, "Green Cloud Computing Using Proactive Virtual Machine Placement: Challenges and Issues", Springer Nature B.V. 2019.
- [32] A. Montazerolghaem, M. H. Yaghmaee, A. L. Garcia, "Green Cloud Multimedia Networking: NFV/SDN based Energy-efficient Resource Allocation", IEEE Transactions on Green Communications and Networking – 2017.
- [33] L. Gu, J. Cai, D. Zeng, Y. Zhang, H. Jin, W. Dai, "Energy efficient task allocation and energy scheduling in green energy powered edge computing", Elsevier – 2019.
- [34] M. Guo, L. Li, Q. Guan, "Energy-Efficient and Delay-Guaranteed Workload Allocation in IoT-Edge-Cloud Computing Systems", 2019 IEEE.
- [35] L. Leonard, B. Miles, B. Heidari, L. Lin, A. M. Castronova, B. Minsker, J. Lee, C. Scaifed, L. E. Band, "Development of a participatory Green Infrastructure design, visualization and evaluation system in a cloud supported jupyter notebook computing environment", 2018 Elsevier Ltd.
- [36] S. Jangiti, E. S. Ram, V. S. S. Sriram, "Aggregated Rank in First-Fit-Decreasing for Green Cloud Computing", Springer Nature Singapore Pte Ltd. 2019.

# Expert Review on Mobile Augmented Reality Applications for Language Learning

Nur Asyiah Suwadi<sup>1</sup>, Nazatul Aini Abd Majid<sup>2</sup>  
Meng Chun Lam<sup>3</sup>

Mixed Reality and Pervasive Computing Lab, Center for  
Artificial Intelligence Technology, Faculty of Information  
Science & Technology, Universiti Kebangsaan Malaysia  
43600 Bangi, Malaysia

Junaini Kasdan<sup>5</sup>

Institut Alam & Tamadun Melayu (ATMA), Universiti  
Kebangsaan Malaysia, 43600 Bangi

Nor Hashimah Jalaluddin<sup>4</sup>, Aznur Aisyah Abdullah<sup>6</sup>

Center for Research in Language and Linguistics  
Faculty of Social Sciences and Humanities  
Universiti Kebangsaan Malaysia, 43600 Bangi, Malaysia

Afifuddin Husairi Hussain<sup>7</sup>, Azlan Ahmad<sup>8</sup>  
Daing Zairi Ma'arof<sup>9</sup>

Pusat Citra Universiti, Universiti Kebangsaan Malaysia  
43600 Bangi, Malaysia

**Abstract**—Many mobile applications that can increase user engagement and promote self-learning have been developed to date. Nevertheless, mobile applications specific to Malay language learning for non-native speakers with relevant materials are still lacking. Moreover, expert reviews are needed to identify usability issues and check whether such applications can meet the learning goal with relevant materials features. This study developed an augmented reality (AR)-based mobile application called *RakanBM* for learning the Malay language (i.e. the language officially spoken in Malaysia), and then performed an expert review on the application contents, text presentations, learning outcomes, assessments, effectiveness, efficiency, and satisfaction. The expert review was conducted by a panel of six experts from two specific fields, namely the Malay language and Human-Computer Interaction (HCI), using methods such as cognitive walkthrough (CW), semi-structured interviews, think-aloud protocols, and survey. The results from CW, semi-structured interviews, think-aloud protocols shows that enhancement was needed on user interface and user experience in term of aesthetic and interactivity. The survey results were classified into two levels: high (mean > 4.0) and satisfied (mean > 3.5). Application factors that were recorded as satisfied were the application contents, text presentations, and satisfaction, while the factors recorded as high were the learning outcomes, assessments, effectiveness, and efficiency. The comments or suggestions for improvement were mainly around the contents of the application. Nevertheless, the application received good comments on its usefulness and the topics covered, which were suitable and best for non-native speakers. The findings of this study can guide developers and researchers in the development of future applications that can support language learning for non-native speakers in particular.

**Keywords**—AR; expert review; HCI; language learning; mobile application; self-learning

## I. INTRODUCTION

Mobile phone device is one of the most popular types of information and communication technology (ICT) as digital learning has been an evolution in the present days[1]. The use of mobile applications for language learning has shown

promising outcomes, especially for language improvement, learner interaction [2, 3], and learner motivation [4]. The use of a mobile phone in and out of the classroom can help students learn more effectively and create a conducive environment for effective teaching and learning [5]. Similarly, flexible learning would be less costly, adaptable, require little instrument, and is easy to use. These advantages allow the implementation of mobile learning in almost all learning environments. Furthermore, such technological advancements can make learning more efficient and enjoyable for students [6]. Previously, several language learning using the mobile application has been invented and conveyed positive feedback from learners, for instance, Mayo language [7], Spanish language [8], Malay language [6] and etc.

In the context of the Malay language, not only the written materials, in fact, the audio and video in electronic forms are far from adequate. It is challenging to learn Malay because it has some elements of modification from other languages such as English and Arabic [9] and was influenced by Indonesian and English pronunciation as well [10]. In another study, [6] introduced the Malay Language Mobile Learning (M-Lang) system using the near field communication (NFC) technology to utilise mobile learning in all learning environments as this technological improvement can make learning more effective and fun for students. However, the system was only in the early stages and excluded AR technologies. The study realised that it was challenging to study and teach foreign languages, which the fundamental principle is to ensure that learners are introduced to the desired foreign language accordingly. At the same time, most of the new applications are limited to elementary-level students[11], and there is also a lack of attractive functionality [12].

Previous studies have highlighted that the Malay language learning deficiency, especially in the mobile application, has become an obstacle for learners to learn the language. Therefore, a better mobile application for Malay language learning are beneficial in ensuring learners, especially foreign students, have a basic knowledge of the language, which could

help them communicate with the locals. This study aimed to validate and ensure that the low-fidelity *RakanBM* prototype was relevant and suitable to support Malay language mobile learning. An expert review was conducted to identify usability issues and check whether the prototype can meet the learning goal with relevant materials features. The remainder of this paper is organised in the following manner: Section II describes the related works and expert reviews methods; Section III presents the evaluation procedure for the developed mobile application; Section IV provides a detailed description of the results and discusses the main features of the application that bring positive results, especially for learning outcomes, assessments, effectiveness, and efficiency; and Section V concludes the findings.

## II. RELATED WORK

The related works highlighted previous studies, including mobile application, language learning, and review method to identify the potential of *RakanBM* application towards users.

### A. Mobile Applications on Languages Learning

Many approaches have been investigated on the use of mobile applications for language learning. For instance, Bojórquez, Villegas [7] aimed to identify the perceptions of undergraduates in the task of learning the Mayo language (i.e. language spoken in north-western Mexico) through a specific mobile AR (MAR) program used by a group of students. The game named *Lotería Mayo* use was based on images and audio using MAR through a card game. A survey was collected from students with items concerning the use and technology acceptance and cultural dimensions. Resultantly, although the MAR system could be easily used, there was still room for improvement, especially on the students' ability to continue their learning experience both within and outside the classroom that should be enhanced and made more effective. Similarly, [8] developed a mobile application having game-like activities with a grammar-focused mobile application to learn Spanish Languages. The study aims to determine the motivational and affective engagement of students towards mobile applications. Results revealed that students' inspiration and affective involvement were growing. The mobile apps allowed learners to work collaboratively and learn about conjugating verbs from each other. In another study, [3] found that *Busuu*, one of the most popular apps for language learning in the market, boosted the use of mobile application technology to a higher level. The app is part of the *Busuu* network for language learning and offers 12 different languages organised in levels. The majority of users evaluated were beginners and learning for personal reasons. The *Busuu* app helped users to better understand the language studied, especially in terms of vocabulary.

Other studies have investigated the learning impact of such applications. For instance, (Ng, Bakri, & Rahman, 2016) investigated the mobile courseware application's impact on children with special needs. The study found that the application was suitable for children with learning difficulties and had positively impacted their learning performance compared to the traditional teaching method. The application, which consists of basic Malay language syllables, was developed to assist educators and parents in teaching children

with special needs to improve their learning progress from time to time.

### B. Mobile Augmented Reality Applications

The ability of AR technology has been investigated by researchers because it has been proven to boost learning performance [13-16]. The AR technology enables a view of reality to be modified by the addition of digital information like three-dimensional (3D) model, two-dimensional (2D) image, video, and audio. The modification improves a person's perception of reality. This technology consists of four main components: (1) marker which is the target object in the reality; (2) a camera of a mobile phone to capture the target object, which is the marker; (3) a mobile phone to store and process information, which is the captured image or the target object (marker); and (4) digital content that will be displayed on the mobile phone screen, where the tracked image by the phone camera is the marker. Fig. 1 shows an example of an AR application where the marker is an image of fried noodles. When the camera phone has tracked the marker, digital information corresponding to the name of the food in Malay which is 'Mi goreng' will be displayed on the mobile screen.

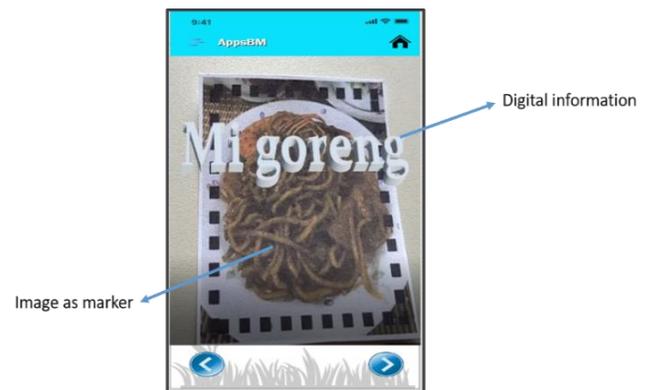


Fig. 1. Addition of Word 'Mi goreng' with Audio on Top of the Marker via AR.

AR provides simulated access to learning methods and has proved to be an effective 3D visualisation technology in educational areas [17, 18]. Ali and Azmi [12] investigated the use of AR for Malay language learning by developing a MAR Malay language application for international students to learn the language. Although the study found that students were satisfied with the developed application, the features and contents could be further extended. Moreover, the application was only in the early stages and not yet published publicly [12]. Based on the review of relevant studies, it can be concluded that studies on Malay language learning utilising AR are still limited, and further research is needed to deepen the knowledge, especially in supporting language learning. Therefore, this study introduced a Malay language mobile application known as *RakanBM* with comprehensive content embedded with AR technology to fulfill the current limitation of the domain.

### C. Expert Review Method

In this section, the expert review method is further described. An expert review is a form of testing that can be used to ensure that students are not exposed to any

inappropriate procedure that could affect their learning [19]. The selected expert evaluation method was appropriate because only a small sample of feedback was required to evaluate and support the application development. As such, the value of this expert review method has been recognised in software quality assessment [20]. This method can be classified into four categories: CW, semi-structured interviews, thinks-aloud protocols, and surveys.

1) *CW*: Walkthroughs take place where the activities as carried out in the user testing process are conducted by experts. Cognitive and pluralistic walkthroughs are the two primary walkthrough forms. CW seeks to simulate the problem-solving skill of users in each separate task, and it also relies on assessing how learnable the method is [21]. In addition, CW determines whether the end-users background knowledge and the technological cues embedded in the computer system interface are adequate to help the end-users accomplish a task. Furthermore, CW focuses on cognitive behaviour like recognising icons and behavioural or physical actions like mouse clicks necessary to complete tasks. This approach is extremely helpful when designing technologies for inexperienced users because it can recognise usability challenges that can impede task completion [22, 23]. A CW technique is a test that uses a sequence of actions or steps on a user interface to achieve a specific goal, and it is often used to test usability based on actions and ways of thinking. Besides seeking to identify problems and measure the level of complexity of each task scenario, another goal is to get an idea of the extent to which the interface supports a positive level of user experience or identify any areas that may cause difficulties [24]. CW is also a platform to detect misunderstandings between the user and the designer about a certain task involved [25]. In this study, the expert review using CW employed experts from the Malay language and HCI fields of expertise.

2) *Semi-structured interviews*: Typically, semi-structured interviews are in the form of a face-to-face interview on a relevant platform (e.g. digital) that focuses on usability-related topics such as the application's functionality, navigability, and ease of use. Such engagements are helpful to collect knowledge about a person's behaviours, values, practices, and experiences [26]. In this study, semi-structured interviews were conducted with six experts on the application prototype. The focus was on the content and interface of the materials and potential improvements based on their recommendations. The interviews determined that one of the main goals of the interactive experience should be to foster user experience while using the application [27].

3) *Think-aloud protocols*: Many studies have used the think-aloud protocol to evaluate the websites and mobile applications concerning their usability [28]. The method is a usability assessment that gathers information on functionality, navigability, and ease of use while end-users interact with the application. As part of a heuristic evaluation, users (i.e. end-users and/or experts) communicate their opinions and concerns in real-time as they perform tasks, enabling observers to see the

cognitive process involved. During the think-aloud assessment, the researcher usually uses software to record the users' responses, e.g. verbal comments and physical responses such as eye movements. This approach examines real issues faced by end-users as well as the factors causing those problems, offering insight into usability deficiencies [22, 29].

4) *Survey*: A questionnaire used in survey is a set of questions or items in form of writing. It is a method designed specifically to collect information for analytical purposes that can answer research questions. Researchers use several standardised and validated questionnaires to quantitatively evaluate the questionnaire [30]. Typically, a survey involves participants scoring items in questionnaires using a predetermined scale. This study obtained feedback from expert evaluators (respondents) on the mobile application design using a set of questions, which helped evaluate the low-fidelity application in terms of contents, text presentation, learning outcome, assessment, effectiveness, efficiency, and satisfaction. In other words, the questionnaire measured the level of user experience on the prototype. The questionnaire technique consisted of open and closed structured questions. In principle, closed-ended questionnaire questions offer a set of answer choices and are used to obtain uniform answers. On the contrary, open-ended questions provide an opportunity for respondents to give opinions or suggestions, and they complement closed-ended questions [31].

### III. METHODOLOGY

In this section, the design of the application and evaluation procedure for the developed mobile application is presented through Phase I, Phase II and Phase III. There are seven main chapters in the RakanBM application: vowel and consonant systems, greetings, numbers and currency, time, day, direction, and food. Furthermore, some elements (e.g. videos, listening exercises, quizzes, vocabulary, and practices using AR technology) diversify the approach and attract users to learn the Malay language. Interactivity is also offered by providing users with scores for each exercise (i.e. a set of tasks) completed. At the same time, the application also comes with feedback (e.g. "excellent", "very good", "keep trying", and "try again") interface, displayed according to the users' achievements after completing a task as a medium to increase user motivation and continue using the mobile learning application.

#### A. Phase I: The Development of RakanBM

The *RakanBM* prototype was developed in collaboration with experts in the Malay language and then evaluated using CW, semi-structured interviews, think-aloud protocols, and surveys (i.e. open and closed structure questions) methods. Fig. 2 illustrates the application developed using Adobe Xd software based on digital prototyping. The hardware required included a notebook and a smartphone. In addition, the related software and programming language for the application development were such as 3D Viewer - for AR model, Adobe Photoshop - for editing marker, Vuforia - for generating marker, Filmora - for video and sound editing, Unity - as the engine, and C# - for coding.

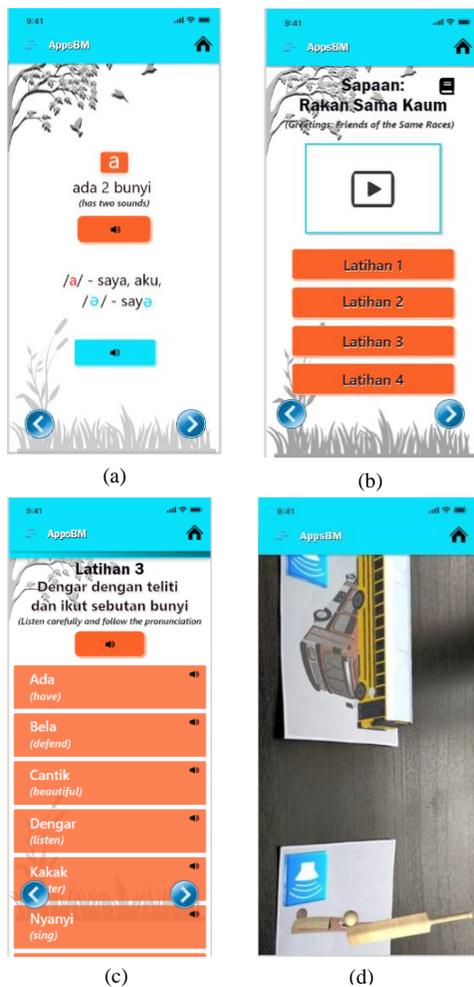


Fig. 2. Screenshots of the RakanBM Prototype. (a) Text Content. (b) Video Screen. (c) Audio Screen. (d) AR Content.

Fig. 2 shows four screenshots of the RakanBM application: Fig. 2(a) illustrates the text content used to present the language learning basics on vowels and consonants. Each vowel and consonant is supported with audio features for users to learn reading and at the same time to listen to the correct pronunciation of the particular Malay words; Fig. 2(b) illustrates the video screen concerning the daily routine conversation. From this approach, users can apply the language in their surroundings. Fig. 2(c) illustrates the audio screen for exercise. Users can learn the pronunciation of the listed words by clicking the sound button. Users also can repeat the exercise several times to ensure mastery of words, and Fig. 2(d) presents the advanced feature of the application, the AR-based content, designed to attract users' attention towards learning via the latest technology. The AR screen shows a 3D model used in several topics in the applications, such as number, currency, and time. The markers shown are images of a bus and that of a bat. Apart from a 3D model (i.e. the digital content), an audio icon appeared on the same screen when the phone camera tracked the markers. Therefore, users can relate the static images with better visualisation of the object with accurate pronunciation repeatedly.

**B. Phase II: Evaluation Procedure for CW, Semi-Structured Interviews and Think-Aloud Protocols**

One of the advantages of an expert review is that it requires only a small number of experts to identify the flaw of the mobile application (Beecham et al., 2005). This study performed an expert evaluation to ensure the relevance of the RakanBM application prototype. The expert evaluation involved the perspective of contents and interface of the prototype. Table I provides the background of the six experts recruited for the review. The selected experts were from two fields, namely the HCI and the Malay language. The demographics of the experts are as follows:

- Malay language: The experts consisted of educators who specialise in the field of the Malay language and have more than five years of work experience in related fields.
- HCI: The experts consisted of individuals with more than five years of experience in the mobile application development field.

TABLE I. DEMOGRAPHIC OF EXPERTS (I.E. EVALUATORS)

Expert	Specialisation	Year of Experience	Gender
A	Malay language expert	25	Female
B	Malay language expert	11	Female
C	Malay language expert	31	Female
D	Malay language expert	28	Male
E	HCI expert	20	Female
F	HCI expert	20	Female

The Fig. 3 illustrates the evaluation procedures involved. This study started the testing by explaining the evaluation objectives to the experts. The experts were then introduced to the mobile application and explained the concept of the developed application prototype. Next, the RakanBM application workflow was described in detail to the experts for clarity on the activity workflow. Afterward, activities such as prototype testing using CW techniques, semi-structured interviews, and think-aloud protocols were also carried out.

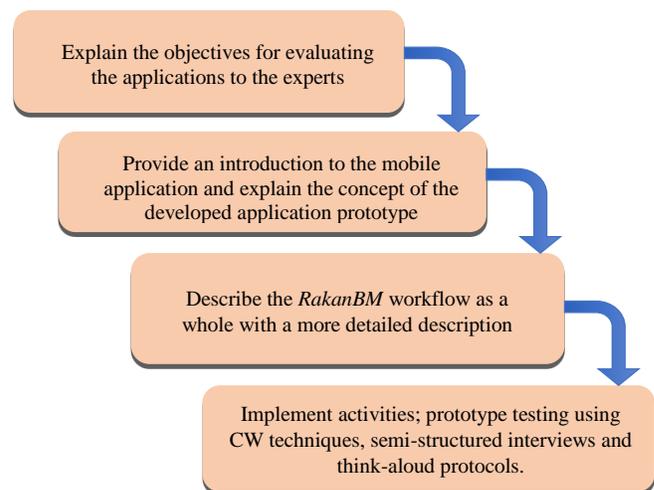


Fig. 3. Evaluation Procedure for the RakanBM Prototype using CW Techniques, Semi-Structured Interviews and Think-aloud Protocols.

For the CW, the experts evaluated the developed application for two weeks. Guidance was given to the experts on the needed steps to undergo a CW test on the prototype. During the testing process, the experts provided views and comments. Subsequently, semi-structured interviews were conducted to get feedback on the prototype from the experts. During the semi-structured interview, the experts gave their opinion on the application interface and contents as a whole. The experts' user experience was an extra knowledge that should be considered [27] to improve the application features and make it suitable for non-native speakers. The problems and requirements stated by the experts were recorded and then summarised in Table IV, which clearly shows that most of the feedback on the RakanBM prototype was related to its interface. Under the think-aloud protocol, the experts evaluated the prototype alongside researchers. During this session, the experts asked the researchers any questions or portrayed their feelings verbally about the current prototype. The session was screen recorded to allow researchers to refer again to the responses and behaviours of the experts. At the same time, the usability of the prototype was evaluated using the think-aloud protocol, whereby the experts directly gave their comments and suggestions to meet the aim of the developed application.

### C. Phase III: Evaluation Procedure for Survey

Questionnaires used for the survey in this research were adapted from Goal Question Metric (GQM) considering effectiveness, efficiency, and satisfaction as a construct [32-34]. Besides, construct named application content, text presentation, learning outcome, and assessment were built based on the studies requirement discussed by the Malay language teachers. This questionnaire was adapted into current research to describe the research objectives with the required data. It will be conducted at the end of the study. The developed questionnaire was given to the experts to identify their background and obtain their expectations on the application. Fig. 4 illustrates the evaluation procedures involved in survey techniques. In addition, the questionnaire technique was used to measure the level of user experience on the prototype.

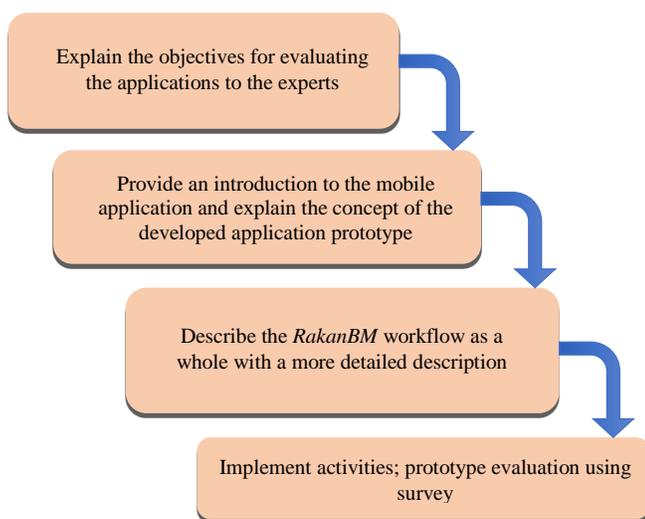


Fig. 4. Evaluation Procedure for the RakanBM Prototype using Survey.

1) *Produce questionnaire questions to users:* The questionnaire was developed in Malay language. The expert has no problem understanding the real meaning conveyed by the questionnaire. The questionnaire for this study consists of seven constructs, namely application content, text presentation, learning outcome, assessment, effectiveness, efficiency, and satisfaction. Application content was a question regarding user feedback on the content of the application. Text presentation was a question that required users to give their feedback towards the user interface available on the apps. The learning outcome was a question about the outcome that users may gain from the particular apps. The assessment was about scoring and interactive feedback provided by the apps. Last but not least, three constructs adapting GQM to gain information of effectiveness, efficiency, and satisfaction from a user by using RakanBM apps. All the constructs used a Likert five-point scale.

2) *Questionnaire reliability analysis:* The questionnaire was tested with Cronbach's alpha values to test the reliability of the questionnaire. Data should be unidimensional and consistent for purposes of internal consistency through Cronbach's alpha analysis [35]. Internal consistency can be measured in a number of ways. The most frequently used statistic was Cronbach's alpha [36]. In this study, a questionnaire was answered by six experts. The application contents constructs consisted of 10 items ( $\alpha = .89$ ), text presentations constructs consisted of 5 items ( $\alpha = .88$ ), learning outcome constructs consisted of 5 items ( $\alpha = .86$ ), assessment constructs consisted of 5 items ( $\alpha = .78$ ), effectiveness constructs consisted of 5 items ( $\alpha = .87$ ), efficiency constructs consisted of 5 items ( $\alpha = .89$ ) and satisfaction constructs consisted of 5 items ( $\alpha = .97$ ). The Cronbach's alpha values shows an excellent ( $\alpha \geq 0.9$ ), good ( $0.9 > \alpha \geq 0.8$ ) and accepted ( $0.8 > \alpha \geq 0.7$ ) internal consistency according to Tavakol and Dennick [37] benchmark.

## IV. RESULTS AND DISCUSSION

In this section, the results of the low-fidelity testing and evaluation process are further elaborated and discussed, especially concerning the field of language learning with apps. Furthermore, the gathered results provided substantial data in response to the experts' review on the RakanBM application.

### A. CW, Semi-Structured Interviews and Think-Aloud Protocol Results

The collected data were analysed and the results are as shown in Table II, specifically in terms of comments and suggestions. During this process, things that were noted were the feasibility of the experts on the given task, the accuracy of the process flow, the information developed, and the solution of the task scenario provided. Experts were required to provide feedback on whether they could perform the task or not. The experts were also free to comment on new ideas and suggestions for improvement. Open-ended questions were posed to get more complex feedbacks. Each question was analysed using a coding scheme by category adopted from Moustakas [38].

TABLE II. PROTOTYPE EVALUATION ANALYSIS RESULTS BASED ON CW, SEMI-STRUCTURED INTERVIEWS, AND THINK-ALOUD PROTOCOL

No.	Comments/Suggestions	No. of Feedback	Percentage (%)
1	Improvement on affix used	3	50
2	Improvement on the video content	2	33
3	Increase the interactivity of the application content	1	16
4	Restructure the content	4	66
5	Applying the application with others help	1	16
6	Introduce level in application	4	66
7	Improvement on aesthetic	4	66
8	Uniformity of the design	2	33

The results revealed that the task scenario completion level was 6/6, which indicates that the experts were able to complete the given task. In other words, this means that the experts completed 100% of the tasks, they were able to understand the application flow, and were aware of and knew the actions taken during the testing process. From Table IV, it can be concluded that the application's content and interface needed enhancement to increase user engagement in the self-learning applications. The results also confirmed that the function modelling and flow of the RakanBM application process were correct, but some improvisation is needed. For instance, the use of buttons, information displays, and contents needed some modification. Nonetheless, the experts agreed that the developed prototype was able to meet the needs of the user, but with some enhancements needed.

It should be noted that the open-ended questions supported the results of the questionnaire. For instance, most of the experts suggested an improvement in the content structure by adding more English translations on the earlier topics in the application. The experts also agreed on the need to introduce levels in the application. In short, the suggestions by experts to increase the aesthetic value on the current prototype supported (validated) the lowest mean value obtained by the text presentation factor of the questionnaire (see Table II).

The overall results revealed that the materials of the *RakanBM* mobile application for Malay Language learning for non-native speakers were relevant, validated by the factors that recorded a high mean: learning outcomes, assessments, effectiveness, and efficiency. The results were similar to previous studies where the mobile application was able to support language learning [6-8, 12]. In general, the *RakanBM* application is focused on Malay language learning with validated benefits. For instance, it is a novel creation for Malay language learning with complete topics suitable and best for non-native speakers. At the same time, the application is student-friendly, and users can use it easily, anytime, and anywhere. Furthermore, AR technology is also integrated into the mobile application to increase students' engagement and relate their surroundings to the learning activity.

### B. Survey Results

Descriptive statistical analysis was carried out to identify the mean, the percentage, and the standard deviation (SD) for

each item of the application factors: contents, text presentations, learning outcomes, assessments, effectiveness, efficiency, and satisfaction. Table III shows the mean for each of the items and factors, respectively. The calculated mean for each factor ranged from 3.53 to 4.50, while the average mean (for all factors) is 3.96. The results indicate that, in general, the evaluators tend to agree that the developed low-fidelity prototype was able to satisfy the factors' requirements. The results were then classified into two levels: high (mean > 4.0) and satisfied (mean > 3.5).

TABLE III. PERCENTAGE (SCALE 1 TO 3) AND (SCALE 4 TO 5) FOR THE SEVEN FACTORS OF USING THE RAKANBM APPLICATION

No.	Factor/Item	Percentage (%) (scale of 1 to 3)	Percentage (%) (scale of 4 to 5)	Mean (SD)
<b>1.0</b>	<b>Application contents</b>			<b>3.80 (1.05)</b>
1.1	The contents provided are suitable to the novice level	16.7	83.3	4.17 (1.17)
1.2	The contents provided have a clear continuity	33.4	66.6	3.83 (1.17)
1.3	The theme of the contents provided is appropriate to the novice level of learning	16.7	83.3	4.00 (1.10)
1.4	The chapters provided are adequate for the novice level	33.4	66.6	3.83 (1.17)
1.5	The language used is appropriate to the novice level of the student	50.0	50.0	3.17 (1.33)
1.6	The exercise provided is adequate	16.7	83.3	4.17 (0.75)
1.7	The exercise provided corresponds to the level of learning	16.7	83.3	4.00 (0.63)
1.8	Listening exercise through audio is adequate	16.7	83.3	4.17 (0.75)
1.9	The audio is clear and helps students listen well	16.7	83.3	3.83 (0.98)
1.10	Translation into English is limited to chapter 1 only	66.6	33.4	2.83 (1.47)
<b>2.0</b>	<b>Text presentations</b>			<b>3.53 (0.92)</b>
2.1	Presentation of contents using attractive graphics	66.6	33.4	2.83 (0.98)
2.2	The graphics used can help students understand the situation	16.7	83.3	4.33 (0.82)
2.3	The colours in the text are interesting	50.0	50.0	2.67 (0.82)
2.4	The length of the text for one chapter is sufficient	16.7	83.3	4.00 (0.63)
2.5	The presentation of the content is appropriate to the age level of the target students	50.0	50.0	3.83 (1.33)
<b>3.0</b>	<b>Learning outcomes</b>			<b>4.03 (1.00)</b>

No.	Factor/Item	Percentage (%) (scale of 1 to 3)	Percentage (%) (scale of 4 to 5)	Mean (SD)
3.1	Students will learn something new from this contents	0.0	100.0	4.67 (0.52)
3.2	Students are able to understand the Malay language is the basis of this contents	16.7	83.3	4.00 (1.55)
3.3	Students can also learn cultural information from this contents	33.4	66.6	4.00 (0.89)
3.4	Students will be excited to continue to level 2	50.0	50.0	3.83 (0.98)
3.5	These contents are sufficient for novice students	33.4	66.6	3.67 (1.03)
<b>4.0</b>	<b>Assessments</b>			<b>4.03 (0.79)</b>
4.1	The scoring for each exercise is balanced	16.7	83.3	4.00 (1.10)
4.2	Assessment is appropriate to the student's level of competence	0.0	100.0	4.17 (0.41)
4.3	The emojis used are appropriate to the student's level of competence	33.4	66.6	4.00 (1.26)
4.4	The assessment rubric is appropriate to the student's level of competence	16.7	83.3	4.17 (0.75)
4.5	Written, graphic/picture and oral tests can measure students' level of competence	33.4	66.6	3.83 (0.41)
<b>5.0</b>	<b>Effectiveness</b>			<b>3.97 (0.93)</b>
5.1	The learning contents displayed by this application are accurate and complete	33.4	66.6	3.67 (1.03)
5.2	Functions and learning contents on the application produce accurate output	33.4	66.6	3.83 (0.75)
5.3	Use of this application will increase the effectiveness in learning Malay	33.4	66.6	4.17 (0.98)
5.4	This application provides audio assistance in learning the Malay language	16.7	83.3	4.50 (0.84)
5.5	The terms contained in this application are clear and not confusing	33.4	66.6	3.67 (1.03)
<b>6.0</b>	<b>Efficiency</b>			<b>4.50 (0.91)</b>
6.1	This application helps learning the Malay language quickly	0.0	100.0	4.50 (0.55)
6.2	This application is able to increase student achievement in Malay language learning	16.7	83.3	4.33 (0.82)
6.3	Navigating this application is easy	33.4	66.6	4.00 (1.26)

No.	Factor/Item	Percentage (%) (scale of 1 to 3)	Percentage (%) (scale of 4 to 5)	Mean (SD)
6.4	This application allows for effective learning	16.7	83.3	4.17 (0.75)
6.5	The information available on this application is organised	33.4	66.6	3.83 (1.17)
<b>7.0</b>	<b>Satisfaction</b>			<b>3.90 (0.97)</b>
7.1	I am satisfied with this application	50.0	50.0	3.50 (1.05)
7.2	I would recommend my friends to use this application	50.0	50.0	4.00 (1.10)
7.3	I enjoy using this application	50.0	50.0	4.00 (1.10)
7.4	This application works just as well as I want it to	50.0	50.0	3.67 (0.82)
7.5	I want to use this application	16.7	83.3	4.33 (0.82)

Consequently, the factors that were recorded as high were the learning outcomes, assessments, effectiveness, and efficiency, while the factors that were recorded as satisfied were the application contents, text presentations, and satisfaction. The efficiency factor obtained the highest mean value of 4.50 with an SD of 0.91, which indicates that the experts (evaluators) tend to agree that the application was very efficient and necessary to help non-native speakers improve their Malay language basics, especially with the assistance of teachers. Meanwhile, the assessments (mean = 4.03, SD = 0.97) and learning outcomes factors (mean = 4.03, SD = 1.00) both obtained a mean value of 4.03, the second-highest mean value. The rest of the factors in the order of descending mean value are effectiveness (mean = 3.97, SD = 0.93), satisfaction (mean = 3.90, SD = 0.97), application content (mean = 3.80, SD = 1.05), and text presentation (mean = 3.53, SD = 0.92). The lowest mean value for the text presentation factor was likely due to feedback from some evaluators stating that the RakanBM interface was less aesthetic. Nevertheless, the positive responses were still more than the negative ones in which the percentage value for factors having a scale of more than 4 was 53% (i.e. agreed by 53% of experts).

The experts' opinions on the positive and negative aspects of the RakanBM prototype application were also collected and listed in Table IV. Following the prototype evaluation, the experts tend to agree with its interface features, elements, and functions. The experts also agreed that the application achieved a positive level of user experience. Nevertheless, analysis of the experts' opinions (i.e. related to the positive and negative aspects) and comments revealed that some improvements were needed.

Feedback on the positive aspects indicated that the application was student-friendly, a more compact learning material, and provided a more accessible and interactive Malay language learning experience. On the other hand, the negative aspects highlighted the difficulty of certain words, more interactive aspects needed, and more effective technique for

assessment required. The items that need to be improved, as indicated in Table III and Table IV will be addressed in the next prototype development to develop a more effective Malay language learning application.

TABLE IV. FEEDBACK ON POSITIVE AND NEGATIVE ASPECTS OF RAKANBM APPLICATION

Expert	Positive Aspect	Negative Aspect
A	<ul style="list-style-type: none"><li>“This application is very student-friendly, the content and learning materials are also presented in a very simple, easy, and compact way.”</li></ul>	<ul style="list-style-type: none"><li>None</li></ul>
B	<ul style="list-style-type: none"><li>“The first complete application was produced, very useful and easy for international students and can be applied on Android and iPhone”.</li><li>“Topics are very suitable and best for non-native speakers.”</li></ul>	<ul style="list-style-type: none"><li>None</li></ul>
C	<ul style="list-style-type: none"><li>“Content. Use of different languages (pronouns) according to the conversation situation as shown in Chapter 1. Various exercises such as True / False, Multiple Choice and Vocabulary that tests listening and viewing skills and the application of those skills.”</li></ul>	<ul style="list-style-type: none"><li>“As a novice student, it is quite difficult to comprehend the rich words. Words exist in conversation.”</li></ul>
D	<ul style="list-style-type: none"><li>“An effort made to develop Malay language application for foreign speakers use.”</li></ul>	<ul style="list-style-type: none"><li>“Need to add more interactive aspects.”</li></ul>
E	<ul style="list-style-type: none"><li>“Malay language learning is more accessible and interactive even on its own.”</li></ul>	<ul style="list-style-type: none"><li>None</li></ul>
F	<ul style="list-style-type: none"><li>“There is an AR element. AR can be used for collaborative teaching.”</li></ul>	<ul style="list-style-type: none"><li>“Assessment items should be based on audio not surrounding objects.”</li></ul>

Furthermore, the study finding corresponded to past research where mobile application utilization enhanced user performance and language learning [3, 7, 8]. The implementation of gamification in education has increased engagement and achieved learning more effectively[39]. For instance, the study of Sorrentino and Sorrentino and Spano [40] and Fang, Yeh [41]. Both of these studies prove how the use of mobile apps with the mobile application has really helped improve the English proficiency of non-native students. Among the focuses given were mastery of vocabulary, pronunciation practices, and the construction of simple sentences. Besides, Wang and Han [42] have used English language learning modules for native Chinese speaking students to further improve their mastery of communication strategies in English. This learning module was based on digital games using the smartphone application "Liulishou" (fluent in English). This study shows that this digital learning material has been able to help improve the level of pronunciation accuracy, fluency in communication, and the production of complex sentence structures orally among students. Another interesting mobile application was developed by Yamamoto, Rodriguez [43], who sought to innovate FinDo, which is a smartphone app capable of listing vocabulary related

to where users are located. For example, when a consumer is in a supermarket, the consumer can learn all the words related to the objects around it. Specifically, it turns out that all studies on language learning using mobile devices improved students' language proficiency well.

However, there were some challenges that lie within this expert review on mobile augmented reality applications for language learning studies. Since the whole process is majorly held by online meetings, it becomes boundaries in communication involving the experts. Nevertheless, the researchers' team has planned the method so well to lessen the impact as the situation was unavoidable due to pandemic times. Further guidelines can be taken for future research methods, especially in order to make progress more effective and efficient.

This whole chapter discusses the expert review ranging from prototype testing using CW techniques, semi-structured interviews, think-aloud protocols, and prototype evaluation using surveys upon completion of the test. It has been proven that RakanBM application was relevant and suitable to support Malay language mobile learning in line with previous studies where mobile learning has increased user's performance, especially in education [44, 45]. The analysis was conducted on seven construct and open-ended questionnaires to obtain expert feedback on the positive and negative aspects of the application as well. The analysis results show that the usefulness and the topics covered were suitable and best for foreign speakers.

## V. CONCLUSION

In this study, a review panel of six experts from the Malay language and HCI fields evaluated *RakanBM*, a newly developed mobile application prototype for Malay language learning for first speakers and foreign speakers. The evaluation methods consisted of CW, semi-structured interviews, think-aloud protocols, and surveys. The findings were analysed and summarised to determine the usability of the application and have contributed to new knowledge. In this study, it has been found that the expert review was in line with the previous literature where the mobile application was able to support learning language. The *RakanBM* application aimed to assist foreign users, especially novice user learning in classroom environments. The mobile application proved to be interesting, and the experts saw high potential in the application, especially if the needed changes could be implemented. The experts' recommendations were presented for the benefit of researchers and developers for the future development of Malay language learnings. Further research involving usability testing will be done for the target user - the non-native speakers – taking into consideration the findings of this present study.

## ACKNOWLEDGMENT

This study is supported by the Universiti Kebangsaan Malaysia under research grant scheme of GPK-PBM-2020-015.

## REFERENCES

- [1] Poulsakis, S., et al., The management of Digital Learning Objects of Natural Sciences and Digital Experiment Simulation Tools by teachers. *Advances in Mobile Learning Educational Research*, 2021. 1(2): p. 58-71.

- [2] Gang, B., et al., A Bahasa Malaysia Interactive Book App as A Speech-Language Therapy Tool for Children with Language Delay. *Asia-Pacific Journal of Information Technology and Multimedia*, 2017. Vol. 6 No. 1, June 2017: 23 - 37.
- [3] Rosell-Aguilar, F., Autonomous language learning through a mobile application: a user evaluation of the busuu app. *Computer Assisted Language Learning*, 2018. 31(8): p. 854-881.
- [4] Huynh, D. and H. Iida, An Analysis of Winning Streak's Effects in Language Course of "Duolingo". *Asia-Pacific Journal of Information Technology and Multimedia*, 2017. Vol. 6 No. 2.
- [5] Razak, N.A., H. Saeed, and H. Alakrash, Pedagogical issues of using ICT applications in Iraq. *Asia-Pacific Journal of Information Technology and Multimedia*, 2019. 7(2-2): p. 158-168.
- [6] Shawai, Y.G. and M.A. Almaiah, Malay language mobile learning system (MLMLS) using NFC technology. *International Journal of Education and Management Engineering*, 2018. 8(2): p. 1.
- [7] Bojórquez, E.M., et al., study on mobile augmented reality adoption for Mayo language learning. *Mobile Information Systems*, 2016.
- [8] Cho, M.-H. and D.A. Castañeda, Motivational and affective engagement in learning Spanish with a mobile application. *System*, 2019. 81: p. 90-99.
- [9] Halid, N.A. and N. Omar, Malay Part Of Speech Tagging Using Ruled-Based Approach. *Asia-Pacific Journal of Information Technology and Multimedia*, 2017. 6(2): p. 91-107.
- [10] Tiun, S., A.L. Salikin, and S.K. Muhammad, Using FOSS TTS Developer Tool to build Malay TTS System. *Asia-Pacific Journal of Information Technology and Multimedia*, 2016. Vol. 4 No. 2.
- [11] Shadieff, R., W.-Y. Hwang, and Y.-M. Huang, Review of research on mobile language learning in authentic environments. *Computer Assisted Language Learning*, 2017. 30(3-4): p. 284-303.
- [12] Ali, S.K. and N.S. Azmi, Augmented Reality in learning Malay Language. in *2019 2nd International Conference on Applied Engineering (ICAE)*. 2019. IEEE.
- [13] Abd Majid, N.A. and N. Abd Majid, Augmented reality to promote guided discovery learning for STEM learning. *Int. J. on Advanced Science, Engineering and Information Technology*, 2018. 8(4-2): p. 1494-1500.
- [14] Che Hashim, N., et al., User satisfaction for an augmented reality application to support productive vocabulary using speech recognition. *Advances in Multimedia*, 2018.
- [15] Lam, M.C., M.J. Sadik, and N.F. Elias, The effect of paper-based manual and stereoscopic-based mobile augmented reality systems on knowledge retention. *Virtual Reality*, 2020: p. 1-16.
- [16] Lam, M.C., et al., Interactive Augmented Reality with Natural Action for Chemistry Experiment Learning. *TEM Journal*, 2020. 9(1): p. 351.
- [17] Hanafi, H.F., et al. Improving students' motivation in learning ict course with the use of a mobile augmented reality learning environment. in *IOP Conference Series: Materials Science and Engineering*. 2017. IOP Publishing.
- [18] Nordin, N.A.A., N.A. Abd Majid, and N.F.A. Zainal, Mobile augmented reality using 3D ruler in a robotic educational module to promote STEM learning. *Bulletin of Electrical Engineering and Informatics*, 2020. 9(6): p. 2499-2506.
- [19] Botha, B.S., L. de Wet, and Y. Botma, Experts' review of a virtual environment for virtual clinical simulation in South Africa. *Computer Animation and Virtual Worlds*, 2020: p. e1983.
- [20] Beecham, S., et al., Using an expert panel to validate a requirements process improvement model. *Journal of Systems and Software*, 2005. 76(3): p. 251-275.
- [21] Lazar, J., J.H. Feng, and H. Hochheiser, Research methods in human-computer interaction. 2017: Morgan Kaufmann.
- [22] Jaspers, M.W., A comparison of usability methods for testing interactive health technologies: methodological aspects and empirical evidence. *International journal of medical informatics*, 2009. 78(5): p. 340-353.
- [23] Kaufman, D.R., et al., Usability in the real world: assessing medical information technologies in patients' homes. *Journal of biomedical informatics*, 2003. 36(1-2): p. 45-60.
- [24] Zimmermann, P.G., Beyond usability: measuring aspects of user experience. 2008, ETH Zurich.
- [25] Mourouzis, A., I. Chouvarda, and N. Maglaveras, Mhealth: common usability and user experience practices and flaws. in *European, Mediterranean & Middle Eastern Conference on Information Systems* 2015. 2015.
- [26] DiCicco-Bloom, B. and B.F. Crabtree, The qualitative research interview. *Medical education*, 2006. 40(4): p. 314-321.
- [27] Schaper, M.-M., et al., Learning about the past through situatedness, embodied exploration and digital augmentation of cultural heritage sites. *International Journal of Human-Computer Studies*, 2018. 114: p. 36-50.
- [28] Beauchemin, M., et al., A multi-step usability evaluation of a self-management app to support medication adherence in persons living with HIV. *International journal of medical informatics*, 2019. 122: p. 37-44.
- [29] Yen, P.-Y. and S. Bakken, Review of health information technology usability study methodologies. *Journal of the American Medical Informatics Association*, 2012. 19(3): p. 413-422.
- [30] Gruenstein, A., I. McGraw, and I. Badr, The WAMI toolkit for developing, deploying, and evaluating web-accessible multimodal interfaces. in *Proceedings of the 10th international conference on Multimodal interfaces*. 2008.
- [31] Ssemugabi, S. and M. De Villiers, Effectiveness of heuristic evaluation in usability evaluation of e-learning applications in higher education. *South African computer journal*, 2010. 2010(45): p. 26-39.
- [32] Fabil, N.B., A. Saleh, and R.B. Isamil, Extension of PACMAD model for usability evaluation metrics using Goal Question Metrics (GQM) Approach. *Journal of Theoretical and Applied Information Technology*, 2015.
- [33] Hussain, A., et al., A metric-based evaluation model for applications on mobile phones. *Journal of Information and Communication Technology*, 2013. 12: p. 55-71.
- [34] Weichbroth, P., Usability of mobile applications: a systematic literature study. *IEEE Access*, 2020. 8: p. 55563-55577.
- [35] Talib, O., SPSS: Analisis data kuantitatif untuk penyidik muda. 2015: MPWS Rich Publication Sdn. Bhd.
- [36] Pallant, J., SPSS survival manual. 2013: McGraw-hill education (UK).
- [37] Tavakol, M. and R. Dennick, Making sense of Cronbach's alpha. *International journal of medical education*, 2011. 2: p. 53.
- [38] Moustakas, C., Phenomenological research methods. 1994: Sage publications.
- [39] Kalogiannakis, M., S. Papadakis, and A.-I. Zourmpakis, Gamification in science education. A systematic review of the literature. *Education Sciences*, 2021. 11(1): p. 22.
- [40] Sorrentino, F. and L.D. Spano, Post-it notes: supporting teachers in authoring vocabulary game contents. *Multimedia Tools and Applications*, 2019. 78(16): p. 23049-23074.
- [41] Fang, W.-C., et al., Effects of mobile-supported task-based language teaching on EFL students' linguistic achievement and conversational interaction. *ReCALL*, 2021. 33(1): p. 71-87.
- [42] Wang, Z. and F. Han, Developing English language learners' oral production with a digital game-based mobile application. *Plos one*, 2021. 16(1): p. e0232671.
- [43] Yamamoto, K., J. Rodriguez, and Y. Tsujino, FinDo: A Foreign Language Vocabulary Learning System Based on Location-Context. in *2019 20th IEEE/ACIS International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD)*. 2019. IEEE.
- [44] Papadakis, S., et al., Developing and exploring an evaluation tool for educational apps (EAEA) targeting kindergarten children. *Sustainability*, 2020. 12(10): p. 4201.
- [45] Papadakis, S., M. Kalogiannakis, and N. Zaranis, Designing and creating an educational app rubric for preschool teachers. *Education and Information Technologies*, 2017. 22(6): p. 3147-3165.

# Arabic Semantic Similarity Approach for Farmers' Complaints

Rehab Ahmed Farouk<sup>1</sup>, Mohammed H. Khafagy<sup>2</sup>, Mostafa Ali<sup>3</sup>, Kamran Munir<sup>4</sup>, Rasha M.Badry<sup>5</sup>

Department of Information Systems, Faculty of Computers and Information, Fayoum University, Fayoum 63511, Egypt<sup>1,2,3,5</sup>  
Department of Computer Science and Creative Technologies, University of the West of England<sup>4</sup>  
BS16 1QY, Bristol, United Kingdom<sup>4</sup>

**Abstract**—Semantic similarity is applied for many areas in Natural Language Processing, such as information retrieval, text classification, plagiarism detection, and others. Many researchers used semantic similarity for English texts, but few used for Arabic due to the ambiguity of Arabic concepts in both sense and morphology. Therefore, the first contribution in this paper is developing a semantic similarity approach between Arabic sentences. Nowadays, the world faces a global problem of coronavirus disease. In light of these circumstances and distancing's imposition, it is difficult for farmers to physically communicate with agricultural experts to provide advice and find suitable solutions for their agricultural complaints. In addition, traditional practices still are used by most farmers. Thus, our second contribution is helping the farmers solve their Arabic agricultural complaints using our proposed approach. The Latent Semantic Analysis approach is applied to retrieve the most problem-related semantic to a farmer's complaint and find the related solution for the farmer. Two methods are used in this approach as a weighting schema for data representation are Term Frequency and Term Frequency-Inverse Document Frequency. The proposed model has also classified the big agricultural dataset and the submitted farmer complaint according to the crop type using MapReduce Support Vector Machine to improve the performance of semantic similarity results. The proposed approach's performance with Term Frequency-Inverse Document Frequency-based Latent Semantic Analysis achieved better than its counterparts with an F-measure of 86.7%.

**Keywords**—Semantic similarity; latent semantic analysis; big data; MapReduce SVM; COVID-19; agriculture farmer's complaint

## I. INTRODUCTION

The semantic analysis field has an essential role in the research related to text analytics. Measuring the semantic similarity between sentences is a long-standing problem in the Natural Language Processing (NLP) field [1], [2]. With the growth of text data over time, NLP became essential to be worthy of attention for Artificial Intelligence (AI) experts [3], [4]. Semantic similarity is used for several fields in NLP like information retrieval, text summarization, plagiarism detection, question answering, document clustering, text classification, machine translation, and others [5], [6]. It is defined as determining whether two concepts are similar in meaning or not [7]. The concepts are words, sentences, or paragraphs. Each concept takes a score. When the concept has a high score refers to high similarity or semantic equivalence to another concept [8]. Concepts can have two ways to be similar that are either

lexically or semantically. Concepts are lexical similarly if words have similar character sequences and are performed using a String-based algorithm. Concepts are semantic similarly if words depend on information acquired from massive corpora, even if they have a different lexical structure. Semantic similarity can be done by a corpus-based algorithm or knowledge-based algorithm [9], [10]. Several research works of semantic similarity have been developed for English sentences. On the other side, few research works have been used for the Arabic language because Arabic is considered a complex morphological language [11]. However, the Arabic language considers the fifth most spoken language in the world. Also, it participates in the most critical foreign languages with over 300 million speakers and a wide range of functionalities that no other language can have [12]. Therefore, this paper will apply a semantic similarity approach to the Arabic dataset.

Currently, the world faces a huge disaster that threatens the world is the global Coronavirus disease (COVID-19) pandemic. COVID-19 causes destructive economic, political, and social crises in each country. All fields have been affected by the global Coronavirus, especially the agriculture field. In our life, Agriculture plays a critical role in the entire life of the economy. It can be one source of Livelihood, contributes to national revenue, the supply of food, and marketable surplus. Moreover, it provides job opportunities to a huge percentage of the population and supplies the country with an important portion from its foreign exchange through agriculture exports. Therefore, due to COVID-19 that compounds pre-existing vulnerabilities in the field of agriculture in Egypt. Initial analyzes of this epidemic have shown disrupting access to agricultural inputs, including employment, extension, advising services, and producing markets for farmers. Most significant countries became deserted that people stay indoors, either by choice or by the government, to reduce the spread of this pandemic. Because of this, the curfew and distancing imposed by COVID-19 cause many problems for farmers. So, it is difficult for farmers to communicate and interact with agricultural experts to present their complaints and find suitable solutions. Therefore, it is essential to find an appropriate way to help in solving the farmers' complaints. Agriculture Research Center (ARC) and Virtual Extension and Research Communication Network (VERCON) [13] in Egypt provide a large group of farmers' complaints and their solutions in Arabic deployed on a public cloud. The agricultural experts have resolved these complaints. Thus, under these difficult circumstances of the spread of the COVID-19, this paper aims to develop an approach for farmers to help, support, and find the

most suitable solution for their agricultural complaints. The proposed approach is based on latent semantic analysis (LSA) to measure the semantic similarity score between Arabic farmers' complaints and the Arabic agricultural dataset, further retrieving the related solution to the farmer. As an example, the farmer's complaint is "مهاجمة دودة ورق القطن لحقول البرسيم فما هي المقاومة؟" and its English equivalent is "Cotton leaf worm attack alfalfa fields, what is the resistance?". After applying the proposed model, the recommended solution is "تقاوم دودة ورق القطن في البرسيم باستخدام احد المبيدات الموصى بها مثل لانيت 90% بمعدل 300 جم/ف ثم الري بالسولار بمعدل 200 لتر للفدان" and its English equivalent is "The cotton leafworm is resisted in alfalfa by using one of the recommended pesticides such as Lannet 90% at a rate of 300 g/f, then irrigation with diesel at a rate of 200 liters per feddan."

To improve the performance of the semantic similarity approach, we used the classification. Text Classification (TC) is an active research field and an essential in information retrieval technology [14]. It aims to classify text documents into one or more predefined categories. TC is applied in many applications like sentiment analysis, sentence classification, and document classification [15], [16]. TC can use many methods such as Decision Trees, Support Vector Machine (SVM), Artificial Neural Networks (ANN), Naïve Bayes (NB), K-Nearest Neighbor (KNN), etc. [17], [18].

SVM is an extremely powerful classifier in the machine learning field and is widely used in text classification [19]. However, it is fast and easy to implement. Therefore, we applied SVM on the agricultural dataset to classify Arabic complaints into crops. But, SVM didn't achieve better accuracy results. Thus, to improve performance in classifying our Arabic agricultural dataset, we resort to a parallel programming model like MapReduce. So, this paper applied the classification by MapReduce SVM using Hadoop to classify the Arabic agricultural dataset according to its crop type.

Most of the previous works applied Arabic semantic similarity to small datasets and achieved low accuracy results. Moreover, fewer of them tested on agriculture datasets and didn't use the classification.

Thus, the main objectives in this paper are as follow:

- 1) Applying the proposed model on a big agricultural dataset with real complaints facing Egypt's farmers.
- 2) The proposed model can help farmers, especially in the circumstances of COVID-19, by providing advice and finding appropriate solutions for their complaints to enhance agriculture productivity.
- 3) Developing a semantic similarity model between Arabic complaints and obtaining better results.
- 4) Using a parallel programming model like MapReduce based on SVM to classify the agricultural dataset and improve the performance of a semantic similarity model.
- 5) Testing and validating the proposed model performance by implementation multiple experiments and applying previous models on our Arabic agricultural dataset.

The remaining parts of the paper will be structured so that Section II presents related work; Section III includes materials and methods; Section IV covers discussion; Section V shows

the experimental results. Finally, in Section VI, the conclusion is produced.

## II. RELATED WORK

This section will introduce related work about Arabic text classification and Arabic semantic similarity. Mostafa et al. [20] Proposed two models to classify the Arabic farmers' complaints based on different diseases that may affect crops. The Arabic complaint is classified into its respective crop and a specific disease in the first model. The second model could classify the complaint directly into diseases. Each preprocessed complaint is represented into a binary vector form using the vector space model by helping the crop lexicon. Experiments are conducted on the dataset by changing the training percentage with many trials using SVM and KNN classifiers. The results are shown that the proposed model is performed on par with the human expert and can be applicable for real-time operations. Moreover, Raed Al-khurayji and Ahmed Sameh [21] presented an approach that depends on a Kernel Naive Bayes classifier to solve the non-linearity problem of Arabic text classification. First, they applied preprocessing techniques on Arabic datasets like tokenization, stop word removal, and light stemmer. Then, they used the TF-IDF technique on Arabic words for feature extraction to convert them into the vector space. Experimental results are shown that the proposed approach achieved good accuracy and time compared with other classifiers. While Abutiheen et al. [22] proposed the Master-Slaves (MST) technique to classify Arabic texts. The proposed approach consisted of two phases. In the first phase, Arabic corpus text files are collected. These text files are classified manually into five categories. In the second phase, four classifiers were implemented on the Arabic collected corpus. The four classifiers were NB, KNN, Multinomial logistic regression, and maximum weight. NB classifier was applied as Master and the others as Slaves. The slave classifiers' results were used to change the NB classifier probability (Master). Each document in a corpus was represented as a vector of weights. The results of the MST have achieved a good improvement in accuracy compared with the other techniques.

Schwab et al. [23] presented a technique that depends on word embedding for measuring semantic relations among Arabic sentences. This technique relies on the characteristic of semantic words in the model of word embedding. This technique has applied three methods: no weighting method, Inverse Document Frequency (IDF) weighting method, and part-of-speech (POS) weighting method. No weighting method is used by summing the word vectors of each sentence. To improve the results, use the IDF weighting method to calculate IDF weight for each word and add the word vectors with IDF weights for each sentence. Also, use the POS tagging method that supposes weight for each POS and calculate POS for each word, then for each sentence, sum the words vectors with POS weights. This technique is evaluated the results on a small dataset. This paper demonstrated how weighing IDF and POS tagging supports highly descriptive word determination in any sentence. The performance of both IDF and POS weighting techniques achieved better results. While Amine et al. [24] proposed an Arabic search engine method depending on the MapReduce method. This method is used for finding semantic similarity among an Arabic query and the large corpus of

existing documents in the Hadoop Distributed File System (HDFS). It is also used to obtain the most relevant documents. It uses two measures in MapReduce: Wu and Palmer (WP) measure and Learrock and Chodorow (LC) measure. The results appeared that WP and LC obtained better results than the existing approaches of semantic similarity. Mahmoud et al. [25] suggested a semantic similarity technique in paraphrase identification for Arabic. This technique depends on the combination of various NLP like the TF-IDF technique and the word2vec algorithm. TF-IDF technique is used to ease the identifying of highly descriptive terms in each sentence. The word2vec algorithm is used for representations of distributed word vectors. Also, word2vec can minimize computation complexity and optimize the likelihood of word prediction in producing a model of sentence vector. This paper applied the similarity using various comparison metrics, like Cosine Similarity and Distance Euclidean. Finally, the proposed technique was tested on the Open-Source Arabic Corpus OSAC and achieved a reasonable rate. In [26] used a semantically reduced dimensional vector to represent high dimensional Arabic text. It has been accomplished by extending the standard vector space model (VSM) to enhance the representation of text that utilizes Linguistic and semantic properties from Arabic WordNet and Name Entities' gazetteers. If synonyms and similar terms obtain from the same root in clusters, the vector size reduces, and the shorter NE represents the chosen cluster members. The word similarity is also determined using distributional similarity to collect similar terms into clusters. Results demonstrated the size, form of the analysis windows, and the text's nature and category based on how much it reduced. In [27] suggested a method for finding the semantic similarity among two Arabic texts. This approach used hybrid similarity measures that are edge-counting semantic approach, cosine similarity, and N-gram similarity. The edge-counting semantic approach determined the value of a threshold. If the first approach's similarity result was lower than the threshold value, then cosine similarity is applied. Moreover, if the cosine similarity value compared with the predefined threshold was not appropriate, use N-gram similarity. This hybrid approach addresses problems of writing mistakes like repetitive, incomplete, and substituted characters. The hybrid similarity results outweigh the results of any of the three measures that have been used individually.

### III. MATERIAL AND METHODS

The proposed model aims to measure the semantic similarity's score between the current farmer's complaint and the available historical agricultural problems to provide an adequate solution to the farmer's complaint. Our proposed model was applied and tested on the agriculture problems dataset and their solutions. ARC and VERCON. It contains complaints of various causes, such as harmful weeds, fungal diseases, and other diseases that affect plants and their solutions. It also includes complaints belongs to 31 governorates and their directorates. It contains more than 10,000 complaints. The complaints are written in the Arabic language in an unstructured form and not well-formatted. These complaints related to different crops such as "rice, okra, wheat, corn, cotton, beans, etc...". It is also associated with different categories, which are "Administrative, Productivity, Marketing, and Environmental".

Due to the variety of crops in the agriculture dataset, the proposed model applied a classification method to classify the farmer complaints dataset according to the crop type.

Table I shows some examples of the dataset's complaints related to different crops and their English translation.

TABLE I. EXAMPLES FOR ARABIC FARMERS' COMPLAINTS AND THEIR ENGLISH EQUIVALENT

Complaints in the English Language	Complaints in the Arabic Language
Yellow spots on the leaves of onion plants.	وجود بقع صفراء على اوراق نباتات البصل.
The presence of whiteflies strongly in cotton.	وجود ذبابة بيضاء بشدة في القطن.
The wheat was infested with aphids.	اصابة القمح بحشرة المن.
The presence of spots on the upper surface of okra leaves with the appearance of a spider thread on its lower surface	وجود بقعة على السطح العلوي من اوراق الباميا مع ظهور خيط عنكبوتي على سطحها السفلي.
The lack of water in the Arimon canal for more than a month exposes the existing winter crops to fallow, such as clover.	عدم وجود مياه بترعة اريمون منذ اكثر من شهر مما يعرض المحاصيل الشتوية القائمة للوبار مثل البرسيم.

The proposed model consists of four phases, as shown in Fig. 1 Preprocessing, MapReduce SVM classification, and Latent Semantic Analysis. The last phase is the ranking and selection to choose the most semantically relevant solution to the farmer's complaint. The next sections explain in detail the phases of the proposed model.

#### A. Preprocessing Phase

The preprocessing phase is an essential step for Natural Language Processing (NLP) tasks. It transforms input text into a more desired form for performing better for further steps [28]. Unfortunately, the complaints' meaning is difficult to understand and interpret since farmers typically write complaints without following the Arabic grammar rules.

Data preprocessing includes four operations: tokenization, stop word removal, complaints auto-correction, normalization, and lemmatization, as shown in Fig. 1.

- Tokenization: It is a method for breaking texts into tokens. Words are separated from their neighboring words by blanks such as white space, periods, commas, semicolons, and quotations [29]. For example, The Arabic complaint is "وجود بقع صفراء لها مظهر مسحوقى فى صفوف طوليه على ورقه القمح".

After applying the tokenization, the Arabic complaint is:

And its equivalent English is: "The presence of yellow spots that have a powdery appearance in longitudinal rows on the wheat leaf."

"وجود", "بقع", "صفراء", "لها", "مظهر", "مسحوقى", "فى", "صفوف", "طوليه", "على", "ورقه", "القمح".

- Stop Word Removal: The most popular undesirable term is either a punctuation mark or a stop word. Therefore, they are eliminated from complaints since they do not have any meaning or indications about the content. We used an online Arabic stop words list for elimination [30]. Examples of these unimportant words in the Arabic language such as:

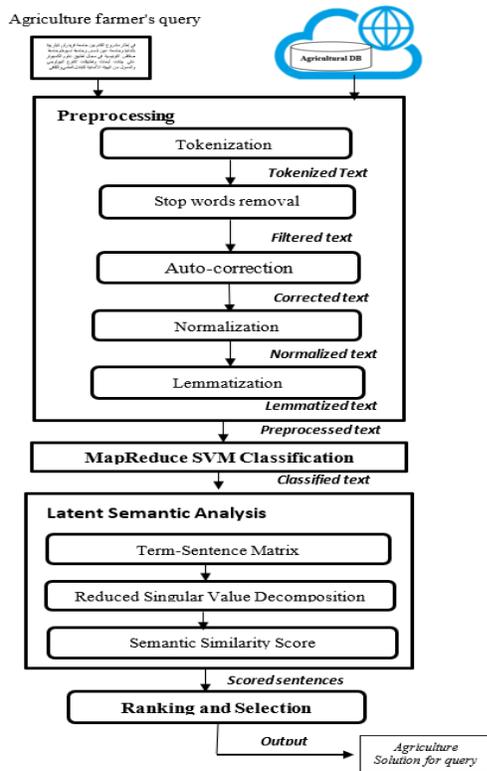


Fig. 1. The Proposed Architecture.

(كلما, اولاً, حول, اين, طالما, التي, من, الى, على, فوق, تحت, الخ.

And in the English language are (Whenever, first, about, where, as long as, which, from, to, on, above, below, etc.)

In addition, eliminating all symbols such as: (@, #, &, %, and \*).

- Auto-correction: The farmers may write their complaints with spelling errors. For example, the crop name of tomatoes "طماطم" may be incorrectly written in slag way as "اوطه", the crop name of corn "نزه" may be incorrectly written as "ززه" and the name of rice crop "ارز" may be incorrectly written as "رز" [20]. Therefore, we use auto-correction to solve these problems by substituting the incorrect word with the correct one.
- Normalization: Text normalization is transforming the input text into a canonical (standard) form. It is critical for noisy texts like comments on social media and text messages that are popular in abbreviations and misspellings. Moreover, it concentrates on removing the inconsistent language variations. For example, In English, the word "croooop" can be transformed into its canonical form "crop" and also in Arabic like "محصولوول" is normalized into "محصول" [31], [32]. So, we applied some methods for normalization such as the letters "أ، ا، إ" will convert into one form "ا." Also, the letter "ة" will replace by "ه", the letter "ي" will convert to "ى." Also, remove the diacritics from the words such as "أشجار" will convert to "اشجار". Furthermore, if there are more spaces between words, then we removed

them. We also convert numbers into words such as "15" will convert to "خمسة عشر."

- Lemmatization: It is an essential step in the preprocessing phase and a significant component for many applications of natural language processing. It is an operation to find the base form for a word. For example, in Arabic words like (ثمر) has the root "ثمر." Also, in English, "fruits" has the root "fruit." We used an online Farasa lemmatization [33].

### B. MapReduce SVM Classification Phase

Text Classification is the process of distributing each document to its labeled class [34]. MapReduce is a popular programming model developed by Google. It can process massive datasets in a parallel manner and achieves a high performance [35], [36]. The main idea of MapReduce comes from the divide and conquer algorithms which are used to divide a large problem into smaller subproblems. Therefore, we apply MapReduce SVM to classify big data preprocessed agricultural complaints according to their crop type, such as rice, wheat, okra, etc. MapReduce SVM uses the Hadoop framework to share the classification between many machines using HDFS to store the preprocessed agricultural complaints to classify and store the classification result. MapReduce model is divided into two tasks which are Map and Reduce [37]. It divides the dataset into smaller chunks and then assigns each chunk to a single map task. Map tasks' number is equal to the number of data chunks. Thus, each map task processes each data chunk in a parallel way. The model shuffles and sorts the Map outputs and transfers them to the Reduce tasks. The Reduce task is a summarization step that all associated records are processed together by a single entity. The Map and Reduce tasks are mathematically represented in (1) and (2), respectively [38].

$$Map: (K_1, V_1) \rightarrow [(K_2, V_2)] \quad (1)$$

$$Reduce: (K_2, [V_2]) \rightarrow [(K_3, V_3)] \quad (2)$$

The  $(K_1, V_1)$ ,  $(K_2, V_2)$ , and  $(K_3, V_3)$  represent the key-value pairs for map and reduce tasks.

After this phase, each complaint is classified according to its crop type. Table II shows the number of Arabic agricultural complaints in each crop after applying the MapReduce SVM model.

### C. Latent Semantic Analysis Phase

In this phase, LSA is applied to measure the semantic similarity among the agriculture dataset and the farmer complaint. It is a technique used for representing documents as a vector. It helps to find the similarity between agricultural complaints by calculating the distance between vectors.

There are three main steps for the LSA-based algorithm:

- Creating the input matrix (Term-Sentence matrix)
- Applying reduced singular value decomposition (RSVD) on the created matrix
- Calculating the semantic similarity score between the farmer's complaint and complaints document.

TABLE II. THE NUMBER OF ARABIC AGRICULTURAL COMPLAINTS IN EACH CROP

Crop Name (English)	Crop Name (Arabic)	Number of Arabic Complaints	Crop Name (English)	Crop Name (Arabic)	Number of Arabic Complaints
Wheat	قمح	890	Apples	التفاح	837
Rice	ارز	754	Orange	البرتقال	458
Cotton	قطن	735	Lettuce	الخس	579
Tomatoes	طماطم	692	Cabbage	الكرنب	699
Beans	الفاصوليا	572	Garlic	الثوم	276
Potato	البطاطس	379	Guava	الجوافة	497
Clover	البرسيم	437	Okra	الباميا	238
Peach	الخوخ	288	Banana	الموز	798
Onions	البصل	583	Peas	البسلة	436
Apricot	المشمش	400	Watermelon	البطيخ	972
Lentils	العدس	389	Mandarin	اليوسفي	697
Grapes	العنب	457	Cowpea	اللوبيا	793
Eggplant	البانجان	389			

These steps will be explained in detail in the following sections.

1) *Term-sentence matrix*: In this phase, an input matrix is created for the farmer's complaint query and classified complaints document. Each row in the matrix represents the word or term in the farmer's complaint or classified complaints document [39]. Each column represents the complaints. The cell value is the result of the intersection between term and complaint. There are two methods used as a weighting schema for data presentation for filling the cell values: Frequency (TF) or Term Frequency-Inverse Document Frequency (TF-IDF).

In TF-based LSA, the cells are filled with the term frequency (TF<sub>i</sub>) of terms in the complaint statement (C<sub>j</sub>) as in (3).

$$W(t_{ij}) = tf_{ij} \quad (3)$$

Where  $W(t_{ij})$  is the weight of a term (i) in each complaint statement (j) and  $tf_{ij}$  is the frequency of a term (i) in each complaint statement (j).

TF\_IDF-based LSA, the cells are filled with the weight of (TF\_IDF) of the term (i) in complaint statement (C<sub>j</sub>) as shown in (4) and (5).

$$TF\_IDF_{ij} = TF_{ij} * IDF_{ij} \quad (4)$$

Where  $TF\_IDF_{ij}$ : TF is the frequency of a term (i) in each complaint statement (j), and IDF reflects the importance of term among all sentences

$$IDF_{ij} = \log \frac{N}{ComplaintFreq(f)} \quad (5)$$

Where  $N$  represents the number of complaints in the collection, and  $ComplaintFreq(f)$  is the number of complaints containing the term.

2) *Reduced singular value decomposition*: Singular value decomposition (SVD) is an algebraic method that plays an essential role in text mining and natural language processing. SVD is used to improve the term sentence matrix, remove noise, and determine the relationships between terms and complaints statements [40]. SVD decomposes the Term Sentence Matrix into three matrices that detect all the important properties and features of the matrices.

Equation (6) shows the SVD decomposition of the  $m \times n$  matrix.

$$SVD = USV^T \quad (6)$$

Where  $U$  is the  $m$ -dimensional matrix,  $V$  is the  $n$ -dimensional matrix, and  $S$  is the diagonal matrix.

Moreover, RSVD is applied to improve and enhance the performance of SVD and reduce the matrix dimensionality.

3) *Semantic similarity score*: After applying RSVD, RSVD results are used to calculate semantic similarity between the farmer query and classified complaints document. The semantic score is calculated using the most common similarity method, which is the cosine similarity. Equation (7) represents the calculation of cosine similarity.

$$Cos\ similarity(A, B) = \frac{A \cdot B}{||A|| * ||B||} \quad (7)$$

Where  $Cos\ similarity(A, B)$  is the similarity score between the farmer query and complaints document, A is the weight of the term in the query, and B is the weight of the term in the complaint statement.

#### D. Ranking And Selection Phase

In this phase, rank the complaints according to the semantic score, then select the complaint of the highest score. Finally, retrieve the solution of the complaint with the highest score to the farmer query.

### IV. DISCUSSION

F-measure is used to evaluate the performance for the proposed classification approach and semantic similarity approach.

#### A. Classification Evaluation

The performance of the MapReduce SVM classifier using Hadoop is evaluated. Also, we compared our classification results with the previous classification works as in Mostafa et al. [20] and Mohammad et al. [41]. Authors in [20] applied two classifiers that are SVM and KNN, on the same agricultural dataset to classify agricultural complaints into crops.

Moreover, authors in [41] used two classifiers that are the Naive Bayes algorithm (NB) and the Hybrid Naive Bayes with Multilayer Perceptron network (NB-MLP), to classify the dataset into positive or negative sentiment. Therefore, we applied NB and NB-MLP algorithms to our agricultural dataset to classify complaints into crops.

TABLE III. EVALUATION OF MAPREDUCE SVM CLASSIFIERS COMPARED WITH PREVIOUS MODELS

Class	NB			NB-MLP			SVM			KNN			MapReduce SVM		
	Precision	Recall	F-Measure	Precision	Recall	F-Measure									
Wheat	91.71	94.54	93.10	92.54	95.91	94.19	93.68	97.49	95.55	93.96	97.58	95.74	94.2	98.4	96.3
Rice	90.83	92.32	91.57	94.72	95.73	95.22	89.13	97.27	93.02	96.85	89.71	93.14	97.4	98.3	97.8
Cotton	92.52	94.84	93.67	93.03	95.45	94.22	93.06	95.32	94.18	83.87	93	88.2	94.7	97.4	96
Beans	93.77	95.61	94.68	94.18	96.48	95.32	96.82	75.43	84.8	95.24	97.62	96.42	97.5	98.8	98.1

Table III shows a comparison between our MapReduce SVM evaluation results and previous works that used NB, NB-MLP, SVM and KNN classifiers. We evaluated the results on four crops, such as wheat, rice, cotton, and beans, familiar with authors in [20].

As a conclusion, the evaluation results of MapReduce SVM achieved better results than previous classifiers of NB, NB-MLP, SVM and KNN.

### B. Semantic Similarity Evaluation

The proposed semantic similarity approach using TF-based LSA and TF\_IDF-based LSA are tested and evaluated. And finally, the results of the proposed approach are compared with the previous models. The tests applied on twenty-five crops which are Okra, Mandarin, Watermelon, Wheat, Rice, Cotton, Beans, Tomatoes, Potato, Peach, Apricot, Lentils, Onions, Clover, Apples, Eggplant, Grapes, Orange, Banana, Guava, Peas, Cowpea, Cabbage, Garlic, and Lettuce.

TABLE IV. THE NUMBER OF ARABIC QUERIES IN EACH CROP

Crop Name (English)	Crop Name (Arabic)	Number of Arabic Complaints	Number of Arabic Complaint Queries
Wheat	قمح	890	222
Rice	ارز	754	188
Cotton	قطن	735	183
Tomatoes	طماطم	692	173
Beans	الفاصوليا	572	143
Potato	البطاطس	379	94
Clover	البرسيم	437	109
Peach	الخوخ	288	72
Onions	البصل	583	145
Apricot	المشمش	400	100
Lentils	العنيس	389	97
Grapes	العنب	457	114
Eggplant	الباذنجان	389	97
Apples	التفاح	837	209
Orange	البرتقال	458	114
Lettuce	الخس	579	144
Cabbage	الكرنب	699	174
Garlic	الثوم	276	69
Guava	الجوافة	497	124
Okra	الباميا	238	59
Banana	الموز	798	199
Peas	البسلة	436	109
Watermelon	البطيخ	972	243
Mandarin	اليوسفي	697	174
Cowpea	اللوبيا	793	198

In addition, we tested 25 % of different queries on each crop. Table IV shows the number of Arabic complaint queries for each crop.

TABLE V. EXAMPLES FOR ARABIC COMPLAINTS QUERIES AND THEIR ENGLISH EQUIVALENT

Complaints queries in the English language	Complaints queries in the Arabic language
The presence of aphids inside the okra fruits.	وجود حشرة المن داخل ثمار الباميا.
The presence of brown spotting on apricot trees.	وجود بقع بني على اشجار المشمش.
The appearance of black spots on the potato leaves.	ظهور بقع سوداء على اوراق البطاطس.
The appearance of oval spots of different sizes on the onion leaves	ظهور بقع بيضاوية مختلفة الحجم على اوراق البصل.
The appearance of a minute white layer on the peach trees.	ظهور طبقة بيضاء دقيقة على اغصان اشجار الخوخ.
High rates of apple fruit fall.	ارتفاع نسب تساقط ثمار التفاح.
Yellowing of mandarin trees, complete yellowing with their fall.	اصفرار شجرة اليوسفي اصفرار كامل مع تساقط معظم اوراق اليوسفي.

TABLE VI. EXAMPLES OF EVALUATION RESULTS FOR TF-BASED LSA APPROACH

Crops Name	Evaluation Methods		
	Average Precision	Average Recall	Average F-Measure
الباميا (Okra)	83.5%	80.3%	81.9%
اليوسفي (Mandarin)	86.5%	83.3%	84.9%
البطيخ (Watermelon)	84.7%	82.0%	83.3%
القمح (Wheat)	85.6%	82.3%	83.9%
الارز (Rice)	86.2%	83.2%	84.7%
القطن (Cotton)	85.5%	83.3%	84.4%
الفاصوليا (Beans)	83.5%	81.7%	82.6%
الطماطم (Tomatoes)	86.0%	80.4%	83.1%
البطاطس (Potato)	80.7%	78.5%	79.6%
الخوخ (Peach)	86.4%	82.3%	84.3%
المشمش (Apricot)	81.5%	80.4%	80.9%
العنيس (Lentils)	85.0%	83.5%	84.2%
البصل (Onions)	79.8%	76.7%	78.2%
البرسيم (Clover)	83.5%	80.3%	81.9%
التفاح (Apples)	80.0%	78.4%	79.2%
الباذنجان (Eggplant)	82.5%	80.3%	81.4%
العنب (Grapes)	79.5%	77.7%	78.6%
البرتقال (Orange)	81.5%	80.8%	81.1%
الموز (Banana)	85.4%	81.5%	83.4%
الجوافة (Guava)	81.7%	79.5%	80.6%
البسلة (Peas)	85.7%	80.6%	83.1%
اللوبيا (Cowpea)	80.0%	78.5%	79.2%
الكرنب (Cabbage)	80.5%	76.3%	78.3%
الثوم (Garlic)	81.0%	79.5%	80.2%
الخس (Lettuce)	83.7%	79.8%	81.7%

Table V shows some examples of the Arabic queries complaints related to different crops and their English translation.

In TF-based LSA, average Precision, Recall, and F-measure values for the twenty-five crops are shown in Table VI.

In TF\_IDF-based LSA, we also apply the previous Arabic queries in Table IV on each crop of the previous twenty-five crops. Thus, average Precision, Recall, and F-measure values of the TF\_IDF-based LSA for the twenty-five crops are shown in Table VII.

As a conclusion, by comparing the evaluation results of the TF-based LSA approach with the TF\_IDF-based LSA approach, we conclude that the results of TF\_IDF-based LSA approach achieved the best results since TF-IDF measures how important a term in complaints that give high weight for important terms while TF shows the only number of times that a term appears in a complaint.

TABLE VII. EXAMPLES OF EVALUATION RESULTS FOR TF\_IDF-BASED LSA APPROACH

Crops Name	Evaluation Methods		
	Average Precision	Average Recall	Average F-Measure
الباميا (Okra)	85.4%	83.0%	84.2%
اليوسفي (Mandarin)	88.3%	85.2%	86.7%
البطيخ (Watermelon)	87.0%	84.9%	85.9%
القمح (Wheat)	86.5%	83.3%	84.9%
الأرز (Rice)	86.7%	84.0%	85.3%
القطن (Cotton)	86.8%	84.3%	85.5%
الفاصوليا (Beans)	84.3%	82.7%	83.5%
الطماطم (Tomatoes)	87.4%	83.7%	85.5%
البطاطس (Potato)	81.6%	80.5%	81.0%
الخوخ (Peach)	86.7%	84.4%	85.5%
المشمش (Apricot)	82.1%	81.1%	81.6%
العدس (Lentils)	85.4%	83.6%	84.5%
البصل (Onions)	81.3%	79.4%	80.3%
البرسيم (Clover)	84.8%	81.5%	83.1%
التفاح (Apples)	82.5%	80.4%	81.4%
الباذنجان (Eggplant)	84.0%	83.2%	83.6%
العنب (Grapes)	81.5%	79.3%	80.4%
البرتقال (Orange)	82.6%	81.7%	82.1%
الموز (Banana)	87.8%	84.6%	86.2%
الجوافة (Guava)	83.4%	81.3%	82.3%
البسلة (Peas)	87.0%	82.8%	84.8%
اللوبيا (Cowpea)	81.0%	79.8%	80.4%
الكرنب (Cabbage)	82.0%	78.5%	80.2%
الثوم (Garlic)	82.6%	81.5%	82.0%
الخس (Lettuce)	84.5%	82.3%	83.4%

TABLE VIII. EXAMPLES OF EVALUATION RESULTS FOR PREVIOUS MODELS

Crops Name	Evaluation Methods		
	Average Precision	Average Recall	Average F-Measure
الباميا (Okra)	79.3%	76.7%	78.0%
اليوسفي (Mandarin)	83.9%	80.4%	82.1%
البطيخ (Watermelon)	81.0%	77.9%	79.4%
القمح (Wheat)	81.8%	79.5%	80.6%
الأرز (Rice)	82.5%	79.4%	80.9%
القطن (Cotton)	83.5%	80.0%	81.7%
الفاصوليا (Beans)	80.3%	78.5%	79.4%
الطماطم (Tomatoes)	83.4%	77.7%	80.4%
البطاطس (Potato)	77.8%	76.0%	76.9%
الخوخ (Peach)	83.5%	79.4%	81.4%
المشمش (Apricot)	80.4%	78.0%	79.2%
العدس (Lentils)	82.9%	81.2%	82.0%
البصل (Onions)	78.0%	75.6%	76.8%
البرسيم (Clover)	79.4%	78.7%	79.0%
التفاح (Apples)	78.0%	76.8%	77.4%
الباذنجان (Eggplant)	81.0%	79.9%	80.4%
العنب (Grapes)	77.9%	76.8%	77.3%
البرتقال (Orange)	80.6%	79.9%	80.2%
الموز (Banana)	82.4%	78.3%	80.3%
الجوافة (Guava)	80.5%	78.2%	79.3%
البسلة (Peas)	84.1%	79.6%	81.8%
اللوبيا (Cowpea)	78.8%	75.9%	77.3%
الكرنب (Cabbage)	78.4%	75.8%	77.1%
الثوم (Garlic)	78.6%	76.4%	77.5%
الخس (Lettuce)	80.3%	78.6%	79.4%

Finally, we compared our results with the previous models as Schwab et al. [23]. They applied three methods that are no weighting method, IDF weighting method, and POS weighting method. Schwab concluded that applying both the IDF and POS weighting methods achieved better results in performance. Therefore, we apply the previous models (IDF and POS weighting methods) to our agricultural dataset.

Table VIII shows the average Precision, Recall, and F-measure values for the previous models. We also apply IDF and POS weighting methods on the same twenty-five crops used in our proposed TF-based LSA and TF\_IDF-based LSA approach.

Finally, Fig. 2 show the F-measure evaluation results of our two proposed model TF\_IDF-based LSA and TF-based LSA compared with the previous models of IDF and POS weighting methods.

The comparison figure shows that the proposed TF\_IDF-based LSA achieves better results than the proposed TF-based LSA and previous models of IDF and POS weighting methods.

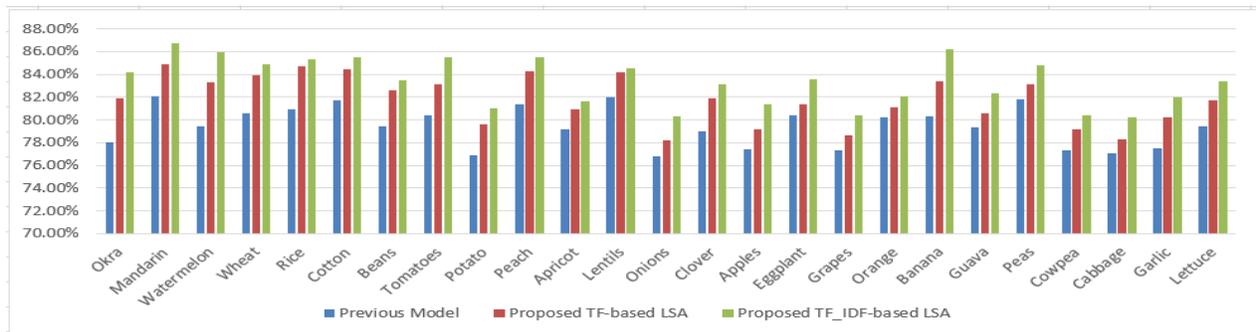


Fig. 2. Average F-Measure Values for Our Two Proposed Models and Previous Models.

V. RESULT

The LSA-based proposed model is applied to retrieve the most relevant complaint and its solution to the farmer query.

Consider the example in Table IX for an Arabic farmer query.

TABLE IX. EXAMPLE FOR ARABIC FARMERS' QUERY AND ITS ENGLISH EQUIVALENT

Arabic Farmer Query	English Farmer Query
وجود ديدانان في الباميا	Presence of worms in okra

As shown in Table IX, the Arabic farmer query is "وجود ديدانان في الباميا" and in English equivalent is "Presence of worms in okra".

The model will be followed step by step as follows:

Firstly, apply the preprocessing steps on the Arabic farmer query and all complaints in the dataset. Table X represents preprocessing steps on the Arabic farmer query.

Secondly, applying classification by MapReduce SVM approach using Hadoop to classify Arabic farmers' query into a crop that belongs to. As in Arabic farmer query "وجود ديدان باميا", this query is classified into "okra" crop.

Thirdly, applying LSA steps that the input matrix is created for Arabic farmer query and all complaints that belong to okra crop. Then, apply RSVD to the input matrix.

TABLE X. PREPROCESSING STEPS FOR ARABIC FARMERS' QUERY AND ITS ENGLISH EQUIVALENT

Preprocessing steps	Arabic farmer query after preprocessing	English farmer query after preprocessing
Tokenization	"وجود", "ديدانان", "في", "الباميا"	'Presence', 'worms', 'in', 'okra'
Stop Words Removal	"وجود", "ديدانان", "الباميا"	'Presence', 'worms', 'okra'
Auto-correction	"وجود", "ديدانان", "الباميا"	'Presence', 'worms', 'okra'
Normalization	"وجود", "ديدانان", "الباميا"	'Presence', 'worms', 'okra'
Lemmatization	"وجود", "ديدانان", "باميا"	'Presence', 'worms', 'okra'

Finally, the output of RSVD is used to measure the semantic similarity score between the farmer query and the complaints document.

According to the proposed two LSA methods, which are TF-based LSA and TF\_IDF-based LSA, Table XI shows the results semantic similarity score between the farmer query and the complaints document.

As shown in Table XI, the results of the semantic similarity score using TF\_IDF-based LSA are better than the semantic similarity score using TF-based LSA since TF-IDF shows how important a term is in complaints while TF shows the number of times that a term appears in a complaint.

Fourthly, rank the complaints according to the semantic similarity score of TF-based and TF\_IDF-based LSA, as shown in Table XII and Table XIII, respectively, then select the complaint with the highest score.

TABLE XI. SEMANTIC SIMILARITY SCORE USING TF AND TF\_IDF-BASED LSA BETWEEN THE FARMER QUERY AND THE COMPLAINTS DOCUMENT

Arabic farmer query	Complaints	Semantic similarity score using TF_IDF-based LSA	Semantic similarity score using TF-based LSA
وجود ديدانان في الباميا Presence worms in okra	تلاحظ وجود حشرة المن على نباتات الباميا. Note the presence of aphids on okra plants.	0.977	0.941
	سأل المزارع عن كيفية حفظ محصول الباميا وطريقة حفظها لاستعمالها في الوقت الغير متوفره فيها. The farmer asked how to preserve the okra crop and how to preserve it for use at a time not available in it.	0.045	0.994
	وجود ديدان صغيره داخل ثمار الباميا. The presence of small worms inside the okra fruits.	0.9998	0.865
	وجود بقع دقيقة على سطحى الورقة لنبات الباميا تتحول هذه البقع الى اللون البنى وتجف الاوراق المصابة و تموت مما يؤدي الى صغر حجم النبات. The presence of minute spots on the two leaf surfaces of the okra plant, these spots turn brown, and the affected leaves dry and die, which leads to the small size of the plant.	0.315	0.713
	وجود ثقوب في ازهار نباتات الباميا و جفاف وسقوط الازهار مع وجود ديدان في بعض الازهار. The presence of holes in the flowers of the okra plants, drought, and fall of the flowers, with the presence of worms in some flowers.	0.994	0.687
وجود بقع صفراء على بعض الأوراق في نباتات الباميا مع وجود أوراق صفراء ( تلاحظ وجود الحشرة الكاملة للذبابة البيضاء على الأوراق ) The presence of yellow spots on some leaves in okra plants, with yellow leaves (the presence of the adult whitefly insect is noticed on the leaves)	0.654	0.933	

TABLE XII. THE RANKED COMPLAINTS ACCORDING TO THE TF\_IDF-BASED SEMANTIC SIMILARITY SCORE

Arabic farmer query	Complaints	Ranked semantic similarity score using TF_IDF-based LSA
وجود ديدان في الباميا Presence worms in okra	وجود ديدان صغيرة داخل ثمار الباميا. The presence of small worms inside the okra fruits.	0.9998
	وجود ثغوب في ازهار نباتات الباميا و جفاف وسقوط الازهار مع وجود ديدان في بعض الازهار. The presence of holes in the flowers of the okra plants, drought, and fall of the flowers, with the presence of worms in some flowers.	0.994
	تلاحظ وجود حشرة المن على نباتات الباميا. Note the presence of aphids on okra plants.	0.977
	وجود بقع صفراء على بعض الأوراق في نباتات الباميا مع وجود أوراق صفراء ( تلاحظ وجود الحشرة الكاملة للذبابة البيضاء على الأوراق ). The presence of yellow spots on some leaves in okra plants, with yellow leaves (the presence of the adult whitefly insect is noticed on the leaves)	0.654
	وجود بقع دقيقة على سطح الورقة لنبات الباميا تتحول هذه البقع الى اللون البني و تجف الاوراق المصابة و تموت مما يؤدي الى صغر حجم النبات. The presence of minute spots on the two leaf surfaces of the okra plant, these spots turn brown, and the affected leaves dry and die, which leads to the small size of the plant.	0.315
سأل المزارع عن كيفية حفظ محصول الباميا و طريقة حفظها لاستعمالها في الوقت الغير متوفره فيها. The farmer asked how to preserve the okra crop and how to preserve it for use at a time not available in it.	0.045	

As shown in Table XII, after ranking semantic similarity score and selecting the highest score that is 0.9998 and its complaint is "وجود ديدان صغيرة داخل ثمار الباميا" which is the nearest complaint to farmer query.

As shown in Table XIII, after ranking semantic similarity score and selecting the highest score that is 0.994 and its complaint is "سأل المزارع عن كيفية حفظ محصول الباميا و طريقة حفظها" which is not the nearest complaint to farmer query.

By comparing the results of both the TF\_IDF-based LSA approach and the TF-based LSA approach, we conclude that the TF\_IDF-based LSA approach is the best method for measuring the semantic similarity score.

Finally, based on the results of TF\_IDF-based LSA approach in Table XII, the solution for the farmer query "وجود ديدان في الباميا" according to the agricultural problems/solutions dataset is "جمع القرون المصابة و اعدامها لعدم امكانية" as shown in Table XIV.

TABLE XIII. THE RANKED COMPLAINTS ACCORDING TO THE TF-BASED SEMANTIC SIMILARITY SCORE

Arabic farmer query	Complaints	Ranked semantic similarity score using TF-based LSA
وجود ديدان في الباميا Presence worms in okra	سأل المزارع عن كيفية حفظ محصول الباميا و طريقة حفظها لاستعمالها في الوقت الغير متوفره فيها. The farmer asked how to preserve the okra crop and how to preserve it for use at a time not available in it.	0.994
	تلاحظ وجود حشرة المن على نباتات الباميا. Note the presence of aphids on okra plants.	0.941
	وجود بقع صفراء على بعض الأوراق في نباتات الباميا مع وجود أوراق صفراء ( تلاحظ وجود الحشرة الكاملة للذبابة البيضاء على الأوراق ). The presence of yellow spots on some leaves in okra plants, with yellow leaves (the presence of the adult whitefly insect is noticed on the leaves)	0.933
	وجود ديدان صغيرة داخل ثمار الباميا. The presence of small worms inside the okra fruits.	0.865
	وجود بقع دقيقة على سطح الورقة لنبات الباميا تتحول هذه البقع الى اللون البني و تجف الاوراق المصابة و تموت مما يؤدي الى صغر حجم النبات. The presence of minute spots on the two leaf surfaces of the okra plant, these spots turn brown, and the affected leaves dry and die, which leads to the small size of the plant.	0.713
	وجود ثغوب في ازهار نباتات الباميا و جفاف وسقوط الازهار مع وجود ديدان في بعض الازهار. The presence of holes in the flowers of the okra plants, drought, and fall of the flowers, with the presence of worms in some flowers.	0.687

TABLE XIV. SOLUTION FOR THE FARMER QUERY

Farmer query	Complaint	Solution
وجود ديدان في الباميا Presence worms in okra	وجود ديدان صغيرة داخل ثمار الباميا. Presence of small worms inside the okra fruits.	جمع القرون المصابة واعدامها لعدم امكانية رش القرون قبل الاستهلاك (The infected pods were collected and destroyed because the pods could not be sprayed before consumption.)

## VI. CONCLUSION

Agriculture has an important role in the economy of every country. Not only supplying foods for the whole population of a country but also it helps to connect and interact with all the relative industries of the country. Due to the world's current conditions from the spread of COVID-19, the imposition of a curfew, and adequate spacing between citizens, all fields are affected, especially the agriculture field. Farmers may have problems and complaints related to the agriculture process and the productivity of the percentage of the crops. It is difficult for farmers to communicate with agricultural experts to find appropriate solutions for their complaints. A semantic similarity approach for agriculture farmers' complaints is developed to solve these issues. This approach is based on LSA to measure semantic similarity between farmer query and the complaints document. The proposed model is applied to the MapReduce SVM using Hadoop for classifying the big agricultural dataset and the farmer complaint according to the crop type to improve the performance of the proposed approach. The results are evaluated on twenty-five crops and tested 25% of different complaint queries on each crop of them. These evaluations applied to our two proposed models of TF-based LSA, TF\_IDF-based LSA, and previous work methods. The developed approach with TF\_IDF-based LSA achieved better results than the TF-based LSA and previous work methods with an F-measure of 86.7%.

## ACKNOWLEDGMENT

This work was supported by a Newton Institutional Links grant, ID 347762518, under the Egypt Newton-Mosharafa Fund partnership. The grant is funded by the 'UK Department for Business, Energy and Industrial Strategy' and 'Science and Technology Development Fund (STDF)' and delivered by the British Council. For further information, please visit [www.newtonfund.ac.UK](http://www.newtonfund.ac.UK).

## REFERENCES

- [1] A. Pawar and V. Mago, "Challenging the Boundaries of Unsupervised Learning for Semantic Similarity," *IEEE Access*, vol. 7, no. January, pp. 16291–16308, 2019.
- [2] M. K. and D. Chidambaram, "A Hybrid Approach for Measuring Semantic Similarity between Documents and its Application in Mining the Knowledge Repositories," *Int J Adv Comput Sci Appl*, vol. 7, no. 8, pp. 231–237, 2016.
- [3] D. Hussen Maulud, S. R. M. Zeebaree, K. Jacksi, M. A. Mohammed Sadeeq, and K. Hussein Sharif, "State of Art for Semantic Analysis of Natural Language Processing," *Qubahan Acad J*, vol. 1, no. 2, 2021.
- [4] A. B. Soliman, K. Eissa, and S. R. El-Beltagy, "AraVec: A set of Arabic Word Embedding Models for use in Arabic NLP," *Procedia Comput Sci*, vol. 117, no. September, pp. 256–265, 2017.
- [5] M. Atabuzzaman, M. Shajalal, M. E. Ahmed, M. I. Afjal, and M. Aono, "Leveraging Grammatical Roles for Measuring Semantic Similarity between Texts," *IEEE Access*, vol. 9, pp. 62972–62983, 2021.
- [6] A. Bordes, S. Chopra, and J. Weston, "Question answering with subgraph embeddings," *EMNLP 2014 - 2014 Conf Empir Methods Nat Lang Process Proc Conf*, pp. 615–620, 2014.

- [7] A. Y. Ichida, F. Meneguzzi, and D. D. Ruiz, "Measuring Semantic Similarity between Sentences Using A Siamese Neural Network," *Proc Int Jt Conf Neural Networks*, vol. 2018-July, pp. 1–7, 2018.
- [8] B. Hassan, S. E. Abdelrahman, R. Bahgat, and I. Farag, "UESTS: An Unsupervised Ensemble Semantic Textual Similarity Method," *IEEE Access*, vol. 7, pp. 85462–85482, 2019.
- [9] D. Chandrasekaran and V. Mago, "Evolution of Semantic Similarity-A Survey," *ACM Comput Surv*, vol. 54, no. 2, pp. 1–35, 2021, doi: 10.1145/3440755.
- [10] W. H.Gomaa and A. A. Fahmy, "A Survey of Text Similarity Approaches," *Int J Comput Appl*, vol. 68, no. 13, pp. 13–18, 2013.
- [11] M. A. R. Abdeen, S. AlBouq, A. Elmahalawy, and S. Shehata, "A closer look at arabic text classification," *Int J Adv Comput Sci Appl*, vol. 10, no. 11, pp. 677–688, 2019.
- [12] and O. A.-M. Mohammad, Adel Hamdan, Tariq Alwada'n, "Arabic text categorization using support vector machine, Naïve Bayes and neural network," *GSTF J Comput* 51, vol. Volume 5, no. 1, pp. 40–44, 2016.
- [13] "VERCON." <http://www.vercon.sci.eg/> (accessed Sep. 02, 2021).
- [14] S. Boukil, M. Biniz, F. El Adnani, L. Cherrat, and A. E. El Moutaouakkil, "Arabic text classification using deep learning technics," *Int J Grid Distrib Comput*, vol. 11, no. 9, pp. 103–114, 2018.
- [15] R. Duwairi and M. El-Orfali, "A study of the effects of preprocessing strategies on sentiment analysis for Arabic text," *J Inf Sci*, vol. 40, no. 4, pp. 501–513, 2014.
- [16] A. Tripathy, A. Anand, and S. K. Rath, "Document-level sentiment classification using hybrid machine learning approach," *Knowl Inf Syst*, vol. 53, no. 3, pp. 805–831, 2017.
- [17] C. A. Flores, R. L. Figueroa, and J. E. Pezoa, "Active Learning for Biomedical Text Classification Based on Automatically Generated Regular Expressions," *IEEE Access*, vol. 9, pp. 38767–38777, 2021.
- [18] H. Al Saif and T. Alotaibi, "Arabic text classification using feature-reduction techniques for detecting violence on social media," *Int J Adv Comput Sci Appl*, vol. 10, no. 4, pp. 77–87, 2019.
- [19] F. Ö. Çatak and M. E. Balaban, "A Map Reduce-based distributed SVM algorithm for binary classification," *Turkish J Electr Eng Comput Sci*, vol. 24, no. 3, pp. 863–873, 2016.
- [20] M. Ali, D. S. Guru, and M. Suhil, *Classifying Arabic Farmers' Complaints Based on Crops and Diseases Using Machine Learning Approaches*, vol. 1037. Springer Singapore, 2019.
- [21] R. Al-khurayji and A. Sameh, "An Effective Arabic Text Classification Approach Based on Kernel Naive Bayes Classifier," *Int J Artif Intell Appl*, vol. 8, no. 6, pp. 01–10, 2017.
- [22] and K. B. A. Abutiheen, Zinah Abdulridha, Ahmed H. Aliwy, "Arabic text classification using master-slaves technique," *J Phys Conf Ser*, vol. 1032, no. May, 2018.
- [23] E. M. B. NAGOUDI, J. Ferrero, and D. Schwab, "LIM-LIG at SemEval-2017 Task1: Enhancing the Semantic Similarity for Arabic Sentences with Vectors Weighting," *Proc 11th Int Work Semant Eval*, no. June, pp. 134–138, 2018.
- [24] A. El Hadi, Y. Madani, R. El Ayachi, and M. Erritali, "A new semantic similarity approach for improving the results of an Arabic search engine," *Procedia Comput Sci*, vol. 151, pp. 1170–1175, 2019.
- [25] A. Mahmoud and M. Zrigui, "Semantic similarity analysis for paraphrase identification in Arabic texts," *PACLIC 2017 - Proc 31st Pacific Asia Conf Lang Inf Comput*, pp. 274–281, 2019.
- [26] A. Awajan, "Semantic similarity based approach for reducing Arabic texts dimensionality," *Int J Speech Technol*, vol. 19, no. 2, pp. 191–201, 2016.
- [27] S. Malallah, A. Qassim, and A. Alameer, "Finding the Similarity between Two Arabic Text," *Iraqi J Sci*, vol. 58, no. 1, pp. 152–162, 2017.

- [28] A. El Kah and I. Zeroual, "The effects of Pre-Processing Techniques on Arabic Text Classification," *Int J Adv Trends Comput Sci Eng*, vol. 10, no. 1, pp. 41–48, 2021.
- [29] A. Ayedh, G. TAN, K. Alwesabi, and H. Rajeh, "The Effect of Preprocessing on Arabic Document Categorization," *Algorithms*, vol. 9, no. 2, 2016.
- [30] K. Darwish and H. Mubarak, "Farasa: A new fast and accurate Arabic word segmenter," *Proc 10th Int Conf Lang Resour Eval Lr 2016*, pp. 1070–1074, 2016.
- [31] B. Li, Z. Li, T. Li, and J. Liu, "A portable embedded automobile exhaust detection device based," *2013 IEEE 3rd Int Conf Inf Sci Technol ICIST 2013*, no. December, pp. 126–128, 2013.
- [32] F. S. Al-Anzi and D. AbuZeina, "Toward an enhanced Arabic text classification using cosine similarity and Latent Semantic Indexing," *J King Saud Univ - Comput Inf Sci*, vol. 29, no. 2, pp. 189–195, 2017.
- [33] A. Abdelali, K. Darwish, N. Durrani, and H. Mubarak, "Farasa: A Fast and Furious Segmenter for Arabic," *Proc 2016 Conf North Am chapter Assoc Comput Linguist Demonstr*, vol. 2016, pp. 11–16, 2016.
- [34] D. AlSaleh and S. Larabi-Marie-Sainte, "Arabic Text Classification using Convolutional Neural Network and Genetic Algorithms," *IEEE Access*, vol. 9, pp. 91670–91685, 2021.
- [35] M. S. Shanoda, S. A. Senbel, and M. H. Khafagy, "JOMR: Multi-join optimizer technique to enhance map-reduce job," *2014 9th Int Conf Informatics Syst INFOS 2014*, no. May, pp. PDC80–PDC87, 2015.
- [36] M. H. Mohamed and M. H. Khafagy, "Hash semi cascade join for joining multi-way map reduce," *IntelliSys 2015 - Proc 2015 SAI Intell Syst Conf*, no. November, pp. 355–361, 2015.
- [37] M. Aksa, J. Rashid, M. W. Nisar, T. Mahmood, H. Y. Kwon, and A. Hussain, "Bitmapaligner: Bit-parallelism string matching withmapreduce and hadoop," *Comput Mater Contin*, vol. 68, no. 3, pp. 3931–3946, 2021.
- [38] N. K. Nagwani, "Summarizing large text collection using topic modeling and clustering based on MapReduce framework," *J Big Data*, vol. 2, no. 1, pp. 1–18, 2015.
- [39] R. M. Badry and I. F. Moawad, *A Semantic Text Summarization Model for Arabic Topic-Oriented*, vol. 921, no. January. Springer International Publishing, 2020.
- [40] A. V. Nimkar and D. R. Kubal, "A survey on word embedding techniques and semantic similarity for paraphrase identification," *Int J Comput Syst Eng*, vol. 5, no. 1, p. 36, 2019.
- [41] M. S. Al-Batah, S. Mrayyen, and M. Alzaqebah, "Arabic Sentiment Classification using MLP Network Hybrid with Naive Bayes Algorithm," *J Comput Sci*, vol. 14, no. 8, pp. 1104–1114, 2018.

# An NB-ANN based Fusion Approach for Disease Genes Prediction and LFKH-ANFIS Classifier for Eye Diseases Identification

Samar Jyoti Saikia<sup>1</sup>

Gauhati University, Guwahati-781014, Assam, India  
Assam Don Bosco University, Guwahati-781017  
Assam, India

Dr. S. R. Nirmala<sup>2</sup>

Gauhati University, Guwahati-781014, Assam, India  
KLE Technological University, Hubli-580031  
Karnataka, India

**Abstract**—A key step to apprehend the mechanisms of cells related to a particular disease is the disease gene identification. Computational forecast of disease genes are inexpensive and also easier compared to biological experiments. Here, an effectual deep learning-centered fusion algorithm called Naive Bayes-Artificial Neural Networks (NB-ANN) is proposed aimed at disease gene identification. Additionally, this paper proposes an effectual classifier, namely Levy Flight Krill herd (LFKH) based Adaptive Neuro-Fuzzy Inferences System (ANFIS), for the prediction of eye disease that are brought about by the human disease genes. Utilizing this technique, completely '10' disparate sorts of eye diseases are identified. The NB-ANN includes these '4' steps: a) construction of '4' Feature Vectors (FV), b) selection of negative data, c) training of FV utilizing NB, and d) ANN aimed at prediction. The LFKH-ANFIS undergoes Feature Extraction (FE), Feature Reduction (FR), along with classification for eye disease prediction. The experimental outcomes exhibit that method's efficiency with regard to precision and recall.

**Keywords**—Disease gene identification; eye disease identification; deep learning; adaptive neuro-fuzzy inferences system (ANFIS); levy flight based krill herd (LFKH); principle component analysis (PCA)

## I. INTRODUCTION

Disease genes are the dysfunction of a collection of genes, which in turn leads to Complex diseases [1] [2]. A key step towards enlightening the fundamental molecular operations of diseases is the recognition of genes concerned with genetic as well as rare diseases [3]. Prioritizing the candidate genes using experimental approaches is very costly and tedious [4]. Matrix decomposition along with Network propagation is the '2' categories under which all these existing techniques for the prediction can well be summarized [5]. In current years, technologies, say higher-throughput [6] gene expressions profiling has permitted the characterization of molecular differences betwixt healthy and disease states, bringing about the recognition of an augmenting number of disease-linked genes [7]. A great quantity of machine learning-centered computational methods was generated for predicting disease genes [8], say restricted Boltzmann machines [9], deep belief network [10], linear regressions model [11], support vectors machine [12], multilayer perceptions (MLP) [13], et cetera. These often attain greater prediction accuracy on larger data

sets [14]. Nonetheless, on account of the lower statistical power brought about by means of smaller samples in biomedical data, the issue of smaller samples typically causes poor reproducibility of prediction outcomes among disparate patients [15]. To trounce such downsides, in this paper, an NB-ANN is proposed for identifying the disease genes as well as the LFKH-ANFIS is proposed for the identification of eye-linked diseases triggered by means of those recognized disease genes.

## II. LITERATURE REVIEW

Chen BoLin et al.[16] proffered a kernel-centric Markov random field approach. This approach was deployed for capturing the genes-diseases associations on the base of biological networks. Here, three sorts of kernels were deployed for delineating the overall relations of vertices in 5 biological networks, respectively, and weighted methodology was built with the proffered approach to merge those data. It acquired 0.771- Area under the ROC Curves (AUC) score when merging all the concerned biological data. Here, Markov Exponential Diffusions (MED) kernel rendered the low AUC performance contrasted with Laplacian Exponential Diffusions (LED) kernel on integrated '3' network situation.

Abdulaziz Yousef and Nasrollah Moghadam Charkari [17] rendered a disease gene identification technique centered on amino acids' physicochemical properties as well as classification algorithm. Amino acids physic-chemical properties were utilized to change the sequences of protein into numerical vector for the feature vector generation. Support vector data description algorithm was employed to envisage the disease genes. The rendered method performed better contrasted with the prevailing methods concerning precision, recall, along with F-measure. Data standardization was required for Principle Component Analysis (PCA) utilization. The standardization absence brought about the PCA's failure in finding optimal components which in turn affected this model's performance.

Zhen Tian et al. [18] paid attention on a framework, termed RWRB, for inferring the causal genes of disease. The Similarity Networks (SN) of 5 genes (protein) was individually constructed grounded on countless genomic data. The integrated gene SN was re-developed in respect of the SN fusion approach. The restart along with random walk algorithm

was deployed on a Phenotype-Gene (PG) bi-layer network, which integrated phenotype SN, PG association, and integrated gene SN for proffering the priority for the candidate genes (disease-associated ones). Outcomes corroborated that the RWRB was accurate when analogized to certain methods regarding the evaluation metrics. This method rendered the degraded performance with respect to Number of Successful Predictions (NSP) metric when the jumping probability is above 0.6 in disparate experiments.

Mehdi Joodaki et al. [19] put forward a gene ranking approach, named as Random Walks with Restart on a Heterogeneous Networks with Fuzzy Fusions (RWRHN-FF). Here, first, centred on disparate genomic sources, '4' gene-gene similarity networks were generated, and then, they were joined utilizing the type-II fuzzy voter scheme. The resultant gene to gene network was linked with the disease-disease similarity network. By means of integrating '4' sources via a '2'-part disease gene network, the disease-disease similarity network was created. RWRHN analyzed this network. While considering Area Under ROC Curves (AUC) as well as convergence time, the presented approach trounced the prevailing methods. On account of the bad data integration of manifold sources, the precision metric of this method was declined.

Pradipta Maji and Ekta Shah [20] recognized the disease-associated genes with the utilization of a gene selection algorithm, named SiFS. The SiFS algorithm gathered countless genes as of micro-array data as diseased genes by elevating the functional and significance similarity of the chosen gene subset. Contrarily, a similarity metric was instated for computing the functional similarity betwixt 2 genes. The experimental outcomes on disparate data sets corroborated that the algorithm recognized more disease-associated genes when analogized to prevailing disease gene selection methodologies. The similarity measure of the presented method was affected by the low coverage of human genes and reliability of protein-protein interaction (PPI).

### III. PROPOSED METHODOLOGY

Here, a novel sequence-based fusion method (NB-ANN) is proposed aimed at disease genes identification, and the LFKH-ANFIS is proposed aimed at identifying eye-related diseases that are triggered by those disease genes, say Age-associated Macular Degenerations (AMD), cataract, glaucoma, inherited optics neuropathies, Marfan syndrome polypoidal choroidals vasculopathies, retinitis pigmentosas, Stargardt disease, along with uveal melanoma.

The proposed method's architecture is exhibited in Fig. 1. Fig. 1 exhibits the proposed methodology's architecture. In the initial phase, representation methods are used to achieve the FV as of the disease and unknown disease genes. In the 2<sup>nd</sup> phase, a dataset with positive as well as reliable negative instances is created by selecting negative protein set. In the 3<sup>rd</sup> phase, disparate FV of the same instances are categorized using the NB classifier. In the 4<sup>th</sup> phase, ANN fuses together the NB classifiers to enhance the accuracy. After the identification of disease gene, FE is done. It extracts the features as of the identified disease genes for classifying the eye-related diseases caused via the disease genes. Next, PCA is employed for FR

for removing the redundant features. Lastly, the LFKH-ANFIS algorithm takes care of the eye disease classification.

#### A. Disease Gene Identification

Here, the technique for identifying along with prioritizing disease genes is elucidated. The proposed work comprises '4' steps: (i) Translate equivalent gene products (proteins) into '4' numerical FV utilizing '4' sorts of protein sequence translator, (ii) choosing negative data as of unknown genes, (iii) modeling every FV utilizing NB, (iv) ANN is utilized for making the last decision via fusing the envisaging outcomes of the base NB classifiers.

#### B. Protein Sequence Translation

Extracting FV aimed at disease and unknown genes is the utmost vital challenges while identifying disease-gene issues utilizing a machine learning algorithm. Here, for characterizing genes, equivalent gene products (Proteins) are utilized. Hereof, to extract the vital information of protein wherein fully encoded is taken, '4' sorts of representation techniques were utilized, they are i) Normalized Moreau-Broto autocorrelation (NA), ii) Geary autocorrelations (GA), iii) auto covariances (AC), and iv) Moran auto-correlations (MA). The reason for utilizing these representation techniques is to evade losing imperative information that is concealed in the protein sequences. All of these techniques are centered upon the physicochemical properties of amino acids since sequence of amino acid determines the protein. In other words, amino acids are the building block of protein. Here, '12' physic-chemical properties are employed as a descriptor to render more information concerning the amino acid sequence. These properties comprise entropy of formations (EOF), partitions coefficient (PC), polarity (POL), amino acid compositions (AAC), residue accessible surface areas in tripeptide (RAS), transfer-free energy (TFE), CC on regressions analysis (CC), hydrophilicity (HY-PHIL), polarizability (POL2), hydrophobicity (HY-PHOB), solvations free energy (SFE), along with graph shapes index (GSI), correspondingly. Min-Max normalization technique is employed for normalizing these physicochemical properties since it ensures that all physicochemical properties have exact same scale.

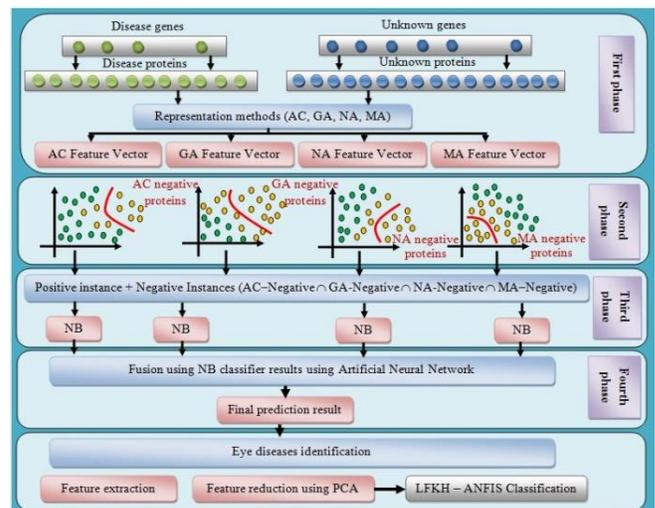


Fig. 1. Proposed Architecture.

### C. Negative Data Generation

Subsequent to generating the FV for all genes, it is essential to select a negative protein set as of the unknown proteins to construct a dataset with positive as well as reliable negative instances. With regard to it, a '6' steps algorithm is proposed.

Step1: Define four negative sets as an empty set for each of the feature vectors as

$$D_{AC} = \Phi; D_{GA} = \Phi; D_{MA} = \Phi; D_{NA} = \Phi \quad (1)$$

Step2: Second, representing each protein  $R_i$  (disease and unknown proteins) into four vector:  $S_{AC}^{R_i}, S_{GA}^{R_i}, S_{MA}^{R_i}, S_{NA}^{R_i}$  using AC, GA, MA, and NA representation methods can well be expressed as

$$S_{AC}^{R_i} = AC(R_i) \quad (2)$$

$$S_{GA}^{R_i} = GA(R_i) \quad (3)$$

$$S_{MA}^{R_i} = MA(R_i) \quad (4)$$

$$S_{NA}^{R_i} = NA(R_i) \quad (5)$$

Step3: Calculate the positive mean vector  $M_p$  of all positive proteins for every represented vectors.

$$M_p(AC) = \sum_{k=0}^n \frac{S_{AC}^{P_k}}{|D|} \quad (6)$$

$$M_p(GA) = \sum_{k=0}^n \frac{S_{GA}^{P_k}}{|D|} \quad (7)$$

$$M_p(MA) = \sum_{k=0}^n \frac{S_{MA}^{P_k}}{|D|} \quad (8)$$

$$M_p(NA) = \sum_{k=0}^n \frac{S_{NA}^{P_k}}{|D|} \quad (9)$$

Step4: Fourth, calculate the similarity,  $Sim_j$  between each unknown protein ( $R_i \in U_R$ ) and the mean vectors ( $M_p$ ) that can well be expressed as.

$$P_{U_R}^{AC}(j) = P(S_{AC} U_R, M_p(AC)) \quad (10)$$

$$P_{U_R}^{GA}(j) = P(S_{GA} U_R, M_p(GA)) \quad (11)$$

$$P_{U_R}^{MA}(j) = P(S_{MA} U_R, M_p(MA)) \quad (12)$$

$$P_{U_R}^{NA}(j) = P(S_{NA} U_R, M_p(NA)) \quad (13)$$

Step5: Fifth, for each FV, choose  $g$  negative proteins as of  $U_R$  set by selectig the  $g$  farthest proteins as of the  $M_p$ , which can well be specified as.

$$D_{AC} = \text{sort}(D_{U_R}^{AC}) \quad (14)$$

$$D_{GA} = \text{sort}(D_{U_R}^{GA}) \quad (15)$$

$$D_{MA} = \text{sort}(D_{U_R}^{MA}) \quad (16)$$

$$D_{NA} = \text{sort}(D_{U_R}^{NA}) \quad (17)$$

$$P_{AC} = \text{select}(D_{U_R}^{AC}(1:g)) \quad (18)$$

$$P_{GA} = \text{select}(D_{U_R}^{GA}(1:g)) \quad (19)$$

$$P_{MA} = \text{select}(D_{U_R}^{MA}(1:g)) \quad (20)$$

$$P_{NA} = \text{select}(D_{U_R}^{NA}(1:g)) \quad (21)$$

Manhattan distance measure is utilized as a distance measurement to gauge the distance betwixt  $R_j$  and  $M_p$ . As the number of unknown proteins is much more than disease proteins, ascertaining the appropriate number ( $g$ ) of chosen negative proteins has a direct effect on the prediction model construction.

Step6: Lastly, the proteins ascertained by means of the intersection of chosen negative protein sets will be selected as reliable negative data ( $R_{NS}$ ).

$$R_{NS} = P_{AC} \cap P_{GA} \cap P_{MA} \cap P_{NA} \quad (22)$$

### D. Naive Bayes Algorithm

Naive Bayes (NB) stands as a probabilistic classifier stimulated by the Bayes theorem under a simple assumption, i.e., the attributes are autonomous conditionally. NB is a particularly simple algorithm to execute, and good outcomes have been attained in the utmost instances. Nevertheless, utilizing the same classifier (NB) to categorize the disparate FV of the same instances produces some uncertainties and also makes some individual errors. Therefore, a practical fusion of these classifiers will more likely lessen the overall prediction inaccuracies and renders better prediction outcomes by reducing the negative effects of noise data which proportionally increases with rising negative data ratio. Here, the ANN is utilized as a fusion method in the 4<sup>th</sup> layer. The general explanation concerning the ANN is rendered in the section below

### E. Artificial Neural Network

ANN classifier comprises countless interconnected artificial neurons which have multiple interconnections connected to the adjustable weights. The inputted patterns are transmitted through the layers to solve the problem. By employing the corresponding synaptic weights, the information is mapped.

Step1: Make arbitrary weights in the interval [0, 1] and allocate it to the Hidden Layer (HL) neurons as well as the Output Layer (OL) neurons. Maintain a unity value weight for all neurons of the inputted layer for easy computation and to attain better performance together with outcomes.

Step2: Calculate the output of the hidden layer as shown in below eq.

$$H_o = B_i + \sum_{i=1}^L NB_i W_i \quad (23)$$

Where,

$B_i$  - Bias value,

$NB_i$  - Output of previous NB layer values,

$W_i$  - Weight value of the given input features.

Step3: To find the final output unit, the hidden unit is multiplied with the weight of the hidden layer output, which is given in the equation (23).

$$O_i = B_i + \sum_{i=1}^m H_o W_{ik} \quad (24)$$

Where,

$H_o$  - Hidden unit

$W_{ik}$  - Weights of the hidden layer

$O_i$  - Output unit.

The activation function for the output layer is estimated as

$$Active(o_i) = \frac{1}{1 + e^{-o_i}} \quad (25)$$

Step4: Recognize the learning error as offered beneath

$$e_r = \sum z_i - o_i \quad (26)$$

Where,

$e_r$  - Error rate,

$z_i$  - Target output value,

$o_i$  - Actual output value.

It is apparent that the NB-centered classifiers construct the model for the same dataset utilizing disparate FV. Therefore, fusing the NB-based predictors' outputs utilizing the ANN brings about concurrent utilization of optional feature descriptors along with classification procedures.

## F. Feature Extraction

After the disease gene identification, this phase is done to extract the features as of the identified disease genes for classifying the eye-related diseases caused through the disease genes. The features, namely Katz Fractal Dimension (KFD), Log Energy (LE), Hurst exponent (HE), Shannon Entropy (SE), Skewness, Mean, Kurtosis, Detrended Fluctuation Analysis (DFA), Discrete Wavelet Transforms, and also Standard Deviation are extracted.

## G. Feature Reduction

Following feature extraction, feature reduction is done with the utilization of PCA. PCA that conserves the existent information and eliminates the redundant constituents is employed to discover significant features. PCA acts as a linear combination where one set of variables in  $P_m$  space into another set in  $P_n$  space containing the maximum amount of variance in the data where  $n < m$ . This is obtained in the following steps:

Step1: Evaluate the covariance matrix " $C_m$ " as,

$$C_m = \frac{1}{N} \sum_{k=0}^N (F_k - m)(F_k - m)^T \quad (27)$$

Where,

$$m = \frac{1}{N} \sum_k F_k \text{ - Original feature vectors.}$$

Step2: Determinr the eigenvectors " $v_i$ " and Eigen values " $\mu_i$ " of the  $C_m$  by solving the subsequent decomposition

$$\mu_i v_i = L v_i \quad (28)$$

Where,

$L$  - Matrix having the properties of eigen value and eigen vector.

Step3: Sort the outcomes in decreasing order of  $\mu_i$

Step4: Choose the indispensable components (that is, features).

## H. Classification for the Identification of Eye Diseases

Here, the related eye disease prediction is performed with the utilization of the LFKH-ANFIS algorithm. Gradient-centric learning is the standard learning process in ANFIS but it is prone to trap in local minima. On this account, the ANFIS is ameliorated with the utilization of LFKH for lessening its complexity and for elevating the classification accuracy. And thereby, the ANFIS is termed as LFKH based ANFIS (LFKH-ANFIS). The ANFIS has 2 fuzzy IF-THEN rules as specified in the equations (28) and (29).

Rule i: If  $F_1$  is  $A_i$  and  $F_2$  is  $B_i$  then,  $\bar{Q}_i$

$$Rules_i = cF_i + d_iF_{i+1} + e_i \quad (29)$$

Rule ii: If  $F_1$  is  $A_{i+1}$  and  $F_2$  is  $B_{i+1}$  then,

$$Rules_{i+1} = c_{i+1}F_i + d_{i+1}F_{i+1} + e_{i+1} \quad (30)$$

Where,

$A_i, B_i, A_{i+1}$  and  $B_{i+1}$  - Fuzzy sets,

$c_i, d_i, e_i, c_{i+1}, d_{i+1}$  &  $e_{i+1}$  - Predicted design parameters during training,

$F_i$  and  $F_{i+1}$  - Disparate reduced feature values acquired as of PCA.

These provided parameters are optimized with the assist of the LFKH algorithm for attaining a better outcome. The ANFIS encompasses some layers as elucidated below,

Layer1: The first layer named a fuzzification layer gathers the input values and finds their membership functions (MF) as proffered below.

$$Z_{1,i} = \chi_i(F_i) \quad (31)$$

Where,

$F_i$  - Input to node  $i$ ,

$\chi_i$  - MF of the input  $F_i$ .

Each node here is adapted well to a functional parameter. The output acquired from each node acts as a degree of membership value that is provided by the input of an MF. The MF utilized in the proposed work is Gaussian kernel MF. The reason for choosing Gaussian kernel MF is to diminish the computational price of ANFIS since Gaussian kernel MF has least number of modifiable parameters. The MF used in the proposed work is specified in the succeeding equation.

$$\chi_i = \exp\left(-\frac{\|c_i - d_i\|^2}{2e_i^2}\right) \quad (32)$$

Where,

$c_i, d_i$  and also  $e_i$  - MF parameters that could alter the MF's shape and are concerned as the premise parameters.

Layer2: This layer named the rule layer is accountable for creating the firing strengths (FS) for the rules. The incoming signals are mathematically multiplied to acquire the output that means the FS of a rule.

$$Z_{2,i} = Q_i = \chi_i(F_i) \times \chi_i(F_{i+1}) \quad (33)$$

Layer3: It aids to normalize the evaluated FSs by dividing every value with a total FS. The  $i^{th}$  node evaluates the ratio  $(\bar{Q}_i)$  betwixt the  $i$  th rule's FS and the sum value of all rules' FSs to generate its output.

$$Z_{3,i} = \bar{Q}_i = \frac{H_i}{Q_1 + Q_2 + Q_3 + Q_4 + Q_5 + Q_6}, \quad i = 1, 2..6 \quad (34)$$

Layer4: It takes the above attained normalized values as inputs (resultant parameter sets) and it has adaptive nodes with a node function.

$$Z_{4,i} = \bar{Q}_i \cdot Rules_i \quad (35)$$

Where,

$\bar{Q}_i$  - Normalized FSs from the former layer and

$Rules_i$  - system rule. And here, the deployed parameters are named as succeeding parameters.

Layer5: The former fourth layer proffers the defuzzificated values and these values are transmitted to the fifth layer for acquiring the final output. All incoming signals are summated to acquire overall output, and here, the circle node is labeled as  $\sum$

$$Z_{5,i} = \sum_i Q_i Rules_i = \frac{\sum_i Q_i Rules_i}{\sum_i Q_i} \quad (36)$$

From the LFKH-ANFIS, the 10 classes of eye diseases for the identified disease gene, that is, Age-related Macular Degeneration (AMD), cataract, Marfan syndrome, glaucoma, inherited optic neuropathies, polypoidal choroidal vasculopathies, retinitis pigmentosa, uveal melanoma, and Stargardt disease are acquired.

### I. Levy Flight based Krill Herd Algorithm

The Krill Herd (KH) algorithm has the potential to effectively determine the optimum solution for certain search spaces configurations. With the futile exploration of KH's search approach, it is incompetent to assure convergence. This proposed method utilizes the Levy flight (LF) in KHA with the intention of resolving the aforesaid difficulty. Hence, the parameter tuning for ANFIS utilizing this optimization is termed as LF based KH (LF-KH). With the utilization of the Lagrangian model, the krill's location is evaluated as,

$$\frac{dXi}{dt} = H_i + F_i + D_i \quad (37)$$

Where,

$H_i$  - Motion guided by other KI,

$F_i$  - Foraging motion,

$D_i$  - Physical diffusion of the  $i^{th}$  KI's.

The steps that are done in this algorithm are,

Step1: The krill individuals (KI) endeavor to hold a high density and move on account of their mutual effects. The direction of KI motion is ascertained by the density of the local - target and repulsive - swarms. The KI movement is written as:

$$H_i^{new} = H^m \alpha_i + \omega_n H_i^{old} \quad (38)$$

Where,

$H^m$  - Maximal induced speed,

$\omega_n$  - Motion' inertia weight in [0, 1],

$H_i^{old}$  - Last motion-induced.

Here,  $\alpha_i$  is evaluated as follows,

$$\alpha_i = \alpha_i^{local} + \alpha_i^{t\ arg\ et} \quad (39)$$

Where,

$\alpha_i^{local}$  - Local effects of neighbors of the  $i^{th}$  individual,

$\alpha_i^{t\ arg\ et}$  - Best solution direction as of the  $i^{th}$  individual.

The  $\alpha_i^{local}$  in a KI movement is evaluated as:

$$\alpha_i^{local} = \sum_{j=1}^{MM} \widehat{K}_{i,j} \widehat{H}_{i,j} \quad (40)$$

$$\widehat{H}_{i,j} = \frac{H_j - H_i}{\|H_j - H_i\| + \epsilon} \quad (41)$$

$$\widehat{K}_{i,j} = \frac{K_i - K_j}{K^{worst} - K^{best}} \quad (42)$$

Where,

$K^{best}$  - Best-fitness (BF) values of the KIs,

$K^{worst}$  - Worst-fitness values of the KIs

$K_i$  - Objective function or the fitness of the  $i^{th}$  KI,

$H$  - Associated positions,

$K_j$  - Fitness of  $j$ th neighbors ( $j = 1, 2, \dots, MM$ ),

$MM$  - Number of prevailing neighbors.

The least positive number termed “ $\lambda$ ” is added to the denominator for averting the singularities. Utilizing the KIs' original behavior, a sensing distance ( $S_d$ ) is evaluated as

$$S_{d,i} = \frac{1}{5M} \sum_{j=1}^N \|H_i - H_j\| \quad (43)$$

Where,

$S_{d,i}$  - Sensing distance for the  $i^{th}$  KI,

$N$  - Number of KIs,

Factor 5 - Empirically acquired value. The effect of the KI with the BF on the  $i^{th}$  KI is regarded utilizing Equation (44).

$$\alpha_i^{t\ arg\ et} = C^b \widehat{K}_{i,best} \widehat{H}_{i,best} \quad (44)$$

Where,

$C^b$  - Effective co-efficient of the KI bearing the BF to the  $i^{th}$  KI.

This coefficient is defined because  $\alpha_i^{t\ arg\ et}$  directs the solution to the global optima and it must be more effective when analogized to other KI, that is, neighbors. Herein, the  $C^b$  is evaluated as

$$C^b = 2 \left( rd + \frac{I}{I_{max}} \right) \quad (45)$$

Where,

$I$  - Actual iteration number,

$I_{max}$  - Maximal iterations.

For enhancing exploration, “ $rd$ ” which is a random value lies in the gamut of (0, 1) is utilized. The proposed approach utilizes the LF for the process of a random walk rather than a simpler one to overcome the incapability of KH search approach which led to its inability to ensure convergence. LF maximizes the efficiency of the searches in uncertain environments. Whilst generating a new solution  $X_i'$  for the  $i^{th}$  solution by performing LF, the new candidate is evaluated as,

$$X_i' = X_i \oplus \alpha \text{Levy}(\beta) \quad (46)$$

Where,

$\alpha$  - Random step size parameter

$\beta$  - LF distribution parameter

$\oplus$  - Entry wise multiplication

Here, the equation (45) is rewritten as,

$$C^b = 2 \left( X_i' + \frac{I}{I_{max}} \right) \quad (47)$$

Step2: The foraging motion is also known as searching motion is evaluated in respect of 2 vital effective parameters like i) food location along with ii) the prior experiences of the KIs' food location. They are evaluated as

$$Fa_i = F_s \gamma_i + \omega_l Fa_i^{old} \quad (48)$$

Where  $\gamma_i = \gamma_i^{best} + B_i^{best}$  (49)

Where,

$F_s$  - Foraging speed,

$w_l$  - Inertia weight for foraging,

$B_i^{best}$  - Best solution

Step3: The physical diffusion process of the KI is an arbitrary one and is the motion associated to  $Df_i$  and  $\delta$ . Its equation is,

$$Df_i = Df_m \delta \quad (50)$$

Where,

$Df_i$  - Maximal diffusion speed,

$\delta$  - Random directional vector together with its arrays of arbitrary values in (-1, 1).

The KH movement is concerned as a process on the way to the BF. So, the KI position is proffered by.

$$X_i(t + \Delta t) = X_i(t) + \Delta t \frac{dX_i}{dt} \quad (51)$$

Where,

$\Delta t$  - Scale factor of the speed vector

$\Delta t$  is an imperative parameter, and it must be adjusted in respect of the optimization issue. Its value is completely contingent on the provided search space.

#### IV. RESULT AND DISCUSSION

Here, the proposed system is analyzed and its performance is analogized to the existing algorithms regarding certain performance metrics. To ascertain the proposed method's robustness, to lessen the over fitting and to lessen the bias in the estimate of the classification model, 5 fold cross-validations have been employed utilizing a dataset with 10,000 instances (that is, 5000 positive and 5000 negative instances). Table I proffers the values acquired by the proposed NB-ANN predictor and some NB based classifiers regarding their prediction performance.

Table I evinces the f-measure, precision, together with recall values attained by the NB-based and fusion-based

predictions. The AC-NB shows 81.6% precision, which is higher when analogized to that of GA-NB (74), NA-NB (76.54), and MA-NB (72.4). But, only the proposed fusion methodology acquires the highest precision (83.52) amongst others. Likewise, for f-measure and recall, the proposed NB-ANN classifier proffers the higher most values when analogized to other NB based approach. It is found that the fusion predictor shows the topmost performance when analogized to each NB-based predictor. As the classification of disparate FVs of the same data utilizing the same classifier generates certain uncertainties, fusing the classifier outcomes would diminish the overall classification errors. Fig. 2 evinces the comparison of NB-ANN and other existing approaches regarding f-measure, precision, together with recall.

Fig. 2 contrasts the proposed NB-ANN to some existing approaches regarding f-measure, precision, together with recall. The proposed NB-ANN acquires the 86-precision, 89.2-recall, and 88-f-measure, whereas, the existing ones acquire lower values for those measures when analogized to the proposed NB-ANN. For instance, the PUDI, ProDige, and SVM-C4.5 acquired 78.3, 72.5, and 82.4 precision values, 84.2, 78.8, and 85.2-recall values, and 80, 74.6, and 83-f-measure results. Here, the existing SVM-C4.5 shows greater performance. But, when analogized to the proposed NB-ANN, the existing ones show the least performance. From this comparison, the proposed NB-ANN is confirmed to acquire a remarkable performance for disease gene identification, and it worked well than other approaches. Then, the next experiment is performed for analyzing the proposed LFKH-ANFIS and comparing the LFKH-ANFIS with the existing techniques centered on performance regarding sensitivity, precision, specificity, recall, accuracy, f-measure, PPV, NPV, MCC, and FDR. Table II proffers the outcomes of LFKH-ANFIS and some existing algorithms.

TABLE I. COMPARISON OF PROPOSED AND EXISTING TECHNIQUES

Methods	Precision (%)	Recall (%)	F-measure (%)
AC-NB	81.6	73.2	74.5
GA-NB	74	84.6	80.47
NA-NB	76.54	83.2	79.8
MA-NB	72.4	88	79.6
NB-ANN	83.52	86.47	83

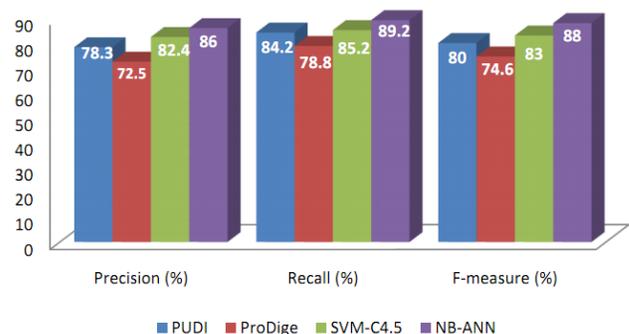


Fig. 2. Performance Graph for the NB-ANN with Existing Techniques.

TABLE II. RESULTS COMPARISON OF THE PROPOSED LFKH-ANFIS WITH EXISTING TECHNIQUES

Performance Metrics	Proposed LFKH-ANFIS	ANFIS	DNN	ANN	KNN
Sensitivity	0.9314	0.8442	0.7412	0.7845	0.7624
Specificity	0.9561	0.9315	0.8845	0.8412	0.9142
Accuracy	0.9947	0.8965	0.8874	0.8432	0.8398
Precision	0.9412	0.8417	0.8254	0.8347	0.7648
Recall	0.9412	0.8417	0.8254	0.8347	0.7648
F-measure	0.9412	0.8417	0.8254	0.8347	0.7648
NPV	0.9847	0.9321	0.9047	0.9075	0.9254
FPR	0.0072	0.0587	0.0784	0.0984	0.0871
FNR	0.0689	0.5245	0.7478	0.8471	0.8124
MCC	0.9343	0.6471	0.4728	0.5471	0.6547
FRR	0.0547	0.6417	0.874	0.8325	0.7841

Table II could be utilized for contrasting the results of the LFKH-ANFIS and the existing classifiers. The LFKH-ANFIS acquires 0.9412 for precision, f-measure, and recall, whereas, the existing ANFIS, DNN, ANN, and KNN proffered the values of 0.8417, 0.8254, 0.8347, and 0.7648 for precision, recall, f-measure. On considering the sensitivity, specificity, accuracy, NPV, and MCC, the LFKH-ANFIS evinces superior performance. Likewise, for MCC and NPV, the LFKH-ANFIS proffers the greatest outcomes analogized to existing algorithms. From these results, the proposed LFKH-ANFIS is confirmed to be better when analogized to other existing algorithms for eye disease identification. The error rate measures of the classification algorithm, namely FPR, FRR, and FNR, define the error that transpires at the time of performing classification.

For an effectual and excellent classification algorithm, the error rate measures must be low and that is achieved only by the proposed LFKH-ANFIS algorithm.

## V. CONCLUSION

When analogized to the existing PUDI, ProDige, and SVM-C4.5, the proposed NB-ANN acquires the higher most values of precision, f-measure, and recall. Likewise, the LFKH-ANFIS shows the topmost performance by acquiring the highest results of sensitivity, precision, specificity, recall, accuracy, f-measure, NPV, and MCC when analogized to ANN, KNN, DNN, and ANFIS. And, the proposed LFKH-ANFIS acquires the lowest error rates (FNR, FPR, and FRR) for eye disease identification, which evinces the proposed method's efficiency. Therefore, the disease gene identification and the possibility of eye disease incurred by those disease genes are identified more accurately using both classification algorithms. For future work, more number of physicochemical properties of amino acids will be considered for better performance in classification. For future work, more number of physicochemical properties of amino acids will be regarded for better performance in classification.

## REFERENCES

[1] Syedda Farah, Sushma M. S, Asha T, Cauvery B, and Shivanand K. S., "DNA Based Disease Prediction Using Pathway Analysis", In IEEE 7th

International Advance Computing Conference (IACC), IEEE, pp. 629-634, 2017, 10.1109/IACC.2017.0133.

- [2] Ping Luo, Li-Ping Tian, Jishou Ruan, and Fang-Xiang Wu, "Disease gene prediction by integrating ppi networks, clinical rna-seq data and omim data", IEEE/ACM Transactions on Computational Biology and Bioinformatics, vol. 16, no. 1, pp. 222-232, 2017.
- [3] Kuo Yang, Ruyu Wang, Guangming Liu, Zixin Shu, Ning Wang, Runshun Zhang, Jian Yu, Jianxin Chen, Xiaodong Li, and Xuezhong Zhou, "HerGePred: heterogeneous network embedding representation for disease gene prediction", IEEE journal of biomedical and health informatics, vol. 23, no. 4, pp. 1805-1815, 2018.
- [4] Xiwei Tang, Xiaohua Hu, Xuejun Yang, and Yuan Sun, "A algorithm for identifying disease genes by incorporating the subcellular localization information into the protein-interaction networks", In IEEE International Conference on Bioinformatics and Biomedicine (BIBM), IEEE, pp. 308-311, 2016, 10.1109/BIBM.2016.7822537.
- [5] Lvxing Zhu, Zhaolin Hong, and Haoran Zheng, "Predicting gene-disease associations via graph embedding and graph convolutional networks", In IEEE International Conference on Bioinformatics and Biomedicine (BIBM), IEEE, pp. 382-389, 2019, 10.1109/BIBM47256.2019.8983350.
- [6] Jie Yuan, Xingpeng Jiang, Tingting He, Yan Wang, and Xiyue Guo, "Predicting disease genes based on normalized protein modules and phenotype ontology", In IEEE International Conference on Bioinformatics and Biomedicine (BIBM), IEEE, pp. 1177- 1183, 2015, 10.1109/BIBM.2015.7359849.
- [7] TengJiao 7, Wang, Wei Liu HaiLin, Tang Wei Zhang, ChangMing Xu, HanChang Sun, Hui Liu, and HongWei Xie, "Predicting potential disease-related genes using the network topological features", In Proceedings International Conference on Human Health and Biomedical Engineering, IEEE, pp. 871-876, 2011, 10.1109/HHBE.2011.6028961.
- [8] Xiaochan Wang, Yuchong Gong, Jing Yi, and Wen Zhang, "Predicting gene-disease associations from the heterogeneous network using graph embedding", In IEEE International Conference on Bioinformatics and Biomedicine (BIBM), IEEE, pp. 504-511, 2019, 10.1109/BIBM47256.2019.8983134.
- [9] Jiang X, Zhang H, Duan F, and Quan X, "Identify Huntington's disease associated genes based on restricted Boltzmann machine with RNA-seq data," BMC Bioinf, vol. 18, no. 1, pp. 439-447, 2017.
- [10] Ngiam J, Khosla A, Kim M, Nam J, and Ng A. Y, "Multimodal deep learning," in Proc. 28th Int. Conf. Mach. Learn. (ICML), Bellevue, WA, USA, pp. 1-8, 2011.
- [11] Dibendu Bikash Seal, Vivek Das, Saptarsi Goswami, and Rajat K. De, "Estimating gene expression from DNA methylation and copy number variation: A deep learning regression model for multi-omics integration", Genomics, 2020, 10.1016/j.ygeno.2020.03.021.
- [12] Konstantina Kourou, Costas Papaloukas, and Dimitrios I. Fotiadis, "Identification of differentially expressed genes through a meta-analysis approach for oral cancer classification", In 39th Annual International Conference of the IEEE Engineering in Medicine and Biology Society (EMBC), IEEE, pp. 3876-3879, 2017, 10.1109/EMBC.2017.8037703.
- [13] Shin-Jye Lee, Ching-Hsun Tseng, GT-R. Lin, Yun Yang, Po Yang, Khan Muhammad, and Hari Mohan Pandey, "A dimension-reduction based multilayer perception method for supporting the medical decision making", Pattern Recognition Letters, vol. 131, pp. 15- 22, 2020.
- [14] Han Zhang, Xueting Huo, Xia Guo, Xin Su, Xiongwen Quan, and Chen Jin, "A disease-related gene mining method based on weakly supervised learning model", BMC bioinformatics, vol. 20, no. 16, pp. 1-11, 2019.
- [15] Xue Jiang, Jingjing Zhao, Wei Qian, Weichen Song, and Guan Ning Lin, "A Generative Adversarial Network Model for Disease Gene Prediction With RNA-seq Data", IEEE Access, vol. 8, pp. 37352-37360, 2020.
- [16] BoLin Chen, Min Li, JianXin Wang, and Fang-Xiang Wu, "Disease gene identification by using graph kernels and Markov random fields", Science China Life Sciences, vol. 57, no. 11, pp. 1054-1063, 2014.
- [17] Abdulaziz Yousef and Nasrollah Moghadam Charkari, "A novel method based on physicochemical properties of amino acids and one class classification algorithm for disease gene identification", Journal of Biomedical Informatics, vol. 56, pp. 300-306, 2015.

- [18] Zhen Tian, Maozu Guo, Chunyu Wang, LinLin Xing, Lei Wang, and Yin Zhang, "Constructing an integrated gene similarity network for the identification of disease genes", *Journal of biomedical semantics*, vol. 8, no. 1, pp. 32, 2017.
- [19] Mehdi Joodaki, Nasser Ghadiri, Zeinab Maleki and Maryam Lotfi Shahreza, "A scalable random walk with restart on heterogeneous networks with Apache Spark for ranking disease-causing genes using type-2 fuzzy data fusion", *Biorxiv*, pp. 1-20, 2019.
- [20] Pradipta Maji, and Ekta Shah, "Significance and functional similarity for identification of disease genes", *IEEE/ACM transactions on computational biology and bioinformatics*, vol. 14, no. 6, pp. 1419-1433, 2016.

# Load Balanced and Energy Aware Cloud Resource Scheduling Design for Executing Data-intensive Application in SDVC

Ms. Shalini. S<sup>1</sup>, Dr. Annapurna P Patil<sup>2</sup>

Department of Computer Science and Engineering, ACM Engineering College, Bangalore, India<sup>1</sup>  
Department of Computer Science and Engineering, Ramaiah Institute of Technology, Bangalore, India<sup>2</sup>

**Abstract**—Cloud computational platform provisions numerous cloud-based Vehicular Adhoc Network (VANET) applications. For providing better bandwidth and connectivity in dynamic manner, Software Defined VANET (SDVN) is developed. Using SDVN, new VANET framework are modeled; for example, Software Defined Vehicular Cloud (SDVC). In SDVC, the vehicle enables virtualization technology through SDVN and provides complex data-intensive workload execution in scalable and efficient manner. Vehicular Edge Computing (VEC) addresses various challenges of fifth generation (5G) workload applications performance and deadline requirement. VEC aid in reducing response time, delay with high reliability for workload execution. Here the workload tasks are executed to nearby edge devices connected to Road Side Unit (RSU) with limited computing capability. If the resources are not available in RSU, then the task execution is offloaded through SDN toward heterogeneous cloud server. Existing workload scheduling in cloud environment are designed considering minimizing cost and delay; however, very limited work has been done considering energy minimization for workload execution. This paper presents a Load Balanced and Energy Aware Cloud Resource Scheduling (LBEACRS) design for heterogeneous cloud framework. Experiment outcome shows the LBEACRS achieves better makespan and energy efficiency performance when compared with standard cloud resource scheduling design.

**Keywords**—Cloud computing; data-intensive applications; heterogeneous server; IEEE 802.11p; software defined network; software defined vehicular cloud; vehicular adhoc network; workload scheduling; road side unit; vehicular edge cloud

## I. INTRODUCTION

As of late, its seen that the amount of Internet associated gadgets are more when compared with the quantity of people in the world, Internet-associated gadgets are expected to exceed thirty billion by 2020, as per report suggested in [1], thus, accidentally apprehending the IoT models. As there is an enormous increase in the vehicles which are connected to the internet, the normal VANETs are merged into these Internet of Vehicles (IoV). In the Internet of Vehicles period, smart devices and sensors are connected to the vehicles which can give smart vehicle maneuvering, video streaming, prevention of accidents, traffic management, navigating capabilities, just as a large group of arising intelligent applications, a particularly augmented and virtual reality. A vast majority of these applications require complicated computation and various methods to recognize the patterns, which can compute

intensive data and thus need a processor which can provide a powerful and dedicated virtual machine for the computation. The restricted capability for the computation and the because of less resource's capacity in the vehicles, it is a challenging task for the decision-making, networking and data processing in real-time. Due to this problem, it develops an issue for computing the data and allocating the resources to the different applications in the VANETs which have limited resources.

To resolve the problems of unstable computation in the vehicles, the usage of the vehicle nodes is suggested. For the improvement of the safety and comfort for the travelers in a cloud-based vehicle network a method using the Road Side Units (RSUs) can be used. In the RSU, using the computing methods and an integrated communication technology, various offload task can be done using the cloud, hence this reduces the power consumption and the storage capacity in the Onboard Unit which is present in the vehicles. This method is called as Mobile Cloud-Computing (MCC), which provides an improved utilization of the resource, better performance for computation and also gives many benefits, yet not restricted to, 1) increasing the lifetime performance of the battery by offloading the consumption of energy to the cloud, 2) empowering complex memory exploiting gadgets to portable clients, and 3) giving more memory-storage to the clients. Nonetheless, thinking about the limit constraint and fluctuation in the delay for transmitting the data to backbone and backhaul systems [2], placing the cloud network far from the vehicular network can reduce the efficiency of the offload. All the things considered, the vehicle edge computing (VEC) has been given which places the cloud networks near the edge of the radio access organization, to be specific, near the Road Side Units, which gives the computation results within the range of communication with the help of SDN.

The concentrated idea of Vehicular Edge Computing presents critical difficulties particularly in a profoundly unique condition like VANET. Besides, in vehicles having high mobility [3], [4], particularly in roads encountering more traffic, requires an appropriate scheduling to prepare the offloaded complicated workload assignments which can oblige the tasks which are delay tolerant (for example safety related application, accident prevention) just as computationally thorough assignments (for example video observation and dynamic image/video-based applications). The intercommunication requests for quality of experience (QoE) and quality of services (QoS) to understand the related

advantages like maximized throughput, low latency, fast communication, high reliability and hence forth These prerequisites makes workload resource scheduling more testing in vehicular cloud environment [5].

In addressing above discussed research problem and challenges existing workload scheduling methods either focused on minimizing energy or makespan individually; and very limited work have been emphasized in building scheduling optimization considering both together. However, existing model failed balance load for scheduling of newly arrived task. As a result, induce scheduling delay and increases operation cost because of higher SLA violation. In addressing performance issues the future design must incorporate effective load balancing technique with energy-makespan tradeoff requirement as a major objective. This motivates the research work to develop an improved scheduling designing incorporating effective load-balancing technique namely load balanced energy aware cloud resource scheduling. The LBEACRS design present an efficient design to schedule backlog task with high resource utilization. Further, for selecting cloud resource to execute workload a tradeoffs metric of energy maximization with high resource utilization meeting task deadline is presented.

The manuscript significance is described below:

- This paper presents a load balanced and energy aware cloud resource scheduling method for executing data-intensive workload on software defined vehicular cloud (SDVC).
- The SDN is used to offload workload execution to cloud environment. It also maintains routing table for delivering the workload execution outcome to respective vehicle users.
- The LBEACRS model is designed in such a way that it can balance load among different server, maximize resource utilization and reduce energy consumption by running less number of server and also guarantee dead requirement of workload with high makespan efficiency.
- The LBEACRS reduce energy consumption and achieve better makespan performance in comparison with existing DCOH workload scheduling methodology.

The manuscript is articulated as follow. In Section II, survey of existing model and limitation is described. In Section III the present propose methodology for workload scheduling in SDN enabled VANET-Cloud environment. In Section IV, experiment analysis is presented. Finally, the research work of LBEACRS is concluded with future research direction.

## II. LITERATURE SURVEY

This section carry out critical review of various workload scheduling technique in reducing cost, makespan with deadline constraint; however, very limited work has been done to minimize energy constraint for workload execution in heterogeneous cloud environment [6]. In [6] presented energy

aware scheduling strategy for executing workload and showed heterogeneous computing platform provide multiple processing core for executing large-scale workload. However, these strategies induce high computation overhead and induce energy overhead considering different levels of computational process and storage operations [7]. In [8], analysis on a super personal computer has been performed which has 16 thousand nodes utilizes more energy. The consumption of energy is a critical problem which has a huge impact in the computation of the data and for the improvement of the system. In a heterogeneous cloud computing (HCC) condition, Directed Acyclic Graph (DAG) is used by an application which is running parallelly to allocate the jobs according to the priority. Moreover, the Directed Acyclic graph represents the edges and jobs which portrays the messages correspondingly to the different jobs [9]. In [10], it showed the critical difficulties exist for responsibility planning in a hybrid cloud environment. These are distinctive Cloud Service Providers (CSP), heterogeneous workload, which tell how to send and port the administration in the cloud environment having negligible financial spending plan. For guaranteeing prevalent asset usage they introduced a heterogeneous workload planning for the remote cloud environment. Additionally, to guarantee the execution of the workload, the execution is finished inside less time limitation a workload planning component is introduced utilizing the Backhaul Propagation Neural-Network in the hybrid cloud framework. In [11], recommended that the work process scheduling configuration considers the financial spending plan and time required for the computation in a hybrid cloud environment. The first scheduling-algorithm is planned utilizing the single-objective which works specifically for the DCOH technique. This technique is planned to decrease the monetary spending plan of workload scheduling with cut-off time essential. After this, they have introduced multi-objective on the basis of workload scheduled strategy to the specific MOH technique. This technique is intended to bring the trade-offs among the financial spending plan and execution time for workload execution. Notwithstanding, this technique is not much productive to reduce the energy for the logical work process computation in heterogenous cloud network. In Cloud network, which provides service to the market, the clients aid the cloud administrations given by CSP to perform the execution of the workload. Workload for the most part includes certain cut-off time essential for guarantying QoS. Simultaneously, the poor performance of QoS can force exacting a penalty on the CSP. Notwithstanding, the existing algorithm for workload scheduling accepts the time for the makespan of the tasks in the data concentrated workload application are fixed. In any case, this theory is for the cloud servers which have efficiently begun to help in the optimization of the energy, which is not utilized in the workload-scheduling model [11], [12].

From extensive study it can be seen existing cloud resource management technique either focused on reducing energy or makespan. Very few model presented to optimize time and cost together employing multi-objective optimization. Further, these model fails to meet dynamic load requirement of workload application; thus, limit the adoption dynamic workload application real-time requirement; in addressing an effective

load balancing mechanism is needed which is presented in next section.

### III. LOAD BALANCED AND ENERGY AWARE CLOUD RESOURCE SCHEDULING DESIGN FOR TASK EXECUTION IN SDN ENABLED VANET-CLOUD PLATFORM

This section presents load balanced energy aware cloud resource scheduling design for SDN enabled VANET-Cloud. First, we describe the system model for SDN enabled VANET-Cloud. Second, presents load balanced and energy aware cloud resource Scheduling workload execution in SDN enabled VANET-Cloud. The software architecture of the defined VANET-Cloud is shown in Fig. 1.

#### A. System Model of SDN enabled VANET-Cloud

This section present system model used for task scheduling in SDN enabled VANET-Cloud. Here the vehicle moves at varying speed in particular direction and execute different kind of data intensive and scientific applications. Here the vehicles are connected to RSU which are placed in fixed position. These RSU are connected to SDN controllers through which task execution process is outsourced to cloud computing environment. The work aimed at minimizing task execution time with minimal energy consumption aiding better resource utilization through better load balancing strategy. The cloud environment used in this work is heterogeneous in nature which has different energy consumption and processing capability for executing different task.

#### B. Load Balanced and Energy Aware Cloud Resource Scheduling Design for Workload Execution in SDN enabled VANET-Cloud

This section present load balanced energy aware cloud resource scheduling (LBEACRS) method for workload execution in SDN enabled VNET-Cloud environment. Here the workload task submitted by vehicle is submitted to near-by RSU. The RSU execute the workload if it has resource available or it is offloaded to heterogeneous cloud server connected through SDN controller. The LBEACRS method is designed in a way that can optimally distribute the task with minimal consumption of energy and meeting task deadline constraint without overloading the particular server. As this work considers dispatching task to multi-server environment here a task backlog scheduling model is presented. A backlog scheduling model for a set of  $o$  multi-server platform  $T_1, T_2, \dots, T_o$  with size  $n_1, n_2, \dots, n_o$  and its processing speed is  $t_1, t_2, \dots, t_o$  is modelled in this work. Let consider that heterogeneous multi-server platform  $T_j$  is composed of  $n_j$  similar servers with processing capability  $t_j$ .

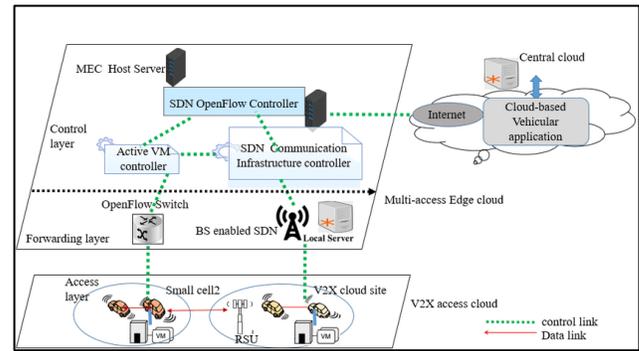


Fig. 1. Architecture of Software Defined VANET-Cloud.

Let consider a Poisson process with  $M/M/m$  backlog scheduling model considering sequence of tasks with incoming load  $\alpha$ . The incoming load is identical and independent in nature which distributed exponentially randomly ( $s$ ) with average ( $\bar{s}$ )  $1/\alpha$ . The LBEACRS method divide these task sequence into  $o$  sub-sequences, in such way that the  $j^{th}$  sub-sequences with incoming load  $\alpha_j$  is transmitted to multi-server platform  $T_j$ , where  $1 \leq j \leq o$ ,  $\alpha = \alpha_1 + \alpha_2 + \dots + \alpha_o$ . A multi-server platform  $T_j$  keeps a buffer with unbounded capability for waiting task when entire server  $n_j$  is busy. Here the tasks are executed in first come first basis considering multi-server platform with task execution are identical and independent with exponential random parameter  $s$  and average  $\bar{s}$ . The  $n_j$  servers of multi-server platform  $T_j$  possess identical execution processing capability  $t_j$ ; thus, task processing makespan on respective sever of multi-server platform is identical and independent with exponential randomness as follows.

$$\gamma_j = \frac{s}{t_j} \quad (1)$$

with average

$$\bar{\gamma}_j = \frac{\bar{s}}{t_j} \quad (2)$$

The average amount of task that can be completed by respective server within  $T_j$  (i.e., average workload execution rate) is obtained using following equation.

$$\beta_j = \frac{1}{\bar{\gamma}_j} \quad (3)$$

The server utilization (i.e., the mean percentage of time a server will be busy) is obtained using following equation.

$$\gamma_j = \frac{\alpha_j}{n_j \beta_j} = \frac{\alpha_j \bar{\gamma}_j}{n_j} = \frac{\alpha_j \bar{s}}{n_j t_j} \quad (4)$$

Let  $p_{j,l}$  represent the probability that  $l$  task will be processed or in waiting in backlogging system considering multi-server platform  $T_j$  and is obtained using following equation.

$$p_{j,l} = \begin{cases} p_{j,0} \frac{(n_j \gamma_j)^l}{l!}, & l < n_j; \\ p_{j,0} \frac{n_j^j \gamma_j^l}{l!}, & l \geq n_j; \end{cases} \quad (5)$$

where

$$p_{j,0} = \left( \sum_{l=0}^{n_j-1} \frac{(n_j \gamma_j)^l}{l!} + \frac{(n_j \gamma_j)^{n_j}}{n_j!} \cdot \frac{1}{1-\gamma_j} \right)^{-1} \quad (6)$$

The probability of freshly arrived workload task that must be waited i.e. (backlogged) in multi-server platform  $T_j$  when entire server in  $T_j$  is busy is computed using following equation.

$$P_{r,j} = \frac{q_j n_j}{1-\gamma_j} = p_{j,0} \frac{n_j}{n_j!} \cdot \frac{\gamma_j^{n_j}}{1-\gamma_j} \quad (7)$$

The mean amount of workload task that are being in execution processes or waiting within multi-server platform  $T_j$  is computed using following equation.

$$\bar{O}_j = \sum_{l=0}^{\infty} l p_{j,l} = n_j \gamma_j + \frac{\gamma_j}{1-\gamma_j} P_{r,j}. \quad (8)$$

Similarly, the mean workload task response makespan of multi-server platform  $T_j$  is computed using following equation.

$$U_j = \frac{\bar{O}_j}{\alpha_j} = \bar{y}_j + \frac{P_{r,j}}{n_j(1-\gamma_j)} \bar{y}_j = \bar{y}_j \left( 1 + \frac{P_{r,j}}{n_j(1-\gamma_j)} \right) \quad (9)$$

For simplicity the mean workload task response makespan of multi-server platform  $T_j$  is computed using following equation.

$$U_j = \frac{\bar{s}}{t_j} \left( 1 + p_{j,0} \frac{n_j^{j-1}}{n_j!} \cdot \frac{\gamma_j^{n_j}}{(1-\gamma_j)^2} \right) \quad (10)$$

The energy consumed for executing task is obtained using following equation.

$$Q = aC\mathcal{V}^2\mathcal{F} = \delta t^\mu$$

where  $a$  defines the task activity features,  $\mathcal{V}$  defines voltage,  $C$  represent load capacitance, and  $\mathcal{F}$  defines clock frequency,  $t$  defines processor execution speed. The parameter  $\delta$  is computed using following equation.

$$\delta = \frac{a\ell^2c}{c^2\rho+1} \quad (11)$$

where  $\ell$  and  $\rho$  are some constant greater than 0. The parameter  $\mu$  is computed using following equation.

$$\mu = 2\rho + 1. \quad (12)$$

This work consider heterogeneous multi-server platform; thus, the value of  $\delta$  and  $\mu$  is different for different server. Here we consider two different energy mode such as idle and active mode. In idle mode, the machine do not execute any workload task and energy consumed is obtained using following equation.

$$Q_j = n_j (\gamma_j \delta_j t_j^{\mu_j} + Q_j^*) = \alpha_j \bar{t} \delta_j t_j^{\mu_j-1} + n_j Q_j^*. \quad (13)$$

Similarly, in active mode the server is running and waiting for incoming workload task and energy consumed is obtained using following equation.

$$Q_j = n_j (\delta_j t_j^{\mu_j} + Q_j^*) \quad (14)$$

This work aimed at allocating ideal resource with minimal execution time for executing workload task under multi-server platform with varying processing speed and power consumption. Let consider a  $o$  number of multi-server cloud platform with size of  $n_1, n_2, \dots, n_o$ , with varying power consumption and processing capability for executing workload with requirement  $\bar{s}$  with task arrival rate  $\alpha$ , and establish load distribution  $\alpha_1, \alpha_2, \dots, \alpha_o$  in achieving high performance efficiency is obtained by minimizing following equation.

$$\min U(\alpha_1, \alpha_2, \dots, \alpha_o) \quad (15)$$

The above equation is subject to following constraint

$$G(\alpha_1, \alpha_2, \dots, \alpha_o) = \alpha, \quad (16)$$

where

$$G(\alpha_1, \alpha_2, \dots, \alpha_o) = \alpha_1 + \alpha_2 + \dots + \alpha_o, \quad (17)$$

and  $\gamma_j < 1, \forall 1 \leq j \leq o$ . Here the workload task are scheduled by minimizing Eq. (15) and meeting constraint defined in Eq. (16) and (17) in order to achieves high resource utilization and performance efficiency with minimal energy dissipation.

#### IV. SIMULATION ANALYSIS AND RESULTS

Here experiment is conducted for evaluating LBEACRS algorithm methodology over standard cloud resource scheduling algorithm [11], [12]. Energy efficiency and makespan are performance metrics used for validating performance. For carrying out experiment SIMITS simulator [13] is used. Further, for incorporating software defined vehicular cloud architecture CloudSimSDN [14] which is an extension of CloudSim simulator which is incorporated into SIMITS. Further for providing secure communication among communicating device such as vehicle, RSU, and SDN controller the message in SDN enabled vehicular adhoc network are encrypted using elliptical curve cryptography. Further, this assumes that each device is composed of tamper proof device obtained from trust authority for carrying out authentication and pseudo-identity-based data signing that assures anonymity of data owner and secure communication. For evaluating performance experiment is conducted by considering dynamic radio propagation model where vehicle will move from urban-to-rural-to-highway and vice versa. Experiment is conducted considering two workload such as Montage and CyberShake workload [15]. The Montage and CyberShake workflow have been used for experiment. The Montage workflow requires high I/O resource; however, the CyberShake requires CPU and memory resource. The simulation parameter considers for carrying out experiment are described Table I.

Fig. 2 shows the graphical representation of how the montage workflow is stored. Similarly in Fig. 3 the graphical representation of the CyberShake workflow has been represented.

##### A. Makespan Performance Evaluation

Here makespan performance is evaluated for both proposed LBEACRS and existing DCOH workload scheduling methodology. Two different workloads such as Montage and

CyberShake is considered for evaluation. First experiment is conducted using Montage workload where the job size is varied and makespan induced for executing workload using DCOH and LBEACRS is graphically shown in Fig. 4. The LBEACRS improves makespan performance by 66.955%, 81.48%, 86.14%, and 89.83% over DCOH when job size is 25, 50, 100, and 1000, respectively. An average makespan performance enhancement of 81.1% is achieved using LBEACRS over DCOH for executing Montage workload.

TABLE I. SIMULATION PARAMETERS CONSIDERED

Network Parameter	Value
SDN enabled vehicular Adhoc network Size	50km * 50km
Number of Vehicles	40
Number of RSU	1 per region
Modulation scheme	QAM-64
Mobility of devices	3 cycle per frame
SDN enabled vehicular Adhoc network coding rate	0.75
SDN enabled vehicular Adhoc network bandwidth	27 Mbps
SDN enabled vehicular Adhoc network data channel size	6
SDN enabled vehicular Adhoc network control channel size	1
Number of SDN switches per RSU	1
SDN enabled vehicular Adhoc network time slot size	8 $\mu$ s
Message information size	27 bytes
Radio propagation mobility model	Dynamic environment such as urban, rural, and highway
MAC used	ENCCMA, TECA & ERS
Resource scheduling used	LBEACRS & DCOH
Workload used	Montage & CyberShake

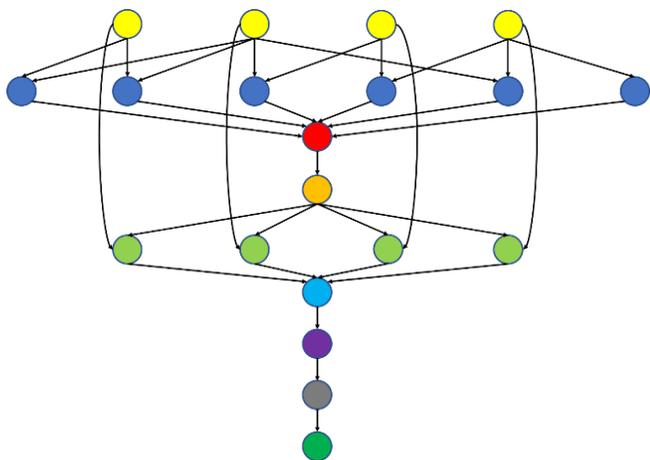


Fig. 2. A Sample Graphical Representation of Montage Workflow.

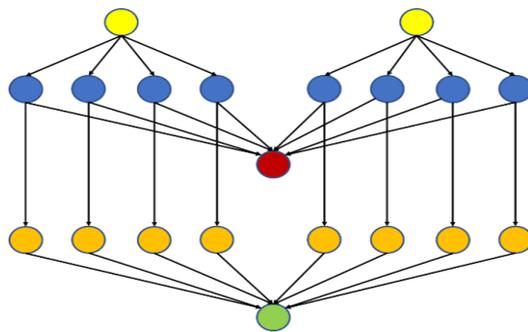


Fig. 3. A Sample Graphical Representation of CyberShake Workflow.

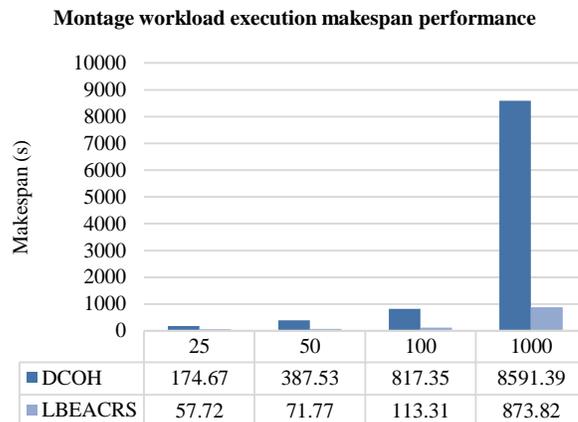


Fig. 4. Makespan Performance for Executing Montage Workload with different Workload Size.

Similarly, experiment is conducted using CyberShake workload where the job size is varied and makespan induced for executing using DCOH and LBEACRS is graphically shown in Fig. 5. The LBEACRS improves makespan performance by 69.95%, 82.14%, 89.23%, and 92.29% over DCOH when job size is 30, 50, 100, and 1000, respectively. An average makespan performance enhancement of 83.4% is achieved using LBEACRS over DCOH for executing CyberShake workload.

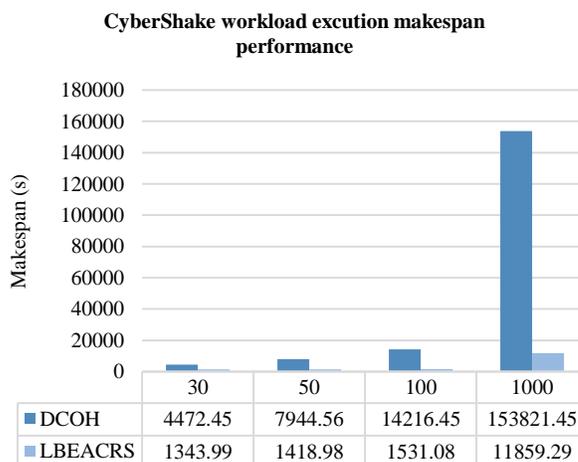


Fig. 5. Makespan Performance for Executing CyberShake Workload with different Workload Size.

**B. Energy Consumption Performance Evaluation**

Here energy performance is evaluated for both proposed LBEACRS and existing DCOH workload scheduling methodology. Two different workloads such as Montage and CyberShake is considered for evaluation. First experiment is conducted using Montage workload where the job size is varied and total energy induced for executing workload using DCOH and LBEACRS is graphically shown in Fig. 6. The LBEACRS improves energy efficiency performance by 74.63, 85.78%, 89.36%, and 92.19% over DCOH when job size is 25, 50, 100, and 1000, respectively. An average total energy consumption reduction of 85.49% is achieved using LBEACRS over DCOH for executing Montage workload. Further, the average energy incurred for executing each sub-task using DCOH and LBEACRS is graphically shown in Fig. 8. The LBEACRS improves average energy induced per task performance by 23.229% over DCOH for executing Montage workload.

Similarly, experiment is conducted using CyberShake workload where the job size is varied and total energy induced for executing workload using DCOH and LBEACRS is graphically shown in Fig. 7. The LBEACRS improves energy efficiency performance by 75.17%, 95.30%, 96.12%, and 93.63% over DCOH when job size is 30, 50, 100, and 1000, respectively. An average total energy consumption reduction of 90.057% is achieved using LBEACRS over DCOH for executing CyberShake workload. Further, the average energy incurred for executing each sub-task using DCOH and LBEACRS is graphically shown in Fig. 9. The LBEACRS improves average energy induced per task performance by 41.35% over DCOH for executing CyberShake workload.

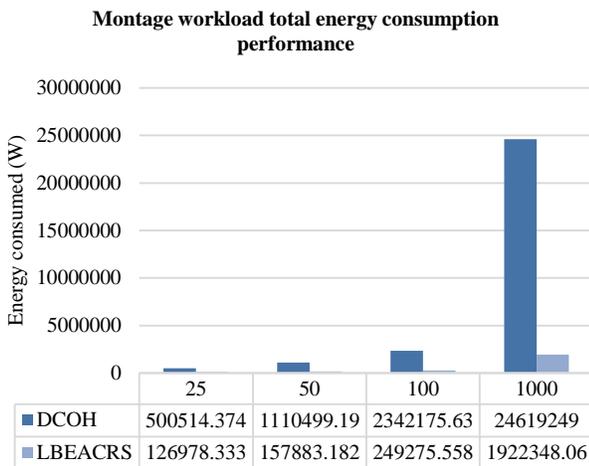


Fig. 6. Energy Consumption for Montage Workload Execution with different Workload Size.

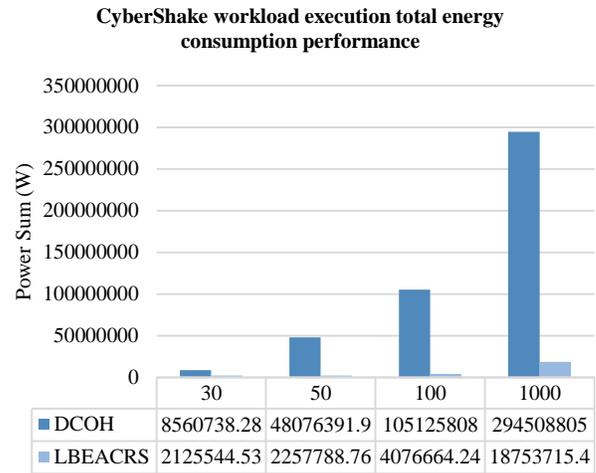


Fig. 7. Energy Consumption for CyberShake Workload Execution with different Workload Size.

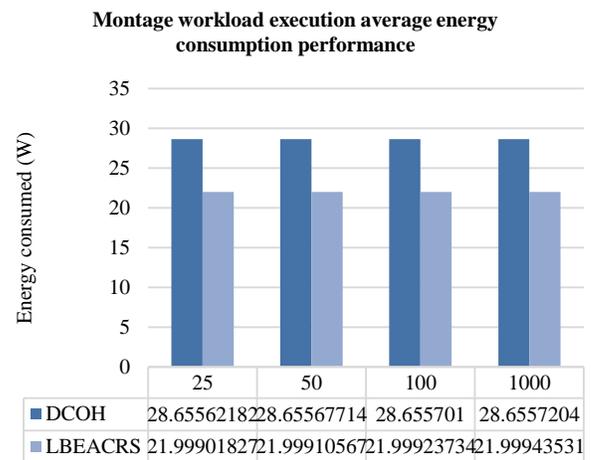


Fig. 8. Average Energy Consumption for Montage Workload Execution with different Workload Size.

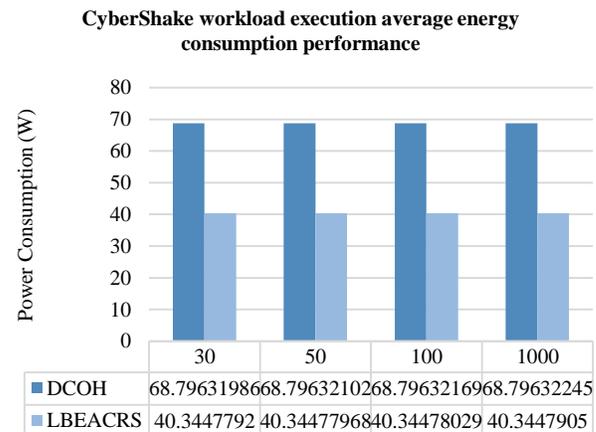


Fig. 9. Average Energy Consumption for CyberShake Workload Execution with different Workload Size.

From overall result attained it can be stated LBEACRS is scalable with respect to varying workload size and works well for both small and larger workload. And also shows they are efficient in provisioning CPU, memory and I/O intensive task.

#### V. CONCLUSION

This work studies the challenges involved in workload scheduling of data-intensive application on SDN enabled VANET-Cloud environment. From study we noted most of existing workload scheduling are done by predominantly considering minimizing makespan and also minimizing cost with deadline constraint. Further, doesn't balance load among processing node. In standard the cost is generally computed based on time spent. However, reducing energy plays major role as different countries has different prices. Thus, here a load balanced energy aware cloud resource scheduling is presented. Here the tasks are scheduled to node that consumes less energy with better resource utilization. Experiments are conducted using two workloads, namely Montage and CyberShake. These workloads are CPU, I/O, and memory intensive in nature. An average makespan performance enhancement of 81.1% and 83.4% is achieved using LBEACRS over DCOH for executing Montage and CyberShake workload, respectively. An average total energy consumption reduction of 85.49% and 90.057% is achieved using LBEACRS over DCOH for executing Montage and CyberShake workload, respectively. The LBEACRS improves average energy induced per task performance by 23.229% and 41.35% over DCOH for executing Montage and CyberShake workload, respectively. From overall result we can state that the LBEACRS is scalable irrespective of workload complexity and is robust with respect to CPU, I/O and memory intensive application.

Future work would consider introducing SLA with quality of experience guarantee in proving resource to VANET users. Further, incorporate effective security mechanism that can reduce key management, storage, and computation overhead.

#### REFERENCES

- [1] K. Chopra, K. Gupta and A. Lambora, "Future Internet: The Internet of Things-A Literature Review," 2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon), 2019, pp. 135-139, doi: 10.1109/COMITCon.2019.8862269.
- [2] N. Abbas, Y. Zhang, A. Taherkordi and T. Skeie, "Mobile Edge Computing: A Survey," in IEEE Internet of Things Journal, vol. 5, no. 1, pp. 450-465, Feb. 2018, doi: 10.1109/JIOT.2017.2750180.
- [3] R. Hussain and S. Zeadally, "Autonomous cars: Research results, issues, and future challenges," IEEE Commun. Surveys Tuts., vol. 21, no. 2, pp. 12751313, 2nd Quart., 2019.
- [4] R. Lu, L. Zhang, J. Ni and Y. Fang, "5G Vehicle-to-Everything Services: Gearing Up for Security and Privacy," in Proceedings of the IEEE, vol. 108, no. 2, pp. 373-389, Feb. 2020, doi: 10.1109/JPROC.2019.2948302.
- [5] I. Din, B.-S. Kim, S. Hassan, M. Guizani, M. Atiquzzaman, and J. Rodrigues, "Information-centric network-based vehicular communications: Overview and research opportunities," Sensors, vol. 18, no. 11, p. 3957, Nov. 2018.
- [6] G. Xie, G. Zeng, R. Li and K. Li, "Energy-Aware Processor Merging Algorithms for Deadline Constrained Parallel Applications in Heterogeneous Cloud Computing," in IEEE Transactions on Sustainable Computing, vol. 2, no. 2, pp. 62-75, 1 April-June 2017.
- [7] Z. Li, J. Ge, H. Hu, W. Song, H. Hu and B. Luo, "Cost and Energy Aware Scheduling Algorithm for Scientific Workflows with Deadline Constraint in Clouds," in IEEE Transactions on Services Computing, vol. 11, no. 4, pp. 713-726, 1 July-Aug. 2018.
- [8] K. Li, "Power and performance management for parallel computations in clouds and data centers," J. Comput. Syst. Sci., vol. 82, no. 2, pp. 174-190, Mar. 2016.
- [9] G. Xie, L. Liu, L. Yang, and R. Li, "Scheduling trade-off of dynamic multiple parallel workflows on heterogeneous distributed computing systems," Concurrency Comput.-Practice Exp., vol. 29, no. 8, pp. 1-18, Jan. 2017.
- [10] Chunlin, L., Jianhang, T. & Youlong, L., "Hybrid Cloud Adaptive Scheduling Strategy for Heterogeneous Workloads", J Grid Computing (2019) 17: 419. <https://doi.org/10.1007/s10723-019-09481-3>.
- [11] Junlong Zhou et al., Cost and makespan-aware workflow scheduling in hybrid clouds. <https://doi.org/10.1016/j.sysarc.2019.08.004>, 2019.
- [12] Neelima, P., Reddy, A.R.M. An efficient load balancing system using adaptive dragonfly algorithm in cloud computing. Cluster Comput 23, 2891-2899, 2020.
- [13] Mario Manzano, Felipe Espinosa; Ning Lu; Xuemin Shen; Mark, J.W.; Fuqiang Liu, "Cognitive Self-Scheduled Mechanism for Access Control in Noisy Vehicular Ad Hoc Networks," Hindawi Publishing Corporation, Mathematical Problems in Engineering, Volume 2015, Article ID 354292, 2015.
- [14] J. Son, A. V. Dastjerdi, R. N. Calheiros, X. Ji, Y. Yoon and R. Buyya, "CloudSimSDN: Modeling and Simulation of Software-Defined Cloud Data Centers," 2015 15th IEEE/ACM International Symposium on Cluster, Cloud and Grid Computing, Shenzhen, 2015, pp. 475-484.
- [15] Z. Zhu, G. Zhang, M. Li and X. Liu, "Evolutionary Multi-Objective Workflow Scheduling in Cloud," in IEEE Transactions on Parallel and Distributed Systems, vol. 27, no. 5, pp. 1344-1357, 1 May 2016.

# Design and Implementation of Collaborative Management System for Effective Learning

Tochukwu A. Ikwunne<sup>1</sup>, Wilfred Adigwe<sup>2</sup>, Christopher C. Nnamene<sup>3</sup>  
Noah Oghenefego Ogwara<sup>4</sup>, Henry A. Okemiri<sup>5</sup>, Chinedu E. Emenike<sup>6</sup>

Department of Computer Science & Informatics, Alex Ekwueme Federal University Ndufu-Alike, Abakaliki, Nigeria<sup>1, 3, 5, 6</sup>  
Department of Computer Science, Delta State University of Science and Technology, Ozoro, Nigeria<sup>2</sup>  
School of Engineering Computer and Mathematical Science, Auckland University of Technology, Auckland, New Zealand<sup>4</sup>

**Abstract**—Recently, the need for online collaborative learning in educational systems has increased greatly because of COVID-19 pandemic. The pandemic has provided an opportunity for introducing online collaboration and learning among instructors and students in Nigeria. Currently, several schools, colleges, universities in Nigeria have discontinued face to face teaching and learning. Many schools resorted to ineffective alternatives such as the use of televisions and radio programmes to carry out distance education (DE). These alternatives have challenges such as lack of monitoring and evaluation of students' learning. Collaborative Learning Management System (CLMS) is a research project that aims to assist instructors in achieving their pedagogical goals, organizing course content, collaborating, monitoring, and supporting students' online learning. It is an interactive, online based as well as android based system that has been designed, implemented, tested. The system demonstrates that it is robust, interactive, and achieves the predefined goals. As a Software Development Approach, it was created using the Rapid Application Development (RAD) Methodology. It also provides a secured and reliable platform for the schools, colleges, and universities to implement an online learning system.

**Keywords**—Collaborative learning; conventional education; effective learning; e-portfolio; interactive board

## I. INTRODUCTION

The COVID-19 pandemic has caused significant disruption to educational activities around the world, particularly in Nigeria. Many countries resorted to online based distance education (DE) for learning continuity. However, many schools in Nigeria are applying the method of use of television and radio-based programmes, to carry out distance education. This method poses a great challenge because it's difficult to monitor and evaluate students learning. A few institutions in Nigeria are now carrying out their academic activities using one form or another of Information Communication Technology (ICT). However, for some institutions in Nigeria, the desire to engage in online learning remains a dream due to inadequate ICT infrastructure. However, the rapid development of ICTs in Nigeria presents an opportunity to consider its use in the promotion of distance education [1]. According to the authors in [2], DE is regarded as a novel method for delivering computer-mediated, well-designed, student-centered, and interactive learning environments to students at any time and from any location by utilizing the internet and digital technologies in conjunction with instructional design guidelines. It benefits students by increasing access to learning

opportunities, at the right time and place, making a wide range of learning resources available, improving opportunities for personalized learning [3, 4], and ushering in more powerful cognitive tools. However, the educational sector in Nigeria continues to rely on conventional teaching methods that are incompatible with students and teachers in an age of ICT development [5].

The authors in [6] stated that the conventional education at this present time has not added educational contents to the new generation students. Conventional education has not keep-pace with modern thought and the educational sectors need, to suit with type of students in the twenty first century [6]. The Collaborative Learning Management System (CLMS) is a collaborative learning platform used to manage and integrate online learning courses between teachers and students for effective delivery of lectures through the internet. At the moment, online learning management systems (CLMS) are commonly used in educational sectors all over the world because they make it simple to create, deliver, and learn course content, as well as track and report on course and student performance [7].

The online learning system is a supplement to the conventional concept of education; the current education system is shifting from the teacher imparting knowledge to the students, to promoting the students' desire to learn. This type of transition can inspire an individual to develop a love of learning, problem solving, and comprehension, as well as a strong long-term memory. In such a learning environment, students can actively learn and acquire skills to solve a variety of problems, as well as assess and value their own works and ideas. The lecturing, listening, and note-taking processes do not entirely disappear in the CLMS, but they are supplemented by other processes based on student discussion and active work with the course material. Collaborative learning teachers see themselves as master creators of intellectual experiences for students rather than expert transmitters of information to students [8].

In view of the above discussion, this work focused on the design and implementation of CLMS to enhance, integrate an effective learning process. In general, components of the system contain interactive management features, quiz and assessment utilities and announcement medium. The assessment utilities allow instructors to systematize basic assessment tasks to the students. Assessments are delivered to

<sup>1</sup><https://blog.capterra.com/what-is-rapid-application-development/>

the students online, and upon conclusion, grades and detailed feedbacks are delivered to the students. The system provides the following solutions: collaborative learning through interactive tools, easy knowledge management, assessments, and quiz. Chats between instructors to students and students to students. Repository of course materials via e-portfolio, Personalize learning management tools, secure and customizable learning system.

The other sections of this paper presents: (1) a literature review on the need to reconsider the design of conventional educational system to include online collaborative learning in educational systems and the importance and features of online collaborative learning management system, (2) identification of problems with the conventional system of education and presented objective of this study, (3) presentation of the system overview and architecture of a new online collaborative management system and the test results and (4) conclusion and recommendations.

## II. LITERATURE REVIEW

The need to reconsider the design of conventional educational system to include online collaborative learning in educational systems has increased greatly because of COVID-19 pandemic. The pandemic has provided an opportunity for introducing online collaboration and learning among instructors most especially in Nigeria. Many schools, colleges, and higher institutions in Nigeria have discontinued face to face teaching and learning and relied on ineffective alternatives such as the use of televisions and radio programmes to carry out distance education (DE) [8]. These alternatives have challenges such as lack of monitoring and evaluation of students' learning. As a result, an online collaborative learning management System (CLMS) is required to assist teachers in achieving their pedagogical goals, organizing course content, collaborating, monitoring, and supporting students' online learning.

The process of standardizing collaborative learning technology is taking the lead in research efforts into online-based education [9]. The author in [10] emphasized the importance of researchers conducting additional research on the role of collaboration in learning in order to develop deeper theoretical frameworks that can better guide the development of technology-supported learning settings.

Some trends have necessitated the use of online-based learning. Platforms for collaborative learning management systems (CLMS) have abundant resources, sharing, and convenience. All these characteristics combine to make it one of the more potent learning tools. CLMS has good functionality for assisting students' learning and encourages positive attitudes in both students and teachers [11]. On-line collaborative learning is heavily reliant on the internet and employs collaborative learning methods. The methods make full use of internet resources, promoting learners' abilities to self-learn, communicate, and direct learners' activities with others, as well as assisting in supporting learners to solve practical problems. Based on what has been discussed thus far, one can reasonably conclude that online collaboration can be

delivered in the form of discussion among the entire group or students or within smaller groups of students, however, [12] emphasized that smaller groups make better learning outputs. The author in [13] posited that collaborative learning can help in demonstrating new knowledge.

Collaborative learning is known by a variety of names. Cooperative learning, collaborative learning, collective learning communities, peer teaching, peer learning, and team learning are some examples. All of these names have one thing in common: they all necessitate collaboration. Furthermore, research suggests that collaboration may provide more opportunities for equality in group work than conventional face-to-face group work [9], because the latter approach frequently bases group "decision-making" on students who are considered "bright" by their teachers in the class. The section that follows discusses the various types of CLMS and their features.

### A. Collaborative Learning Management System (CLMS) and their Features

There are several types of CLMS available on the market [14], including commercial or proprietary, as well as free software or free courses [15]. Among the various types of CLMS types that are implemented in higher institutions are Blackboards (proprietary environment). The best CLMS for a given institution is determined by its characteristics and objectives [15]. According to [16], several researchers investigated the necessary elements for selecting a CLMS. A team from the Federal University of Rio de Janeiro (UFRJ) Technology, Education, and Society Group [17], for example, identified seven major categories of tools in an educational platform in 2004. The categories are interface, navigation, evaluation, didactic resources, communication / interaction, coordination, and administrative support.

There are classes that enable efficient Collaborative Learning Management System (CLMS). They are 1) Interface category which creates communication between users and system. 2) Navigation category that establishes easy flow between Collaborative Learning Management System (CLMS) pages. It includes evaluation forms to determine whether a student has fully grasped the material. 3) The Communication / Interaction category that depicts flow of information between learners in a Collaborative Learning Management System. 4) The Coordination category focuses on the instructors' actions of module planning, creation, execution, and control. 5) The Administrative Support category focuses on both the administration tools and environmental management [17].

In order to analyze student interaction in online-based courses, students' interactions are divided into two main categories which include content interaction and social interaction [18]. The content interaction is focuses on the module content such as the study materials, assignment and any other important information that help the effectiveness of the student study. Social Interaction aids students to learn about their peers and resist the separation and frustration of an individual student that are common problems in Web-based course.

The presence of online CLMS to support continuing of teaching and learning will guide the implementation of education system during this challenging crisis of COVID 19 pandemic.

### III. STATEMENT OF THE PROBLEM

The following challenges are associated with the conventional education system and current alternative methods:

- 1) Learning is restricted to a specific time, this results to an inadequate attention of the student.
- 2) Inability for student in distance locations to participate in learning making it difficult for those that is far from the location to be involved in the learning.
- 3) Limited access to the learning materials to the students making it difficult for student to have access to all the study materials at a particular time.
- 4) Students are required to physically be present in the classroom in order to gain knowledge, sacrificing all other responsibilities.
- 5) Students submit assignment to the lecturer through hard copies.
- 6) The lack pre-existing collaborations for the design and broadcasting of the educational content via television and radio.

### IV. OBJECTIVES OF THE STUDY

The aim of this work is to develop and implement the Collaborative Learning Management System for online distance education with the specific objectives as follows:

- 1) To create an interactive board where student can interact and share idea with each other.
- 2) To integrate an e-portfolio in the system which would serves as the repository storage of learning material needed for the student.
- 3) To develop a web based CLMS application for student effective learning.
- 4) To create user interface is compatible and responsive to any device being used.

### V. SYSTEM OVERVIEW

The design of this collaborative learning management system platform is based on the need to provide a system that would ensure that a student is fully involve in learning activities of the institution irrespective of the geographical location. The system would provide some functionality such as interactive board/chat box which would aid student to lay comment as well allows the student-student and lecturer/teachers interactions. Also, an integration of e-portfolio in the system which would serves as the repository storage of learning material needed for the student. The system graphical user interface would be made to be easily accessible via web browsers and compatible and responsive in any device being used. Rapid Application Development (RAD)<sup>1</sup> Software methodology was adopted in the design of the proposed system. The RAD methodology has the following phases:

- Requirement planning: Also known as a project scoping meeting. Although the planning phase is shorter in this methodology than in others, it is critical to the overall success of the CLMS development. The phase specifies the reporting functions and data subject areas of the CLMS, as well as the system's scope. It is also known as the concept definition stage.
- User Design: This is also referred to as functional design. Once the project has been scoped, development can begin, fleshing out the user design through multiple prototype iterations and user feedback. We worked with users to create a functional prototype of CLMS components.
- Construction: The physical CLMS is completed during the construction phase, the conversion system is built, and a user aid and implementation work plan is developed. This stage, also known as the development stage, is broken down into several smaller steps, including program development, coding, and unit, integration, and system testing.
- Cutover: This stage, also known as the implementation phase, includes final user testing, training data conversion, and application system implementation.

The high-level model of CLMS is shown in Fig. 1. It is broken down into units and subunits so that the CLMS can be easily understood starting from the subunits. Fig. 2 shows the system architecture of the new CLMS. It defines the behaviour and structure of a system.

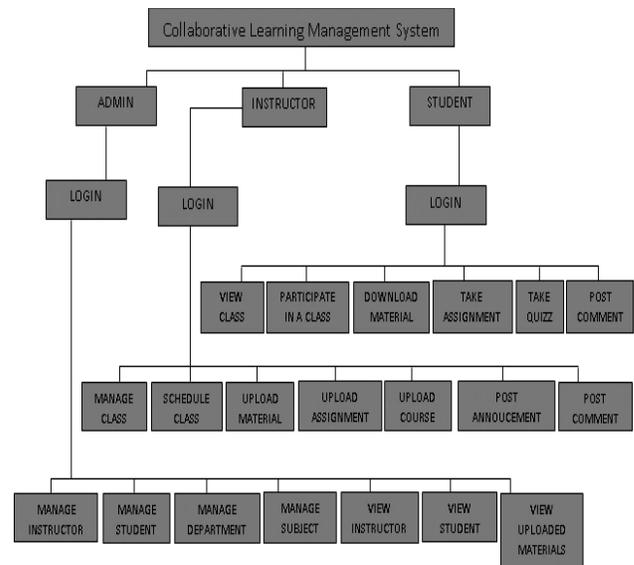


Fig. 1. High-level Model of the New CLMS.

### VI. SYSTEM ARCHITECTURE

The CLMS architecture presents a set of artifacts and their relationships, which guide the system's selection, creation, and implementation. Fig. 2 depicts the new CLMS's system architecture. These sets of artifacts depict the relationships between CLMS components and are represented in Fig. 3 by a use case diagram and Fig. 4 by an entity relationship diagram.

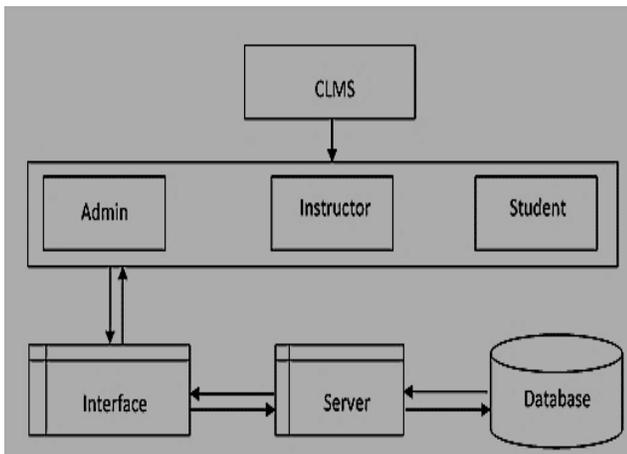


Fig. 2. System Architecture Diagram of the New CLMS.

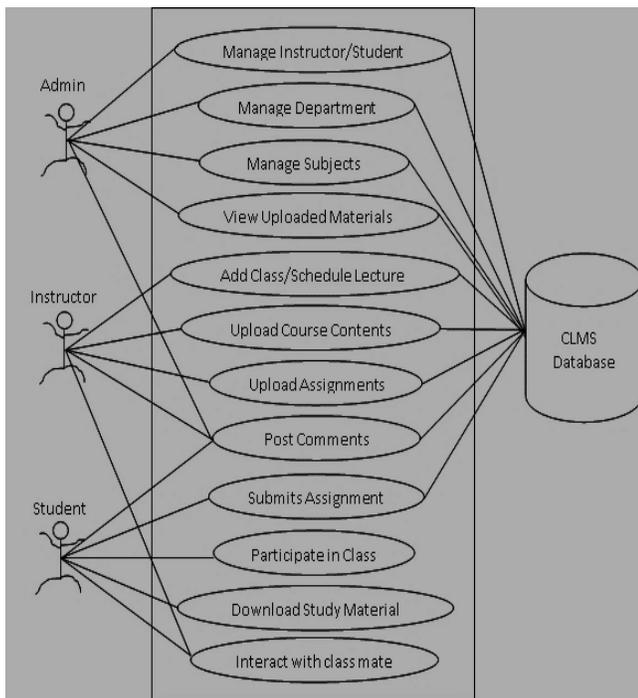


Fig. 3. The use Case Diagram of the System.

- Entity Relationship Diagram (ERD): The Entity Relationship Diagram (shown in Fig. 4) provides a clear picture of the relationships between the various entities associated with the system. It describes how one entity's flow of action is related to other system entities.

#### A. Menu Design

The main menu of this system is design in such a manner that it will enable the users of the system to easily navigate or taken to the submenu to carry out specified tasks. At the menu they are required to provide their login details after which access to other sub modules would be granted to them. There are three main group of users captured in this system. These are the Administrator of the system, the Instructor/teacher, and the Student. The main menu interface will allow either the admin or instructor and student to navigate to the various sections which will enable module to have their own menu that

serves the main functions to enable them to effectively manage the system. The diagram in Fig. 5 shows the main menu for instructors and student log in. Fig. 6 displays the main menu design for Admin.

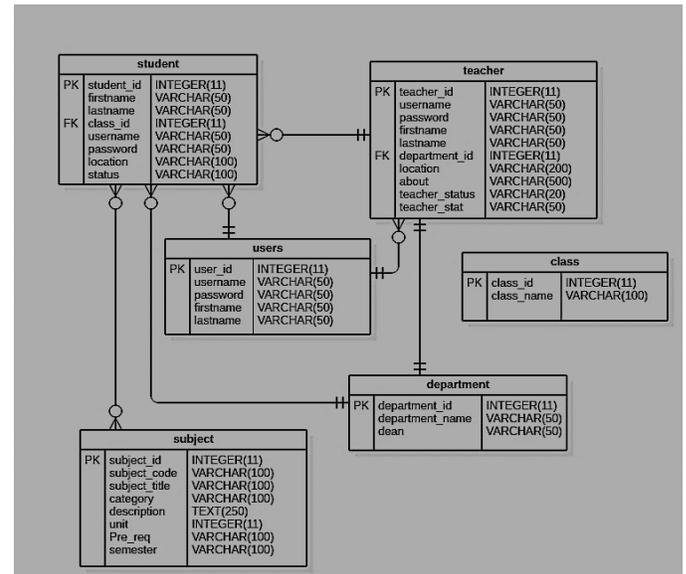


Fig. 4. Entity Relationship Diagram (ERD) of the New System.



Fig. 5. The Instructor/Student Login Page.

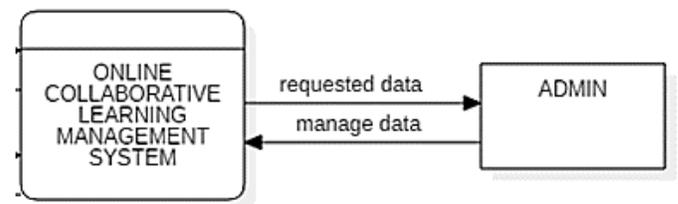


Fig. 6. Main Menu Design for Admin.

1) *Subsystem design*: The entire system consists of subsystems whose purpose is to help to achieve the aim of the system. The subsystems include:

a) *Subsystem design*: The entire system is made up of subsystems whose purpose is to help the system achieve its goal. The subsystems are as follows: a) The Admin Sub System, depicted in Fig. 7, is designed to allow administrators to manage students and instructors.

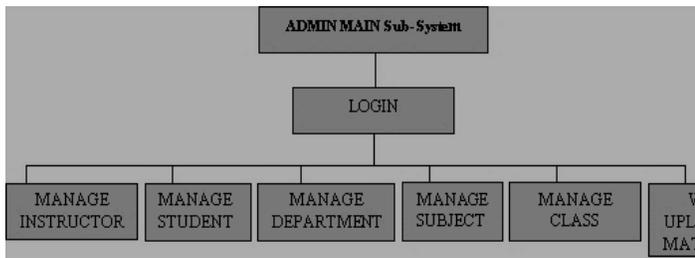


Fig. 7. The Admin Platform.

b) *The Instructors/Teachers Subsystem*, depicted in Fig. 8, is intended for instructors to perform a variety of tasks such as managing classes, scheduling classes, uploading materials, and uploading files.

c) *The Student Subsystem*, depicted in Fig. 9, is intended to allow students to interact with educational content.

2) *Design of program modules*: The new system is made up of several modules that work together to form the entire system. Here are a few examples:

- The admin subsystem consists of manage/view instructor module, manage/view student module, manage subject module, manage department module, view uploaded materials module.
- While the instructor and student subsystem consist of manage class module, schedule class module, upload material module, upload assignment module, upload course module, post comment module and view class module, submit assignment module, download material module, post comment module, respectively.

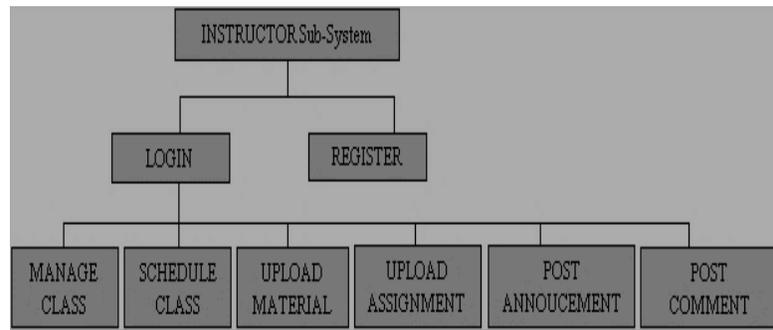


Fig. 8. The Instructor Sub System.

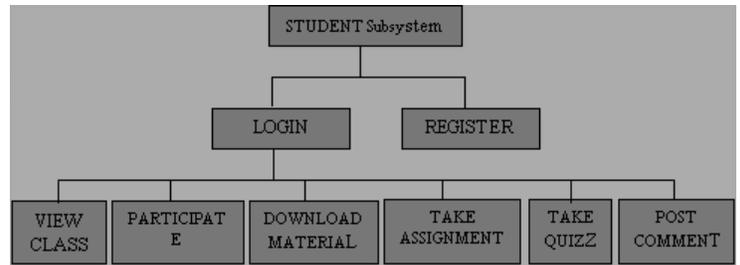


Fig. 9. The Student Platform.

3) *Database development tools and structure*: MYSQL, one of the most powerful powering tools for software that runs on the XAMPP server, was used in the development of this system. It has customizable views, query caching, cross-platform support, triggers, and built-in replication. A relational database management system (RDBMS), specifically MYSQL Server, is used to implement the database design. Tables I and II show some of the tables that were used. Table I depicts the student table, while Table II depicts the administrative table.

TABLE I. THE STUDENT TABLE

#	Name	Type	Collation	Attributes	Null	Default	Extra
1	student_id	Int(11)			NO	None	Auto_Increment
2	firstname	Varchar(50)			NO	None	
3	lastname	Varchar(50)			NO	None	
4	Class_id	Int(11)			NO	None	
5	username	Varchar(50)			NO	None	
6	password	Varchar(50)			NO	None	
7	location	Varchar(100)			NO	None	
8	status	Varchar(100)			NO	None	

TABLE II. THE ADMIN TABLE

#	Name	Type	Collation	Attributes	Null	Default	Extra
1	user_id	Int(11)			NO	None	Auto_Increment
2	username	Varchar(50)			NO	None	
3	password	Varchar(50)			NO	None	
4	firstname	Varchar(50)			NO	None	
5	lastname	Varchar(50)			NO	None	

### B. Admin Menu Implementation

This menu allows the CLMS administrator to manage instructors and students. It was designed to monitor all the activity progress of both students and instructors. Fig. 10 depicted the picture of the admin main menu showing its entire menu at the left side bar navigation. The center content is the information feature that presents activity progress of all activities of the instructor and student perform on their home pages. This Admin managed the instructors, set up the modules and could create/edit/delete users. The administrator has direct access to the database.



Fig. 10. The Admin View Implementation.

### C. Students Menu Implementation

Students complete their profile on the system on first login. Fig. 11 shows the program Flowchart for Student Registration and Verification. Upon login, checks for notification of any task. They can also receive a text message on their phone via web service notifying them of any task. The user can also see his or her group members whenever a group task is given. The user can also respond to any task as appropriate by uploading files, posting answers on the joint collaborators widget and posting links for references in other for group member to read further and communicates to the instructors if need be.

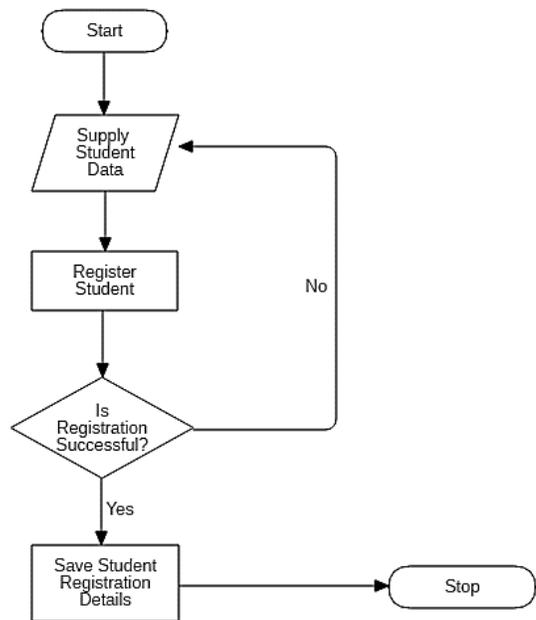


Fig. 11. Program Flowchart for Student Registration and Verification.

### D. Subsystem Implementation

1) *Manage/view instructor and students module:* The manage/view instructor and students' module are one of the modules that made up the admin subsystem. At this module, the admin must have sign in into the system to view this module. This module displays the list of all eligible students and teacher/instructor. Fig. 12 presents the add/view of student sub system module.

2) *Manage/add department module:* This module is made up of the instructor/lecturer subsystem. At this module, the instructor must be signed in before viewing the modules that were created in the department. Fig. 13 displays the add department module design.

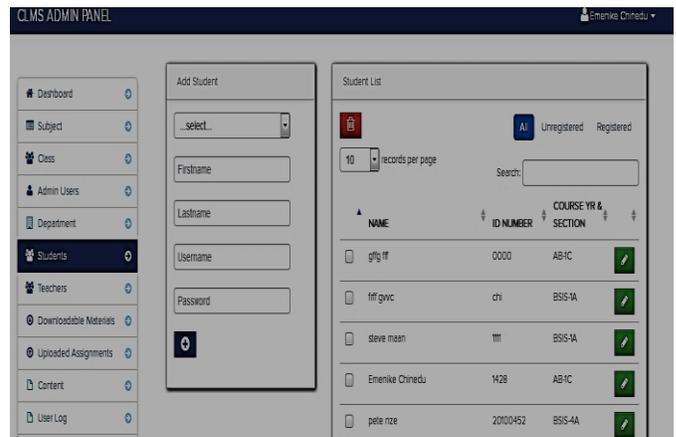


Fig. 12. Add/View of Student Sub System Module.

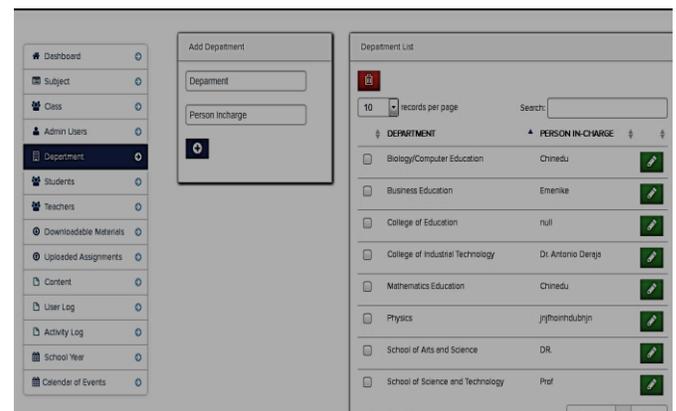


Fig. 13. Add Department Module Design.

3) Algorithm for the module of subsystem implementation:

In this section, we focused on the underground implementation of the scheduled class session in the instructors' and students' dashboards. Algorithms that implement these modules of systems in natural language are shown in Fig. 14 and Fig. 15, respectively.

- Step1: start
- Step2: display instructor dashboard after successful login
- Step3: click on my class
- Step4: click on my class name
- Step5: click on schedule class
- Step6: click on live lecture to start the class
- Step7: if class is over (complete) Go to step2

Fig. 14. The Algorithm for Schedule Class Session in the Dashboard of the Instructor.

- Step1: start
- Step2: display student dashboard after successful login
- Go to Step 3
- Step3: click on my class
- Step4: click on my class name
- Step5: click on participate in class
- Step6: click on join to start the class
- Step7: if class is over (Complete) Go to step2.

Fig. 15. The Algorithm for Class Session of the Students.

VII. TEST RESULTS

These are the outcomes of the feasibility test for the tested system. They demonstrate a fully implemented system when tested with real-time data. The following testing and debugging methods were applied namely, Unit Testing, Integration Testing, and Alpha Testing.

Unit Testing: This test was carried out on every module of the system to verify proper functionality and ascertain if they were error free. Error found were noted down and corrected immediately.

Integration Testing: This test involves testing of how the various modules interact. This was done by combining the system modules to see how they interact and ensuring that their performance does not affect or obstruct the functionality of others.

Alpha Testing: Sample data were used to test the system's functionality to see if it would perform as expected and meet requirements without errors.

Fig. 16 shows a sample output for a message module for instructors' view.

A. System Integration

The system integration depicted in Fig. 17 shows how the various subsystems were combined to form the main system. The following elements were incorporated: a) The Student Subsystem b) The Instructor/Teacher Subsystem c) The Adm Subsystem.

B. Choice of Programming Language

In the development of the CLMS, PHP (PHP: Hypertext Pre-processor) was chosen as the server-side scripting language for the back-end development of the system. MYSQL was used

for the database design. This is the database development language that served as the back end of the software for storing information because of its high maintenance and security. It was used in creating communication and connection between the application and the database. JavaScript was also used along with AJAX to make the web application interactive. It is a high-level interpreted language. JQUERY were also used for carrying out client-side manipulations. Other languages for the client side (front end development) such as HTML (Hyper Text Markup Language) used to lay out the web pages, CSS (Cascading Style Sheets) to describe hoe HTML elements are to be displayed on screen, and BOOTSRAP which consists of HTML CSS JavaScript framework used to make the design responsive on laying out the web pages.

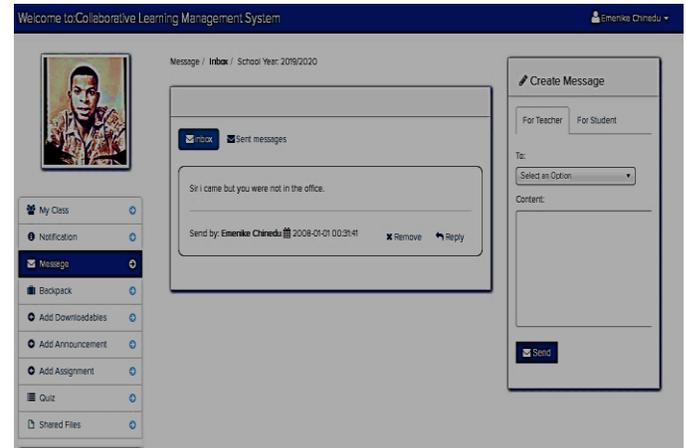


Fig. 16. Message Module Instructor View.

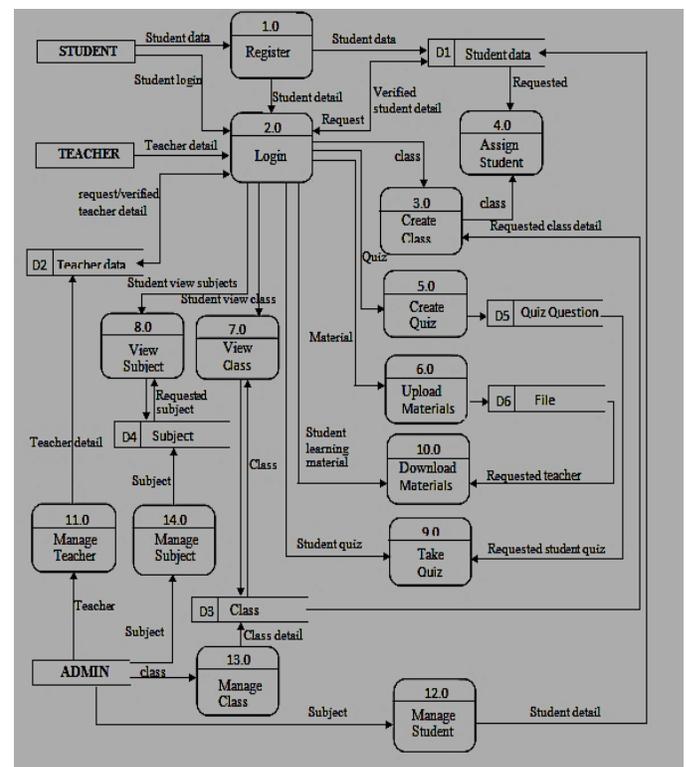


Fig. 17. An Integration of the System Subsystems.

## VIII. CONCLUSION

The challenges of conventional student teaching and learning in educational systems, as well as the abrupt disruption of our education system due to the COVID 19 pandemic, prompted this research. Despite the existence of strategies to compensate for the effects of discontinued face-to-face teaching and learning as a result of the pandemic, such as the use of televisions and radios to compensate for the effects of discontinued face-to-face teaching and learning, such alternatives have not contributed to effective student learning. This paper suggests that these issues can be addressed by implementing a new collaborative management system centered on effective learning and employing an integrated approach. As a result, the following inputs were considered during this study:

1) The system that allows a collaborative learning through interactive tools that entails receiving feedback from instructors easy knowledge management, assessments, and quiz. Providing an interactive chats box between instructors and students and students to students and providing repository of course materials via e-portfolio that students can access.

2) Instructors' module which enable instructors to various tasks to be assigned to students, set deadline for task, track and monitor the progress of each student and generate report for assessment-based students' participations on the collaborative platform of the system.

3) Students Module that allow students to complete their profile on the system on first login, checks for notification of any task. Also, the students receive a text message on their phone via web service notifying them of any task. Update's students whenever a group task is given. Students respond to any task as appropriate by uploading files, posting answers on the joint collaborator's widget, and posting links for references for other group members to read and communicates back to instructor.

The future iteration of this study will involve understanding instructors and students' perceptions about their experience of using CLMS to ascertain whether the CLMS system impacted positively to teaching and learning, and whether the use of CLMS minimize numerous learning problems with the conventional classroom learning environment in Nigeria educational system. This is importance in order to know the impact and efficacy of the CLMS with users in an educational setting.

## REFERENCES

- [1] S. C. Eze, V.C. Chinedu-Eze, C.K. Okike, A.O. Bello. Factors influencing the use of e-learning facilities by students in a private Higher Education Institution (HEI) in a developing economy. *Humanities and Social Sciences Communications*. 2020 Oct 27;7(1):1-5.
- [2] N. Hedge, L. Hayward . Redefining Roles: university e-learning contributing to lifelong learning in a networked world?. *E-Learning and Digital Media*. 2004 Mar;1(1):128-45.
- [3] T. Ikunne, S.O. Kide, K.C. Oketa, N. E. Richard-Nnabu, U. Edward . "Mobile Platform for Study and Collaborative Knowledge Construction in Students Course Learning" *International Journal of Computer and Organization Trends* 11.3 (2021): 20-25. K. Elissa, "Title of paper if known," unpublished.
- [4] Y.D. Usman. Educational Resources: An Integral Component for Effective School Administration in Nigeria. *Online Submission*. 2016;6(13):27-37.
- [5] J. König, D.J. Jäger-Biela, N. Glutsch. Adapting to online teaching during COVID-19 school closure: teacher education and teacher competence effects among early career teachers in Germany. *European Journal of Teacher Education*. 2020 Aug 7;43(4):608-22.
- [6] L. Darling-Hammond, L. Flook , C. Cook-Harvey, B. Barron, D. Osher . Implications for educational practice of the science of learning and development. *Applied Developmental Science*. 2020 Apr 2;24(2):97-140.
- [7] H. Meishar-Tal, G. Kurtz, E. Pieterse. Facebook groups as LMS: A case study. *International Review of Research in Open and Distributed Learning*. 2012;13(4):33-48.
- [8] U.N Eze, M.M Sefotho, C.N Onyishi, C. Eseadi. Impact of COVID-19 pandemic on Education in Nigeria: Implications for Policy and Practice of e-learning. *Library Philosophy and Practice*. 2021:1-36.
- [9] P.D. Sharmila. Networked Collaborative Learning. *SCIENCE AND HUMANITIES*. 2017 Jan:345.
- [10] H. Jeong , C.E. Hmelo-Silver. Seven affordances of computer-supported collaborative learning: How to support collaborative learning? How can technologies help?. *Educational Psychologist*. 2016 Apr 2;51(2):247-65.
- [11] B. Edmunds, M. Hartnett. Using a learning management system to personalise learning for primary school students. *Journal of Open, Flexible and Distance Learning*. 2014 Jan;18(1):11-29.
- [12] Y. Xiong , HK Suen. Assessment approaches in massive open online courses: Possibilities, challenges and future directions. *International Review of Education*. 2018 Apr;64(2):241-63.
- [13] H. Le, J. Janssen, T. Wubbels. Collaborative learning practices: teacher and student perceived obstacles to effective student collaboration. *Cambridge Journal of Education*. 2018 Jan 2;48(1):103-22.
- [14] D. Barreto, A. Rottmann,, & S. Rabidou, (2020). *Learning Management Systems*. EdTech Books. [https://edtechbooks.org/learning\\_management\\_systems](https://edtechbooks.org/learning_management_systems).
- [15] E. Van Laar , A.J. Van Deursen , J.A Van Dijk , J. De Haan . The relation between 21st-century skills and digital skills: A systematic literature review. *Computers in human behavior*. 2017 Jul 1;72:577-88.
- [16] P.C. Oliveira , C.J Cunha , M.K Nakayama . Learning Management Systems (LMS) and e-learning management: an integrative review and research agenda. *JISTEM-Journal of Information Systems and Technology Management*. 2016 May;13:157-80.
- [17] G. Roque, I. Chamovitz, J. Araujo, M. Gouvea, R. Cardoso, S. Azambuja, & S. Moura. Relevant aspects for the development of educational environments for the web. In: *Proceedings of CISCI, 3rd Iberoamerican Conference on Systems, Cybernetics and Informatics*. Miami, United States. 2004.
- [18] S. Mehall . Purposeful Interpersonal Interaction in Online Learning: What Is It and How Is It Measured?. *Online Learning*. 2020 Mar;24(1):182-204.

# Selection of Learning Apps to Promote Critical Thinking in Programming Students using Fuzzy TOPSIS

Kesarie Singh<sup>1</sup>, Nalindren Naicker<sup>2</sup>, Mogiveny Rajkoomar<sup>3</sup>

Department of Information Technology, Durban University of Technology, Durban, South Africa<sup>1</sup>  
Department of Information Systems, Durban University of Technology, Durban, South Africa<sup>2,3</sup>

**Abstract**—The aim of this research was to use intelligent decision support systems to obtain student-centred preferences for learning applications to promote critical thinking in first year programming students. This study focuses on the visual programming environment and critical thinking as the gateway skill for student success in understanding programming. Twenty-five critical thinking criteria were synthesized from the literature. As a quantitative study, 217 randomly selected students from an approximate target population of 500 programming students to rate four learning Apps, namely, Scratch, Alice, Blockly and MIT App Inventor, against critical thinking criteria to establish the App that best promotes critical thinking among first year programming students. There were 175 responses received from the 217 randomly chosen programming students who willingly contributed to the study. Consequently, the distinctiveness of this paper lies in its use of the Fuzzy TOPSIS (Technique for Order Preference by Similarity to Ideal Situation) multi-criteria decision-making algorithm to rank criteria for critical thinking, calculate their weights on the basis of informed opinion and hence scientifically deduce the best rated App among the available alternatives that promote critical thinking among first year programming students. The results showed that Scratch promoted critical thinking skills the best in first year programming students whilst Blockly promoted critical thinking skills the least. As a contribution to the study, policy-makers and academic staff can be potentially supported to make informed decisions about the types of learning Apps to consider for students when confronted with multiple selection criteria.

**Keywords**—Critical thinking; visual programming environment; multi-criteria decision-making; fuzzy TOPSIS

## I. INTRODUCTION

The problem associated with teaching programming to novice learners is exacerbated by the complex and abstract nature of the field and the heavy reliance on 21st century skills such as critical and computational thinking. As a result, a kaleidoscope of research into programming self-efficacy, the complexity of the field, teaching methods and a variety of teaching tools, have emerged over the recent past. Furthermore, learning to program can be perceived as both tedious and difficult to the novice programmer for reasons such as the abstract nature of computational thinking and the burdensome syntax and semantics associated with many programming languages [1-3]. The literature has also repeatedly revealed that visual block-based programming environments have a

positively powerful impact on the performances of novices learning to program [4]. In a case study performed by Pinto-Llorente et al. in [5] on the impact of the visual programming environment (VPE) among primary school learners, it was determined to have promoted their critical thinking skills and problem solving abilities. Various other studies have revealed that visual programming environments support the constructivist approach to learning and contribute to enhancing one's skills of independent learning, creative thinking, problem-solving, reflection and collaboration [6-12]. This has resulted in an upsurge of educational programming environments and tools aimed at stimulating the learners' interest, making programming accessible to people of all interests and ages and minimizing the challenges of understanding programming [13].

The significant growth in diverse learning Apps in the last decade and the varying commercial aspirations these Apps may be designed to serve, have impacted on the need for university academics to make rigorous and well-considered decisions around their choice of learning App. Further, an online learning App becomes especially appropriate post Covid-19, where higher education institutions are strategically searching for alternate teaching methodologies to the traditional teaching approach. Interestingly, a number of learning Apps originated over the years with a variety of different characteristics, each serving a slightly different need [4]. Multi-criteria group decision-making (MCDM) entails weighing each of several alternatives against multiple, conflicting, quantitative decision criteria executed by many decision-makers to derive the optimal alternative [14-16]. The various criteria will be synthesized from an in-depth analysis of the literature in the relevant field.

According to Başaran and Haruna in [17], manually selecting these Apps can be biased, tedious, inconsistent and time-consuming, ultimately resulting in a premature selection. Therefore, to address ambiguity and uncertainty associated with human judgements, this quantitative study will use the Technique for Order Preference by Similarity to an Ideal Solution (TOPSIS), a scientific and mathematical technique in multi-criteria decision-making (MCDM) that preserves integrity and objectivity of process [16, 18]. The TOPSIS method, developed in 1981 by Yoon and Hwang, was grounded on the fundamental principle that the best option from a range of alternatives will be positioned closest to the

positive ideal solution and farthest from the negative ideal solution [19].

In a study conducted by Junior, Osiro and Carpinetti in [39], a comparison of the Fuzzy AHP and Fuzzy TOPSIS methods was undertaken to choose from a number of suppliers. The criteria central to the comparison were: “adequacy to changes of alternatives or criteria; agility in the decision process; computational complexity; adequacy to supporting group decision-making; the number of alternatives and criteria, and modelling of uncertainty”. The study revealed that Fuzzy TOPSIS provided more rigor in the decision process, lower time complexity when there was a large number of decision-makers, offered no restrictions on the number of criteria and alternatives and became the preferred choice when there were changes to alternatives or criteria as rank reversal posed a potential problem with Fuzzy AHP.

Fuzzy set theory, which was introduced by Zadeh in 1965, can be used to manage the uncertainties and subjectivity of the evaluation process [15]. More specifically, this study will implement an expansion of the TOPSIS method to accommodate fuzziness in the decision problem setting. Fuzzy TOPSIS is widely and extensively applied among researchers in diverse fields of economics, business management, engineering, ICT and education, to solve various MCDM problems associated with site selection in mining and engineering, equipment selection, risk analysis for complex infrastructure projects, portfolio selection, selection of e-Learning approaches, supplier selection and software selection [16-23]. The advantages of Fuzzy TOPSIS include its ease of implementation, capacity to compare the strongest and weakest alternatives quantitatively, that it enables linguistic expressions to be represented as fuzzy numbers, and its practicality and ability to handle incomplete or partial quantitative data [24]. A questionnaire disseminated to 217 first year programming students is used as a tool to gather the ratings of alternatives against multiple selection criteria, and the different weightings per criteria are obtained from academic experts in the field. These sets of evaluations use logical interval judgements represented by linguistic terms which can be parameterized by triangular fuzzy numbers [24].

Choosing an optimal learning application (App) is therefore a complex problem requiring an intelligent decision support system that will use multiple decision-makers to simultaneously ruminate multiple criteria such as the prior skills of the learner, the technical infrastructure of the learning environment and the 21st century skills required for success in the higher order thinking of computer programming [25]. There are no studies in the extant literature that use an intelligent decision support system that is able to find the optimal choice of learning App to suit the needs of the instructors and learners in acquiring improved student success not only to encourage their interest and excitement for programming, but also to acquire a proficiency to create their own applications. The aim of this paper is to use the fuzzy TOPSIS multi-criteria decision-making technique to rank learning Apps according to its potential to promote critical thinking among programming students. The paper comprises five sections, namely, section 1 introduces the topic, section two surveys the extant literature, section three presents the

fuzzy TOPSIS method, section four explains the results and section five culminates with the findings of the study.

## II. LITERATURE REVIEW

The definition and promotion of critical thinking for learning has become increasingly important in the 21st century information and digital age, where organizations are competing for applicants who have the ability to investigate, apply, and transform data, to collaborate and innovate, to reflect, analyze and think critically, and to arrive at optimal decisions [26]. The literature defines the higher order thinking processes associated with programming as closely aligned with the concept of computational thinking (CT), where problem-solving is implemented through the mental process of abstraction, logic, analysis, synthesis and constructive thinking [5, 27-28]. It has been justified through various studies that CT skills should not just be accessible to everyone at a much younger age, but also have the potential to be applied to various disciplines and hence to be incorporated into the basic curriculum [2, 5].

There are a variety of learning resources and learning Apps to develop CT [29, 30] and each of these include aspects of robotics [2, 4, 31-32], gaming [33-34], augmented reality simulation [35] or multimedia such as graphics, sound and animation, with the latter referred to as visual programming environments [4, 9, 28]. This study is significant in its application as it aims to extend multi-criteria decision-making using Fuzzy TOPSIS with multiple decision-makers choosing the most appropriate learning App based on well-synthesized critical thinking criteria.

Multi-criteria decision analysis (MCDA) has successfully been applied to solve a wide range of complex real-life decision problems in a variety of fields [36], despite researchers encountering many challenges associated with partial ignorance and unquantifiable, incomplete, unobtainable, uncertain, ambiguous and vague information [15]. The choice of MCDA technique rests predominantly on the nature of the decision problem and its ability to address many of the aforementioned challenges. The fuzzy approach is best suited to scenarios that are prone to ambiguity, subjectivity and uncertainty when the decision-maker is expected to make an evaluation [18, 37]. Furthermore, the TOPSIS method suggested by Hwang and Yoon in 1981, is a popular method that can rank the best alternatives quickly, address conflicting situations, is easy to use and can be integrated with other decision-making methods [18]. The fuzzy set theory combined with TOPSIS has the added advantage of addressing any uncertainty encompassing the assessment process [15].

Several refined MCDA methods have been introduced over the years. Some of the popular methods include the analytic hierarchy process (AHP) requiring many comparisons based on human preferences, with the possibility of compromising the consistency of the decisions when compared to the best-worst method developed to reduce the number of comparisons in traditional AHP; the TOPSIS method and simple additive weighting (SAW), which depend on mathematical operations, and the outranking models like ELECTRE and PROMETHEE, which are premised on the assumption that the decision is a process whereby decision-makers can alter their preferences after thorough reflection. The hierarchical model of the AHP

method requires the decision-maker to pairwise-compare multiple criteria and uses ratio and semantic scales to arrive at the decision-maker's preference. Memari et al. in [21] compared the TOPSIS method with two outranking methods namely, PROMETHEE and ELECTRE. According to the authors, TOPSIS is easy to learn and apply compared to outranking methods which proved to be more complex and less transparent to decision-makers. Sahin et al. in [38] included TOPSIS in their study due to its unique approach to the problem and it's intuitively appealing and easy to understand qualities. Palczewski and Sałabun in [36] further highlighted simplicity, computational efficiency and comprehensive mathematical concept as well as its support for group decision-making as key contributing factors to the popularity of the Fuzzy TOPSIS technique.

In the learning App selection problem, the multi-criteria decision-making approach to be applied needs to be carefully considered. The number of decision-makers, the various types of measures to promote critical thinking, the method used to weight the various criteria and the degree of uncertainty and vagueness encompassing the problem scenario are some of the qualifying factors. This study involves a sample of 217 first year programming students and questions on the performance of each alternative against multiple critical thinking criteria, some more easily measurable than others. Nursal, Omar and Nawi in [14], identify the TOPSIS method with assigning crisp or exact numerical values when rating alternatives against criteria and when rating criteria importance, which are also inadequate to simulate human judgements in real-life scenarios. Therefore, to accommodate the imprecise or vague nature of the group decision-making assessment pertaining to critical thinking criteria, this study will use a more authentic approach by enabling the use of linguistic variables to capture the decision-maker's rating more accurately and consistently [40]. Hence the Fuzzy TOPSIS approach is being more suitably applied to model the linguistic ratings as a fuzzy triplet (a, b, c) because the most promising value b will better capture the rating compared to parameter a representing the smallest possible value and parameter c representing the largest possible value in a fuzzy event [40, 41]. This becomes especially important in the group decision-making process.

The research has demonstrated various MCDM problems being solved through the application of fuzzy logic. These include facility location selection, machine tool selection problem, plant layout design problem and robot selection [42] to equipment selection [16] and supplier selection [21, 36, 40]. Although this study uses the quantitative approach, it also identifies some subjective criteria that are difficult to measure, hence the need for fuzzy sets which are capable of representing vague data [41]. According to Kahraman et al. in [42], the strength of fuzzy logic lies in its ability to imitate human reasoning capabilities during the cognitive process of decision-making, to be captured mathematically and more precisely, resulting in a better expected performance in this case scenario.

In everyday pragmatic circumstances which are frequently unpredictable, it is often inadequate to describe phenomena in crisp and precise terms. Therefore, fuzziness occurs in many areas of human judgement, reasoning, evaluations and decision-making. In this study, for example, the evaluation of

learning Apps against various subjective critical thinking criteria are more easily articulated in natural language terms such as very good, poor or satisfactory, which may affect vagueness and ambiguity. However, fuzzy set theory, introduced by Zadeh (1965), offers a rigorous mathematical framework to efficiently resolve the indistinctness associated with the subjectivity of human judgements, and in which vagueness and uncertainty can be precisely and rigorously studied [43].

Rashidi and Cullinane in [40] highlighted fuzzy sets and fuzzy logic (FL) as "powerful mathematical tools for modelling uncertain systems in industry", while de Barros et al. [44] define fuzzy logic as a "multivalued logic, that uses intermediary values between conventional evaluations such as true/false, yes/no or high/low". According to de Barros et al. [44], the language of linguistics is helpful in describing uncertain and ill-defined qualitative data, which otherwise cannot be subjected to quantitative analysis. These linguistic variables can then be represented as computational-efficient fuzzy-triples for appropriately quantifying vague information [37].

According to Samaie et al. in [37], elements in a fuzzy set have different degrees of membership, designated by membership functions, which allocates a grade of membership ranging between 0 and 1. In applications that use fuzzy techniques the decision problem can have complex mathematical membership functions such as triangular or trapezoidal. According to Rajak and Shaw in [18], modelling the decision problem using triangular fuzzy numbers yields a better result. The graphical representation of a membership function  $F(x)$  of a triangular fuzzy number  $\tilde{A}$ , is illustrated in Fig. 1 where the x axis represents the universe of discourse and the y axis represents the degrees of membership in the [0,1] interval [37, 40].

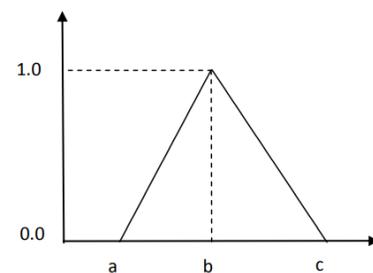


Fig. 1. A Membership Function  $F(X)$  of a Triangular Fuzzy Number  $\tilde{a}$  (Han and Trimi 2018).

A triangular fuzzy number is defined in Fig. 1 and expressed as a membership function in Fig. 2.

$$F(x) = \begin{cases} \frac{x-a}{b-a}, & a \leq x \leq b \\ \frac{c-x}{c-b}, & b \leq x \leq c \\ 0, & \text{otherwise} \end{cases}$$

Fig. 2. Membership Function of a Triangular Fuzzy Number (Han and Trimi 2018).

TABLE I. LINGUISTIC TERMS FOR CRITERIA AND ALTERNATIVES RATINGS (HAN AND TRIMI 2018)

Criteria	Alternatives	
	Linguistic term	Triangular fuzzy numbers
Very low (VL)	Very poor (VP)	(1,1,3)
Low (L)	Poor (P)	(1,3,5)
Medium (M)	Fair (F)	(3,5,7)
High (H)	Good (G)	(5,7,9)
Very high (VH)	Very good (VG)	(7,9,9)

In fuzzy set theory, linguistic terms are converted into fuzzy triples using conversion scales. Usually, a scale of 1 to 9 is applied for weighting the criteria and ranking the alternatives, as illustrated in Table I. Uniform intervals are used to represent the fuzzy triangular numbers for each of the five linguistic ratings [23].

### III. METHODOLOGY

In this research paper fuzzy set theory is introduced to model ambiguity and uncertainty in a MCDM problem and integrated with TOPSIS to appreciate the benefits of its practicality and ease of use, enabling evaluations to be expressed in a linguistic language and then converted to triangular fuzzy numbers and implementing the algorithm using a software tool.

Assume the decision problem has  $k$  decision-makers ( $D_1, D_2 \dots D_k$ ), with  $m$  possible alternatives ( $A_1, A_2 \dots A_m$ ), which is evaluated against  $n$  criteria ( $C_1, C_2 \dots C_n$ ). The rating of criteria and weight with respect to each criterion can be accurately represented in the form of matrices for each decision-maker.

$$\tilde{D} = \begin{matrix} & C_1 & C_2 & & C_n \\ \begin{matrix} A_1 \\ A_2 \\ \dots \\ A_m \end{matrix} & \begin{pmatrix} \tilde{x}_{11} & \tilde{x}_{12} & \dots & \tilde{x}_{1n} \\ \tilde{x}_{21} & \tilde{x}_{22} & \dots & \tilde{x}_{2n} \\ \dots & \dots & \dots & \dots \\ \tilde{x}_{m1} & \tilde{x}_{m2} & \dots & \tilde{x}_{mn} \end{pmatrix} \end{matrix} \quad (1)$$

$$\tilde{W} = (\tilde{w}_1, \tilde{w}_2, \dots, \tilde{w}_n)$$

Where for all  $x_{ij}$  and  $w_{ij}$   $i = 1, 2 \dots m$  and  $j=1, 2 \dots n$ .

Hence  $x_{ij} = (a_{ij}, b_{ij}, c_{ij})$  and  $w_j = (a_j, b_j, c_j)$  are triangular fuzzy numbers representing linguistic variables.

The Fuzzy TOPSIS procedure includes the following steps [24]:

Step 1: Assign ratings to the criteria and alternatives. The criteria weights are denoted by

$$W_{NK} \quad (N = 1, 2, \dots, n; K = 1, 2, \dots, k)$$

and the performance ratings of alternatives with respect to criteria by experts are denoted as

$$X_{NKM} \quad (N = 1, 2, \dots, n; K = 1, 2, \dots, k; M = 1, 2, \dots, m).$$

Step 2: Aggregate the evaluation of the criteria and alternatives. fuzzy ratings  $W_{NK}$  and  $X_{NKM}$  is described as

triangular fuzzy numbers  $(a_K, b_K, c_K)$  where  $K = 1, 2, \dots, k$ , then the aggregated importance can be evaluated as:

$$a = \min\{a_K\} \quad b = \frac{1}{K} \sum_{K=1}^K b_K \quad c = \max\{c_K\} \quad (2)$$

Step 3: Normalize triangular fuzzy numbers. The raw data is normalized using linear scale transformation to bring the various criteria scales into a comparable scale. If  $W_{NK}$  represents benefit criteria, then:

$$\left( \frac{a_K}{c}, \frac{b_K}{c}, \frac{c_K}{c} \right) \quad (3)$$

If  $W_{NK}$  represents cost criteria, then:

$$\left( \frac{a}{c_K}, \frac{a}{b_K}, \frac{a}{a_K} \right) \quad (4)$$

Where  $(a = \min\{a_K\}, c = \max\{c_K\})$

Step 4: Compute weighted normalized fuzzy values.  $W_{NK} *$  becomes  $W_{NK}$  after normalization,  $X_{NKM} *$  is new  $X_{NKM}$  after aggregation. Let the weighted normalized value be  $V_{NKM}$ .

$$V_{NKM} = W_{NK} * X_{NKM} * \quad (5)$$

where  $N = 1, 2 \dots n; K = 1, 2 \dots k; M = 1, 2 \dots m;$

The corresponding triangular fuzzy number of  $V_{NKM}$  is

$$(a_{V_{NKM}}, b_{V_{NKM}}, c_{V_{NKM}}) \quad (6)$$

Step 5: Calculate fuzzy positive ideal solutions (FPIS) and fuzzy negative ideal solutions (FNIS);

$$FPIS = (C_V, C_V, C_V) \text{ where } C_V = \max\{C_{V_{NKM}}\} \quad (7)$$

$$FNIS = (a_V, a_V, a_V) \text{ where } a_V = \min\{a_{V_{NKM}}\} \quad (8)$$

Step 6: Calculate the distance of each alternative from  $FPIS (d^+)$  and  $FNIS (d^-)$  which is calculated, respectively, as follows:

$$d^+ = \sqrt{\frac{1}{3} [(a_{V_{NKM}} - c_V)^2 + (b_{V_{NKM}} - c_V)^2 + (c_{V_{NKM}} - c_V)^2]} \quad (9)$$

$$d^- = \sqrt{\frac{1}{3} [(a_{V_{NKM}} - a_V)^2 + (b_{V_{NKM}} - a_V)^2 + (c_{V_{NKM}} - a_V)^2]} \quad (10)$$

Step 7: Calculate the closeness coefficient ( $CC_M$ )

$$CC_M = \frac{\sum_1^n d_{NM}^-}{\sum_1^n d_{NM}^+ + \sum_1^n d_{NM}^-}, N = 1, 2 \dots n; M = 1, 2 \dots m \quad (11)$$

The  $CC_M$  value is then used to determine the ranking order of all alternatives for the purpose of selecting the best one from among a set of feasible alternatives.

### IV. RESULT

In this section, the results produced from the Fuzzy TOPSIS software application implemented on MatLab R2020a is presented with explanations in steps according to input and outputs of the application. This application utilized complex mathematical equations on the backend which corresponds with the Fuzzy TOPSIS method presented in the methodology

section. The results are based on preferences shown by decision-makers (first year programming students) on choice of visual programming learning applications based on set critical thinking criteria.

Table II shows the fuzzy rating scale where linguistic terms, namely, Not Important (N), Slightly Important (SI), Moderately Important (MI), Important (I) and Very Important (VI) are expressed as a fuzzy triple using integers in the range 1 to 9. These linguistic terms are used to rate the criteria.

Table III presents the measures for critical thinking (criteria) synthesized from the extant literature. Symbols C1 to

C25 are used to represent the critical thinking criteria for selection of programming learning applications for first year university students.

TABLE II. LINGUISTIC AND FUZZY TRIPLE FOR RATING CRITERIA

Linguistic term	Membership function
Not Important (N)	(1,1,3)
Slightly Important (SI)	(1,3,5)
Moderately Important (MI)	(3,5,7)
Important (I)	(5,7,9)
Very Important (VI)	(7,9,9)

TABLE III. MEASURES FOR CRITICAL THINKING (CRITERIA)

No.	Critical Thinking Criteria
C1	Feedback: The App helped me correct my errors while I was coding
C2	Feedback: The App alerted me to incorrect code
C3	Interactivity: The App tells me where my error lies
C4	Problem-solving: The App allows me to solve large, complex, real world, authentic problem scenarios
C5	Collaboration: The App allows me to work on a shared program with my friends
C6	Collaboration: The App allows me to re-use my code or re-use my peers' solutions
C7	Collaboration: The App allows me to communicate with my friend about my questions and queries about our projects
C8	Metacognition: The App allows me to easily and repeatedly make changes to my solution
C9	Logic: The App helped me to improve my logic skills
C10	Logic and reasoning: The App quickly alerts me when the sequencing of steps in my solution is logically incorrect
C11	Evaluation: The App helps me to make my code more efficient
C12	Evaluation: The App is able to evaluate my work
C13	Evaluation: The App allows me to compare my solution against my peers
C14	Alternate solutions: The App helps me to think about solving the problem in different ways
C15	Synthesis: The App allows me to solve problems where I have to draw my knowledge from different programming topics
C16	Application: The App allows me to apply the concepts of sequence, selection and iteration
C17	Metacognitive monitoring: The App interface is designed in a way that encourages me to improve my solution
C18	Multimedia: The interface is visually rich in multimedia and includes sound, color, graphics and animation
C19	Simulation programming: The App uses simple statements to mimic a high-level programming language in an active learning environment
C20	Creativity: The App allows me to create useful and original applications like games and movies
C21	Creativity: The App has various features that enable me to use my creative skills
C22	Creativity: The App supports the simulation of many creative ideas when solving the problem
C23	Analysis: When interpreting the problem statement, the App interface gives me clues on how to solve the problem
C24	Complexity of problem: The App allows me the flexibility to elaborate or build on my idea
C25	Disposition: The App forces me to have an enquiring mind

TABLE IV. LINGUISTIC AND FUZZY TRIPLE FOR THE CRITICAL THINKING ATTRIBUTES (CRITERIA)

Linguistic Values	CRITERIA																								
	C 1	C 2	C 3	C 4	C 5	C 6	C 7	C 8	C 9	C1 0	C1 1	C1 2	C1 3	C1 4	C1 5	C1 6	C1 7	C1 8	C1 9	C2 0	C2 1	C2 2	C2 3	C2 4	C2 5
D1	I	V	M	V	M	M	I	I	V	VI	VI	I	MI	VI	VI	VI	MI	SI	SI	MI	I	I	VI	I	I
D2	I	V	I	M	I	SI	I	M	V	VI	VI	I	MI	I	I	VI	I	MI	MI	I	MI	MI	MI	I	I
D3	V	V	I	V	I	I	M	I	I	VI	VI	MI	MI	I	I	I	MI	SI	SI	SI	SI	SI	I	I	I
D4	I	I	I	I	I	I	M	V	V	VI	VI	I	MI	VI	VI	VI	MI	MI	MI	MI	MI	MI	I	I	VI
D5	V	V	I	M	V	V	I	V	V	VI	I	I	MI	I	I	VI	I	MI	I	VI	I	VI	VI	VI	VI
D6	V	V	V	M	M	M	I	V	V	VI	VI	I	I	VI	MI	VI	I	I	I	MI	MI	MI	I	I	VI
D7	S	V	I	I	M	SI	SI	I	I	VI	SI	SI	SI	VI	I	I	I	SI	SI	MI	SI	SI	MI	VI	VI
D8	I	I	I	V	M	M	M	V	V	VI	I	I	MI	I	VI	VI	I	I	I	I	MI	I	VI	VI	VI
D9	V	M	I	M	I	V	V	V	V	VI	VI	I	I	VI	VI	VI	MI	MI	MI	VI	MI	I	VI	I	I
D10	V	SI	V	I	SI	SI	I	V	V	VI	I	SI	I	VI	SI	I	I	MI	I						

Table IV shows the linguistic rating of the 25 criteria by 10 Academic Experts teaching programming at university level.

Their input values are represented by the symbols D1 to D10 in the table below.

The Best Non-fuzzy Performance value (BNP) for a criterion weighting  $j$ , can be calculated using the following equation [13]:

$$BNP_{wj} = [(Upper\ bound_{wj} - lower\ bound_{wj}) + (Middle\ bound_{wj} - lower\ bound_{wj})]/3 + lower\ bound_{wj} \tag{12}$$

The BNP values give an indication of the relative importance of the criteria. Table V shows the aggregated score for each criterion.

Table V also shows the calculated BNP value for each criteria using Equation 12. Linguistic Weights were assigned based on the BNP values according to descriptions given in Table II.

Table VI shows the ranking of the criteria based on the BNP values indicated in Table V.

Table VI shows that C10 (Logic and reasoning: The App quickly alerts me when the sequencing of steps in my solution is logically incorrect) was the most highly ranked criteria by the expert decision-makers. The second most highly recommended criterion is C9 (Logic: The App helped me to improve my logic skills), followed by C16 (Application: The App allows me to apply the concepts of sequence, selection and iteration) and C14 (Alternate solutions: The App helps me to think about solving the problem in different ways). The least important criterion to decision-makers is criterion C18 (Multimedia: The interface is visually rich in multimedia and includes sound, color, graphics and animation).

TABLE V. AGGREGATED SCORES AND BNP VALUES FOR CRITICAL THINKING ATTRIBUTES (CRITERIA)

Criteria	Aggregated Fuzzy Score	BNP Value	Linguistic Weight
C1	1, 7,4, 9	5,8	I
C2	1, 7,2, 9	5,733333	I
C3	1, 7, 9	5,666667	I
C4	1, 6, 9	5,333333	MI
C5	1, 5, 9	5	MI
C6	1, 4,4, 9	4,8	SI
C7	1, 5,4, 9	5,133333	MI
C8	1, 7,8, 9	5,933333	I
C9	5, 8,6, 9	7,533333	VI
C10	7, 9, 9	8,333333	VI
C11	1, 7,8, 9	5,933333	I
C12	1, 6,2, 9	5,4	MI
C13	1, 4,2, 9	4,733333	SI
C14	5, 8,2, 9	7,4	VI
C15	1, 7,6, 9	5,866667	I
C16	5, 8,6, 9	7,533333	VI
C17	1, 5,4, 9	5,133333	MI
C18	1, 3, 9	4,333333	SI
C19	1, 4, 9	4,666667	SI
C20	1, 5,4, 9	5,133333	MI
C21	1, 3,2, 9	4,4	SI
C22	1, 4,8, 9	4,933333	SI
C23	1, 7, 9	5,666667	I
C24	1, 7,2, 9	5,733333	I
C25	5, 8, 9	7,333333	VI

TABLE VI. RANKED CRITERIA BASED ON BNP VALUES

Ranked Criteria					
1.	C10	11.	C24	21.	C6
2.	C9	12.	C3	22.	C13
3.	C16	13.	C23	23.	C19
4.	C14	14.	C12	24.	C21
5.	C25	15.	C4	25.	C18
6.	C8	16.	C7		
7.	C11	17.	C17		
8.	C15	18.	C20		
9.	C1	19.	C5		
10.	C2	20.	C22		

Table VII shows the fuzzy rating scale for weighing critical thinking criteria. Linguistic terms such as Very Poor (VP), Poor (P), Satisfactory (S), Good (G) and Very Good (VG) are expressed as a fuzzy triple with integers in the range 1 to 9. The Not Sure (N) option expressed as (0, 0, 0) is included in the application to cater for students who are not sure what rating to assign to criteria.

Table VIII shows the numeric labels for Learning Apps (Alternatives).

Table IX presents a snapshot of the assigned ratings by 175 student decision-makers to assess Scratch using the 25 critical thinking criteria in linguistic terms as shown in Table VII.

TABLE VII. LINGUISTIC AND FUZZY TRIPLE FOR THE CRITICAL THINKING ALTERNATIVES (LEARNING APPS)

Linguistic term	Membership function
Not Sure (N)	(0,0,0)
Very Poor (VP)	(1,1,3)
Poor (P)	(1,3,5)
Satisfactory (S)	(3,5,7)
Good (G)	(5,7,9)
Very Good (VG)	(7,9,9)

TABLE VIII. NUMERIC LABELS FOR THE PROGRAMMING LEARNING APPS (ALTERNATIVES)

Programming Learning Apps	Alternatives Label
Alice	1
Scratch	2
Blockly	3
MIT App Inventor	4

TABLE IX. ASSIGNED RATING BY DECISION-MAKERS FOR SCRATCH

Criteria	C1	C2	C3	C4	C5	C6	C7	...	C25
DM1	G	G	VG	G	VG	VG	G	...	VG
DM2	P	S	S	G	G	S	G	...	G
DM3	G	VG	G	VG	G	VG	VG	...	VG
DM4	VG	VG	VG	G	VG	VG	VG	...	VG
DM5	VG	VG	VG	VG	G	VG	VG	...	VG
DM6	VG	G	VG	VG	VG	VG	VG	...	VG
DM7	G	G	G	VG	G	S	G	...	S
DM8	G	P	S	VG	G	G	S	...	VG
DM9	S	G	S	S	G	S	S	...	VG
DM10	P	P	VP	G	VP	VP	VP	...	VG
...	...	...	...	...	...	...	...	...	...
...	...	...	...	...	...	...	...	...	...
DM173	G	G	S	S	G	VG	VG	...	VG
DM174	VG	S	VG	VG	S	VG	VG	...	G
DM175	VG	S	G	G	G	G	VG	...	G

TABLE X. NORMALIZED FUZZY DECISION MATRIX

	<b>Alice (A1)</b>	<b>Scratch (A2)</b>	<b>Blockly (A3)</b>	<b>MIT Inventor (A4)</b>
C1	[0,0.657142857142857,1]	[0,0.761269841269841,1]	[0,0.639365079365079,1]	[0,0.671111111111111,1]
C2	[0,0.656507936507937,1]	[0,0.711111111111111,1]	[0,0.627936507936508,1]	[0,0.660952380952381,1]
C3	[0,0.666031746031746,1]	[0,0.700952380952381,1]	[0,0.615238095238095,1]	[0,0.657777777777778,1]
C4	[0,0.693333333333333,1]	[0,0.766984126984127,1]	[0,0.622222222222222,1]	[0,0.719365079365079,1]
C5	[0,0.639365079365079,1]	[0,0.687619047619048,1]	[0,0.596190476190476,1]	[0,0.661587301587302,1]
C6	[0,0.690158730158730,1]	[0,0.743492063492063,1]	[0,0.633650793650794,1]	[0,0.663492063492064,1]
C7	[0,0.651428571428572,1]	[0,0.685714285714286,1]	[0,0.594285714285714,1]	[0,0.619682539682540,1]
C8	[0,0.760000000000000,1]	[0,0.829206349206349,1]	[0,0.710476190476191,1]	[0,0.720634920634921,1]
C9	[0,0.739682539682540,1]	[0,0.828571428571429,1]	[0,0.716190476190476,1]	[0,0.721269841269841,1]
C10	[0,0.655238095238095,1]	[0,0.714920634920635,1]	[0,0.640634920634921,1]	[0,0.686984126984127,1]
C11	[0,0.704126984126984,1]	[0,0.789206349206349,1]	[0,0.674920634920635,1]	[0,0.725079365079365,1]
C12	[0,0.740952380952381,1]	[0,0.795555555555556,1]	[0,0.723809523809524,1]	[0,0.738412698412698,1]
C13	[0,0.664126984126984,1]	[0,0.721269841269841,1]	[0,0.645714285714286,1]	[0,0.656507936507937,1]
C14	[0,0.749841269841270,1]	[0,0.802539682539682,1]	[0,0.688888888888889,1]	[0,0.726984126984127,1]
C15	[0,0.704761904761905,1]	[0,0.751111111111111,1]	[0,0.636825396825397,1]	[0,0.700952380952381,1]
C16	[0,0.735873015873016,1]	[0,0.779047619047619,1]	[0,0.681904761904762,1]	[0,0.706031746031746,1]
C17	[0,0.730793650793651,1]	[0,0.800000000000000,1]	[0,0.693333333333333,1]	[0,0.716825396825397,1]
C18	[0,0.741587301587302,1]	[0,0.806984126984127,1]	[0,0.666666666666667,1]	[0,0.676825396825397,1]
C19	[0,0.733968253968254,1]	[0,0.780952380952381,1]	[0,0.678095238095238,1]	[0,0.686349206349206,1]
C20	[0,0.725714285714286,1]	[0,0.708571428571429,1]	[0,0.640000000000000,1]	[0,0.666031746031746,1]
C21	[0,0.771428571428572,1]	[0,0.798095238095238,1]	[0,0.687619047619048,1]	[0,0.729523809523810,1]
C22	[0,0.756825396825397,1]	[0,0.773333333333333,1]	[0,0.689523809523810,1]	[0,0.714920634920635,1]
C23	[0,0.641269841269841,1]	[0,0.673650793650794,1]	[0,0.634285714285714,1]	[0,0.620952380952381,1]
C24	[0,0.738412698412698,1]	[0,0.775873015873016,1]	[0,0.674285714285714,1]	[0,0.708571428571429,1]
C25	[0,0.727619047619048,1]	[0,0.791111111111111,1]	[0,0.726349206349206,1]	[0,0.749841269841270,1]

Table X presents the results of the Normalised Fuzzy Decision Matrix from the MatLab R2020a application. This matrix was generated using Equation 3.

Table XI shows the results for FNIS and FPIS generated from the MatLab R2020a Application using Equations 8 and 7 respectively.

Table XII gives the results of the Closeness Coefficient values generated by the MatLab application. These values are generated by the MatLab App using Equation 11.

The C<sub>CCi</sub> value is a ratio scale rating showing the ranking of learning App by 175 decision- makers from highest to lowest,

C<sub>CCi</sub> (Scratch) > C<sub>CCi</sub> (Alice) > C<sub>CCi</sub> (MIT Inventor) > C<sub>CCi</sub> (Blockly).

The results show that Scratch is the most preferred application for learning programming as it had the highest C<sub>CCi</sub> value. This is congruent with various studies that compared visual programming environments using different methods under different contexts and found Scratch to be the most preferred learning tool [4, 11, 45]. The App with the lowest C<sub>CCi</sub> value is Blockly, which therefore is the least preferred application.

TABLE XI. NORMALIZED FUZZY DECISION MATRIX

FNIS (A-)	FPIS (A+)
[0,4.4755555555556,9]	[0,5.3288888888889,9]
[0,4.3955555555556,9]	[0,4.9777777777778,9]
[0,4.3066666666667,9]	[0,4.9066666666667,9]
[0,3.1111111111111,7]	[0,3.8349206349206,7]
[0,2.98095238095238,7]	[0,3.43809523809524,7]
[0,1.90095238095238,5]	[0,2.23047619047619,5]
[0,2.97142857142857,7]	[0,3.42857142857143,7]
[0,4.9733333333333,9]	[0,5.8044444444444,9]
[0,6.44571428571429,9]	[0,7.45714285714286,9]
[0,5.76571428571429,9]	[0,6.43428571428571,9]
[0,4.7244444444444,9]	[0,5.5244444444445,9]
[0,3.61904761904762,7]	[0,3.9777777777778,7]
[0,1.93714285714286,5]	[0,2.16380952380952,5]
[0,6.2000000000000,9]	[0,7.22285714285714,9]
[0,4.4577777777778,9]	[0,5.2577777777778,9]
[0,6.13714285714286,9]	[0,7.01142857142857,9]
[0,3.4666666666667,7]	[0,4,7]
[0,2,5]	[0,2.42095238095238,5]
[0,2.03428571428571,5]	[0,2.34285714285714,5]
[0,3.2000000000000,7]	[0,3.62857142857143,7]
[0,2.06285714285714,5]	[0,2.39428571428571,5]
[0,2.06857142857143,5]	[0,2.3200000000000,5]
[0,4.3466666666667,9]	[0,4.7155555555556,9]
[0,4.7200000000000,9]	[0,5.4311111111111,9]
[0,6.53714285714286,9]	[0,7.1200000000000,9]

TABLE XII. CLOSENESS COEFFICIENT

Rank Order	Programming Learning App	CCi
2	Scratch	0.9941
1	Alice	0.4345
4	MIT inventor	0.3258
3	Blockly	0.0064

V. CONCLUSION

The study used a population of 500 and a sample population of 217 decision-makers to rate four learning Apps against each of 25 critical thinking criteria. Applying the Fuzzy TOPSIS MCDM method to the decision problem would have made handling the matrices both inconvenient and cumbersome. The researcher created code using MatLab R2020a to automate the process. The implementation of the coding for the Fuzzy TOPSIS MCDM method resulted in the ranking of four learning Apps, from the App that promoted critical thinking the best to the one that promoted it least among 1st year programming learners; these Apps were

Scratch, Alice, MIT App Inventor and Blockly. The study is significant for lecturers teaching introductory programming modules to novice learners across educational institutions, especially during the global Covid-19 pandemic, when online learning has become commonplace and its teaching tools have become a requirement. Although the research suggests the positive impact of the visual programming environment on one’s critical thinking skills, further research is required to investigate its subsequent impact in a text-based programming environment.

REFERENCES

- [1] Tsai, C.-Y. 2019. Improving students' understanding of basic programming concepts through visual programming language: The role of self-efficacy. *Computers in Human Behavior*, 95: 224-232.
- [2] Xu, Z., Ritzhaupt, A. D., Tian, F. and Umaphy, K. 2019. Block-based versus text-based programming environments on novice student learning outcomes: A meta-analysis study. *Computer Science Education*, 29 (2-3): 177-204.
- [3] Medeiros, R. P., Ramalho, G. L. and Falcão, T. P. 2018. A systematic literature review on teaching and learning introductory programming in higher education. *IEEE Transactions on Education*, 62 (2): 77-90.
- [4] João, Nuno, Fábio and Ana. 2019. A cross-analysis of block-based and visual programming apps with computer science student-teachers. *Education Sciences*, 9 (3): 181.
- [5] Pinto-Llorente, A. M., Casillas-Martín, S., Cabezas-González, M. and García-Peñalvo, F. J. 2018. Building, coding and programming 3D models via a visual programming environment. *Quality & Quantity*, 52 (6): 2455-2468.
- [6] Noone, M. and Mooney, A. 2018. Visual and textual programming languages: a systematic review of the literature. *Journal of Computers in Education*, 5 (2): 149-174.
- [7] Kaya, K. Y. and Yildiz, İ. 2019. Comparing three free to use visual programming environments for novice programmers. *Kastamonu Eğitim Dergisi*, 27 (6): 2701-2712.
- [8] Siburian, J., Corebima, A. D. and Saptasari, M. 2019. The correlation between critical and creative thinking skills on cognitive learning results. *Eurasian Journal of Educational Research*, 19 (81): 99-114.
- [9] Papadakis, S. and Orfanakis, V. 2018. Comparing novice programming environments for use in secondary education: App Inventor for Android vs. Alice. *International Journal of Technology Enhanced Learning*, 10 (1-2): 44-72.
- [10] Harrison, T. R. and Lee, H. S. 2018. iPads in the mathematics classroom: Developing criteria for selecting appropriate learning apps. *International Journal of Education in Mathematics, Science and Technology*, 6 (2): 155-172.
- [11] Ropii, N., Hardyanto, W. and Ellianawati, E. 2019. Guided inquiry scratch increase students' critical thinking skills on the linear motion concept: Can it be? *JPPPF: Jurnal Penelitian & Pengembangan Pendidikan Fisika*, 5 (1): 63-68.
- [12] Jahnke, I. and Liebscher, J. 2020. Three types of integrated course designs for using mobile technologies to support creativity in higher education. *Computers & Education*, 146: 103782.
- [13] Ivanović, M., Xinogalos, S., Pitner, T., and Savić, M. 2017. Technology enhanced learning in programming courses – international perspective. *Education and Information Technologies*, 22 (6): 2981-3003.
- [14] Nursal, A.T., M.F. Omar, and M.N.M. Nawi, The application of Fuzzy TOPSIS to the selection of building information modeling software. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 2018. 10 (1-10): p. 1-5.
- [15] Salih, M.M., et al., Survey on fuzzy TOPSIS state-of-the-art between 2007 and 2017. *Computers & Operations Research*, 2019. 104: p. 207-227.
- [16] Yavuz, M. 2016. Equipment selection by using fuzzy TOPSIS method. In: *Proceedings of IOP Conference Series: Earth and Environmental Science*, 44 (4).

- [17] Başaran, S. and Haruna, Y. 2017. Integrating FAHP and TOPSIS to evaluate mobile learning applications for mathematics. *Procedia Computer Science*, 120: 91-98.
- [18] Rajak, M. and Shaw, K. 2019. Evaluation and selection of mobile health (mHealth) applications using AHP and fuzzy TOPSIS. *Technology in Society*, 59: 101186.
- [19] Balioti, V., Tzimopoulos, C. and Evangelides, C. 2018. Multi-criteria decision making using TOPSIS method under fuzzy environment. Application in spillway selection. In: *Proceedings of Multidisciplinary Digital Publishing Institute Proceedings*. 637.
- [20] Ece, O. and A.S. Uludag, Applicability of fuzzy TOPSIS method in optimal portfolio selection and an application in BIST. *International Journal of Economics and Finance*, 2017. 9 (10): p. 107-127.
- [21] Memari, A., et al., Sustainable supplier selection: A multi-criteria intuitionistic fuzzy TOPSIS method. *Journal of Manufacturing Systems*, 2019. 50: p. 9-24.
- [22] Mohammed, H.J., M.M. Kasim, and I.N. Shaharane, Evaluation of E-learning approaches using AHP-TOPSIS technique. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 2018. 10 (1-10): p. 7-10.
- [23] Ranganath, N., Sarkar, D., Patel, P. and Patel, S. 2020. Application of fuzzy TOPSIS method for risk evaluation in development and implementation of solar park in India. *International Journal of Construction Management*: 1-11.
- [24] Han, H. and S. Trimi, A fuzzy TOPSIS method for performance evaluation of reverse logistics in social commerce platforms. *Expert Systems with Applications*, 2018. 103: p. 133-145.
- [25] Kules, B. 2016. Computational thinking is critical thinking: Connecting to university discourse, goals, and learning outcomes. In: *Proceedings of the Association for Information Science and Technology*, 53 (1): 1-6.
- [26] Danczak, S. M., Thompson, C. D. and Overton, T. L. 2020. Development and validation of an instrument to measure undergraduate chemistry students' critical thinking skills. *Chemistry Education Research and Practice*, 21 (1): 62-78.
- [27] Romero, M., Lepage, A. and Lille, B. 2017. Computational thinking development through creative programming in higher education. *International Journal of Educational Technology in Higher Education*, 14 (1): 1-15.
- [28] Turker, P. M. and Pala, F. K. 2019. A study on students' computational thinking skills and self-efficacy of block based programming. *i-Manager's Journal on School Educational Technology*, 15 (3): 18.
- [29] Weintrop, D. and Wilensky, U. 2017. Comparing block-based and text-based programming in high school computer science classrooms. *ACM Transactions on Computing Education (TOCE)*, 18 (1): 1-25.
- [30] Šiaulys, T. 2020. Modeling the system for interactive tasks development: engagement taxonomy for introductory programming tools. Switzerland: Springer.
- [31] Atmatzidou, S., Atmatzidou, S., Demetriadis, S., Demetriadis, S., Nika, P. and Nika, P. 2018. How does the degree of guidance support students' metacognitive and problem solving skills in educational robotics? *Journal of Science Education and Technology*, 27 (1): 70-85.
- [32] Figueiredo, J. and García-Peñalvo, F. J. 2019. Teaching and learning strategies of programming for university courses. In: *Proceedings of the Seventh International Conference on Technological Ecosystems for Enhancing Multiculturality*. 1020-1027.
- [33] Papadakis, S. and Kalogiannakis, M. 2017. Using gamification for supporting an introductory programming course: The case of classcraft in a secondary education classroom. In: *Interactivity, game creation, design, learning, and innovation*. Springer, 366-375.
- [34] Tuloli, M., Latief, M. and Rohandi, M. 2019. Scratching our own itch: Software to teach software programming. In: *Proceedings of International Conference on Education, Science and Technology*. Redwhite Press, 115-121.
- [35] Radianti, J., Majchrzak, T. A., Fromm, J. and Wohlgenannt, I. 2020. A systematic review of immersive virtual reality applications for higher education: Design elements, lessons learned, and research agenda. *Computers & Education*, 147: 103778.
- [36] Palczewski, K. and W. Salabun, The fuzzy TOPSIS applications in the last decade. *Procedia Computer Science*, 2019. 159: p. 2294-2303.
- [37] Samaie, F., Meyar-Naimi, H., Javadi, S. and Feshki-Farahani, H. 2020. Comparison of sustainability models in development of electric vehicles in Tehran using fuzzy TOPSIS method. *Sustainable Cities and Society*, 53: 101912.
- [38] Sahin, B., Yip, T. L., Tseng, P.-H., Kabak, M. and Soylu, A. 2020. An application of a fuzzy TOPSIS multi-criteria decision analysis algorithm for dry bulk carrier selection. *Information*, 11 (5): 251.
- [39] Junior, F.R.L., L. Osiro, and L.C.R. Carpinetti, A comparison between Fuzzy AHP and Fuzzy TOPSIS methods to supplier selection. *Applied Soft Computing*, 2014. 21: p. 194-209.
- [40] Rashidi, K. and Cullinane, K. 2019. A comparison of fuzzy DEA and fuzzy TOPSIS in sustainable supplier selection: Implications for sourcing strategy. *Expert Systems with Applications*, 121: 266-281.
- [41] Chen, C.-T., Extensions of the TOPSIS for group decision-making under fuzzy environment. *Fuzzy Sets and Systems*, 2000. 114(1): p. 1-9.
- [42] Kahraman, C., Ateş, N. Y., Çevik, S., Gülbay, M. and Erdoğan, S. A. 2007. Hierarchical fuzzy TOPSIS model for selection among logistics information technologies. *Journal of Enterprise Information Management*, 20 (2): 143-168.
- [43] Zimmermann, H.J., Fuzzy set theory. *Wiley Interdisciplinary Reviews: Computational Statistics*, 2010. 2 (3): p. 317-332.
- [44] de Barros, L. C., Bassanezi, R. C. and Lodwick, W. A. 2017. The extension principle of Zadeh and fuzzy numbers. In: *A first course in fuzzy logic, fuzzy dynamical systems, and biomathematics*. Springer, 23-41.
- [45] Erol, O. and Kurt, A. A. 2017. The effects of teaching programming with scratch on pre-service information technology teachers' motivation and achievement. *Computers in Human Behavior*, 77: 11-18.

# Complex Plane based Realistic Sound Generation for Free Movement in Virtual Reality

Kwangki Kim

Department of IT Convergence  
Korea Nazarene University, Cheon-an, South Korea

**Abstract**—A binaural rendering is a technology that generates a realistic sound for a user with a stereo headphone, so it is essential for the stereo headphone based virtual reality (VR) service. However, the binaural rendering has a problem that it cannot reflect the user's free movement in the VR. Because the VR sound does not match with the visual scene when the user moves freely in the VR space, the performance of the VR may be degraded. To reduce the mismatch problem in the VR, the complex plane based stereo realistic sound generation method was proposed to allow the user's free movement in the VR causing the change of the distance and azimuth between the user and the speaker. For the calculation of the distance and the azimuth between the user and the speaker by the user's position change, the 5.1 multichannel speaker playback system and the user are placed in the complex plane. Then, the distance and the azimuth between the user and the speaker can be simply calculated as the distance and the angle between two points in the complex plane. The 5.1 multichannel audio signals are scaled by the estimated five distances according to the inverse square law, and the scaled multichannel audio signals are mapped to the newly generated virtual 5.1 multichannel speaker layout using the measured five azimuths and the azimuth by the head movement. Finally, we can successfully obtain the stereo realistic sound to reflect the user's position change and the head movement through the binaural rendering using the scaled and mapped 5.1 multichannel audio signals and the HRTF coefficients. Experimental results show that the proposed method can generate the realistic audio sound reflecting the user's position and azimuth change in the VR only with less than about 5 % error rate.

**Keywords**—*Virtual reality; realistic sound; binaural rendering; constant power panning; head related transfer function*

## I. INTRODUCTION

In general, users should have their own multi-channel audio playback environment to enjoy the realistic sound by multi-channel audio signals. However, most of the users have a stereo headphone environment, so they are unable to enjoy realistic audio by the multi-channel audio signals. Therefore, a head related transfer function (HRTF) [1] based binaural rendering has been proposed to solve this limitation [2-6]. In particular, the binaural rendering is essential to deliver the more realistic audio signal to the users in a system such as a virtual reality (VR) service based on the stereo headphone environment [8-10]. In the binaural rendering, the stereo realistic sound is generated using the multi-channel audio signals and the HRTF coefficients. The stereo realistic sound

generation based on the binaural rendering can efficiently supply the realistic sound with the user in the VR service, but there is a critical limitation that the existing stereo realistic sound generation based on the binaural rendering does not reflect the user's position change. Since the stereo realistic sound generation through binaural rendering with a fixed HRTF cannot reflect the user's position change, there is a gap between the visual scene and the sound causing the performance degradation of the VR service. To solve the fixed sound scene problem in the VR, the sound scene control of the stereo realistic sound in the VR was introduced to reflect the user's head azimuth change [11]. In [11], the HRTF coefficients are replaced by the new HRTF coefficients corresponding to the user's azimuth change, and the realistic sound with the controlled sound scene is calculated with the multi-channel audio signals and the replaced HRTF coefficients. Although the realistic sound generation with the substitution of the HRTF coefficients can successfully generate the stereo realistic sound with the controlled sound scene according to the user's head movement, it needs very high data amount of the stored HRTF coefficients for all azimuth directions. The data rate of the HRTF coefficients are 23.6 Mbytes to be 32 times compared with that of the HRTF coefficients of the 5.1 multi-channel speaker layout. Therefore, the sound scene control of the realistic sound with the substitution of the HRTF coefficients is not suitable for the embedded system with low memory storage. Accordingly, the constant power panning (CPP) based sound scene control of the realistic sound was introduced [12-15]. The CPP based sound scene control scheme used only the HRTF coefficients of the 5.1 multi-channel speaker layout, so the data rate of the HRTF coefficients is exactly same as the original binaural rendering. Instead, the CPP based sound scene control method mapped the original multi-channel audio signals onto the new 5.1 multi-channel speaker layout rearranged by the user's head movement. The CPP based method can be applied to the embedded system with the low memory storage because it can generate the realistic sound reflecting the user's head movement without the increase of the HRTF coefficients.

Meanwhile, the VR service allows the user's free movement in the VR space, so the VR service should consider the user's not only head movement but also position change. Namely, the VR service should generate the realistic sound reflecting the user's free movement. However, since the sound scene control based on the HRTF coefficients and the CPP method only focuses on the modification of the stereo realistic sound scene according to the user's azimuth change, its' stereo realistic sound cannot imply the user's distance change.

---

This work was funded by the research fund of Korea Nazarene University in 2021. Also, this research was supported by Basic Science Research Program through the National Research Foundation of Korea (NRF) funded by the Ministry of Education (2017R1D1A3B03034951).

Therefore, there is still a mismatch between the VR scene and the VR sound when the user freely moves in the VR space and the overall performance of the VR service may be very poor.

The realistic sound generation method based on a complex plane for tracking the user's movement is proposed to improve the performance of the VR service by reflecting the user's free movement in the VR sound. The user's free movement (position change) in the VR space causes both changes of the distance and the azimuth between the user and the speaker, while the user's head movement only effects on the azimuth change. Therefore, the proposed method separately handles the user's position change and the head movement and it calculates the distance and the azimuth between the user and the speaker by the user's free movement. Then, the proposed method can generate the realistic sound by scaling the audio signal using the measured distance and by adjusting the sound scene using the final azimuth formed by adding the measured azimuth for the position change and the azimuth change for the head movement. In conclusion, the proposed method can improve the overall performance of the VR service by generating the realistic sound that reflects the user's free movement including the head movement. This paper consists of as follows. In Section 2, the stereo realistic sound generation through the binaural rendering and the sound scene control of the realistic sound is described. In Section 3, the realistic sound generation for the user's free movement in the VR is proposed. In Sections 4 and 5, the experimental result and the conclusion will be given, respectively.

## II. STEREO REALISTIC SOUND GENERATION BASED ON BINAURAL RENDERING FOR VR

### A. Binaural Rendering for VR

The VR system needed the stereo realistic sound generation method for the immersive effect by the multi-channel audio signals since the VR system used the stereo headphone for the delivery of the VR sound. The VR system adopted the conventional binaural rendering for generating the stereo realistic sound [1-7]. The binaural rendering is a technology that generates the stereo realistic audio sound with the multi-channel audio effect for stereo headphone environment using HRTF coefficients to characterize all signal paths from speakers to human ears [1]. As shown in Fig. 1, the binaural rendering is computed with the input multi-channel signal and the HRTF coefficients. To generate the output stereo realistic sound, the input multi-channel audio signals are convolved with the HRTF coefficients as in (1) [2-4].

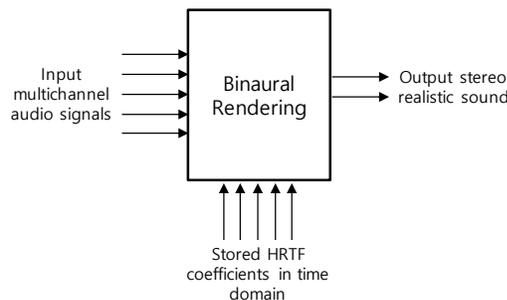


Fig. 1. Stereo Realistic Sound Generation through Binaural Rendering.

$$o_L = \sum_{n=1}^N (s_n \otimes h_n^L), o_R = \sum_{n=1}^N (s_n \otimes h_n^R) \quad (1)$$

where  $h_n^L$  and  $h_n^R$  are the stored HRTF coefficients in time domain from the nth channel to human left and right ear.  $o_L$  and  $o_R$  are the output left and right realistic signals in time domain and  $s_n$  is the nth channel input signal in time domain.  $N$  is the channel number of the multi-channel audio signals and  $\otimes$  is the linear convolution. Since the linear convolution in time domain between the input signals and the HRTF coefficients has very high computational complexity, the binaural rendering is calculated as the multiplication of the input signals and the HRTF coefficients in the frequency domain as in (2)[5] and Fig. 1 is updated as Fig. 2.

$$O_L = \sum_{n=1}^N (S_n \cdot H_n^L), O_R = \sum_{n=1}^N (S_n \cdot H_n^R) \quad (2)$$

where  $H_n^L$  and  $H_n^R$  are the stored HRTF coefficients in frequency domain from the nth channel to human left and right ear.  $O_L$  and  $O_R$  are the output left and right realistic signals in frequency domain and  $S_n$  is the nth channel input signal in frequency domain.

Meanwhile, (2) can be rewritten in matrix form for 5.1 multi-channel audio signals as in (3) [11].

$$\begin{bmatrix} O_L(k) \\ O_R(k) \end{bmatrix} = \begin{bmatrix} H_C^{Left}(k) & H_C^{Right}(k) \\ H_{Lf}^{Left}(k) & H_{Lf}^{Right}(k) \\ H_{Rf}^{Left}(k) & H_{Rf}^{Right}(k) \\ H_{Ls}^{Left}(k) & H_{Ls}^{Right}(k) \\ H_{Rs}^{Left}(k) & H_{Rs}^{Right}(k) \end{bmatrix}^T \times \begin{bmatrix} S_c(k) \\ S_{Lf}(k) \\ S_{Rf}(k) \\ S_{Ls}(k) \\ S_{Rs}(k) \end{bmatrix}, \text{ for } 0 \leq k \leq M-1 \quad (3)$$

where  $O_L(k)$  and  $O_R(k)$  are the output left and right realistic sound.  $S_x(k)$  is the arbitrary channel X signal in frequency domain and  $k$  is the frequency index.  $C, Lf, Ls, Rf$  and  $Rs$  are the center, left front, left surround, right front, and right surround of the 5.1 multi-channel audio signals.  $H_X^{Left}(k)$  and  $H_X^{Right}(k)$  are the stored HRTF coefficients in frequency domain from the arbitrary channel X to human's left and right ear.  $M$  is the number of the FFT size.

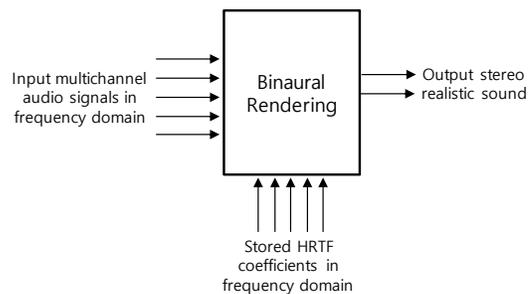


Fig. 2. Stereo Realistic Sound Generation through Binaural Rendering in Frequency Domain.

**B. Sound Scene Control of Stereo Realistic Sound Reflecting Azimuth Change in VR**

Although the conventional binaural rendering was useful for the VR system, it could not reflect the user's azimuth change. Therefore, the sound scene control of the stereo realistic sound was proposed [11, 12]. When the azimuth angle of the user changed in the 5.1 channel reproduction environment, the direction in which the 5.1 channel signal is transmitted to the user or the azimuth angle of the 5.1 channel reproduction environment also changed. So, the existing HRTF coefficients should be replaced by new HRTF coefficients corresponding to the azimuth angle of the new 5.1 channel reproduction environment. The binaural rendering with the sound scene control could generate the realistic sound with the substituted HRTF coefficients and the 5.1 channel audio signal according to the user's azimuth change as in (4).

$$\begin{bmatrix} O_{L,\theta_{hm}}(k) \\ O_{R,\theta_{hm}}(k) \end{bmatrix} = \begin{bmatrix} H_{C-\theta_{hm}}^{Left}(k) & H_{C-\theta_{hm}}^{Right}(k) \\ H_{Lf-\theta_{hm}}^{Left}(k) & H_{Lf-\theta_{hm}}^{Right}(k) \\ H_{Rf-\theta_{hm}}^{Left}(k) & H_{Rf-\theta_{hm}}^{Right}(k) \\ H_{Ls-\theta_{hm}}^{Left}(k) & H_{Ls-\theta_{hm}}^{Right}(k) \\ H_{Rs-\theta_{hm}}^{Left}(k) & H_{Rs-\theta_{hm}}^{Right}(k) \end{bmatrix}^T \times \begin{bmatrix} S_c(k) \\ S_{Lf}(k) \\ S_{Rf}(k) \\ S_{Ls}(k) \\ S_{Rs}(k) \end{bmatrix}, \text{ for } \begin{cases} 0 \leq k \leq M-1 \\ 0^\circ \leq \theta_{hm} \leq 360^\circ \end{cases} \quad (4)$$

where  $O_{L,\theta_{hm}}(k)$  and  $O_{R,\theta_{hm}}(k)$  the output left and right realistic sound with controlled sound scene according to the user's head movement.  $H_{X-\theta_{hm}}^{Left}(k)$  and  $H_{X-\theta_{hm}}^{Right}(k)$  are the substituted HRTF coefficients corresponding to the user's azimuth change from the arbitrary channel X to human's left and right ear.  $\theta_{hm}$  is the angle of the user's head movement.

Here, if the angle of any channel X minus  $\theta_{hm}$  is negative, the final azimuth of any channel is the calculated angle plus 360 degrees. Fig. 3 shows an example of the user's azimuth change in the 5.1 multi-channel speaker layout. Since the angle of the user's azimuth change is 90 degrees, the angle of existing 5.1 multi-channel speaker layout is rearranged as shown in Fig. 3 and the HRTF coefficients are substituted to reflect the rearranged multi-channel speaker layout. The binaural rendering generates the stereo realistic sound with the controlled sound scene using the 5.1 multi-channel audio signals and the substituted HRTF coefficients as in (5). Fig. 4 shows the overall procedure of the sound scene control of the realistic sound based on the substitution of the HRTF coefficients.

$$\begin{bmatrix} O_{L,90^\circ}(k) \\ O_{R,90^\circ}(k) \end{bmatrix} = \begin{bmatrix} H_{270^\circ}^{Left}(k) & H_{270^\circ}^{Right}(k) \\ H_{240^\circ}^{Left}(k) & H_{240^\circ}^{Right}(k) \\ H_{300^\circ}^{Left}(k) & H_{300^\circ}^{Right}(k) \\ H_{160^\circ}^{Left}(k) & H_{160^\circ}^{Right}(k) \\ H_{20^\circ}^{Left}(k) & H_{20^\circ}^{Right}(k) \end{bmatrix}^T \times \begin{bmatrix} S_c(k) \\ S_{Lf}(k) \\ S_{Rf}(k) \\ S_{Ls}(k) \\ S_{Rs}(k) \end{bmatrix}, \text{ for } 0 \leq k \leq M-1 \quad (5)$$

Although the above explained sound scene control scheme of the realistic sound can successfully generate the stereo realistic sound with the controlled sound scene, it needed very high data amount of the stored HRTF coefficients as 23.6 Mbytes. Therefore, the embedded system with the low memory storage could not implement the sound scene control of the realistic sound with the substitution of the HRTF coefficients.

Accordingly, the CPP based sound scene control of the realistic sound was introduced [11-15]. The CPP based sound scene control scheme fixed the HRTF coefficients of the 5.1 multi-channel speaker layout and it mapped the existing multi-channel audio signals onto the new 5.1 multi-channel speaker layout rearranged by the user's head movement. Fig. 5 shows an example of the mapping of the multi-channel audio signals to the newly formed 5.1 multi-channel speaker layout according to the user's head movement. The 5.1 multi-channel speaker layout is newly created around the user's new front, and the existing 5.1 multi-channel audio signals are mapped onto the new speaker layout using the CPP technique. The binaural rendering is performed as in (6) using the mapped 5.1 multi-channel signals and the HRTF coefficients of the 5.1 multi-channel speaker layout to generate stereo realistic sound with the controlled sound scene according to the user's head movement.

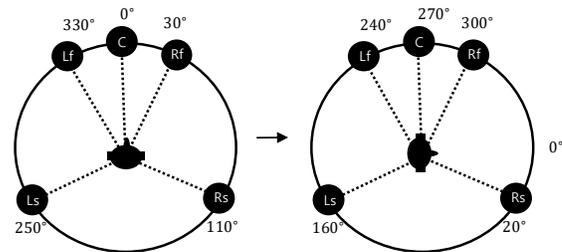


Fig. 3. Example of the user's Azimuth Change in the 5.1 Multi-channel Speaker Layout.

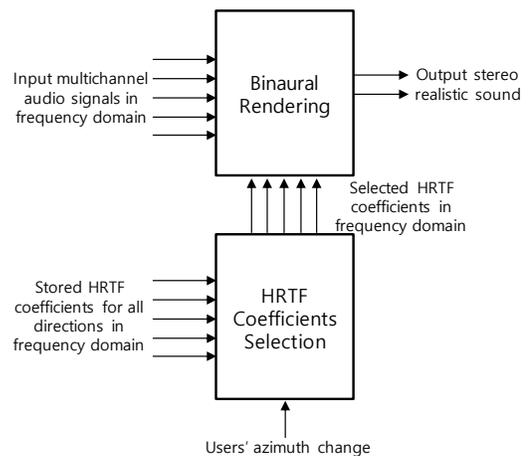


Fig. 4. Overall Procedure of the Sound Scene Control of the Realistic Sound based on the Substitution of the HRTF Coefficients.

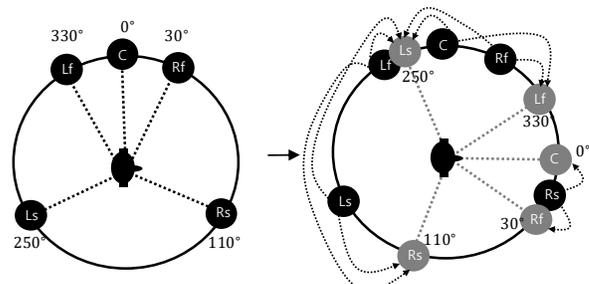


Fig. 5. Example of the Signal Mapping to the Newly Formed 5.1 Multi-Channel Speaker Layout According to the user's Head Movement.

$$\begin{bmatrix} O_L(k) \\ O_R(k) \end{bmatrix} = \begin{bmatrix} H_C^{Left}(k) & H_C^{Right}(k) \\ H_{Lf}^{Left}(k) & H_{Lf}^{Right}(k) \\ H_{Rf}^{Left}(k) & H_{Rf}^{Right}(k) \\ H_{Ls}^{Left}(k) & H_{Ls}^{Right}(k) \\ H_{Rs}^{Left}(k) & H_{Rs}^{Right}(k) \end{bmatrix} \times \begin{bmatrix} S_C^m(k) \\ S_{Lf}^m(k) \\ S_{Rf}^m(k) \\ S_{Ls}^m(k) \\ S_{Rs}^m(k) \end{bmatrix}, \text{ for } 0 \leq k \leq M-1 \quad (6)$$

where  $S_X^m(k)$  is a newly generated signal of any channel X through the mapping of the 5.1 multi-channel audio signals to the newly formed 5.1 multi-channel speaker layout. For the explanation of the signal mapping using the CPP method [14, 15], let's assume that there are two channel speakers (C1 and C2) and any channel (C3) lays in between two channel speakers after the user's head movement as shown in Fig. 6. Then, a signal of channel C3 is mapped onto the channel C1 and C2 using (7) and (8).

$$\theta_{norm} = \frac{(\theta_3 - \theta_1)}{(aperture - \theta_1)} \times \frac{\pi}{2}, \text{ aperture} = |\theta_2 - \theta_1| \quad (7)$$

$$\left. \begin{aligned} S_1^m(k) &= S_1(k) + S_3(k) \times \cos(\theta_m) \\ S_2^m(k) &= S_2(k) + S_3(k) \times \sin(\theta_m) \end{aligned} \right\}, \text{ for } 0 \leq k \leq M-1 \quad (8)$$

Here,  $\theta_{norm}$  is the normalized angle of azimuth of C3 laid in between C1 and C2, and *aperture* is the reference angle between C1 and C2.  $\theta_1$ ,  $\theta_2$  and  $\theta_3$  are the azimuth of C1, C2, and C3.  $S_1(k)$ ,  $S_2(k)$  and  $S_3(k)$  are the signal gains of C1, C2, and C3.  $S_1^m(k)$  and  $S_2^m(k)$  are the new signal gains of C1 and C2 after the mapping of  $S_1(k)$  using the CPP. The signal mapping using the CPP method is applied to the entire 5.1 multi-channel signals to create the new 5.1 multi-channel audio signals with the newly formed 5.1 multi-channel speaker layout according to the user's head movement. Finally, the stereo realistic sound with the controlled sound scene can be generated through the binaural rendering with the new 5.1 multi-channel audio signals and the existing 5.1 multi-channel HRTF coefficients. Fig. 7 shows the overall procedure of the sound scene control of the realistic sound based on the CPP method.

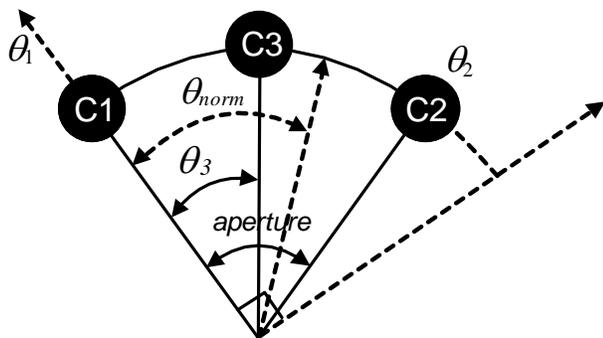


Fig. 6. Example of the Signal Mapping using the CPP.

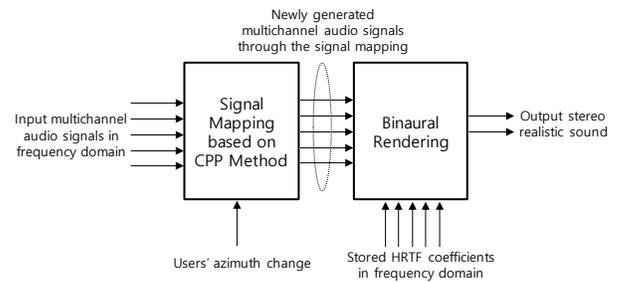


Fig. 7. Overall Procedure of the Sound Scene Control of the Realistic Sound based on the CPP Method.

### III. PROPOSED STEREO REALISTIC SOUND GENERATION FOR FREE MOVEMENT IN VR

In the VR service, the user moves freely in the VR space, so the VR sound must be adjusted according to the VR scene. Namely, the VR service allows the user's head movement and the position change in the VR space and the VR sound in the VR service should reflect the user's free movement. However, since the previously explained sound scene control based on the HRTF coefficients and the CPP method only focused on the modification of the stereo realistic sound scene according to the user's azimuth change, the previous realistic sound could not imply the user's distance change. Therefore, there is still a mismatch between the VR scene and the VR sound when the user freely moves in the VR space and the overall performance of the VR service can be severely degraded. To allow the user's free movement in the VR space and reduce the performance degradation of the VR, the realistic sound generation method based on a complex plane for the user's movement tracking is proposed. The user's position change effected on both changes of the distance and the azimuth between the user and the speaker while the user's head movement only effected on the azimuth change between the user and the speaker. Therefore, the proposed method separately handled the user's position change and the head movement. Namely, the distance and the azimuth between the user and the speaker layout by the user's position change were firstly measured, and then the final azimuth between the user and the speaker by considering two azimuths caused by the user's position change and the head movement was determined. The signal level was modified using the calculated distance between the user and the speaker while the sound scene of the realistic sound was controlled using the measured azimuth. The detail of the realistic sound generation using the calculated distance and azimuth between the user and the speaker is given in the below.

For the calculation of the distance and the azimuth between the user and the speaker by the user's position change, it is assumed that the 5.1 multi-channel speaker playback system located in the complex plane as shown in Fig. 8 and the user moved freely on the complex plane. Based on the assumption, the distance and the azimuth between the user and the speaker by the user's position change could be estimated because the user and the speaker were considered as two points in the complex plane. Meanwhile, as the azimuth measurement method could vary according to the user's location on the complex plane, the distance and azimuth between the user and the speaker were measured based on the user's location divided

into four areas around the speaker as shown in Fig. 9 and 10. Meanwhile, the four areas around the speaker in the complex plane are summarized in Table I. After setting four areas for all speakers in the 5.1 multi-channel speaker layout as shown in Fig. 9, the distance and the azimuth between the user and the speaker were calculated in each area as shown in Fig. 10. In Fig. 10,  $a + jb$  and  $c + jd$  are the position of any speaker X in the 5.1 multi-channel speaker layout and the user in the complex plane, respectively. Table II summarizes the calculation of the distance and azimuth between the user and the speaker for four areas around the speaker according to the user's position change.

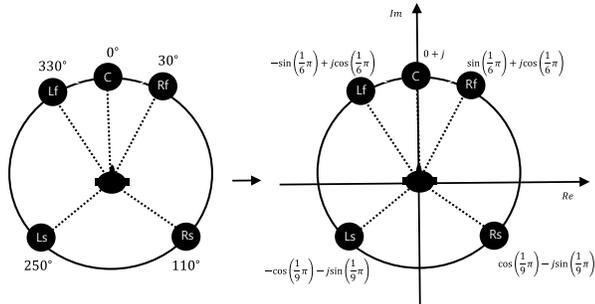


Fig. 8. 5.1 Multi-channel Speaker Placed in the Complex Plane.

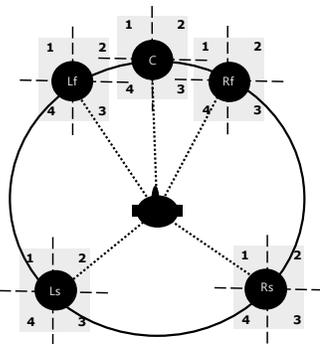


Fig. 9. Four Areas for All Speakers in the 5.1 Multi-channel Speaker Layout.

TABLE I. FOUR AREAS AROUND THE SPEAKER EXPRESSED IN THE COMPLEX PLANE COORDINATE

Area	Complex plane coordinate
Area 1	$Re < 0, Im \geq 0$
Area 2	$Re \geq 0, Im > 0$
Area 3	$Re > 0, Im \leq 0$
Area 4	$Re \leq 0, Im < 0$

For the realistic sound generation by reflecting the user's position change and the head movement, the 5.1 multi-channel audio signals were firstly scaled using the measured five distance values between the moved user and the 5.1 multi-channel speaker. Then, the scaled 5.1 multi-channel audio signals were mapped onto the new multi-channel speaker layout using not only the estimated five azimuths between the moved user and the 5.1 multi-channel speaker but also the azimuth according to the user's head movement. Based on the inverse square law that the sound intensity is inversely

proportional to the distance from the source [16, 17], the scaled 5.1 multi-channel audio signals were calculated using the estimated five distance values. Moreover, because all the distances between the user and the 5.1 multi-channel speaker layout are equal to one, the scaled 5.1 multi-channel audio signals were calculated as in (9).

$$S_c^s(k) = \frac{1}{r_c} S_c(k), S_{L_f}^s(k) = \frac{1}{r_{L_f}} S_{L_f}(k), S_{R_f}^s(k) = \frac{1}{r_{R_f}} S_{R_f}(k),$$

$$S_{L_s}^s(k) = \frac{1}{r_{L_s}} S_{L_s}(k), S_{R_s}^s(k) = \frac{1}{r_{R_s}} S_{R_s}(k) \text{ for } 0 \leq k \leq M-1 \quad (9)$$

where  $S_X^s(k)$  is the scaled signal of any channel X and  $r_X$  is the estimated distance between the user and any channel X. Because the virtual 5.1 channel speaker layout was set around the moved user, the scaled 5.1 multi-channel audio signals were mapped onto the virtual speaker layout using the measured five azimuths and the azimuth by the head movement. The final azimuths could be determined for the signal mapping as in (10).

$$\left. \begin{aligned} \theta_f^C &= \theta_p^C - \theta_{hm} \\ \theta_f^{L_f} &= \theta_p^{L_f} - \theta_{hm} \\ \theta_f^{R_f} &= \theta_p^{R_f} - \theta_{hm} \\ \theta_f^{L_s} &= \theta_p^{L_s} - \theta_{hm} \\ \theta_f^{R_s} &= \theta_p^{R_s} - \theta_{hm} \end{aligned} \right\} \text{for } 0 \leq \theta_{hm} \leq 2\pi \quad (10)$$

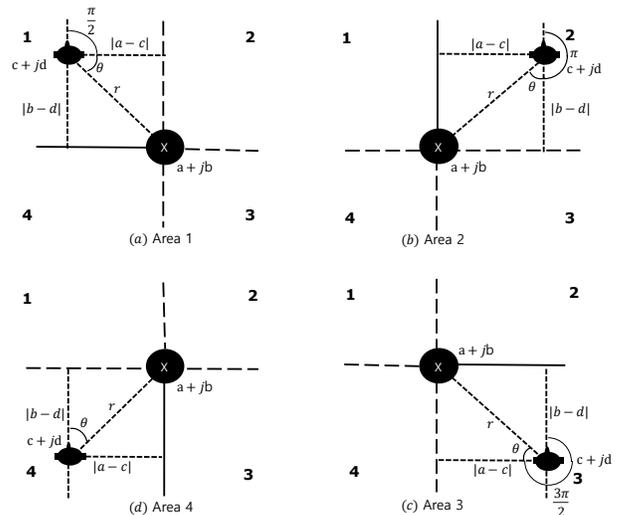


Fig. 10. Calculation of the Distance and the Azimuth in Four Areas.

TABLE II. SUMMARY OF THE CALCULATION OF THE DISTANCE AND THE AZIMUTH BETWEEN THE USER AND THE SPEAKER

Area	Azimuth ( $\theta_p$ )	Distance ( $r$ )
Area 1	$\tan^{-1}\left(\frac{ b-d }{ a-c }\right) + \frac{\pi}{2}$	$\sqrt{(a-c)^2 + (b-d)^2}$
Area 2	$\tan^{-1}\left(\frac{ a-c }{ b-d }\right) + \pi$	
Area 3	$\tan^{-1}\left(\frac{ b-d }{ a-c }\right) + \frac{3\pi}{2}$	
Area 4	$\tan^{-1}\left(\frac{ a-c }{ b-d }\right)$	

where  $\theta_f^X$  is the final azimuth of any channel X for the signal mapping and  $\theta_p^X$  is the estimated azimuth between the user and the any speaker X according to the user's position change. Here, if  $\theta_f^X$  has the minus value,  $\theta_p^X$  is  $\theta_f^X + 2\pi$ . After the signal mapping using the final azimuth as in (10), the final realistic sound could be obtained to allow the user's free movement including the head azimuth change as in (11).

$$\begin{bmatrix} O_L(k) \\ O_R(k) \end{bmatrix} = \begin{bmatrix} H_C^{Left}(k) & H_C^{Right}(k) \\ H_{L_f}^{Left}(k) & H_{L_f}^{Right}(k) \\ H_{R_f}^{Left}(k) & H_{R_f}^{Right}(k) \\ H_{L_s}^{Left}(k) & H_{L_s}^{Right}(k) \\ H_{R_s}^{Left}(k) & H_{R_s}^{Right}(k) \end{bmatrix} \times \begin{bmatrix} S_C^{s,m}(k) \\ S_{L_f}^{s,m}(k) \\ S_{R_f}^{s,m}(k) \\ S_{L_s}^{s,m}(k) \\ S_{R_s}^{s,m}(k) \end{bmatrix}, \text{ for } 0 \leq k \leq M-1 \quad (11)$$

where  $S_X^{s,m}(k)$  is the generated signal of any channel X of the virtual 5.1 multi-channel speaker layout formed by the user's position and head movement through the signal scaling as in (9) and the signal mapping using the final azimuth as in (10). Fig. 11 shows the overall procedure of the proposed the realistic sound generation for the user's free movement in the VR.

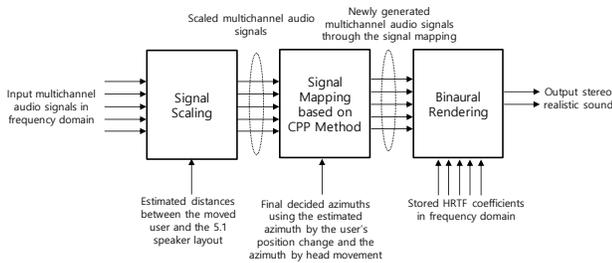


Fig. 11. Overall Procedure of the Proposed the Realistic Sound Generation.

#### IV. RESULTS AND DISCUSSION

To validate the performance of the proposed realistic sound generation method for the user's free movement in the VR, the subjective listening test was performed. Three audio contents were used for the test and listed in Table III. For simplification and clarification of the test, the realistic audio sound only using the left and the right channel signals was separately generated according to the user's position change as shown in Fig. 12. Here, it was assumed that there was no user's head movement. Five listeners participated in the test, and they evaluated the azimuth and distance of the generated realistic audio sound at the changed user's position compared to those of the realistic audio sound at the original position. Meanwhile, the azimuths and distances between the user and the speakers were theoretically calculated in each position as in Table IV.

TABLE III. TEST MATERIALS

Material	Description
Item1	Ambience
Item2	Music (back: direct)
Item3	Pathological

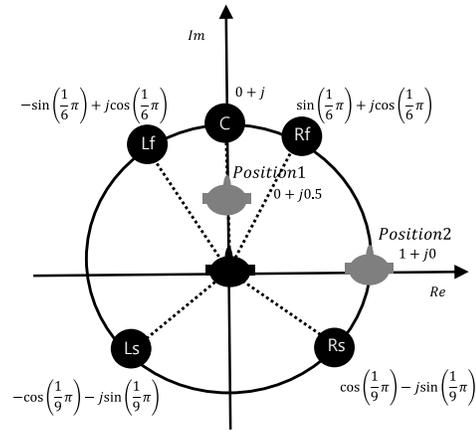


Fig. 12. Two Position Changes for the Test.

TABLE IV. ESTIMATED DISTANCE AND THE AZIMUTH BETWEEN THE GIVEN USER'S POSITION AND THE SPEAKER FOR THE TEST

Position	Ch.	Selected Area	Azimuth ( $\theta_p$ )	Distance ( $r$ )
1	C	Area 4	$\tan^{-1}\left(\frac{ 0-0 }{ 1-0.5 }\right) = 0$	$\sqrt{(0-0)^2 + (1-0.5)^2} = 0.5$
	Lf	Area 3	$\tan^{-1}\left(\frac{\cos(\pi/6)-0.5}{-\sin(\pi/6)}\right) + \frac{3\pi}{2}$ = $\frac{30.62\pi}{18}$ ( $\approx 306^\circ$ )	$\sqrt{(-\sin(\pi/6))^2 + (\cos(\pi/6)-0.5)^2}$ = 0.62
	Rf	Area 4	$\tan^{-1}\left(\frac{ \sin(\pi/6) }{ \cos(\pi/6)-0.5 }\right)$ = $\frac{5.38\pi}{18}$ ( $\approx 53.8^\circ$ )	$\sqrt{(\sin(\pi/6))^2 + (\cos(\pi/6)-0.5)^2}$ = 0.62
	Ls	Area 2	$\tan^{-1}\left(\frac{1-\cos(\pi/9)}{-\sin(\pi/9)-0.5}\right) + \pi$ = $\frac{22.81\pi}{18}$ ( $\approx 228^\circ$ )	$\sqrt{(-\cos(\pi/9)-0)^2 + (-\sin(\pi/9)-0.5)^2}$ = 1.26
	Rs	Area 1	$\tan^{-1}\left(\frac{1-\sin(\pi/9)-0.5}{\cos(\pi/9)}\right) + \frac{\pi}{2}$ = $\frac{13.19\pi}{18}$ ( $\approx 132^\circ$ )	$\sqrt{(\cos(\pi/9)-0)^2 + (-\sin(\pi/9)-0.5)^2}$ = 1.26
2	C	Area 3	$\tan^{-1}\left(\frac{ 1-0 }{ 0-1 }\right) + \frac{3\pi}{2} - \frac{7\pi}{4}$ ( $\approx 315^\circ$ )	$\sqrt{(0-1)^2 + (1-0)^2} = 1.41$
	Lf	Area 3	$\tan^{-1}\left(\frac{\cos(\pi/6)}{-\sin(\pi/6)-1}\right) + \frac{3\pi}{2}$ = $\frac{10\pi}{6}$ ( $\approx 300^\circ$ )	$\sqrt{(-\sin(\pi/6)-1)^2 + (\cos(\pi/6)-0)^2}$ = 1.73
	Rf	Area 3	$\tan^{-1}\left(\frac{\cos(\pi/6)}{\sin(\pi/6)-1}\right) + \frac{3\pi}{2}$ = $\frac{11\pi}{6}$ ( $\approx 330^\circ$ )	$\sqrt{(\sin(\pi/6)-1)^2 + (\cos(\pi/6)-0)^2}$ = 1
	Ls	Area 2	$\tan^{-1}\left(\frac{1-\cos(\pi/9)-1}{-\sin(\pi/9)}\right) + \pi$ = $\frac{26\pi}{18}$ ( $\approx 260^\circ$ )	$\sqrt{(-\cos(\pi/9)-1)^2 + (-\sin(\pi/9)-0)^2}$ = 1.97
	Rs	Area 2	$\tan^{-1}\left(\frac{\cos(\pi/9)-1}{-\sin(\pi/9)}\right) + \pi$ = $\frac{19\pi}{18}$ ( $\approx 190^\circ$ )	$\sqrt{(\cos(\pi/9)-1)^2 + (-\sin(\pi/9)-0)^2}$ = 0.35

Fig. 13 and 14 are the subjective listening test results. In addition, Table V shows the error rate of the proposed method in the azimuth and the distance evaluation, respectively. The test results show that the proposed method could rather successfully generate the realistic sound according to the user's position change because the desired azimuth and distance overlap the confidence intervals of the evaluated ones in most test items. Nevertheless, the confidence intervals of the evaluated azimuth and distance are very wide, so the listening

test results also show that the performance of the proposed method may be rather poor. It is because the proposed method used only the HRTF coefficients of the 5.1 multi-channel speaker layout, namely, the proposed method did not have the sufficient resolution of the HRTF coefficients to generate the realistic audio sound according to the user's free movement in the VR. Therefore, it is necessary to improve the proposed method to generate realistic sound by utilizing HRTF coefficients of the 10.1 or more playback environment.

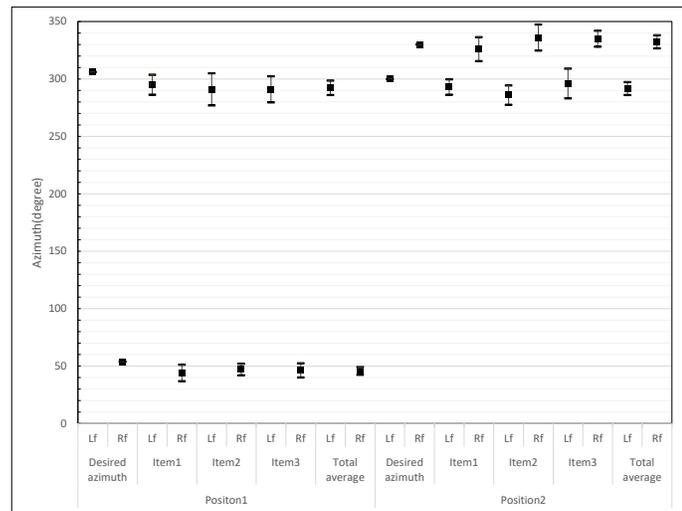


Fig. 13. Subjective Listening Test Result for Evaluation of Azimuth Change.

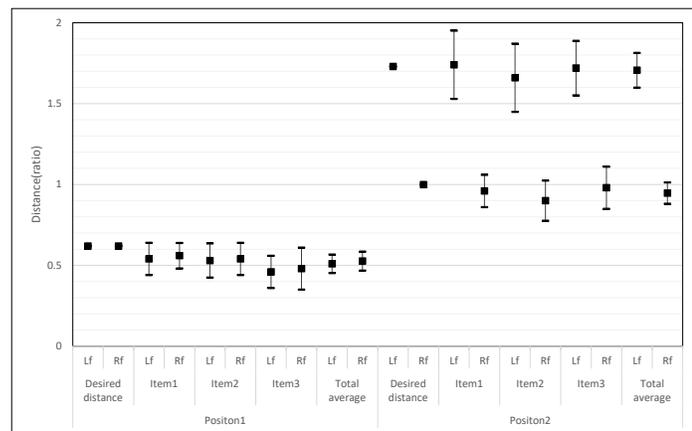


Fig. 14. Subjective Listening Test Result for Evaluation of Distance Change.

TABLE V. ERROR RATE OF THE AZIMUTH AND THE DISTANCE EVALUATION (%)

Position	Channel	Azimuth	Distance
Position1	Lf	4.8	2.3
	Rf	8.1	8.7
Position2	Lf	4.6	1
	Rf	1.2	2.4
Overall		4.7	3.6

## V. CONCLUSION

The realistic audio is essential to enjoy the realistic services such as VR, but there is a limitation that multi-channel audio playback environment is involved for the realistic audio. Although the binaural rendering could solve this limitation to provide the realistic sound in the stereo headphone playback environment, there was a problem that the binaural rendering alone could not reflect the user's free movement in the VR. Therefore, there was the mismatch between the visual scene and the audio sound in the VR, so the performance of the VR was degraded. In this paper, the complex plane based stereo realistic sound generation method was proposed to allow the user's free movement such as the position change and the head azimuth change in the VR. In the proposed method, the variations of the azimuth and distance between the user and the speaker were reflected according to the user's movement in the stereo realistic sound generated by the binaural rendering. The subjective listening test results showed that the proposed method could generate the realistic audio sound that successfully reflected the user's free movement only with less than 5 % error rate of the azimuth and the distance evaluation. In spite of the good performance of the proposed method, the performance improvement of the proposed method through the increase of the resolution of the HRTF coefficients remains as a future work because the proposed method only had the HRTF coefficients of the 5.1 multi-channel speaker layout and it caused the error of the azimuth and the distance evaluation.

## REFERENCES

- [1] B. Gardner and K. Martin, HRTF Measurements of a KEMAR Dummy Head Microphone, MIT Media Lab Perceptual Computing -technical Report #280, 1994.
- [2] J. Breebaart et al., "Multi-channel goes mobile: MPEG Surround binaural rendering," In Proceedings of the Audio Engineering Society Conference: 29th International Conference: Audio for Mobile and Handheld Devices. Audio Engineering Society, 2006.
- [3] J. Breebaart, L. Villemoes, K. Kjörling, "Binaural rendering in MPEG Surround," EURASIP Journal on advances in signal processing, 2008, pp. 1-14.
- [4] K. Kim, J. Kim, "Binaural decoding for efficient multi-channel audio service in network environment," In Proceedings of the 2014 IEEE 11th Consumer Communications and Networking Conference, 2014, pp. 525-526.
- [5] K. Kim, "A study on complexity reduction of binaural decoding in multi-channel audio coding for realistic audio service," Contemporary Engineering Sciences, Vol. 9, no. 1, pp. 11-19, 2016.
- [6] W. Bailey, B. Fazenda, "The effect of visual cues and binaural rendering method on plausibility in virtual environments," In Audio Engineering Society Convention 144. Audio Engineering Society, 2018.
- [7] M. Zaunschirm, M. Frank, F. Zotter, "Binaural rendering with measured room responses: First-order ambisonic microphone vs. dummy head," Applied Sciences, Vol.10, no. 5, 2020.
- [8] W. Li, L. Yang, X. Leng, W. Liu, G. Dai, "Application of virtual reality technology in Wushu education," the International Journal of Electrical Engineering & Education, doi.org/10.1177/0020720920940583, 2020.
- [9] H. Jialiang, Z. huiying, "Mobile-based education design for teaching and learning platform based on virtual reality," International Journal of Electrical Engineering & Education, doi.org/10.1177/0020720920928547, 2020.

- [11] G. Zhang, "Design of virtual reality augmented reality mobile platform and game user behavior monitoring using deep learning," International Journal of Electrical Engineering & Education, doi.org/10.1177/0020720920931079, 2020.
- [12] K. Kim, "Sound scene control of multi-channel audio signals for realistic audio service in wired/wireless network," International Journal of Multimedia and Ubiquitous Engineering, vol. 9, no. 2, 2014.
- [13] K Kim, J Kim, "A Study on Realistic Audio Sound Generation according to User's Movement in Virtual Reality System," Proceedings of the 2019 4th International Conference on Intelligent Information Technology, ACM, 2019.
- [14] E. Zwicker and H. Fastl, Psychoacoustics, Springer-Verlag, Berlin, Heidelberg, 1999.
- [15] V. Pulki, "Virtual sound source positioning using vector base amplitude panning," Journal of Audio Engineering Society, vol. 45, pp. 456-466, 1997.
- [16] M. A. Gerzon, "Panpot laws for multispeaker stereo," In Proceedings of the 92nd Convention of the AES, Journal of Audio Engineering Society, Preprint 3309, 1992.
- [17] Sound intensity as a function of distance from a small source, [https://ocw.upc.edu/webs/42254/Acustica\\_EN/Bloc2/Fitxes/T07\\_05\\_Intensitat\\_i\\_distancia.htm](https://ocw.upc.edu/webs/42254/Acustica_EN/Bloc2/Fitxes/T07_05_Intensitat_i_distancia.htm).
- [18] Inverse-Square law, [https://en.wikipedia.org/wiki/Inverse-square\\_law](https://en.wikipedia.org/wiki/Inverse-square_law)

# Reverse Vending Machine Item Verification Module using Classification and Detection Model of CNN

Razali Tomari<sup>1\*</sup>, Nur Syahirah Razali<sup>2</sup>, Nurul Farhana Santosa<sup>3</sup>, Aeslina Abdul Kadir<sup>4</sup>, Mohd Fahrul Hassan<sup>5</sup>

Institute for Integrated Engineering (IIE)<sup>1</sup>  
Faculty of Electrical and Electronic Engineering<sup>2,3</sup>  
Faculty of Civil Engineering and Built Environment<sup>4</sup>  
Faculty of Mechanical & Manufacturing Engineering<sup>5</sup>  
Universiti Tun Hussein Onn Malaysia  
86400 Parit Raja, Batu Pahat, Johor. Malaysia

**Abstract**—Reverse vending machine (RVM) is an interactive platform that can boost recycling activities by rewarding users that return the recycle items to the machine. To accomplish that, the RVM should be outfitted with material identification module to recognize different sort of recyclable materials, so the user can be rewarded accordingly. Since utilizing combination of sensors for such a task is tedious, a vision-based detection framework is proposed to identify three types of recyclable material which are aluminum can, PET bottle and tetra-pak. Initially, a self-collected of 5898 samples were fed into classification and detection framework which were divided into the ratio of 85:15 of training and validation samples. For the classification model, three pre-trained models of AlexNet, VGG16 and Resnet50 were used, while for the detection model YOLOv5 architecture is employed. As for the dataset, it was gathered by capturing the recycle material picture from various point and information expansion of flipping and pivoting the pictures. A progression of thorough hyper parameters tuning were conducted to determine an optimal structure that is able to produce high accuracy. From series of experiments it can be concluded that, the detection model shows promising outcome compare to the classification module for accomplishing the recycle item verification task of the RVM.

**Keywords**—Convolutional neural network (CNN); classification; detection; reverse vending machine (RVM); You Only Look Once (YOLO)

## I. INTRODUCTION

Malaysia is leaving behind in sustaining waste management awareness, especially in recycling [1]. Currently, the rate of solid waste increase significantly [2] and one of the methods that can be done in managing waste effectively is by boosting recycling activities using interactive Reverse Vending Machine (RVM). RVM works by analyzing every deposit recycle materials to the machine and provide reward to the user accordingly. Previously, a hybrid sensing based RVM [3-4] has been developed and tested in municipal office as shown in Fig. 1. However, it manage to recognize only PET bottle and aluminum can, and required tedious sensor calibration, maintenance and not suitable for long term usage.

To cater such an issue, a vision-based technology is incorporated into the RVM material identification module. Vision system capable to recognizing more types of recycle items with vast amount of the collected data from the sample.

One of the work is from [5] in which they introduced ThrashNet dataset and use SIFT feature with SVM and CNN model of AlexNet-like architecture. The former model manage to obtain average of 63% performance while the latter show deteriorate performance with 22% accuracy, in which the author argue more dataset will yield a better result. Andrey et al. [6] developed a reverse vending machine with several CNN classification model by analyzing effect of training by combining two different dataset cluster during training. In average the CNN model can produce more than 85% accuracy. They later on test the module in real implementation by combining weigh sensor with the CNN for fraud detection [7].

Recently, CNN becomes trends for thrash items classification either using standalone model, combine with conventional classifier or using ensemble CNN architecture. RecycleNet [8] was introduced to exhaustively analyze optimal state of the art CNN structure for the RVM classification task. They exhaustively tune the model based on empty-structure model, with pre-trained and fine tuning. In average for the performance wise, 90% accuracy can be obtained for each models, layer modification is necessary to ensure processing time and accuracy can be well balance. In [9], a combination of GoogleNet with SVM show promising outcome with 97.86% based on TrashNet dataset. Apart from that a MobileNet variants [10] shows at par performance with 96.57% and optimized DenseNet121 model obtain 99.6% accuracy [11] using the same dataset. An ensemble based model that combine GoogleNet, ResNet-50 and MobileNetv2 using unequal precision measurement data fusion been tested using ThrashNet and FourThrash dataset [12], apparently they claim that the combination provide more robust results during data aggregation of the CNN forecasting results.



Fig. 1. Example of RVM using Combination of Sensors.

There are many works that previously focus on classification models and detection models for the RVM application. However, to the best of our knowledge no comparison done to investigate the effectiveness between each of the models. In this paper a CNN classification based model is compare with detection based model to determine optimal structure for RVM implementation. The paper is organize as follow: section II will discuss about methodology use through this project, follow by result and discussion in section III and eventually project conclusion in section IV.

## II. MODELS AND METHOD

In this section, detail explanation about model and architecture used throughout this project is thoroughly explained. It comprises of three main subsections, namely, dataset preparation, classification model development and detection model development.

### A. Datasets Preparation

The arrangement of getting sample image of all classes are as in Fig. 2 in which the camera is vertically locate 21cm above the ground and the sample was placed 51cm from the camera. There are total of 5898 samples collected ranging from three categories of aluminum can, PET bottles and tetra-pak as depicted in Fig. 3. The collected images are then separated into training and validation cluster with a portion of 4961 samples for validation and 937 samples for validation. Details of sample distributions for each cluster can be seen in Table I. It can be noticed that. For the detection task, all images must undergo an annotating process in which in this project a Labellmg software is used.

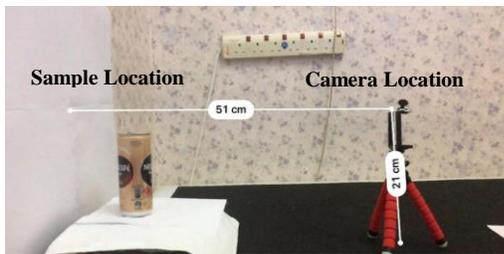


Fig. 2. Setup Arrangement for Dataset Preparation.



Fig. 3. Sample of Tetra-Pak, PET Bottle and Aluminium Can.

TABLE I. NUMBER OF IMAGE DATASET IN EACH RECYCLE ITEM IMAGE CATEGORY

Images	Training	Validation
Aluminum Can	1335	248
PET Bottle	3018	569
Tetra-pak	608	120
Total	4961	937

### B. Classification Model Development

For the classification module, a Convolutional Neural Network (CNN) based model is employ. Basically, CNN comprises two main part which are feature extractor module, also known as convolutional layer, and classification module that will regard as dense layer. The former ensure local features from inputted image can be highlighted, while the latter utilize the extracted local features to identify the trained object inside the image. In this project, a pre-trained CNN model is utilize to recognize the three cluster of the recyclable items. It means that, the parameters from convolutional layer of state of the art CNN model will be reuse to be trained with our own dataset. During the training session, convolutional layer parameters will be frozen while dense layer parameters will by dynamically adjusted to reduce the cost function error.

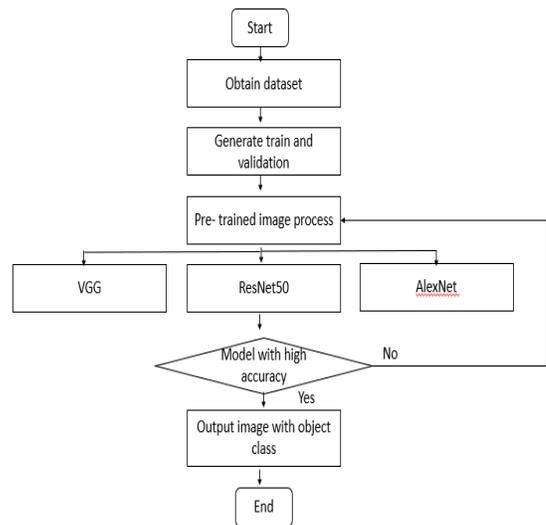


Fig. 4. Block Diagram flow of the Classification Procedure.

Fig. 4 depicted overall system flow of the classification part. From the collected sample set, the training cluster data will be tested with three pre-train models which are VGG, ResNet50 and AlexNet. All the three models will undergo rigorous hyper parameters tuning to analyses the best model that can optimally classify the three types of the recyclable items. In this paper, a free GPU from Google Colab is employed to execute the training process. This platform is a cloud based of Jupyter notebook and can be edited by the team members and easy to access without requiring any setup. It supported many types of machine learning libraries and the sample data can be simply loaded from the user Google drive.

The CNN VGG16 model [13] is the first model that will be access for the classification module. It comprises of systematic architecture of 3x3 filter throughout the 16 layers and was introduced in 2014 as an improvement of Alexnet. The model achieved 92.7% accuracy performance in ImageNe dataset and consists of 138 million parameters and make it a bit slow to train. Fig. 5 shows an architecture of VGG16 model. All the input images will be resized to 224x224 dimension prior to feed to the 13 convolutional layers. Number of channel in this layer is started with 64 channels and was incremented to the factor of two up until 512 channels. In between of the convolutional layer there are five pooling layers that

responsible to down sample an image and was done using maxpooling operation of 2x2 kernel with stride of two. The last convolutional layer outputting feature map with the size of 7x7x512. Then, this 2D features is flattened through the three fully connected layers with ReLU activation in the first two hidden layer and softmax in the output layer.

Residual Network (ResNet) [14] is the second model that will be tested for this project. ResNet is the first model that can be used to generate very deep network from hundreds to thousands layer while still providing a good performance. It able to handle such situation by introducing residual block with a skip connection, which will add a result from previous layer to the next layer of the model as shown in Fig. 6. A very deep network literally will suffer from vanishing gradient problem, in which the back propagate training error value will become smaller from layer to layer and eventually becomes zero. In the layer where the error goes to zero and in its subsequent, no more parameters update will be executed and hence the model unable to converge well with the given data. ResNet handle such situation via the skip connection which allowing the gradient to flow via the alternative path. By doing that, it will ensure the higher layer will perform as good as the lower layer.

In this project, a ResNet50 model is used in which it contains 49 convolutional layers and single dense layer as shown in Fig. 7. The former layer can be further categorize into four main blocks of conv2, conv3, conv4 and conv5 in which each block contain three convolutional layers as shown in Fig. 6. The number of channel in each block is sequentially increment by a factor of two and the model is expected an input image of 224x224 dimension. In summary, the convolutional structure can be visualize as: conv1; 3 x conv2; 4 x conv3; 6 x conv4; 3 x conv5. After series of convolutional layers, a dense layer with 1000 neurons and softmax activation function is add up to classify the dataset cluster accordingly.

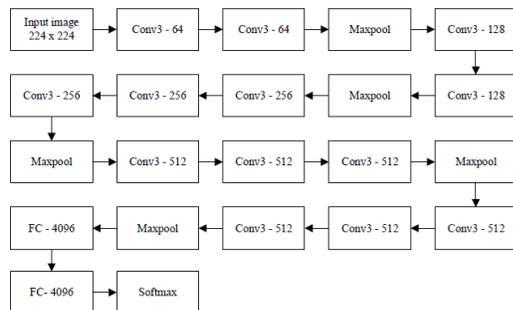


Fig. 5. VGG-16 Structure.

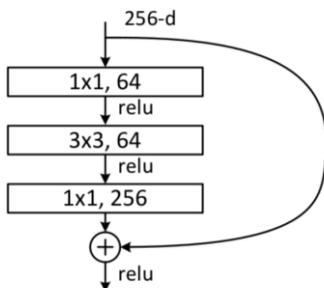


Fig. 6. Residual Block Structure.

layer name	output size	50-layer
conv1	112x112	7x7, 64, stride 2
conv2_x	56x56	3x3 max pool, stride 2
		$\begin{bmatrix} 1 \times 1, 64 \\ 3 \times 3, 64 \\ 1 \times 1, 256 \end{bmatrix} \times 3$
		$\begin{bmatrix} 1 \times 1, 128 \\ 3 \times 3, 128 \\ 1 \times 1, 512 \end{bmatrix} \times 4$
conv3_x	28x28	$\begin{bmatrix} 1 \times 1, 256 \\ 3 \times 3, 256 \\ 1 \times 1, 1024 \end{bmatrix} \times 6$
conv4_x	14x14	$\begin{bmatrix} 1 \times 1, 512 \\ 3 \times 3, 512 \\ 1 \times 1, 2048 \end{bmatrix} \times 3$
conv5_x	7x7	average pool, 1000-d fc, softmax
	1x1	

Fig. 7. ResNet-50 Structure.

The third model that will be analyze is AlexNet architecture [15]. This is one of the simplest and earliest CNN architecture that have firm grip of overfitting problem by introducing data augmentation and dropout layer. Basically AlexNet consist of eight layers that compose of five convolutional layers and three dense layer as shown in Fig. 8. The model also introduce rectify linear unit (ReLU) and max pooling layer to be use along with the convolutional layer. Regarding the input, it must be resize to 227x227 dimension prior feed to the network. In their structure, three size of filter dimensions were utilized which in dimension of 11x11, 5x5 and 3x3.

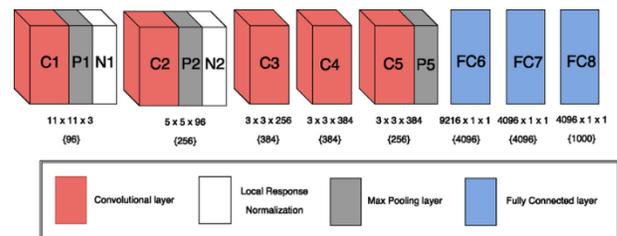


Fig. 8. AlexNet Structure.

To utilize all the mentioned state of the art CNN models in this project, a transfer learning process is implemented. Technically, the process will re-utilize all the convolutional parameters from the model, omit its original dense layer and then hook up our dense layer as shown in Fig. 9. In the figure, shade block area denotes the convolutional layer parameters and will be frozen during training session. On the other hand, the white block area is the new dense layer that consist of two hidden layers with 512 and 128 neuron and one output layer with three neurons that denote our three clusters of aluminium can, PET bottle and tetra-pak. The dense layer, will be dynamically updated during the training session based on the back propagate error value from the output layer.

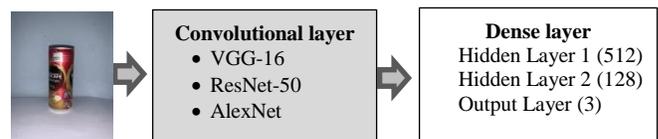


Fig. 9. Visualization of Structure of Transfer Learning Process.

### C. Detection Model Development

For detection module, the main structure employ in this project is based on ‘You Only Look Once’ (YOLO) object detection. Basically, it starts with the forming of grid cells, follow by class prediction across scales, and eventually bounding box location estimation via regression process. The finer grid cell enable for smaller target detection and anchor box make it possible to detect an overlapping object with high accuracy. There are many variants of YOLO model starting from version v1 to version v5 [16-20]. In this project, the recent model which is YOLOv5 is used.

YOLOv5 is a single stage object detector and has three components which are backbone, neck (PANet) and head (output) as depicted in Fig. 10. Model backbone is mostly used to separate significant features from the input image using cross stage partial network (CSPNet) [21]. CSPNet has demonstrated huge improvement in processing time with more profound networks and solves the problems of repeated gradient information in large-scale backbones. Such structure will improve inference, speed, and accuracy and at the same time reduce the model size. In RVM verification task, detection speed, and accuracy is important, and compact model size also determines its inference efficiency on compact device controller.

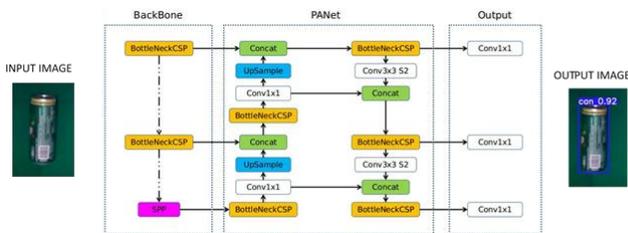


Fig. 10. YOLOv5 Architecture.

Model neck is mostly used to produce feature pyramid to assist models to deduct on object scaling. It assists with recognizing similar item with various sizes and scales. Feature pyramids are extremely valuable and assist models with performing admirably on hidden data. In YOLOv5 path aggregation network (PANet) [22] is utilized as neck to get feature pyramids. PANet improve localization signals accuracy the in lower layers, and hence enhance the location accuracy of the object.

The model head is essentially used to play out the last detection part. It applied three different size of anchor boxes to cater small, medium and big objects on features, and creates final output vectors with class probabilities, object scores, and bounding boxes. The YOLOv5 model head structure is equivalent to the past YOLOv3 and YOLOv4 model.

YOLOv5 has four final architecture which are YOLOv5s (small), YOLOv5m (medium), YOLOv5l (large) and YOLOv5x (xlarge). To balance between speed and accuracy of the system, YOLOv5s which is the smallest and fastest model is utilised for the RVM implementation.

In YOLO family the cost function calculation is source from objectness score, class probability score, and bounding box regression score. YOLOv5 has utilized binary cross-

entropy (BCE) with logits loss equation from for loss calculation of class probability and object score. This loss joins a sigmoid layer and the BCE loss in one single class and more mathematically stable than utilizing a plain sigmoid followed by a BCE loss.

### III. RESULTS AND DISCUSSION

In this section performance of the selected classification and detection model is presented. Basically the section comprises of three main parts which are classification model assessment, detection model assessment and optimal model assessment in live feed video streaming. Part of the samples that will be use during the training and validation session can be seen in Fig. 11 which shown PET bottle samples, aluminum can samples and tetra-pak samples.

#### A. Classification Model Assessment

For the first classification analysis, summary of the outcomes can be seen in Fig. 12. It displays result of training session, validation session and loss in every epochs. Initially, in every training session 50 epoch will be selected, and the location where overfitting start to occurs will be selected as the new epoch for the next training session. The tuning process will be repeated until optimal outcome that well balance between training and validation data is obtained. However, if under fitting condition constantly occurs, then it can be concluded that the model cannot be used for recognizing the given dataset.

As can be seen in figure, the VGG-16 model performance keep under fitting both for training and validation with value of below 70%, and hence it can be summarize that the VGG-16 model unable to works well to classify the data. Next, for the AlexNet model it begins to under fit after 15 epochs and eventually at 50 epochs the performance for training is at 98% while for the validation is at 80%. It can be say that, the ALexNet model works well for memorizing the data but not works well for recognizing unseen data pattern. Finally, for the ResNet-50 model, it can be observed that it able to obtain high accuracy during training session with 92%, but the validation performance fluctuate significantly with the lowest value of 12% after 50 epochs.

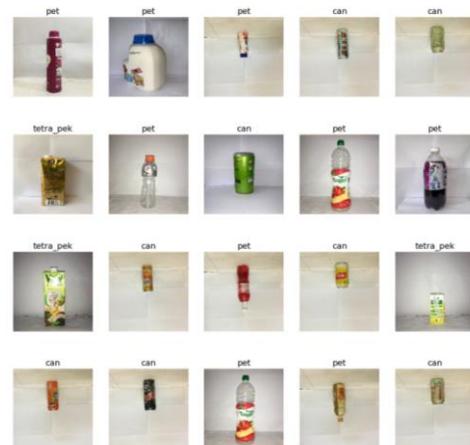


Fig. 11. Sample of Training Images.

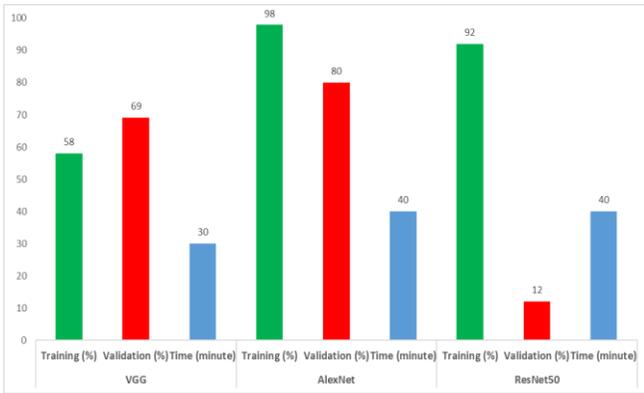


Fig. 12. Summary of Classification Model Analysis.

Based on the finding, for RVM classification model the best structure that can balance trade-off between training and validation is the AlexNet model with 80% performance during validation stage and the highest training performance among other two models. Sample of the classification outcome can be seen in Fig. 13.



Fig. 13. Sample of Classification Module Outcome.

### B. Detection Model Assessment

This section will deliberately discuss result obtained for the YOLOv5 detection module framework. The best variable must be selected to achieve a rapid object detection model with high accuracy. There are three important parameters that are frequently used for object detection assignment: Generalized Intersection over Union (GIoU) graph, Objectness graph and mean Average Precision (mAP) graph.

GIoU graph indicates how near the ground truth with the predicted bounding box, whereas for Objectness graph means confidence score whether there is an object in the grid cell. In the event that the bounding box covers a ground truth object more than others, the relating Objectness score ought to be 1. The third graph that is important is mAP graph where the precision and recall for all the objects introduced in the images ought to be figured. It additionally needs to consider the confidence score for each object detection by the model in the picture. Consider the entirety of the predicted bounding boxes with a confidence score over a specific limit. Bounding boxes over the set threshold value are considered as positive boxes while all predicted bounding boxes underneath the set threshold value are considered as negative. Thus, the higher the threshold value is, the lower the mAP will be, however the confidence is more accurate.

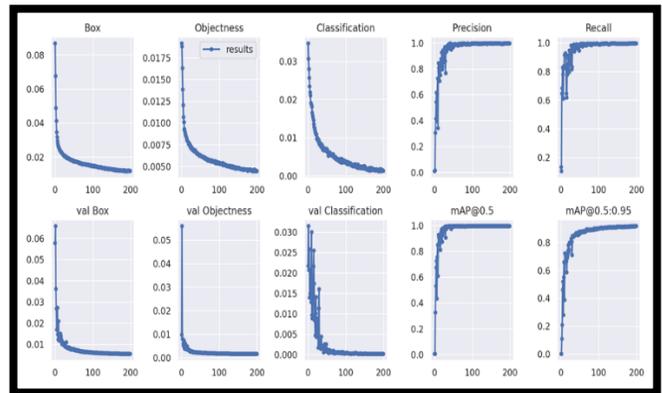


Fig. 14. Detection Training Result of Fine Tuning Process for 200 Epochs.

Fig. 14, summarize the tuning outcome after 200 epochs of training. The first three columns show loss function value for GIoU confident score, Objectness confidence score and classification confidence score, where the upper part denoted the training data while the lower part the validation data. It can be observed that all the loss value decrement constantly near to zero for the three scores. Even there is some fluctuation for the val-classification score in the beginning of training, it becomes constantly goes to zero as the epoch more than 50. Looking at another four remaining curve figures of precision, recall, mAP@0.5 and mAP@0.5: 0.95, the performance gain high confidence score after 100 epochs.

To gain more detail insight of each object class performance, precision and recall curve can be investigated and is shown in Fig. 15. Precision recall curve shows the tradeoff between the exactness and recall esteems for various limits. This curve assists with choosing the best threshold to expand both measurements. As the number of positive samples get higher (high recall), the accuracy of classification of every sample precisely get lower (low precision). From the figure, it can be observed that, the PET bottle shows highest confidence score with 0.997, follow by tetra-pak and finally the aluminium can. In average, overall performance of all class detection is at 0.995 using 0.5 confidence score of mean average precision. The performance for the detection can be conclude as much more better than the one obtain from the classification model based on the given dataset. The resultant images after running the inference/testing process were as in Fig. 16.

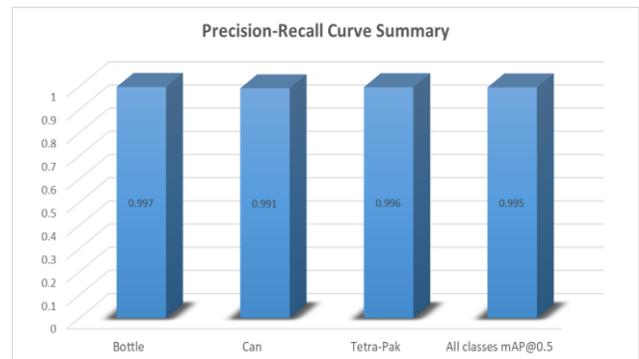


Fig. 15. Precision Recall Curve of the YOLOv5 Model.



Fig. 16. Sample of YOLOv5 Detection Outcome.

### C. Optimal Model Assessment with Live Feed Video

The live feed video application is done to gain insight how well the model works under real implementation scenario of the reverse vending machine. Basically the procedure will include the utilization of the webcam and the recyclable items will be slide within the camera field of view. Since based on the two model analysis the detection based architecture show a better outcome, analysis in this section was done for the detection module part only.

For the first assessment 10 samples for each class which total up to be 30 were feed in the webcam view while the detection algorithm running. The finding is PET bottle class has achieved 100% accuracy as the module correctly detects all of the input that has been fed simultaneously, whereas for aluminium can class, the module only achieved 80% accuracy and for the tetra-pak class 90% accuracy. Based from this outcome, it can be concluded that the module gained average of 90% accuracy in real implementation condition. Sample of the snapshot during experiment is shown in Fig. 17.



Fig. 17. Sample Snapshot during Live Feed Testing of the Detection Module.



Fig. 18. Result after the Detection Module has been Tested under Condition of more than Two Classes in one Frame.

For the second condition, samples of recyclable waste material will be put together in front of the webcam. The aim is to analyze module capability for detecting multiple samples in single feed of camera image. The result will be evaluated whether the module can detect the cluster precisely. Result obtained in this condition is recorded in Fig. 18 and it can be concluded that the module works well to fulfill the task by successfully detecting all the recycle materials given.

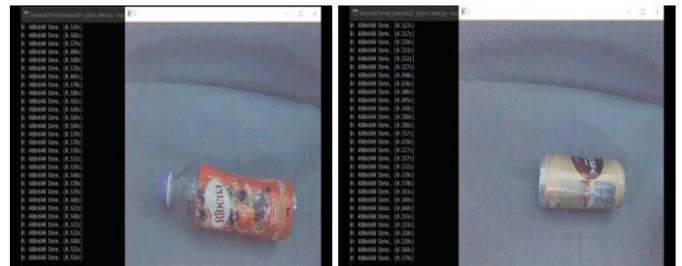


Fig. 19. Detection Result with Low Light Condition.

Finally, to imitate the real condition situation inside RVM, the detection module is tested under low light condition with only exposure from the natural light. The result can be seen in Fig. 19. This shows that, without proper lighting the module unable to works well and hence light source is crucial to guarantee system success. As for the computational cost during live feed assessment, based on the analysis of feeding the detection module with 314 images, it is found that in average the processing time is 482.1 millisecond for color image with dimension of 640x640. The processing speed is acceptable for RVM usage and can be further improve by incorporating GPU based controller such as NVIDIA Jetson Nano or by using OpenCV OAK-1 camera.

### IV. CONCLUSION

In this project, a CNN-based classification and detection module were investigated to be used as RVM verification module. Three class of sample which are PET bottle, aluminium can and tetra-pak are used during the training and validation stage with amount of 4961 and 937 respectively.

The highest performance model either from classification or detection was then undergo live feed video assessment under RVM implementation condition.

For the classification models, three CNN architecture were tested which are VGG-16, ResNet-50 and AlexNet. From series of training and fine tuning, it can be concluded that AlexNet model show high performance with 98% accuracy during training and 80% during validation stage, follow by ResNet-50 and then VGG-16. As for the detection model, YOLOv5 is used and it shows promising outcome with average of 99.5% mAP@0.5 accuracy based on the give training and validation data. Since the detection model show promising outcome compare to the classification model, it was further tested under RVM real implementation condition using a life feed webcam data. From the testing it can be concluded that, the system able to gain 90% accuracy during testing and apparently a good source of light is crucial to ensure the successfulness of the detection process.

The finding in this project is subject to several limitations that could be addressed in future research. First, the system is currently tested in a lab condition that simulating RVM functionality and hence future assessment in actual operation condition is in planning for system assessment. Second, most of the collected sample items were gathered locally and hence there is tendency that the system unable to detect recyclable items from beyond local brand. Finally, the detection model is currently tested with state of the art YOLO detector, in future, other type of detection algorithm such as single shot detector and RCNN variants can be assess to compare its outcome with the YOLO based platform.

#### ACKNOWLEDGMENT

This research is supported by Universiti Tun Hussein Onn Malaysia (UTHM) through Multidisciplinary Research Grant Scheme (MDR) (Vot. No. H495).

#### REFERENCES

- [1] Jereme, I. A., Siwar, C., & Alam, M. M. (2015, October). "Waste recycling in Malaysia: Transition from developing to developed country", *Indian Journal of Education and Information Management*, 4 (1), pp. 1- 14, 2015.
- [2] N.A. Mokhtar, "Malaysia masih ketinggalan dalam amalan kitar semula", *Berita Harian Online*, (2016, October 25).
- [3] R. Tomari, A. A. Kadir, W.N.W Zakaria, M. F. Zakaria, M.H.A Wahab & M.H. Jabbar, "Development of Reverse Vending Machine (RVM) Framework for Implementation to a Standard Recycle Bin", *Procedia Computer Science*, vol. 105, pp. 75-80, 2017.
- [4] R. Tomari, M. F. Zakaria , A. A. Kadir, W.N.W Zakaria, M.H.A Wahab , "Empirical Framework of Reverse Vending Machine (RVM) with Material Identification Capability to Improve Recycling", *Applied Mechanics and Materials*, pp. 114-119, 2019.
- [5] M. Yang and G. Thung, "Classification of trash for recyclability status", *CS229 Project Report* 2016, 2016.
- [6] A. N. Kokoulin, A. I. Tur and A. A. Yuzhakov, "Convolutional neural networks application in plastic waste recognition and sorting," 2018 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIconRus), Moscow, 2018, pp. 1094-1098.
- [7] A. N. Kokoulin and D. A. Kiryanov, "The Optical Subsystem for the Empty Containers Recognition and Sorting in a Reverse Vending Machine," 2019 4th International Conference on Smart and Sustainable Technologies (SpliTech), Split, Croatia, 2019, pp. 1-6,
- [8] C. Bircanoğlu, M. Atay, F. Beşer, Ö. Genç, & M. A. Kızrak, "RecycleNet: Intelligent Waste Sorting using Deep Neural Networks", In 2018 Innovations in Intelligent Systems and Applications (INISTA). 2018, pp. 1-7.
- [9] U. Ozkaya and L. Seyfi, "Fine-Tuning Models Comparisons on Garbage Classification for Recyclability", *arXiv preprint*, arXiv:1908.04393, 2019.
- [10] Z. Dimitris, T. Dimitris, B. Nikolaos and D. Minas, "A Distributed Architecture for Smart Recycling Using Machine Learning", *Future Internet*, 12, 141, 2020, pp 1-13.
- [11] W.-L. Mao, W.-C. Chen, C.-T. Wang, Y.-H. Lin, "Recycling waste classification using optimized convolutional neural network", *Resources, Conservation and Recycling*, vol.164, 2021, 105132,
- [12] H. Zheng and Y. Gu, "EnCNN-UPMWS:Waste Classification by a CNN Ensemble Using the UPM Weighting Strategy", *Electronics*, 10, 427, 2021.
- [13] K. Simonyan, A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition", *arXiv preprint*, arXiv: 1409.1556, 2014.
- [14] K. He, X. Zhang, S. Ren, J. Sun, "Deep Residual Learning for Image Recognition", *arXiv preprint*, arXiv: 1512.03385v1, 2015.
- [15] A. Krizhevsky, I. Sutskever, G.E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks", In *Proc. of 25th International Conference on Neural Information Processing System*, vol. 1, 2012, pp. 1097-1105.
- [16] J. Redmon, S. Divvala, R. Girshick, and A. Farhadi, "You only look once: Unified, real-time object detection," *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit.*, vol. 2016-Decem, pp. 779–788, 2016.
- [17] J. Redmon and A. Farhadi, "YOLO9000: Better, faster, stronger," *Proc. - 30th IEEE Conf. Comput. Vis. Pattern Recognition, CVPR 2017*, vol. 2017-January, pp. 6517–6525, 2017.
- [18] J. Redmon and A. Farhadi, "YOLOv3: An Incremental Improvement," *arXiv preprint arXiv:1804.02767*, 2018.2018.
- [19] A. Bochkovskiy, C.-Y. Wang, and H.Y. M. Liao. Yolov4: Optimal speed and accuracy of object detection. *arXiv preprint arXiv:2004.10934*, 2020.
- [20] G. Jocher, A. Stoken, J. Borovec, NanoCode012, A. Chaurasia, TaoXie, L. Changyu, Abhiram V, Laughing, tkianai, yxNONG, A. Hogan, lorenzomamma, AlexWang1900, J. Hajek, L. Diaconu, Marc, Y. Kwon, oleg, wanghaoyang0106, Y. Defretin, A. Lohia, ml5ah, Ben Milanko, Benjamin Fineran, Daniel Khromov, DingYiwei, Doug, Durgesh, andFrancisco Ingham. ultralytics/yolov5: v5.0 -YOLOv5-P6 1280 models, AWS,Supervise.ly and YouTube integrations, Apr. 2021
- [21] C.Y. Wang, H.Y. Mark Liao, Y.H. Wu, P.Y. Chen, J.W. Hsieh, I.H. Yeh, "CSPNet: A new Backbone that can Enhance Learning Capability of CNN". In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR 2020)*, June 2020; pp. 390–391.
- [22] K. Wang, J.H. Liew, Y. Zou, D. Zhou, J. Feng, " PANET: Few-shot image semantic segmentation with prototype alignment", In *Proceedings of the IEEE International Conference on Computer Vision (ICCV 2019)*, Seoul, Korea, 2019,pp. 9197– 9206.

# How to Analyze Air Quality During the COVID-19 Pandemic? An Answer using Grey Systems

Alexi Delgado<sup>1</sup>, Denilson Pongo<sup>2</sup>, Katherine Felipa<sup>3</sup>, Kiara Saavedra<sup>4</sup>, Lorena Torres<sup>5</sup>, Lourdes Serpa<sup>6</sup>, Ch. Carbajal<sup>7</sup>

Mining Engineering Section, Pontificia Universidad Católica del Perú, Lima, Peru<sup>1</sup>

Environmental Engineering Department, National University of Engineering, Lima, Peru<sup>2,3,4,5,6</sup>

Administration Program, Universidad de Ciencias y Humanidades, Lima, Peru<sup>7</sup>

**Abstract**—The Peruvian government declared a State of National Emergency due to the spread of COVID-19 where the closure of businesses, companies and home isolation was imposed from 03/15/2020 to 06/30/2020. In this context, the research focused on analyzing the characteristics of the air quality in Lima during said period compared to its similar in 2018 and 2019, for this purpose, data from two air quality monitoring stations in PM<sub>2.5</sub>, PM<sub>10</sub>, CO and NO<sub>2</sub> concentrations and the quality levels given by the Air Quality Index (INCA) were used for further processing with the Grey Clustering method, which is based on grey systems. The results showed that during the quarantine, air quality improved significantly, specifically the northern area of Lima, which was favored by the meteorological conditions that will be classified as good quality as well as the reduction of PM<sub>10</sub> by 46% and PM<sub>2.5</sub> in 45% to a lesser extent, NO<sub>2</sub> by 17% and CO in 11%, unlike the southern zone which, although it showed an improvement, it is still classified as moderate quality with reductions in PM<sub>10</sub> by 26%, PM<sub>2.5</sub> by 27%, CO by 19%.; however the concentration NO<sub>2</sub> registered a non-significant increase of 2%. This behaviour is explained by the lower height of the thermal inversion layer, therefore less space for the dispersion of pollutants. Finally, the study obtains essential information for regulatory agencies as it allows understanding the relationship between air quality and control measures at emission sources for the development of public policies on public health and the environment.

**Keywords**—Air quality; COVID 19; grey systems; grey clustering

## I. INTRODUCTION

On March 11, 2020, the World Health Organization (WHO) declared that the COVID 19 - disease caused by the new coronavirus SARS-CoV-2-went from being an epidemic to a pandemic [1]. In Perú, the first confirmed case was reported on March 6, 2020, in Lima, a young man had arrived from a trip to the European continent. To date March 16, there were 86 positive cases of coronavirus, being Lima the department with the highest number (70 cases) [2].

To control the increase in the number of cases confirmed by coronavirus, Peru declared a national state of emergency for a period of 15 days, during which it was decided to establish mandatory social isolation (quarantine), a measure that came into effect March 16. During the quarantine period, public access to premises and establishments (restaurants, museums, cultural, sports and leisure activities, among others) was suspended, except for commercial establishments for the

acquisition of food and basic necessities. Due to the increase in coronavirus cases, the quarantine was extended until June 30.

During and after the declaration of the state of emergency in the country, an extraordinary measure to stop the advance of the coronavirus (COVID-19), it was possible to verify the downward trend in air pollutants such as particulate matter smaller than 2.5  $\mu\text{m}$  diameter (PM 2.5), Lima. During the quarantine days, the environment had a respite and the improvement was evident, as demonstrated by the measurements taken by MINAM which indicated that the air quality in Lima reached the levels recommended by World Health Organization. In addition, there was a reduction in the average concentrations of other parameters, which meant a gradual improvement in air quality in the city, increased by the effect of the reduction in emissions due to the suppression of the flow of vehicles as a result of the mandatory social isolation.

Likewise, in the international context concerning air quality, there is evidence in research conducted in several countries, for example [3], analyzed the results of air quality monitoring and meteorological data recorded in Wuhan in the period from January to May 2020, finding that the Air Quality Index (AQI) reached 90.1% in January-April 2020 being significantly higher than the index recorded in 2017 of 71.9%, in 2018 of 70% and in 2019 of 72.5%, they also found that SO<sub>2</sub>, NO<sub>2</sub>, CO, PM<sub>10</sub> and PM<sub>2.5</sub> concentrations decreased by 6.95%, 38.23 %, 18.24%, 30.25% and 32.92% respectively from 2019 to 2020. Moreover [4], in Brazil, also evaluated the impact of the partial closure of activities such as shopping centers, restaurants, schools and universities on air quality in the state of São Paulo as a measure to stop the advance of COVID-19, for this they analyzed the monthly average concentrations of February, March and April from three air quality stations: Marginal Tietê, Marginal Pinheiros and Downtonwn from the period 2015-2019 for the registered in 2020, they observed significant reductions of NO up to 77.3%, NO<sub>2</sub> by up to 54.3%, CO by up to 64.8% and PM<sub>2.5</sub> by 29.8%.

For the development of the assessment, the Grey Clustering method, which is based on grey systems, specially, the Center-point Triangular Whitenization Weight Functions (CTWF) method and the Entropy weighting method, based on Shannon's entropy, to calculate objective weights for the evaluation criteria within the CTWF method, was used. In this sense, the objective of this study was to evaluate air quality using an artificial intelligence model based on the Grey

Clustering method and Shannon entropy in Lima, Peru before and during the period of total confinement due to the COVID-19 pandemic [5].

## II. MATERIALS AND METHODS

The impact of total confinement on air quality in the city of Metropolitan Lima was evaluated by analyzing the records of the monitoring stations of the National Meteorology and Hydrology Service (SENAMHI by its Spanish acronym) regarding the concentrations of PM10, PM2.5, NO2 and CO. from March 16 to June 30, 2021 (period of total confinement) and its similar in 2018 and 2019.

### A. Metropolitan Lima

Lima is the capital of Peru and the fifth most populous city in Latin America with a population of 9,485,405 people [5]. It is located on the shores of the Pacific Ocean on the Central Coast of Peru with an area of 2,819 km<sup>2</sup> as shown in Fig. 1.



Fig. 1. Geographical Location of Metropolitan Lima, Peru.

According to a study carried out by MINAM in 2014 on mortality and morbidity as a result of air pollution in Metropolitan Lima, 1220 cases of deaths associated with PM10 pollution were found, with respiratory diseases (468 cases) and cardiovascular diseases (165 cases) of higher incidence, being the vehicle fleet the main source of contamination characteristic of an old low-maintenance vehicle fleet [6] [7].

### B. Methodology

In this section, we describe the Grey Clustering method (GCM), which can be described as follows: first, suppose the area is set of  $m$  objects, a set of  $n$  criteria, and a set of  $s$  Grey classes, according to the sample value ( $i = 1, 2, \dots, m; j = 1, 2, \dots, n$ ). Then, the steps of the method can be developed with the following points according to different research.

#### Step 1: Determination of Center Points

The ranges of the criteria are divided into 4 Grey classes, and then their central points are  $\lambda_1, \lambda_2, \dots, \lambda_s$ , this is determined by the Air Quality Index (INCA).

#### Step 2: Dimension Removal

Dimension Removal of values of the Environmental Quality Index: For this second step we have the matrix "I" of

values of the Environmental Quality Index  $I = \{I_{ij}, i = 1, 2, 3, \dots, m; j = 1, 2, 3, \dots, n\}$ , in which "i" represents the central points of the air quality parameters: PM10 (ug / m<sup>3</sup>), PM 2.5 (ug / m<sup>3</sup>), NO<sub>2</sub> (ug / m<sup>3</sup>) and CO (ug / m<sup>3</sup>) and "j" are the quality levels according to INCA: Good, Moderate, Bad and Threshold of care. And we proceed to normalize said matrix into a new matrix "A<sub>ij</sub>", using (1).

$$A_{ij} = \left( \frac{I_{ij}}{\sum_{j=1}^n I_{ij}} \right) \quad (1)$$

Dimension Removal of Sampling data: In the same way as the dimension removal of standard data, it is performed for sampling data, whose matrix is  $M = \{M_{ij}, i = 1, 2, 3, \dots, m; j = 1, 2, 3, \dots, n\}$ , in which "i" represents the sampled air quality parameters and "j" are the sampling stations. Followed, we proceed to normalize the matrix M in a new matrix "B<sub>ij</sub>", using (2).

$$B_{ij} = \left( \frac{M_{ij}}{\sum_{j=1}^n M_{ij}} \right) \quad (2)$$

#### Step 3: Triangular Functions and their Values

The Grey classes are expanded according to the analyzed air quality parameters, this provides us with four quality levels for each parameter, so we will have 4 functions for each parameter or criterion used. These functions will have the form as shown in (3).

$$f_j^k(X_{ij}) \quad (3)$$

Then, we have the triangular functions as represented in (4) – (6).

$$f_j^2(X_{ij}) = \left\{ 0, x \notin [0, \lambda_j^2]; 1, x \in [0, \lambda_j^2]; \frac{\lambda_j^2 - x}{\lambda_j^2 - \lambda_j^1}, x \in [\lambda_j^1, \lambda_j^2] \right\} \quad (4)$$

$$f_j^k(X_{ij}) = \left\{ 0, x \notin [\lambda_j^{k-1}, \lambda_j^{k+1}]; \frac{\lambda_j^{k+2} - x}{\lambda_j^{k+1} - \lambda_j^k}, x \in [\lambda_j^k, \lambda_j^{k+1}]; \frac{x - \lambda_j^{k-1}}{\lambda_j^k - \lambda_j^{k-1}}, x \in [\lambda_j^{k-1}, \lambda_j^k] \right\} \quad (5)$$

$$f_j^4(X_{ij}) = \left\{ 0, x \notin [\lambda_j^3, +\infty]; \frac{x - \lambda_j^3}{\lambda_j^4 - \lambda_j^3}, x \in [\lambda_j^3, \lambda_j^4]; 1, x \in [\lambda_j^4, +\infty] \right\} \quad (6)$$

#### Step 4: Determination of the Weight for each Criteria

To eliminate the uncertainty regarding the calculation of the weight of the criteria, the Shannon entropy weighting method will be applied. Shannon developed measure H which satisfies the following properties for all  $p_i$  within an estimated joint probability distribution [7] [8].

- $H$  is a continuous positive function.
- $H$  should be a monotonic increasing function of  $n$  if all  $p_i$  is equivalent and  $p_i = 1/n$ .
- For all  $n \geq 2, H(p_1, p_2, \dots, p_n) = h(p_1, p_2, \dots, p_n) + (p_1 + p_2)H\left(\frac{p_1}{p_1+p_2}, \frac{p_2}{p_1+p_2}\right)$ .

Shannon showed that the only function which satisfies these properties is obtained by (7).

$$H_{Shannon} = -\sum_i^n p_i \log(p_i) \quad (7)$$

Where:  $0 \leq p_i \leq 1; \sum_{j=1}^n p_j = 1$ .

As shown above, it is assumed that there are  $m$  objects and  $n$  evaluation criteria, which form the following matrix  $X = \{x_{ij}, i = 1, 2, \dots, m; j = 1, 2, \dots, n\}$  [9]. After that, the steps to determine the weights under Shannon entropy are shown:

1) The matrix  $X = \{x_{ij}, i = 1, 2, \dots, m; j = 1, 2, \dots, n\}$  is normalized for each criterion  $C_j (j = 1, 2, \dots, n)$ . The normalization evaluates  $P_{ij}$  are calculated using (8).

$$f_j^1(x_{ij})P_{ij} = \frac{x_{ij}}{\sum_{i=1}^m x_{ij}} \quad (8)$$

2) The entropy of each criterion is calculated using (9).

$$H_j = -k \sum_{i=1}^m P_{ij} \ln(p_i) \quad (9)$$

Where  $k$  is a constant,  $k = (\ln(m))^{-1}$

3) The degree of divergence of the intrinsic information in each criterion  $C_j$  is calculated using (10).

$$div_j = 1 - H_j \quad (10)$$

4) In the weight entropy  $w_j$  of each criterion  $C_j$ , we have to use (11).

$$w_j = n_j = \frac{div_j}{\sum_{j=1}^n div_j} \quad (11)$$

Step 5: Determination of the Clustering coefficient

The classification coefficient "ik" for each sampling station "i = 1, 2, 3, ..., m", with respect to the grey classes "j = 1, 2, 3, ..., n", is calculated using (12).

$$\sigma_i^k = \sum_{j=1}^n f_j^k(X_{ij})n_j \quad (12)$$

Where the triangular function of each class of Grey with respect to each criterion is analyzed, while  $n_j$  are the weights of each criterion [9].

Step 6: Results using the highest Clustering coefficient

Finally, as the last step, the maximum value of the clustering coefficient is calculated [10]:

$$\max_{1 \leq k \leq s} \{\sigma_i^k\} = \sigma_i^k \quad (13)$$

In this way, it will be observed what kind of flock is found in each station studied.

### III. RESULTS AND DISCUSSION

#### A. Method Application

Step 1: Definition of Study Objects

Data from two air quality monitoring stations in Villa María del Triunfo and Carabayllo located south and north of Lima, respectively, were used; both stations managed by the National Meteorology and Hydrology Service (also known as

SENAMHI by its Spanish acronym) of Peru. The parameters analyzed were nitrogen dioxide (NO<sub>2</sub>), carbon monoxide (CO), particulate matter smaller than 10 μm in diameter (PM<sub>10</sub>) and smaller than 2.5 μm in diameter (PM<sub>2.5</sub>) during the period of mandatory social isolation, declared by the Peruvian State in the framework of the National Emergency because of the COVID-19 pandemic from March 16 to June 30, 2020 and what registered in the same period in 2018 and 2019. Table I details the location of the stations represented in Fig. 2.

TABLE I. AIR QUALITY MONITORING STATIONS IN METROPOLITAN LIMA

Station	Code	Coordinates (WGS84)		Sampling height
		East	North	
Villa Maria del Triunfo	VMT	291084	8654309	3m
Carabayllo	CAR	278498	8683451	6m

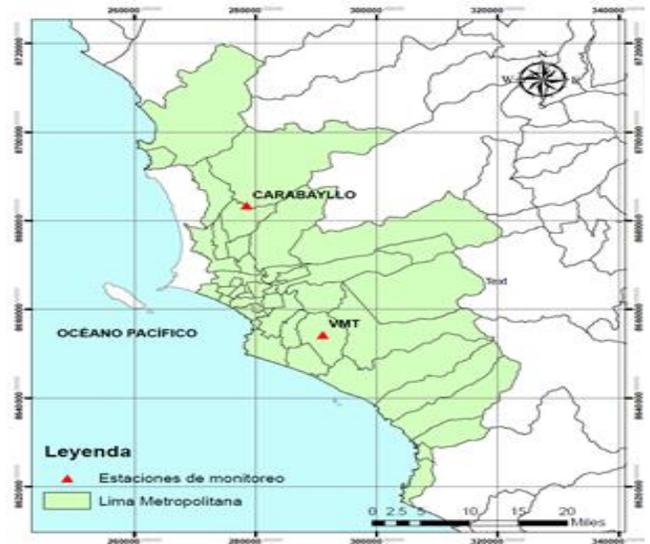


Fig. 2. Air Quality Monitoring Stations in Metropolitan Lima, Peru.

#### Step 2: Definition of Criteria

The evaluation criteria for the present study are determined by the air quality parameters presented in Table II.

TABLE II. CRITERIA FOR AIR QUALITY ASSESSMENT

Criteria	Units	Notation
PM <sub>10</sub>	ug/m <sup>3</sup>	C <sub>1</sub>
PM <sub>2.5</sub>	ug/m <sup>3</sup>	C <sub>2</sub>
NO <sub>2</sub>	ug/m <sup>3</sup>	C <sub>3</sub>
CO	ug/m <sup>3</sup>	C <sub>4</sub>

#### Step 3: Definition of the Grey classes

The classes for the evaluation are four and are based on the air quality levels according to the Air Quality index in Peru according to RM-N°-181-2016-MINAM and D.S. N° 003-2017-MINAM, which are presented in Table III.

TABLE III. AIR QUALITY INDEX STANDARD DATA FOR AIR QUALITY ASSESSMENT

Criteria	Grey Classes			
	Good	Moderate	Poor	Threshold of Care
PM <sub>10</sub>	0-50	51-100	101-200	>200
PM <sub>2.5</sub>	0-12.5	12.6-25	25.1-125	>125
NO <sub>2</sub>	0-100	101-200	201-300	>300
CO	0-5049	5050-10049	10050-15049	>15050

Step 4: Calculations using the CTWF Method

The calculations based on the Grey Clustering method are presented below:

1) Based on the air quality index in Peru, the central values of the parameters to be analysed are obtained. These values are shown in Table IV.

TABLE IV. CENTRAL VALUES OF THE AIR QUALITY INDEX IN PERU

Parameter	Good (λ <sub>1</sub> )	Moderate (λ <sub>2</sub> )	Poor (λ <sub>3</sub> )	Threshold of care (λ <sub>4</sub> )
PM <sub>10</sub>	37.5	113.0	200.5	288.0
PM <sub>2.5</sub>	6.3	18.8	75.0	131.3
NO <sub>2</sub>	50.0	150.5	250.5	350.5
CO	2524.5	7549.5	12549.5	17549.5

2) The non-dimensioned standard values for each parameter, according to the air quality index in Peru, were determined through (1). These values are presented in Table V.

TABLE V. NON-DIMENSIONAL STANDARD VALUE OF THE AIR QUALITY INDEX

Parameter	Good (λ <sub>1</sub> )	Moderate (λ <sub>2</sub> )	Poor (λ <sub>3</sub> )	Threshold of care (λ <sub>4</sub> )
C <sub>1</sub>	0.235	0.707	1.255	1.803
C <sub>2</sub>	0.108	0.325	1.297	2.270
C <sub>3</sub>	0.250	0.751	1.250	1.749
C <sub>4</sub>	0.251	0.752	1.250	1.747

Similarly, based on the results of the air quality monitoring stations in Metropolitan Lima, the values without dimension were obtained for each parameter of the 2 selected monitoring stations. These values are presented in Table VI.

TABLE VI. NON-DIMENSIONAL MONITORING DATA IN METROPOLITAN LIMA

Parameter	2018-2019 period		2020 period	
	VMT	CAR	VMT	CAR
C <sub>1</sub>	0.808	0.611	0.598	0.329
C <sub>2</sub>	0.487	0.428	0.353	0.235
C <sub>3</sub>	0.113	0.073	0.116	0.061
C <sub>4</sub>	0.082	0.117	0.066	0.105

Step 5: Triangular Whitenization Functions

With Table V, the triangular whitenization functions and the values for each parameter were determined as shown in Fig. 3.

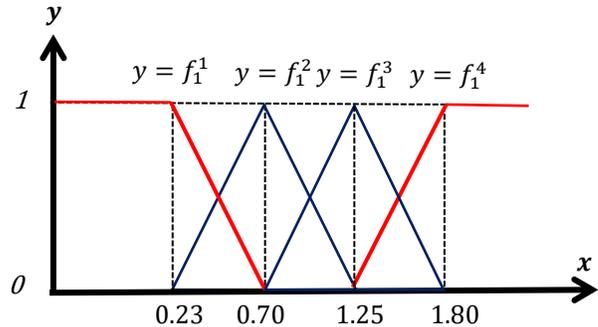


Fig. 3. CTWF for the Parameter of Particles with a Diameter of Less than 10 μm Parameter (PM<sub>10</sub>).

Therefore, the expressions (14) – (17) were obtained.

$$f_1^1(x) = \begin{cases} 1, & x \in [0, 0.235] \\ \frac{0.707-x}{0.707-0.235} & x \in [0.235, 0.707] \\ 0 & x \in [0.707, \infty] \end{cases} \quad (14)$$

$$f_1^2(x) = \begin{cases} 0, & x \notin [0.235, 1.255] \\ \frac{x-0.235}{0.707-0.235} & x \in [0.235, 0.707] \\ \frac{1.255-x}{1.255-0.707} & x \in [0.707, 1.255] \end{cases} \quad (15)$$

$$f_1^3(x) = \begin{cases} 0, & x \notin [0.707, 1.803] \\ \frac{x-0.707}{1.255-0.707} & x \in [0.707, 1.255] \\ \frac{1.803-x}{1.803-1.255} & x \in [1.255, 1.803] \end{cases} \quad (16)$$

$$f_1^4(x) = \begin{cases} 1, & x \in [1.803, \infty] \\ \frac{x-1.255}{1.803-1.255} & x \in [1.255, 1.803] \\ 0 & x \in [0, 1.255] \end{cases} \quad (17)$$

Then, the values obtained for each period and location are displayed in Table VII and Table VIII.

TABLE VII. VALUES OF CTWF FOR VMT

Period of 2018-2019	f <sub>j(x)</sub> <sup>1</sup>	f <sub>j(x)</sub> <sup>2</sup>	f <sub>j(x)</sub> <sup>3</sup>	f <sub>j(x)</sub> <sup>4</sup>
C <sub>1</sub>	0.000	0.816	0.183	0.000
C <sub>2</sub>	0.000	0.833	0.167	0.000
C <sub>3</sub>	1.000	0.000	0.000	0.000
C <sub>4</sub>	1.000	0.000	0.000	0.000
Period of 2020	f <sub>j(x)</sub> <sup>1</sup>	f <sub>j(x)</sub> <sup>2</sup>	f <sub>j(x)</sub> <sup>3</sup>	f <sub>j(x)</sub> <sup>4</sup>
C <sub>1</sub>	0.232	0.768	0.000	0.000
C <sub>2</sub>	0.000	0.971	0.029	0.000
C <sub>3</sub>	1.000	0.000	0.000	0.000
C <sub>4</sub>	1.000	0.000	0.000	0.000

TABLE VIII. VALUES OF CTWF FOR CAR

Period of 2018-2019	$f_{j(x)}^1$	$f_{j(x)}^2$	$f_{j(x)}^3$	$f_{j(x)}^4$
$C_1$	0.203	0.797	0.000	0.000
$C_2$	0.000	0.894	0.106	0.000
$C_3$	1.000	0.000	0.000	0.000
$C_4$	1.000	0.000	0.000	0.000
Period of 2020	$f_{j(x)}^1$	$f_{j(x)}^2$	$f_{j(x)}^3$	$f_{j(x)}^4$
$C_1$	0.800	0.200	0.000	0.000
$C_2$	0.417	0.583	0.000	0.000
$C_3$	1.000	0.000	0.000	0.000
$C_4$	1.000	0.000	0.000	0.000

Step 6: Definition of the Clustering Weight

The clustering weight ( $\eta_i$ ) of each parameter was determined using Shannon entropy. For this, the following procedure:

1) The values of the parameters of the Air Quality index were normalized. These values are presented in Table IX.

TABLE IX. NORMALIZED VALUES OF EACH PARAMETER

Parameter	Good ( $\lambda_1$ )	Moderate ( $\lambda_2$ )	Poor ( $\lambda_3$ )	Threshold of care ( $\lambda_4$ )
$C_1$	0.059	0.177	0.314	0.451
$C_2$	0.027	0.081	0.324	0.568
$C_3$	0.063	0.188	0.313	0.437
$C_4$	0.063	0.188	0.313	0.437

2) The entropy  $H_j$  of each criterion  $C_j$  was calculated through (9). The results are presented in Table X.

TABLE X. VALUES FOR EACH PARAMETER

Entropy	$C_1$	$C_2$	$C_3$	$C_4$
$H_j$	0.863	0.713	0.875	0.875
Degree of divergence	$C_1$	$C_2$	$C_3$	$C_4$
$div_j$	0.137	0.287	0.125	0.125
Clustering Weight	$C_1$	$C_2$	$C_3$	$C_4$
$W_j = \eta_j$	0.204	0.426	0.186	0.185

Step 7: Definition of the Clustering Coefficients

The values of the clustering coefficients ( $\sigma_i^k$ ) were calculated using (12). Then, the results for each period and location are displayed in Table XI and Table XII.

TABLE XI. VALUES OF CLUSTERING COEFFICIENTS FOR VMT

Period of 2018-2019	$f_{j(x)}^1$	$f_{j(x)}^2$	$f_{j(x)}^3$	$f_{j(x)}^4$
$\sigma_j^k$	0.371	0.521	0.108	0.000
Period of 2020	$f_{j(x)}^1$	$f_{j(x)}^2$	$f_{j(x)}^3$	$f_{j(x)}^4$
$\sigma_j^k$	0.418	0.569	0.012	0.000

TABLE XII. VALUES OF CLUSTERING COEFFICIENTS FOR CAR

Period of 2018-2019	$f_{j(x)}^1$	$f_{j(x)}^2$	$f_{j(x)}^3$	$f_{j(x)}^4$
$\sigma_j^k$	0.412	0.543	0.045	0.000
Period of 2020	$f_{j(x)}^1$	$f_{j(x)}^2$	$f_{j(x)}^3$	$f_{j(x)}^4$
$\sigma_j^k$	0.711	0.289	0.000	0.000

Step 8: Definition of Maximum Clustering Coefficient

Finally, the condition was applied: if  $\max \{\sigma_i^k\} = \sigma_i^{k^*}$  it is decided that the object  $i$  belongs to the Grey class  $k^*$ ; for each monitoring station. Therefore, the maximum value obtained is presented in Table XIII.

TABLE XIII. VALUES OF MÁX  $\sigma_i^{k^*}$  AND AQI

Station	2018-2019 period		2020 period	
	Max $\sigma_j^k$	Air Quality Index	Max $\sigma_j^k$	Air Quality Index
VMT	0.521	Moderate	0.569	Moderate
CAR	0.543	Moderate	0.711	Good

B. Discussion about Results on the Case Study

On March 15, a state of emergency was decreed, making Peru the first country in South America to take strict measures to prevent an increase in positive cases of COVID 19. These measures include mandatory social isolation (through a national blockade) and a complete blockade of the border, starting on March 16. On March 18, a curfew was enacted to support mandatory social distancing measures because people did not adhere to lockdown restrictions, and the use of private vehicles was banned as of March 19. Despite all the health measures implemented, the number of confirmed cases in Peru exceeded 100,000 on May 20 [2]. The impact of the measures implemented during the state of emergency was to stop production activities, as reflected by electricity consumption [2].

The decrease in electricity demand reflects the freezing of production activities and possible sources of emissions of atmospheric pollutants. By June 30, 2020, air pollution in the two stations, in terms of PM10, PM2.5 and NO2 and CO2, had decreased (Table XIII), it is observed that there was an improvement in air quality in the station of CAR, being the index of good air quality, while in the VMT station it remains moderate. Likewise, compared to the historical period (the previous two years 2018-2019), it is show that the air quality index in the VMT and CAR stations is moderate [11].

Based on these results from the stations air quality it can be inferred that the northern part as well as the southern part of the territory of Metropolitan Lima has air quality problems, and with measures proposed by the state of emergency it has improved. This due to the fact that, as we can see in Fig. 4, the variation of the concentration of the four parameters during the years 2016 - 2020 for the period of March - June in CAR station, taking into account that the data from the years 2018 were used to perform the calculations of the study - 2019 (period without quarantine) and 2020 (period in quarantine), and show that during the years analyzed a reduction in concentration is observed for the four parameters. On the other hand, in the graph for the PM 2.5 parameter, no information is recorded for the year 2017, so only a trend line was drawn.

Followed, a summarize of the graphic representation is shown in Fig. 5 for a better understanding of the data obtained from the parameters studied in Carabayllo (CAR).

On the other hand, the variation of the concentration of the four parameters is shown in Fig. 6, during the years 2016 -

2020 for the months of March – June in VMT station, taking into account that the data from the years 2018 were used to perform the calculations of the study - 2019 (period without quarantine) and 2020 (period in quarantine). The values show that during the years analyzed a reduction in concentration is observed for the parameters of PM10, PM2.5 and CO, while NO2 shows an increase of around 2%, this can be explained because an average of the years 2018 - 2019, which present a considerable variation of the parameter.

Followed, a summarize of the graphic representation is shown in Fig. 7 for a better understanding of the data obtained from the parameters studied in Villa Maria del Triunfo (VMT).

The dispersion of pollutants in the atmosphere is subject to the meteorological and geographical conditions of the specific place for the city of Lima, the factors that influence the most is the atmospheric layer of thermal inversion and the action of the winds, the latter during March. In 2020, it presented a predominant direction from south to north of Lima with average daily velocity values of 2 to 4 m / s at a height of 10 m from the Surface [12], as shown in Fig. 8.

On the other hand, with respect to the atmospheric layer of thermal inversion, a lower height was evidenced in March 2020 in the southern area of Lima compared to the other areas. It is clear that in the VMT station the height is on average 300 m different from the Carabayllo station with a height above 400 m.

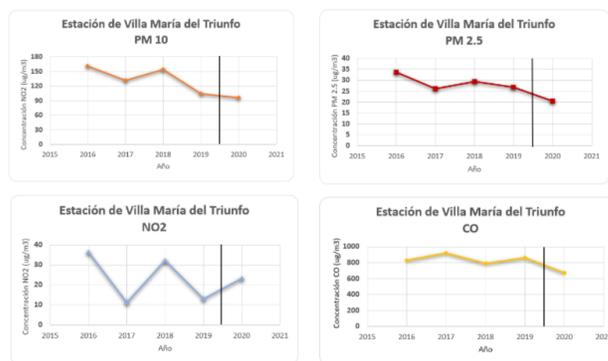


Fig. 6. Graphic Representation for the Four Parameters at Villa Maria del Triunfo (VMT).



Fig. 7. Graphic Representation Summarize for the Four Parameters at Villa Maria del Triunfo (VMT).

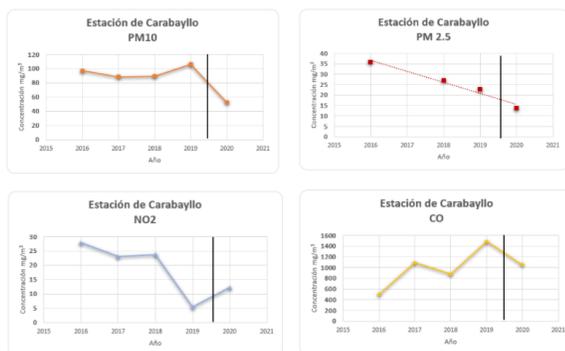


Fig. 4. Graphic Representation for the Four Parameters at Carabayllo (CAR).



Fig. 5. Graphic Representation Summarize for the Four Parameters at Carabayllo (CAR).

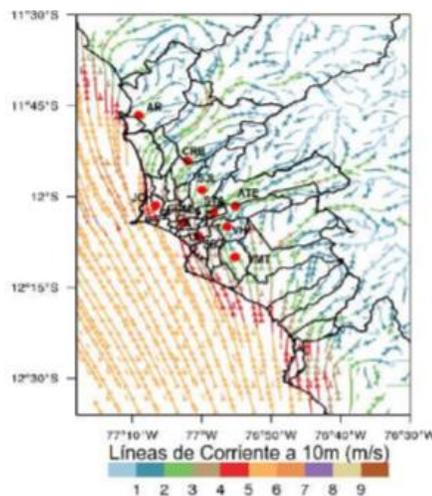


Fig. 8. Power Lines at 10m High during March 2020 in Lima.

Therefore, North Lima evidenced better dispersion conditions than South Lima during March 2020, based on the greater space available for the dispersion of pollutants (greater height of the planetary boundary layer) with respect to wind conditions; the conditions were similar in both areas, as shown in Fig. 9.

In this sense, the CAR station registered a more substantial improvement in air quality during the quarantine period compared to the VMT station because it is located in the north and south of Lima, respectively [13].

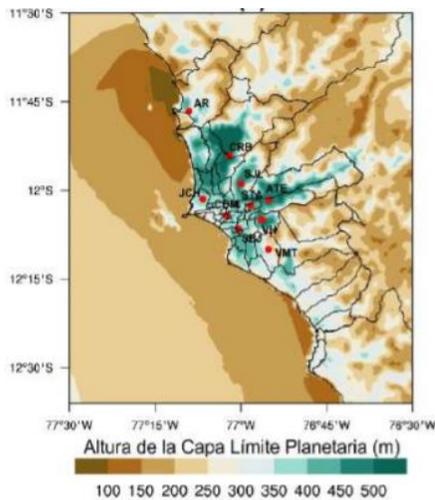


Fig. 9. Average Height of the Planetary Boundary Layer in Lima during March 2020.

### C. Discussion about the Methodology

Unlike the studies carried out in China and Brazil of air quality during the COVID-19 pandemic, the present work carried out a comprehensive methodology using the Grey Clustering method and the Shannon entropy for the same study.

The Grey Clustering method is the most appropriate in matters of high uncertainty [14], such as the evaluation of air quality, where each parameter varies according to environmental conditions.

On the other hand, the Shannon entropy method is very suitable for evaluating air quality after determining the grouping weights ( $\eta_j$ ) for each parameter objectively, without the need to consult an expert and that reduces evaluation costs. Furthermore, this method has multiple applications such as in studies of social conflicts or social impact evaluations [15], due to its great capacity to process information and reduce subjectivity in evaluations.

### IV. CONCLUSION

The air quality in Metropolitan Lima during the national closure in the framework of the state of emergency due to COVID-19 presented significant improvements compared to its similar in 2018-2019; specifically the north of Lima was also favored by the meteorological conditions. This allowed its classification as good quality, unlike the southern zone, which although it showed an improvement, the classification remains of moderate quality.

The Grey Clustering methodology made it possible to evaluate air quality in a comprehensive way based on the most relevant atmospheric pollutants in the study area, unlike conventional methodologies that evaluate individually with respect to each parameter, and also considers the uncertainty within the This analysis is therefore also applicable to problems with insufficient data, on the other hand, in reference to Shannon's entropy, it was possible to determine the weights

of the parameters in an objective manner, free of subjective assessments.

The work generates information of vital importance for future research on air quality using the Grey Clustering methodology as well as its integration into environmental regulatory bodies.

### REFERENCES

- [1] A. O. Strontsitska, O. Pavliuk, R. Dunaev, and R. Derkachuk, "Forecast of the number of new patients and those who died from COVID-19 in Bahrain," 2020 Int. Conf. Decis. Aid Sci. Appl. DASA 2020, pp. 422–426, Nov. 2020, doi: 10.1109/DASA51403.2020.9317122.
- [2] J. A. Lossio-Ventura, H. Alatrística-Salas, K. Barrena, E. Linos, M. Nunez-Del-Prado, and A. Talavera, "DYVIC: DYnamic Virus Control in Peru," Proc. - 2020 IEEE Int. Conf. Bioinforma. Biomed. BIBM 2020, pp. 2264–2267, Dec. 2020, doi: 10.1109/BIBM49941.2020.9313419.
- [3] J. C. et al., "Air quality characteristics in Wuhan (China) during the 2020 COVID-19 pandemic," Environ. Res., vol. 195, Apr. 2021, doi: 10.1016/J.ENVRES.2021.110879.
- [4] L. Y. K. Nakada and R. C. Urban, "COVID-19 pandemic: Impacts on the air quality during the partial lockdown in São Paulo state, Brazil," Sci. Total Environ., vol. 730, p. 139087, Aug. 2020, doi: 10.1016/J.SCITOTENV.2020.139087.
- [5] S. Tabik et al., "COVIDGR Dataset and COVID-SDNet Methodology for Predicting COVID-19 Based on Chest X-Ray Images," IEEE J. Biomed. Heal. Informatics, vol. 24, no. 12, pp. 3595–3605, Dec. 2020, doi: 10.1109/JBHI.2020.3037127.
- [6] R. M. Arias Velásquez, Y. L. Romero Ramos, and J. Noel, "Citizen science approach for spatiotemporal modelling of air pollution quality and traffic in Lima, Peru," SHIRCON 2019 - 2019 IEEE Sci. Humanit. Int. Res. Conf., Nov. 2019, doi: 10.1109/SHIRCON48091.2019.9024879.
- [7] A. Delgado, "Citizen criminality assessment in lima city using the grey clustering method," 2017, doi: 10.1109/INTERCON.2017.8079662.
- [8] Y. Ji, G. H. Huang, and W. Sun, "Risk assessment of hydropower stations through an integrated fuzzy entropy-weight multiple criteria decision making method: A case study of the Xiangxi River," Expert Syst. Appl., vol. 42, pp. 5380–5389, 2015.
- [9] A. Delgado and I. Romero, "Environmental conflict analysis on a hydrocarbon exploration project using the Shannon entropy," in Proceedings of the 2017 Electronic Congress, E-CON UNI 2017, Jun. 2017, vol. 2018-January, pp. 1–4, doi: 10.1109/ECON.2017.8247309.
- [10] L. Sifeng and L. Yi, Grey Systems, Theory and Applications. Chennai, India: Springer, 2010.
- [11] A. Delgado, E. L. Huamaní, H. Obispo-Mego, and D. Justo-López, "Analysis of web platforms of learning management systems for distance education in the face of social isolation," Int. J. Adv. Trends Comput. Sci. Eng., vol. 9, no. 5, 2020, doi: 10.30534/ijatcse/2020/154952020.
- [12] A. Delgado and I. Romero, "Applying the Grey Systems Theory to Assess Social Impact from an Energy Project," in 2018 IEEE XXV International Conference on Electronics, Electrical Engineering and Computing (INTERCON), Aug. 2018, pp. 1–4, doi: 10.1109/INTERCON.2018.8526372.
- [13] Q. Wang, Y. Guo, T. Ji, X. Wang, B. Hu, and P. Li, "Towards Combatting COVID-19: A Risk Assessment System," IEEE Internet Things J., pp. 1–1, 2021, doi: 10.1109/JIOT.2021.3070042.
- [14] S. Liu, C. Lin, and Y. Yang, "Several problems need to be studied in grey system theory," in 2017 IEEE International Conference on Grey Systems and Intelligent Services, GSIS 2017, Oct. 2017, pp. 1–4, doi: 10.1109/GSIS.2017.8077658.
- [15] M. G. B. Borja, A. Delgado, S. Lescano, and J. E. Luyo, "New Approach to Develop Knowledge-Based System for Environmental Conflicts Analysis Using Fuzzy Logic and Grey Systems," Dec. 2018, doi: 10.1109/ANDESCON.2018.8564666.

# Indonesia Sign Language Recognition using Convolutional Neural Network

Suci Dwijayanti\*, Hermawati, Sahirah Inas Taqiyyah, Hera Hikmarika, Bhakti Yudho Suprpto

Department of Electrical Engineering, Universitas Sriwijaya  
Indralaya, Indonesia

**Abstract**—In daily life, the deaf use sign language to communicate with others. However, the non-deaf experience difficulties in understanding this communication. To overcome this, sign recognition via human-machine interaction can be utilized. In Indonesia, the deaf use a specific language, referred to as Indonesia Sign Language (BISINDO). However, only a few studies have examined this language. Thus, this study proposes a deep learning approach, namely, a new convolutional neural network (CNN) to recognize BISINDO. There are 26 letters and 10 numbers to be recognized. A total of 39,455 data points were obtained from 10 respondents by considering the lighting and perspective of the person: specifically, bright and dim lightning, and from first and second-person perspectives. The architecture of the proposed network consisted of four convolutional layers, three pooling layers, and three fully connected layers. This model was tested against two common CNNs models, AlexNet and VGG-16. The results indicated that the proposed network is superior to a modified VGG-16, with a loss of 0.0201. The proposed network also had smaller number of parameters compared to a modified AlexNet, thereby reducing the computation time. Further, the model was tested using testing data with an accuracy of 98.3%, precision of 98.3%, recall of 98.4%, and F1-score of 99.3%. The proposed model could recognize BISINDO in both dim and bright lighting, as well as the signs from the first-and second-person perspectives.

**Keywords**—Indonesia sign language (BISINDO); recognition; CNN; lighting

## I. INTRODUCTION

Humans use language to communicate with others. However, a communication disorder may occur because of various factors that cause an impairment in understanding oral speech [1]. Such factors can arise from a hearing disorder or deafness. Thus, deaf people use sign language or hand gestures to communicate. However, most non-deaf people experience difficulties in understanding sign language. A computerized sign recognizer could be employed as an important tool to enable mutual understanding between deaf and non-deaf people.

Various studies have been proposed to recognize hand gestures or sign languages in different countries because each country has a different sign, such as the American sign language [2], Arabic sign language [3], Bengali sign language [4], Peruvian sign language [5], and Chinese sign language [6] using various methods.

Indonesia has two sign languages: Indonesia Sign Language System (SIBI) and Indonesia Sign Language

(BISINDO). In 1994, SIBI became the language used in formal schools for students with impairments. However, the deaf prefer to use BISINDO instead of SIBI in their daily lives.

Certain studies have been performed to recognize the SIBI. Hand gestures recognition approaches can be divided into vision based and sensor-based [7]. In vision-based approaches, images are acquired through a video camera. Meanwhile, sensor-based recognition needs an instrument to capture the motion, position, or velocity of the hands. Studies in Indonesian sign languages implemented the vision-based approach. A. Anwar et al. used a leap motion controller to recognize Indonesian sign language using feature extraction captured from hand movement [8]. In [9], a Myo Armband tool was used, which has five sensors, namely accelerator, gyroscope, orientation, orientation Euler, and electromyography (EMG). Both vision and sensor-based approaches need the data acquisition and classification stages. Various classification methods have been proposed to recognize patterns carried by input data. The k-nearest neighbor classification method was used to recognize the SIBI [10]. In this study, the distance between the coordinates of each bone distal to the position of the palm was measured using Euclidean distance. Meanwhile, Khotimah et al. implemented weighted k-nearest neighbor classification for dynamic sign language recognition [11]. Rosalina et al. used artificial intelligence to recognize SIBI [12]. Other studies utilized Hidden Markov Model [13] and Naïve Bayes [14] methods. Meanwhile, [15] used the generalized learning vector quantization model to recognize BISINDO and [16] utilized Scale Invariant Features Transform (SIFT) algorithm to recognize Indonesian Sign Language numbers. Iqbal et al. implemented a mobile device using a Discrete Time Warping for recognizing SIBI [17].

Most studies above discussed SIBI; however, BISINDO is the most common sign language used by the deaf in Indonesia. Thus, this study aims to convert hand gestures to text in BISINDO to improve communications between deaf and non-deaf people. In addition, the methods used in other studies depended on feature extraction. To improve performance, this study proposes a method to recognize BISINDO using a convolutional neural network (CNN) which uses the convolution layer as the feature extraction layer [18]. In other studies, a CNN was used by [2] to recognize American Sign Language. They employed a CNN to extract the features from the sign images, and the classifier used was a multiclass support vector machine. Hayani et al. also utilized a CNN coupled with an Adam optimizer to recognize Arabic sign

\*Corresponding Author.  
E-mail: sucidwijayanti@ft.unsri.ac.id

language [3]. Hossen et al. used a deep convolutional neural network to recognize Bengali sign language [4].

However, not many previous works have addressed converting BISINDO sign language to text. Furthermore, there is a need to develop CNN models that have lower computation costs for converting sign language to text. This study addressed both needs by developing a new CNN architecture to perform the BISINDO hand gesture to text, and reduced computation costs by using fewer parameters than the common CNN architectures. The experimental research objective of this study was to compare the BISINDO recognition performance of this simplified CNN model to AlexNet and VGG-16 which are other architectures commonly used in CNNs. We tested the performance using BISINDO standard hand signs recorded by a webcam under bright and dim lightning, and from first and second-person perspectives.

This paper is organized as follows: Section II provides a brief summary of BISINDO, followed by a description of the CNN architecture in Section III. The methods used in this study are described in Section IV. The results and discussion are presented in Section V. Finally, the paper is concluded in Section VI.

## II. INDONESIAN SIGN LANGUAGE

Sign language is a language that is expressed using body gestures and facial expressions as a symbol of the meaning of spoken language [19]. The sign languages of Indonesia can be categorized into two types: SIBI and BISINDO. SIBI was adopted from American Sign Language and is used as the formal sign language in schools for deaf students. However, the deaf prefer to use BISINDO instead of SIBI owing to its better applicability. The signs for the letters and numbers in the BISINDO language are shown in Fig. 1.

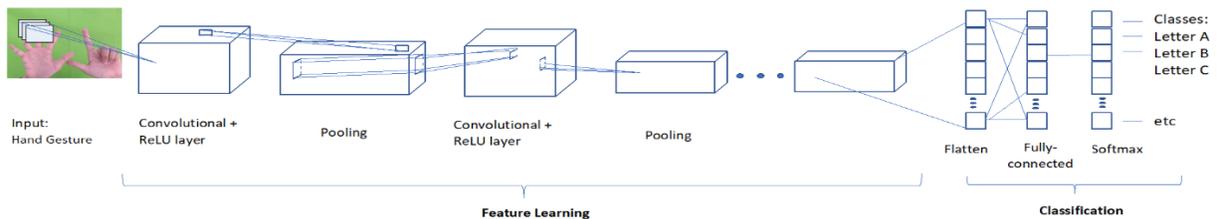


Fig. 2. Architecture of the CNN

The convolution layer extracts the features of images. This results in a linear transformation from the input, which is suitable for the spatial information of the filter. The weights in this layer determine the kernel convolution. Thus, kernel convolution can be trained based on the CNN input. The pooling layer comprises a filter with a stride and a certain size that passes through the path in the feature map. It aims to reduce image size. There are two types of pooling layers: max pooling and average pooling. In this study, max pooling was utilized by determining the maximum value in the vector dimension. After passing the convolution and pooling layers, the output of this process is used as the input to the fully connected layer. However, before this process, the input must be converted into one dimensional data. Finally, the process is performed using Softmax. Softmax calculates the probabilities

for all target classes to determine the classes based on the input [22].

## IV. METHODS

This section provides detailed descriptions of several steps used in our methods. This study was performed using primary data obtained from people who had no prior knowledge of sign language. Here is an overview of the steps. A webcam was used to gather sets of hand sign data from ten people to use as training data. The data were obtained by considering two conditions: lighting and perspective of the person. Then, a new CNN model was designed and trained, which was named model C. For comparison, we trained modified versions of AlexNet and VGG-16. Then, the three models were tested and evaluated against the test data.

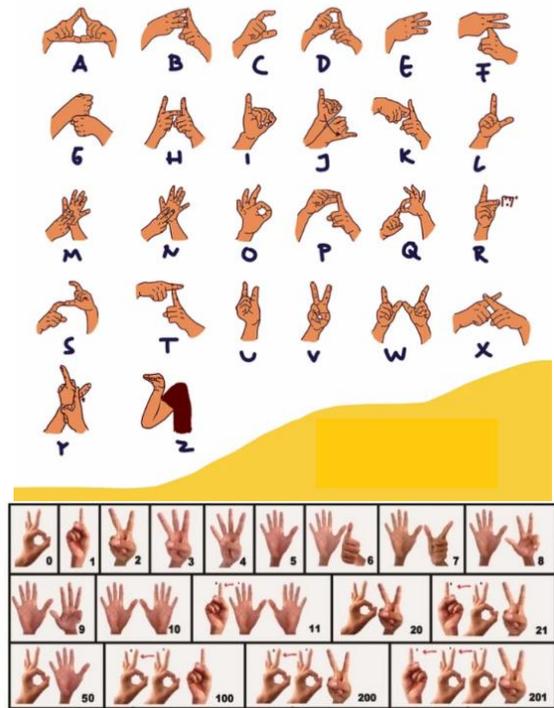


Fig. 1. BISINDO Alphabets [20] and Numbers [21].

## III. CONVOLUTIONAL NEURAL NETWORK (CNN)

A CNN is typically used to detect or recognize images. It has an architecture that consists of a feature extraction layer and a fully connected layer. The feature extraction layer comprises a convolution layer and pooling layer. The general architecture of the CNN is illustrated in Fig. 2.

A. Data

The data used in this study were obtained using the webcam Logitech C922 with a resolution of 1080p and 30 fps. Ten respondents were asked to perform hand gestures, which consisted of 26 letters and numbers from 1 to 10, adhering to the BISINDO standard. Data were acquired 30 cm from the camera, as shown in Fig. 3. A green screen was placed as a background to minimize noise. Data were obtained by considering two conditions: lighting and perspective of the person.

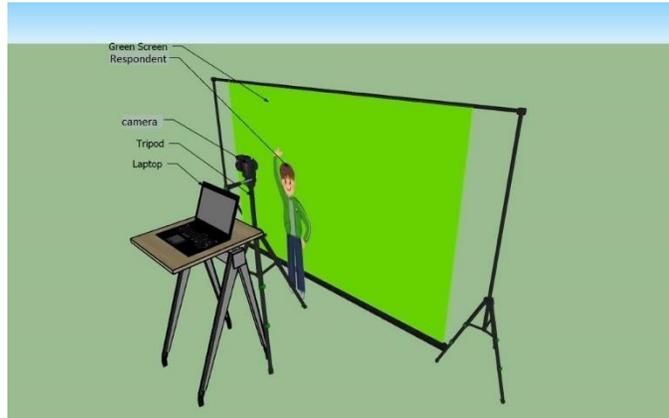


Fig. 3. Overview of the Data Retrieval Process.

B. Architecture of CNN

The CNN architecture used in this study consisted of three architectures, namely, models A, B, and C. Model A was a modified version of AlexNet [23]. The original AlexNet has 24,884,005 parameters, whereas the modified one has 1,432,261. Model B was a modified architecture of the VGG-16 [24]. It was modified to 2,140,405 parameters from its original value of 33,748,837. AlexNet and VGG-16 were chosen because they are the most common architectures used in CNNs. The architectures of models A and B are shown in Fig. 4 and 5, respectively.

This study proposed a new architecture, namely model C. Model C is a simpler architecture that consists of convolutional layer 1, max pooling 1, convolutional layer 2, convolutional layer 3, max pooling 2, convolutional layer 4, max pooling 3, flattened layer, and 3 fully connected layers. The visualization of model C is shown in Fig. 6.

C. Evaluation

This study utilized accuracy, precision, recall, and F1 scores to evaluate the performance of the three models. These parameters were calculated as follows:

$$accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

where True Positive (TP) is the number of positive data correctly predicted as positive, true negative (TN) is the number of negative data correctly predicted as negative, false positive (FP) is the number of negative data incorrectly predicted as positive, and false negative (FN) is the number of positive data incorrectly predicted as negative.

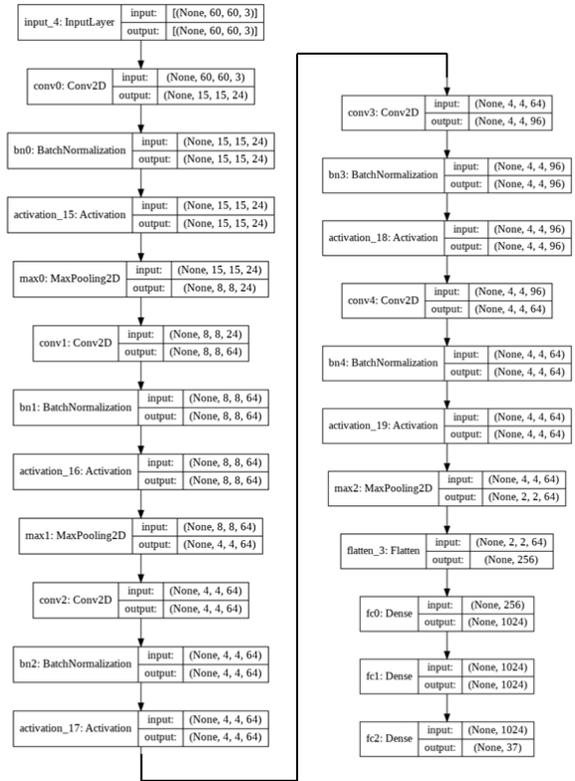


Fig. 4. Architecture of Model A.

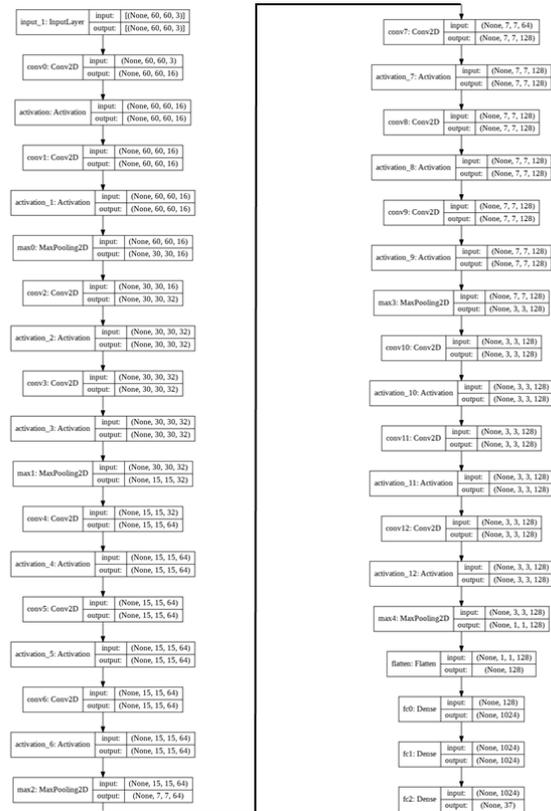


Fig. 5. Architecture of Model B.

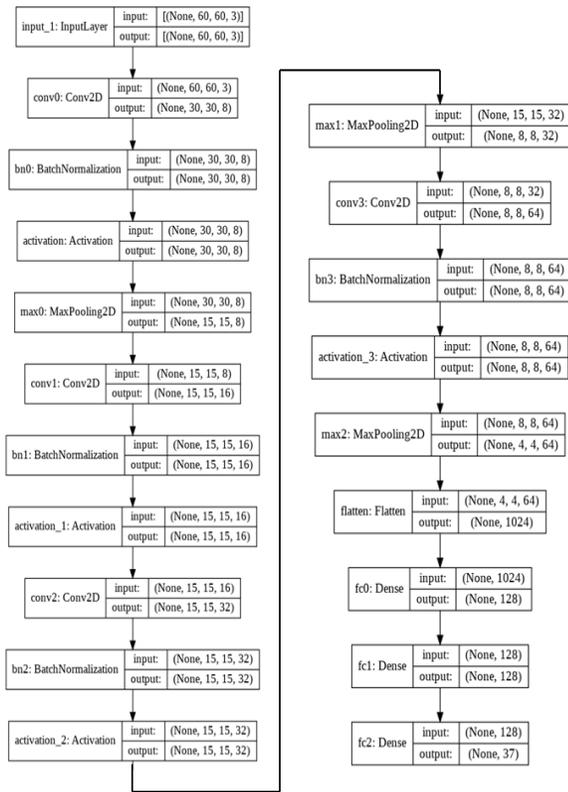


Fig. 6. Architecture of the New Model C.

In addition, precision and recall are also utilized as evaluation parameters. These can be calculated as.

$$precision = \frac{TP}{TP+FP} \quad (2)$$

and

$$recall = \frac{TP}{TP+FN} \quad (3)$$

The balance between precision and recall is determined using the F1-Score, which is obtained as follows.

$$F1\ score = 2 \left( \frac{precision \times recall}{precision + recall} \right) \quad (4)$$

## V. RESULT AND DISCUSSION

### A. Image Dataset

The data used in this study were obtained from 10 respondents under two lighting conditions: dim and bright conditions. The position of the camera was also considered to be from the direction of the object considered (first-person perspective) and from the directions of others who observe the hand gesture (second-person perspective). Both lighting and viewpoints were considered in this study because illumination and viewpoints are challenges in gesture recognition [7]. Each respondent performed 37 hand gestures, consisting of 26 letters and 11 numbers (0–10). The data were recorded in a video format (.mp4) to obtain multiple data varieties. Subsequently, the data obtained were converted into images in the format of .jpg. The total data obtained through this process comprised 39,455 data points. Examples of the data are shown in Fig. 7.

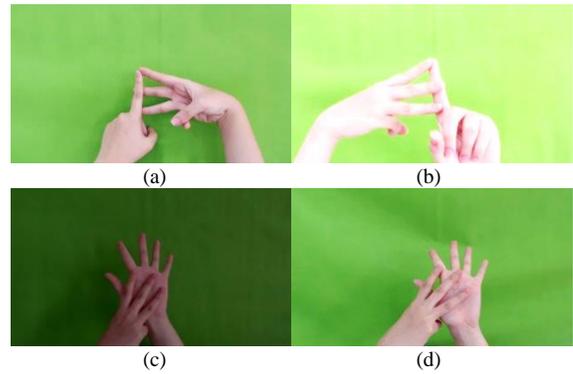


Fig. 7. Examples of Hand Gestures Obtained, (a) From the First-Person Perspective, (b) From the Second-Person Perspective, (c) Images Captured in Dim, and (d) Images Captured in Light.

### B. Data Preprocessing

Before using the data in the CNN, the image data were preprocessed. This stage was performed by resizing the image and scaling the features. The image was resized to the same size of  $60 \times 60$  pixels. Thereafter, feature scaling was performed by dividing the values at each point in the image by 255 such that the data value interval in the image was 0–1. Fig. 8 shows the preprocessed results of the image data.

### C. Data Split

The preprocessed data were then fed as input to the CNN. In total 39,455 data were obtained, which was further divided using the stratified shuffle split method into three parts: training data, validation data, and test data. The division of the data was: 60 % training data, 20 % validation data, and 20 % test data, as shown in Fig. 9.

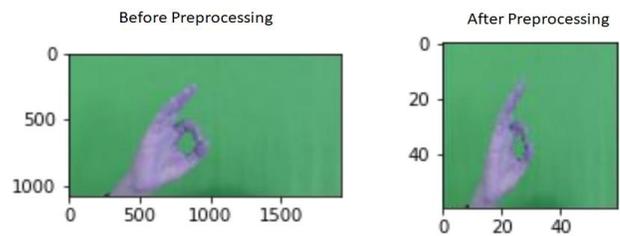


Fig. 8. Example of Preprocessed Result of Image Data.

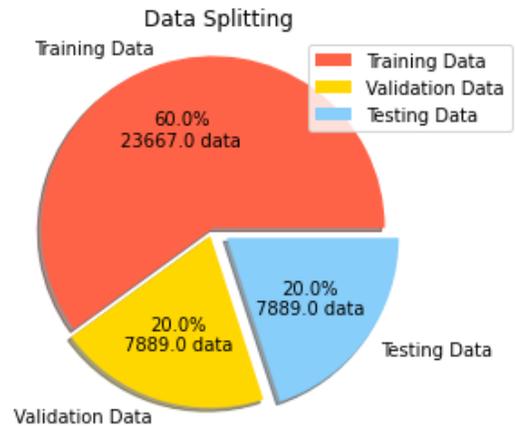


Fig. 9. Data Splitting.

D. Training Process

The training process was conducted using the CNN algorithm. The training parameters for the three models are listed in Table I.

TABLE I. PARAMETERS OF TRAINING

Parameter	Value
Image size	60 x 60
Optimizer	Adam
Epoch	100
Learning Rate	0.001

The loss and accuracy of the training results using models A, B, and C are shown in Fig. 10, 11, and 12, respectively.

As shown in Fig. 10, model A exhibited training and validation losses of 0.011 and 0.096, respectively. Further, the training and validation accuracies were 0.997 and 0.984, respectively. As shown in the loss graph, the model tends to fluctuate, indicating instability. Nevertheless, the model can learn the patterns as shown by the loss values, which tend to zero in each epoch, and the accuracy is improved. In contrast, model B has a high loss value and low accuracy, as shown in Fig. 11. This implies that the model cannot learn the patterns given by hand gestures because the loss values are high. Fig. 12 shows that model C has training and validation losses of 0.020 and 0.079, respectively. In addition, the training and validation accuracies were 0.995 and 0.984, respectively. Thus, model C can learn the hand gestures given because the loss value goes to zero and the accuracy increases. A comparison of these models is shown in Table II.

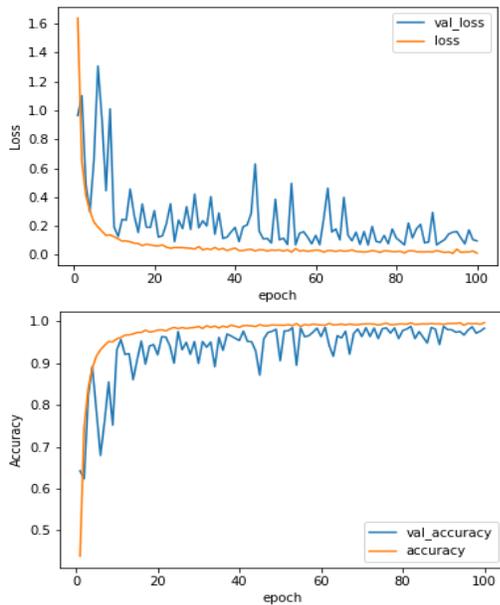


Fig. 10. Loss Value and Accuracy of Model A.

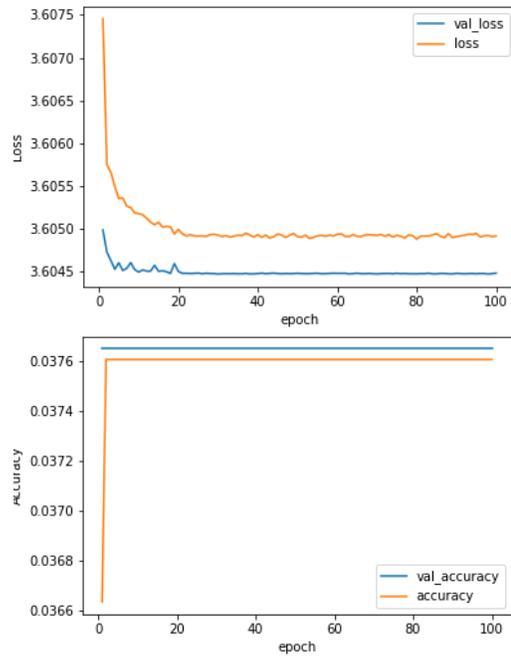


Fig. 11. Loss Value and Accuracy of Model B.

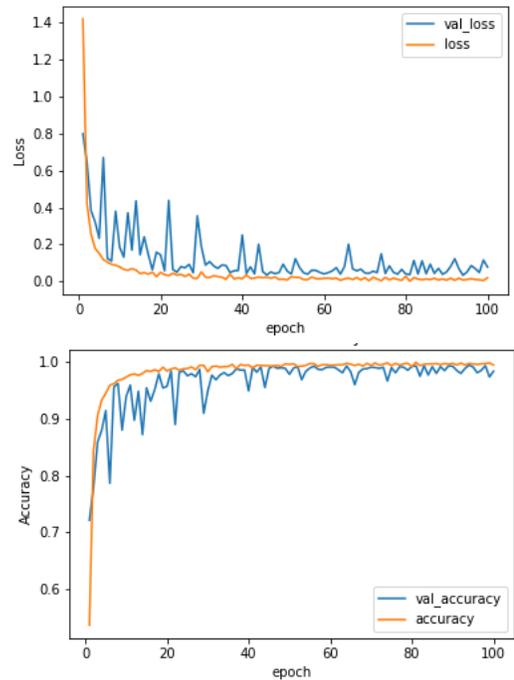


Fig. 12. Loss Value and Accuracy of Model C.

TABLE II. COMPARISON OF TRAINING IN MODEL A, B, AND C

Parameter	Model A	Model B	Model C
Training Loss	0.0113	3.6049	0.0201
Validation Loss	0.0967	3.6045	0.0785
Training Accuracy	0.9972	0.0376	0.9948
Validation Accuracy	0.9839	0.0376	0.9839
Total Parameter	1,432,261	2,140,405	177,373

As shown in Table II, Models A and C have low loss values and high accuracy compared to Model B. Overall, Model A has the lowest training loss value, and high training and validation accuracy. Model C has the lowest validation loss, and high training and validation accuracy. In addition, the total number of parameters used in Model C was 177,383 while Model A had 1,432,261 parameters. Therefore, the computation time in Model C was the smallest compared to the other models. In addition, although Model C still exhibited a fluctuation in validation loss and validation accuracy (Fig. 12), it is lesser than that of Model A (Fig. 10). Thus, Model C has more stable validation loss. Based on these results, Model C exhibited the best performance compared to the other models. Consequently, these models were used to test whether the model is optimal and can generalize the testing data.

### E. Testing

Testing was performed after training to determine the ability of the model to predict the class of hand gestures. The test results are shown in Table III.

TABLE III. EVALUATION OF TESTING DATA

Model	Total Param.	Average prediction time per data (second)	Acc.	F1 Score	Precision	Recall
Model A	1,432,261	0.0002	0.986	0.996	0.987	0.987
Model B	2,140,405	0.0001	0.038	0.002	0.001	0.027
Model C	177,373	0.0001	0.983	0.993	0.983	0.984

As shown in Table III, model A has an accuracy of 0.986, F1 score of 0.996, precision of 0.987, and recall of 0.987. The results of testing using Model C are very similar to model A, with an accuracy of 0.983, F1 score of 0.993, precision of 0.983, and recall of 0.984. Since model B failed to learn, its

test results were very low. Thus, Models A and C obtained the best results. However, Model C has fewer parameters, thereby requiring less time to predict the data compared to Model A. The average prediction time per data for Model C was half the time for Model A: 0.0001 s for Model C and 0.0002 s for Model A. Therefore, Model C is twice as efficient as Model A while achieving near-equivalent performance levels.

1) *Test results by lighting*: This study used two lighting conditions: bright and dim. The performances for both conditions are shown in Table IV.

As shown in Table IV, both Models A and C could recognize the testing data in the two different lighting conditions, and they both had high performance. Meanwhile, Model B performed poorly in recognizing the signs.

2) *Test results by perspective*: This study used the first- and second-person perspectives. The position of the camera was considered to be from the direction of the object considered (first-person perspective) and from the directions of others who observe the hand gesture (second-person perspective). The performances for both conditions are shown in Table V.

Table V shows that Model A and C can recognize the signs in both the first and second-person perspectives with high performance levels. There was a slight improvement with the second-person perspective.

### F. Hand Gesture Prediction Results

The performance of the proposed model for predicting hand gestures was evaluated as well. Each class of hand gestures was performed, and the results obtained are shown in Fig. 13. The proposed model can recognize new data. Further, the hand gesture in the dim condition yielded a higher accuracy than in the light condition for the first-person perspective. In contrast, the second-person perspective exhibited the same performance under both dim and bright conditions. Certain samples of hand gesture recognition are listed in Table VI.

TABLE IV. TESTING RESULTS FOR DIFFERENT LIGHTING CONDITIONS

MODEL	Bright				Dim			
	Accuracy	F1 Score	Precision	Recall	Accuracy	F1 Score	Precision	Recall
A	0.985	0.985	0.986	0.984	0.987	0.987	0.988	0.987
B	0.038	0.002	0.001	0.027	0.038	0.002	0.001	0.027
C	0.979	0.980	0.981	0.981	0.987	0.987	0.987	0.988

TABLE V. TESTING RESULTS FOR DIFFERENT PERSPECTIVES

MODEL	First-person perspective				Second-person perspective			
	Accuracy	F1 Score	Precision	Recall	Accuracy	F1 Score	Precision	Recall
A	0.984	0.984	0.985	0.984	0.987	0.987	0.988	0.987
B	0.031	0.002	0.001	0.027	0.043	0.002	0.001	0.027
C	0.978	0.979	0.980	0.980	0.987	0.987	0.987	0.988

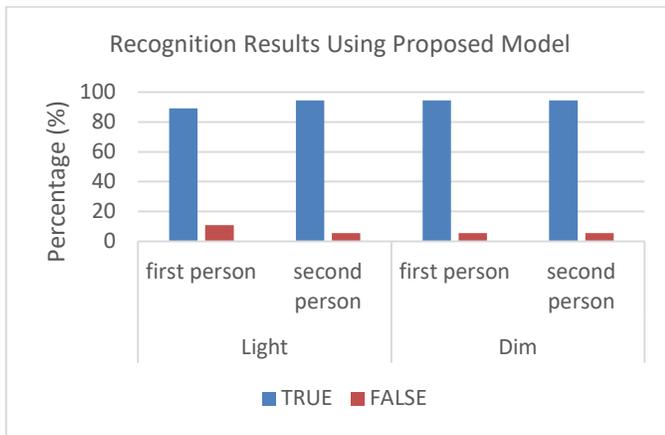


Fig. 13. Recognition Results using Proposed Model C.

TABLE VI. SAMPLE OF HAND GESTURES PREDICTION RESULTS

Data Test	Lighting Condition	Perspective	Actual Class	Result of Prediction
	Bright	First-person	4	4 (True)
	Dim	Second-person	H	H (True)
	Bright	Second-person	S	S (True)
	Dim	First-person	8	8 (True)
	Dim	First-person	B	B (True)
	Bright	Second-person	3	3 (True)
	Dim	First-person	2	V (False)
	Bright	First-person	M	M (False)
	Dim	First-person	N	M (False)
	Dim	Second-person	J	I (False)

As shown in Table VI, the proposed CNN model C works well in predicting hand gestures that were not included in the training data. This implies that the CNN can be implemented to recognize hand gestures. However, certain prediction errors occurred in certain classes, such as 2, M, N, V, and J. The

occurrence of prediction errors due to hand gestures from these classes is almost the same or similar to other classes. The numbers 2 and V have the same hand gesture, thus, an error occurred in the CNN while predicting the class. From the first-person perspective, no difference was observed between the letter M and N hand gestures, thereby resulting in an error in the prediction. Further, the hand gesture for the letter J is not static, thus a prediction error occurred wherein the letter I was predicted because the initial movement of the signal letter J resembles that for the letter I.

## VI. CONCLUSION

The results of this study demonstrated that our new simplified CNN model exhibited good performance in recognizing BISINDO hand gestures. The CNN architecture used was a simple architecture consisting of convolutional layer 1, max pooling 1, convolutional layer 2, convolutional layer 3, max pooling 2, convolutional layer 4, max pooling 3, flattened layer, and 3 fully connected layers. The parameters used were the Adam Optimizer, an iteration parameter of 100 epochs, and a learning rate of 0.001. During the training process, the last epoch resulted in a training loss value of 0.0201, validation loss value of 0.0785, and training accuracy value of 0.9948 with a validation accuracy value of 0.9839. The results of hand signal recognition testing using the CNN model on test data obtained performance results of 98.3%. Thus, this new simplified CNN model can recognize the BISINDO hand gestures well under dim and bright lighting and from the first- and the second-person perspective.

In the future, we will improve Model C to address those performance factors. We also expect to conduct the process of data retrieval with different backgrounds and do further research on real-time implementations of BISINDO hand gestures.

## ACKNOWLEDGMENT

The research/publication of this article was funded by the DIPA of the Public Service Agency of Universitas Sriwijaya 2021. SP DIPA-023.17.2.677515/2021. In accordance with the rector's decree number, 0010/UN9/SK.LP2M.PT/2021 on April 28, 2021.

## REFERENCES

- [1] American Speech-Language-Hearing Association, "Definitions of communication disorders and variations." 1993. [Online]. Available: <https://www.asha.org/policy/RP1993-00208/> [Accessed: August, 2021].
- [2] M. R. Islam, U. K. Mitu, R. A. Bhuiyan, and J. Shin, "Hand gesture feature extraction using deep convolutional neural network for recognizing American sign language," 2018 4th Int. Conf. Front. Signal Process. ICFSP 2018, pp. 115–119, 2018, doi: 10.1109/ICFSP.2018.8552044.
- [3] S. Hayani, M. Benaddy, O. El Meslouhi, and M. Kardouchi, "Arab Sign language Recognition with Convolutional Neural Networks," Proc. 2019 Int. Conf. Comput. Sci. Renew. Energies, ICCSRE 2019, pp. 1–4, 2019, doi: 10.1109/ICCSRE.2019.8807586.
- [4] M. A. Hossen, A. Govindaiah, S. Sultana, and A. Bhuiyan, "Bengali sign language recognition using deep convolutional neural network," 2018 Jt. 7th Int. Conf. Informatics, Electron. Vis. 2nd Int. Conf. Imaging, Vis. Pattern Recognition, ICIEV-IVPR 2018, pp. 369–373, 2019, doi: 10.1109/ICIEV.2018.86409622.
- [5] B. Berru-Novoa, R. Gonzalez-Valenzuela, and P. Shiguihara-Juarez, "Peruvian sign language recognition using low resolution cameras,"

- Proc. 2018 IEEE 25th Int. Conf. Electron. Electr. Eng. Comput. INTERCON 2018, 2018, doi: 10.1109/INTERCON.2018.8526408.
- [6] S. Yuan, Y. Wang, X. Wang, H. Deng, S. Sun, H. Wang, and G. Li., "Chinese Sign Language Alphabet Recognition Based on Random Forest Algorithm," In 2020 IEEE Int. Workshop Metrology Industry 4.0 & IoT, pp. 340-344, June 2020, IEEE.
- [7] M. J. Cheok, Z. Omar, M.H. Jaward, "A review of hand gesture and sign language recognition techniques," *Int. J. Mach. Learn. Cybern.* 10(1), 131-153, 2019.
- [8] A. Anwar, A. Basuki, R. Sigit, A. Rahagiyanto, and M. Zikky, "Feature extraction for Indonesian sign language (SIBI) using leap motion controller," In 2017 21st Int. Comput. Sci. Eng. Conf. (ICSEC) (pp. 1-5). November 2017. IEEE.
- [9] A. Rahagiyanto, A. Basuki, and R. Sigit, "Moment invariant features extraction for hand gesture recognition of sign language based on SIBI," *EMITTER Int. J. Eng. Technol.* 5(1), 119-138, 2019.
- [10] F. M. Humairah, Supria, D. Herumurti, and K. Widarsono, "Real Time SIBI Sign Language Recognition Based on K-Nearest Neighbor," In 2018 5th Int. Conf. on Electrical Engineering, Computer Science and Informatics (EECSI) (pp. 669-673). 2018.
- [11] W. N. Khotimah, N. Suciati, Y.E. Nugyasa, and R. Wijaya, "Dynamic Indonesian sign language recognition by using weighted K-Nearest Neighbor," In 2017 11th Int. Conf. Inform. Commun. Technol. Syst. (ICTS) (pp. 269-274), Oct 2017, IEEE.
- [12] Rosalina, L. Yusnita, N. Hadisukmana, R. B. Wahyu, R. Roestam, and Y. Wahyu, "Implementation of real-time static hand gesture recognition using artificial neural network," *Proc. 2017 4th Int. Conf. Comput. Appl. Inf. Process. Technol. CAIPT 2017*, vol. 2018-Janua, pp. 1-6, 2018, doi: 10.1109/CAIPT.2017.8320692.
- [13] E. Rakun, M. I. Fanany, I. W.W. Wisesa, and A. Tjandra. "A heuristic Hidden Markov Model to recognize inflectional words in sign system for Indonesian language known as SIBI (Sistem Isyarat Bahasa Indonesia)." In 2015 Int. Conf. Technol. Inform. Manag. Eng. Environ. (TIME-E), pp. 53-58. IEEE, 2015.
- [14] Ridwang, Syafaruddin, A. A. Ilham, and I. Nurtanio, "Indonesian Sign Language Letter Interpreter Application Using Leap Motion Control based on Naïve Bayes Classifier," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 676, no. 1, 2019, doi: 10.1088/1757-899X/676/1/012012.
- [15] T. Handhika, D.P. Lestari, I. Sari, and R.I.M. Zen, "The generalized learning vector quantization model to recognize Indonesian sign language (BISINDO)," In 2018 Third Int. Conf. Inform. Comput. (ICIC) (pp. 1-6). Oct 2018. IEEE.
- [16] I. Mahfudi, M. Sarosa, R.A. Asmara, and M.A. Gustalika, "Indonesian Sign Language Number Recognition using SIFT Algorithm," In *IOP Conf. Series: Mater. Sci. Eng.* (Vol. 336, No. 1, p. 012010), April 2018. IOP Publishing.
- [17] M. Iqbal, E. Supriyati, and T. Listiyorini, "SIBI Blue: Developing Indonesian Sign Language Recognition System Based On The Mobile Communication Platform," *Int. J. Inform. Technol. Comput. Sci. Open Source*, 1(1), 2017.
- [18] Q. Liu, N. Zhang, W. Yang, S. Wang, Z. Cui, X. Chen, and L.Chen, "A review of image recognition with deep convolutional neural network," In *International conference on intelligent computing* (pp. 69-80). Springer, Cham., August 2017.
- [19] M. C. Stöppler, "Medical Definition of Sign Language," *MedicineNet*, 2021. [Online]. Available: [www.medicinenet.com/sign\\_language/definition.htm](http://www.medicinenet.com/sign_language/definition.htm). [Accessed: Feb. 02, 2021].
- [20] Gerakan untuk Kesejahteraan Tunarungu Indonesia (GerkatIn) Solo, Bahasa Isyarat Alfabet BISINDO, [Alphabets in Indonesia Sign Language (BISINDO)] (in Indonesian) GERKATIN Solo, 2013. [Online]. Available: <http://gerkatinsolo.or.id/> [Accessed: Feb. 02, 2021].
- [21] Noviani, Bahasa Isyarat Angka BISINDO, [Number in Indonesia Sign Language (BISINDO)] (in Indonesian) Penulis Cilik, 2019. [Online]. Available: <https://www.penuliscilik.com/bahasa-isyarat-angka/> [Accessed: Feb. 02, 2021].
- [22] S. Dwijayanti, R.R. Abdillah, H. Hikmarika, Z. Husin, and B.Y. Suprpto, "Facial Expression Recognition and Face Recognition Using a Convolutional Neural Network," In 2020 3rd Int. Seminar Res. Inform. Technol. Intell. Syst. (ISRITI) (pp. 621-626). Dec 2020, IEEE.
- [23] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," *Commun. ACM*, vol. 60, no. 6, pp. 84-90, 2012.
- [24] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *3rd Int. Conf. Learn. Represent. ICLR 2015 - Conf. Track Proc.*, pp. 1-14, 2015.

# Increasing Randomization of Ciphertext in DNA Cryptography

Maria Imdad<sup>1</sup>, Sofia Najwa Ramli<sup>2</sup>

Center of Information Security Research  
Faculty of Computer Science and Information Technology  
Universiti Tun Hussein Onn Malaysia, Batu Pahat, Malaysia

Hairulnizam Mahdin<sup>3</sup>

Center of Intelligence and Autonomous Systems  
Faculty of Computer Science and Information Technology  
Universiti Tun Hussein Onn Malaysia, Batu Pahat, Malaysia

**Abstract**—Deoxyribonucleic acid (DNA) cryptography is becoming an emerging area in hiding messages, where DNA bases are used to encode binary data to enhance the randomness of the ciphertext. However, an extensive study on existing algorithms indicates that the encoded ciphertext has a low avalanche effect of providing a desirable confusion property of an encryption algorithm. This property is crucial to randomize the relationship between the plaintext and the ciphertext. Therefore, this research aims to reassess the security of the existing DNA cryptography by modifying the steps in the DNA encryption technique and utilizing an existing DNA encoding/decoding table at a selected step in the algorithm to enhance the overall security of the cipher. The modified and base DNA cryptography techniques are evaluated for frequency analysis, entropy, avalanche effect, and hamming weight using 100 different plaintexts with high density, low density, and random input data, respectively. The result introduces good performances to the frequency analysis, entropy, avalanche effect, and hamming weight, respectively. This work shows that the ciphertext generated from the modified model yields better randomization and can be adapted to transmit sensitive information.

**Keywords**—DNA cryptography; avalanche effect; frequency test; entropy; hamming weight

## I. INTRODUCTION

With the amazing development of Deoxyribonucleic Acid (DNA) computing, DNA cryptography is a new advancement in cryptography. DNA molecules are an integral part of a cell and act as genetic information carriers, but when applied in modern cryptography, it serves as a data manipulation tool [1].

The design of an encryption/decryption algorithm should be complex enough to stand for a long time against a security attacks. The best way to reach such complexity in a system is to work towards scalability because this will ultimately lead to large-scale complexity. The main idea to increase the complexity in the system by augmenting its size is to achieve the desired security that will require tremendous efforts to attack the system successfully. These desired properties can be achieved by DNA cryptography as it offers huge parallelism and storage capacity simultaneously [2]. The power of DNA encryption is not only in the molecules or encoding but in the positions where we want to save our data to protect it from attacks for a longer time [3]. Cryptography is the procedure to create such algorithms, whereas; cryptanalysis is the procedure where attackers or the algorithm developers validate the cipher

for its vulnerabilities and improve it by giving insight for future directions [4]. Randomness [5], avalanche effect [6], and entropy per bit [7] are some of the desired properties to evaluate the ciphertext. A cryptographic solution should satisfy this criterion, at least to ensure safety.

Avalanche effect [5] is a compelling test, whereby changing one bit in plaintext or key will change at least 50% of the bits in the ciphertext. This research work focuses on the change in ciphertext from a plaintext perspective. A detailed study of DNA cryptographic encryption algorithm as in [8] indicates that the avalanche effect is considerably less, leading to security vulnerabilities. Specifically, the conversion of the binary data into DNA bases (00 to A, 01 to G, 10 to C, 11 to T) exhibits poor avalanche effect or randomization of the ciphertext. This may cause an attacker to establish a relationship between plaintext and its ciphertext. In this paper, a modified DNA encryption technique with an existing DNA encoding table used in [9] are introduced to the existing algorithm to overcome the mentioned security vulnerability. The proposed encryption technique allows the user to send encrypted information with an extra fold of security. The experimental results have endorsed the effectiveness of the proposed technique by performing a statistical analysis between the base technique and the proposed technique.

The overall structure of the study takes the form of six sections, including this introductory section followed by a literature review in Section 2. Section 3 gives an insight on the encryption algorithm using base and the proposed technique. Section 4 explains the list of tests to measure the randomness in technique. Section 5 has a detailed analysis of results validating the effectiveness of the proposed technique. Section 6 discusses the concluding remarks considering improvements and limitations followed by cited references in a separate section.

## II. RELATED WORK

DNA computing is an increasingly important area in applied cryptography where the inherited property of storing huge data is adopted along with DNA replication to introduce randomness in the cipher. DNA computing can be applied in various forms during the encryption-decryption process; it can either be used as complement operation, digital coding, polymerase chain reaction, or as a security alternative [10]. A large volume of published studies describes the role of DNA in cryptography. This research focuses on DNA digital coding

only with detailed insight into its security impact in cryptographic techniques. In 2012, Noorul Hussain [9] introduced a new concept based on DNA digital coding, where a dynamic DNA encoding table was presented. This encoding table is a 24\*4 matrix of 96 American Standard Code for Information Interchange (ASCII) characters consisting of alphabets, numbers, and special characters. Later this table was used and extended by other researchers [11]-[13]. It is evident that the utilization of this table in an algorithm has improved the randomness of ciphertext and consequently enhanced the system security.

An extended version of the ASCII table was introduced with 256 ASCII character encoding [11]. For a dynamic sequence, table creation, all characters are initially allocated randomly to DNA base sequences followed by an iterative rearrangement using a mathematical pattern, whereas in the encryption process, the plaintext is first converted into DNA bases using the sequence table, followed by the creation of data chunks to encrypt them using an asymmetric cryptosystem and finally to merge the chunks as the ciphertext. The system of dynamic encoding coupled with asymmetric cryptosystem naturally raises the degree of data confidentiality. It is proved by comparison with existing techniques and a statistical suit of randomness defined by the National Institute of Standards and Technology (NIST).

In [12], a network traffic and intrusion detection system is proposed using DNA sequences, where DNA bases are used to encode the 41 attributes of the network. The next attributes have been analyzed for experimentation purposes, and the results indicate a 15% improvement in accuracy, whereby a more complex encoding can effectively improve the accuracy of the intrusion detection system. In [13] and [14], a Dynamic DNA sequence table is used in combination with OTP to improve data security. The attacker must execute all possible DNA sequence variations before getting original data, which is supposed to be very difficult. The proposed technique provides better security than other techniques, in particular against brute force attacks. The algorithm aims to transmit the One-time-pad (OTP) securely, but execution time has been increased as compared to other similar techniques.

Interestingly a cryptographic system is designed, where the authors in [8] apply a delayed Hopfield neural network to generate the cryptographic key before DNA encryption-decryption process. Specifically, the chaotic neural network generates a binary sequence, passed on to the permutation function yielding the first level key for encryption. The system's strength lies in the random selection of trajectories for neural networks, delay function, and DNA cryptography. The authors claim that changing one byte can change 32 out of 128 bits in the ciphertext, which is significantly less than the expected change, where changing one bit in plaintext or key should bring more than 50% change in the ciphertext.

All these research works endorse the fact that DNA encryption using DNA encoding can significantly improve the security of the cryptographic solution. A similar approach in [8] is extended with the existing DNA encoding table at a carefully selected location. The subsequent section explains the encryption process for the base technique followed by the

improved technique with an additional layer of the dynamic sequence table.

### III. METHODOLOGY

#### A. Base Technique

The Hybrid chaotic neural network as in [8] generates the key while the DNA cryptography algorithm encrypts/decrypts the original data. However, this paper only discusses the application of DNA cryptography, so it primarily discusses encryption/decryption without going into details of the key generation process. Plaintext, key, and ciphertext are of equal length, i.e., 128 bits. Following are the steps involved in the encryption process:

- 1) Take plaintext from the user and divide it into fixed-length sub-sequences  $R_j$ .
- 2) A random binary sequence  $S_j$  of equal length is produced using a key generation.
- 3)  $R_j$  is permuted using left cyclic shift yielding  $R'_j$  where the number of bits to be shifted  $V_j$  is pre-calculated by key generation part.
- 4)  $S_j$  is subjected to right cyclic shift producing  $S'_j$  using  $V_j$ .
- 5) To produce the 1st level encrypted text  $C'_j$ , an XOR operation is performed between  $R'_j$  and  $S'_j$  as given below:

$$C'_j = R'_j \oplus S'_j$$

- 6) The second level of encryption is performed on binaries obtained from  $C_j$ . Applying "00" to "A", "01" to "G", "10" to "C", and "11" to "T", yielding  $C_j$  is the DNA encoded ciphertext.

The decryption process is the reverse of the encryption process where DNA decoding produces  $D'_j$  and thus  $D'_j$  as below:

$$D'_j = D'_j \oplus S'_j$$

This  $D'_j$  undergoes permutation and cyclic shift to give the plaintext.

#### B. Proposed Technique

The proposed algorithm works the same way as far as the key generation is concerned in [8], but there is an improvement for encryption and decryption part as in Fig.1.

- 1) The user enters the plaintext, which goes directly to the DNA sequence table and gets encoded.
- 2) Then binary coding is applied as  $A = 00$ ,  $T = 01$ ,  $C = 10$ , and  $G = 11$ .
- 3) Conversion into corresponding decimal values.
- 4) Conversion of decimal values into ASCII characters.
- 5) Split each string into equal size blocks  $R_j$ .

The encryption process continues as the same steps, 3-6 in the base technique. Fig. 1 gives a pictorial representation of the system for the encryption-decryption process. The encryption process is illustrated in green, the key generation process in yellow, and the decryption process is in blue. These steps are similar to the original algorithm, and the improvements are

added as new layers (in red) and displayed distinctively in the encryption and decryption process. Table I indicates the DNA encoding/decoding table being introduced to the algorithm as applied in [9].

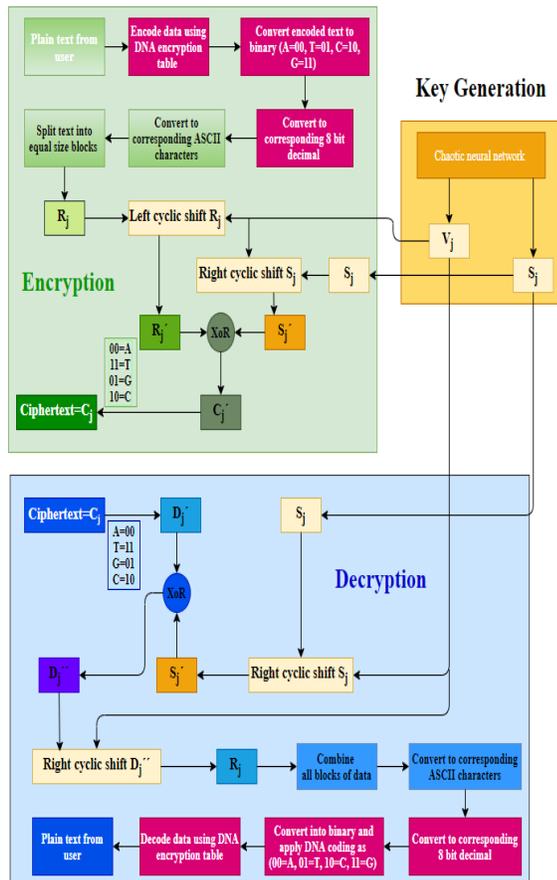


Fig. 1. The Proposed Technique with Detailed Encryption and Decryption

TABLE I. DNA ENCODING/DECODING TABLE [9]

DNA Base Sequence				
ACAT- a	ACTC- q	CAAT- G	ATAA- W	ATTA- ,
ACTG- b	ACCG- r	CATG- H	ATTT- X	ATCC- .
ACCC- c	TCTC- s	CACG- I	ATCG- Y	TTTA- ?
ACGA- d	TCCC- t	CAGT- J	ATGC- Z	TTCG- /
TCAT- e	CCTT- u	GAAG- K	TTAA- 0	CTTC- :
TCTG- f	CCCC- v	GATA- L	TTTT- 1	CTCG- ;
TCCG- g	GCTA- w	GACG- M	TTCC- 2	GTTC- "
TCGT- h	GCCC- x	GAGG- N	TTGG- 3	GTCC- '
CCAG- i	AAAA- y	AATA- O	CTAT- 4	AGAG- {
CCTA- j	AATT- z	AACG- P	CTTG- 5	AGTA- [
CCCG- k	AACC- A	TATC- Q	CTCC- 6	AGCG- }
CCGG- l	AAGG- B	TACG- R	CTGA- 7	AGGG- ]
GCAA- m	TAAT- C	CATC- S	GTAT- 8	TGAA-
GCTT- n	TATG- D	CACC- T	GTTG- 9	TGTT- \
GCCG- o	TACC- E	GATT- U	GTCC- <	TGCG- +
GCGC- p	TAGA- F	GACC- V	GTGT- >	TGGC- =
CGAA- -	CGCC- )	GGAT- *	GGCC- ^	AGTT- \$
CGTT- -	CGGG- (	GGTG- &	GGGA- %	AGCC- #
TGTA- @	TGCC- j	CGTA- ~	CGCG- `	GGCG- £

#### IV. EVALUATION PARAMETERS

In this section, several tests from the literature are performed to evaluate the randomness of the ciphertext produced by the proposed algorithm and the base technique [5], [7], [15]-[17]. These tests can only be performed on binary sequences. Thus, the ciphertext is then converted from DNA sequence into binary to complete the evaluation. Three different datasets have been used as inputs to these tests, categorizing them as low density, high density, and random [18]-[20]. Low and high density are the biased datasets, where plaintext has all zeros and only one 1 bit in string. A high density is an exact opposite with all ones but only 1 zero. The purpose of using biased data is to identify the exact randomness in the ciphertext. For an algorithm being provided with random plaintexts, there are high chances that the generated ciphertext will also be random. On the other hand, for a non-random (biased) dataset, the probability of obtaining a random ciphertext is relatively low. Therefore, the use of different categories of datasets can establish confidence in the improved scheme from security perspectives.

##### A. Frequency (Mono Bit) Test

The frequency test calculates the number of a binary string, 0's and 1's appear in the ciphertext. This test determines that either the number of zeros and ones are equal or not, as this is one of the desired properties of a ciphertext [5]. Value 0.01 is the level of significance for this test which means that only 1 sample out of 100 will be rejected. Ideally, the resultant value should be "1", which means a perfect balance of 0 and 1 in the string. This test assesses the closeness of these values to 1/2 of the total numbers of binary string appeared in the ciphertext, as it is ideal for these values to be equal. For this test, the preliminaries are:

$n$  the length of the bit string,

$\epsilon$  the sequence of bits in the string as  $\epsilon = \epsilon_1, \epsilon_2, \dots, \epsilon_n$

$S_{obs}$  the absolute value for summation of  $X_i$ .

$$X_i = 2\epsilon - 1 = \pm 1 \tag{1}$$

$$S_n = X_1 + X_2 + \dots + X_n \tag{2}$$

$$S_{obs} = \frac{|S_n|}{\sqrt{n}} \tag{3}$$

Finally, the tail probability, i.e., the p-value, is calculated in (4).

$$p\text{-value} = \text{erfc}\left(\frac{S_{obs}}{\sqrt{2}}\right) \tag{4}$$

*erfc* is a complementary error function. This test evaluates the p-value, whereas if the computed value of p is less than 0.01, it is concluded that the given sequence is not random [15], [16]. On the other hand, if the p-value is more than 0.01, the string passed the test and can be declared as a random string.

##### B. Avalanche Effect

A small change in plain text or key yielding a significant change in the ciphertext is called the avalanche effect (5). It's a highly desirable property for algorithm design, such as the higher the avalanche effect, the better the algorithm [21]-[27].

Avalanche > 50% of an exemplary algorithm makes the cipher more random and less predictable for attackers.

$$\text{Avalanche Effect} = \frac{\text{Number of flipped bits in cipher text}}{\text{Total number of bits in cipher text}} \quad (5)$$

### C. Entropy

Shannon introduced the concept of entropy in bits in 1948 [7] and is termed as uncertainty in the expected output bits. Uncertainty of the cipher is determined by the number of plaintext bits that can be recovered from scrambled ciphertext to get the original message [17] successfully. Moreover, entropy is the weighted average of optimal bit representation size, such as the average size of an encoded message. Mathematically, entropy can be defined as in (6).

$$H(X) = - \sum_{x \in X} (\text{Pr}[X] \log_2(\text{Pr}[X])) \quad (6)$$

Here we are calculating the entropy of X with  $X = \{0,1\}$ . Calculating for both bases as in (7).

$$H(X) = -[P(0) \log_2(P(0)) + P(1) \log_2(P(1))] \quad (7)$$

The highest uncertainty is only achieved when the values are equally distributed i.e.

$$H(X) = 1 \quad (8)$$

### D. Hamming Weight

Two strings of equal length having different symbols at some positions; the total number of those positions is called hamming weight [21], [26]. A higher value of the hamming weight represents the better randomness of the binary sequence.

$$\text{Hamming Weight} = \frac{\text{Total number of non zero bits}}{\text{Length of the cipher text}} \quad (9)$$

## V. RESULT AND DISCUSSION

Both techniques discussed in previous sections are implemented in Matlab 2019 to evaluate the randomness of the ciphertext. Tables II and III have results for all of the tests described in Section IV. The value of plaintext is changed by toggling bits across the string followed by a constant key. The plaintexts in Table II are 128 bits long. The key is set to "00011000100101010010010000101011100001101010010001100110000111111000110101100010111011100100100111110011011000001111100110010". The same key is used to produce the ciphertext for further evaluations. As the frequency is one of the tests by NIST [28] and the minimum required length of the string is 100 bits, the ciphertext bits are concatenated to apply this test. Here, we have 33 high density, 33 low density, and 34 random plain texts for evaluation, and, ultimately, the average value of all these observations is calculated.

### A. Frequency Test

As mentioned in the previous section, the frequency test calculates the number of 0's and 1's that appear in the ciphertext. If the p-value calculated on the ciphertext is more than 0.01, the ciphertext is concluded as a random string, or else it is a non-random. Thus, Table II shows the p-value of the ciphertext produced by the base and the improved algorithm using (1), (2), (3), and (4). High density, low density, and random plaintexts are used as inputs to both algorithms.

TABLE II. FREQUENCY ANALYSIS, AVALANCHE EFFECT AND HAMMING WEIGHT TEST FOR THE BASE AND THE IMPROVED TECHNIQUE

Plaintext	Frequency Test		Avalanche Effect		Hamming Weight	
	Base	Improved	Base	Improved	Base	Improved
High density	0.8227	0.9872	38.06 %	52.9 %	62.3	63.5
Low density	0.8953	0.987	40.6 %	55.33 %	63.9	64.2
Random	0.7625	0.9891	37.99%	55.7%	63.5	63.9
<b>Average</b>	<b>0.8268</b>	<b>0.9877</b>	<b>38.55%</b>	<b>54.64%</b>	<b>63.23</b>	<b>63.87</b>

Based on Table II, both techniques have passed the NIST frequency test successfully with the average p-values (y-axis) for three variants of plaintexts are greater than 0.01. Each p-value (y-axis) of the ciphertext generated from those variants of plaintexts is also depicted in Fig. 2 and 3. The ideal p-value for this test is 1, and all the ciphertexts should have a value close to 1. Based on Fig. 2 and 3, it can be seen that there are specific outputs that have successfully achieved a p-value of 1. However, this ratio is minimal in case of the base technique compared to the improved technique. It can be seen from Table II that the average p-value of the improved technique (0.9877) is very close to 1.

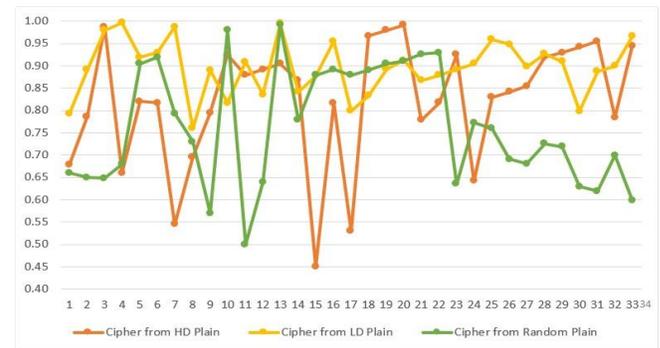


Fig. 2. Frequency Analysis of base Technique.

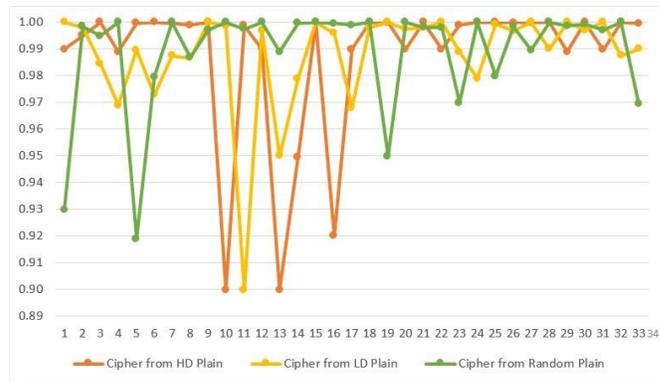


Fig. 3. Frequency Analysis of Improved Technique.

### B. Avalanche Effect

The avalanche effect is a very desirable property when it comes to randomness in the ciphertext. As mentioned earlier, the higher the avalanche effect, the better the security. Any given scenario where the attacker has access to ciphertext tries to establish a relationship between ciphertext and its plaintext.

If changing one bit results in a change of more than 50% bits, it becomes challenging for the attacker to retrieve the original message. In Table II, the base technique has the avalanche effect values, which range from 37.99% for random to 38.06% and 40.6% for high and low density plaintext, respectively. Meanwhile, the improved technique has values ranging from 52.9% to 55.7%, significantly higher than the base technique.

These values are calculated using (5) and presented in Fig. 4 and 5. As depicted in Fig. 4, changing 1 bit in plaintext has generally introduced a difference from 8% to 65%. Whereas by looking at Fig. 5, it is evident that observed values range between 40% and 70%. Row 5 in Table II has the average value of avalanche effect, and it can be observed that this value is 38.55% in the case of the base technique and has significantly improved to 54.64% for the improved technique.

Example scenarios of avalanche effect have been presented in Table III, where “CRYPTOGRAMMATIST” is the original plaintext, feed to the algorithm and the produced ciphertext is used as a reference to calculate the number of flipped bits. For example, changing one bit in the 40th location of the binary sequence in the plaintext yields 24 flipped bits in the ciphertext by the base technique. Thus, the avalanche effect is 18.755%, considering that the length of ciphertext is 128 bits. For the base algorithm, the result shows that the avalanche effects range from 12.5% to 32.0312%, with an average of 19.72% when changing one bit of the binary sequence in the plaintext at different locations (bold and underlined bit). Meanwhile, the improved technique has the avalanche effects range from 53.9% to 61.75%, with an average of 57.4175%. The average avalanche effect indicates a significant improvement of

37.69%. Thus, this new encryption/decryption technique can be used to improve security for an environment in which data sensitivity and randomness are essential.

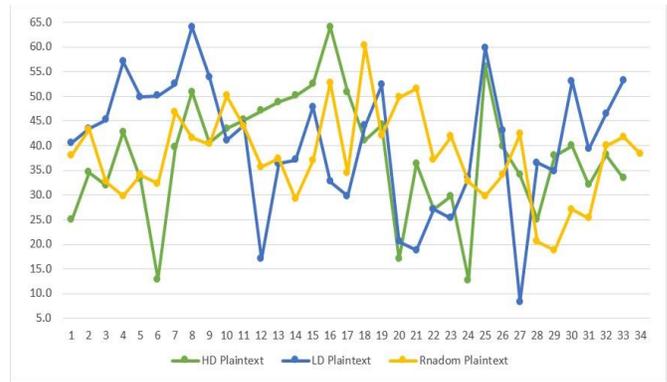


Fig. 4. Avalanche Effect of base Technique.

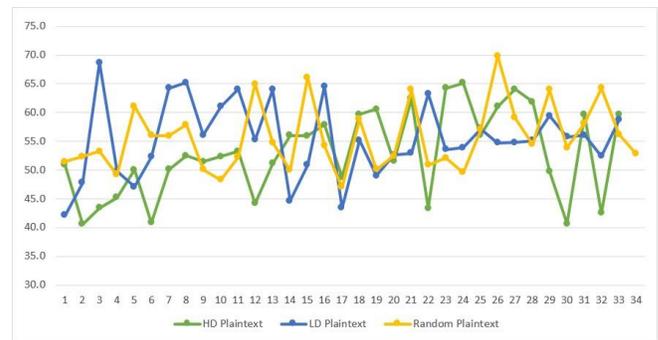


Fig. 5. Avalanche Effect of Improved Technique.

TABLE III. AVALANCHE EFFECT AND ENTROPY FOR THE BASE AND IMPROVED TECHNIQUE

Plaintext	Base Technique			Improved Technique		
	Ciphertext	Avalanche effect	Entropy $H(X)$	Ciphertext	Avalanche effect	Entropy $H(X)$
CRYPTOGRAMMATIST	11001111001001101110011001101000 10001111100000001110101110111111 1101010111101111101100110000001 010000110100100111111010111100100	-----	0.9914	00101100101001010100101011100001 00111011000010100110010111110000 00110100101111111110011011011111 11000110000101000101111010110110	-----	0.9984
CRYPTOGRAMMATIST	11001111001001101110011001101000 10001111100000001110101110111111 11010101111011111000110011010100 00010110000111001010000010110001	24/128= 18.755%	0.9984	001011001000111111010010000001110 11000000101000011000101101011010 10001111000100000101110101110001 0101001101000001000000001011100	79/128 = 61.72%	0.9745
CRYPTOGRAMMATIST	11001111001001101110011001101000 10001111100000011011111011101010 10000000101110101000110011010100 00010110000111001010000010110001	41/128= 32.0312%	0.9972	10110011000100101010010000001011 11101100001101001111000000001101 01100001111010101001111011011111 11000011111010111111010101011101	78/128 = 60.93%	0.9956
CRYPTOGRAMMATIST	11001111001001101110011001101000 10001111100000001110101110111111 1101010111101111101100110000001 01000011010000100000101101011010	16/128= 12.50 %	0.9984	1011010010001111111000101011110 10111011110111110000101110100110 10001111000100000011000101110001 01111001000101000101111011100010	69/128 = 53.9%	0.9972
CRYPTOGRAMMATIST	11001111001001101110011001101000 10001111100000001110101110111111 1101010111101111101100110000001 01000011101100100000101101011010	20/128= 15.625%	0.9956	00100011000110101111000101011011 11000000101000011000101101010101 01100001111011111110011011011010 1001001101000001000010111100011	68/128 =53.12%	0.9998
Average	-----	19.72%	0.9963	-----	57.4175%	0.9931

### C. Entropy

Equation (6) and (7) are applied to find the entropy of ciphertext. In Table III, the entropy of the ciphertext has been calculated for the base and the proposed technique. It can be seen that the entropy of ciphertext in both cases is nearly equal, with a value of 0.9963 for the base technique and 0.9931 for the proposed technique, which is the information content per bit. So it can be said that the information content per bit has not decreased even for the improved technique but has sustained some optimum value throughout the observations. The ideal entropy in the given case is 1, as depicted in (8), but the observed entropy for both techniques is very close to one.

### D. Hamming Weight

Hamming weight has been calculated using (9). In Table II, it is observed that hamming weight for base technique ranges from 62.3 to 63.9, whereas for improved technique, this value ranges from 63.5 to 64. The ideal expected value for hamming weight in a binary string of 128 bits should be 64. The average observed value of 100 plain texts for the base technique is 63.23, whereas, for the improved technique, it's 63.87.

In summary, Tables II and III confirm that the proposed technique performs better for frequency, avalanche effect, and hamming weight. The observed values are not only better than the base technique but are also nearly equal to ideal expected values. Whereas for entropy calculation, the value of the improved technique has not improved yet, the difference from the base technique is quite negligible. Hence, the improved technique is a better alternative to the proposed technique, where enhanced security is offered with all the security considerations of the base technique.

## VI. CONCLUSION

DNA cryptography has served as a better alternative to traditional systems in recent times. Advancement in the study helps to identify the security vulnerabilities in the existing systems. This research highlights that by carefully examining the ciphertext produced by the base technique, in terms of avalanche effect can be further improved. The average avalanche effect is 38.55% when flipping one bit of binary sequence in the plaintext for 100 different plaintexts ranging from high density, low density, and random data set. On the other hand, the average avalanche effect of the proposed technique has increased to 54.64% by introducing a DNA encoding table. The work also includes the frequency, entropy, and hamming weight to test the overall security of the improved system. The results show that the improved technique is better in terms of the frequency's p-value, avalanche effect, and hamming distance than the base technique. For entropy, the value produced by both algorithms is approximately equal. Hence, the improved technique is a better alternative to the proposed technique, and this research. A good future direction of this work can be defining new trajectories in key schedules and analyzing the impact of key changes to the ciphertext.

### ACKNOWLEDGMENT

The authors would like to thank all reviewers for their helpful comments. The authors would also like to thank the

Ministry of Higher Education Malaysia for supporting the research under Fundamental Research Grant Scheme Vot No. FRGS/1/2019/ICT03/UTHM/03/1 and partially sponsored by Universiti Tun Hussein Onn Malaysia.

### REFERENCES

- [1] X. Zhang, Z. Zhou, and Y. Niu, "An image encryption method based on the feistel network and dynamic DNA encoding," *IEEE Photonics Journal*, vol. 10, no. 4, pp. 1-14, 2018.
- [2] S. Sadeg, M. Gougache, N. Mansouri, and H. Drias, "An encryption algorithm inspired from DNA," in 2010 International Conference on Machine and Web Intelligence, 2010, pp. 344-349: IEEE.
- [3] H. M. Bahig and D. I. Nassr, "DNA-based AES with silent mutations," *Arabian Journal for Science and Engineering*, vol. 44, no. 4, pp. 3389-3403, 2019.
- [4] B. M. Kumar, B. R. S. Sri, G. Katamaraju, P. Rani, N. Harinadh, and C. Saibabu, "File Encryption and Decryption Using DNA Technology," in 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), 2020, pp. 382-385: IEEE.
- [5] Y. Zhang, "The image encryption algorithm based on chaos and DNA computing," *Multimedia Tools and Applications*, vol. 77, no. 16, pp. 21589-21615, 2018.
- [6] A. Rukhin, J. Soto, J. Nechvatal, M. Smid, and E. Barker, "A statistical test suite for random and pseudorandom number generators for cryptographic applications," *Booz-allen and hamilton inc mclean va2001*.
- [7] C. E. Shannon, "A mathematical theory of communication," *The Bell system technical journal*, vol. 27, no. 3, pp. 379-423, 1948.
- [8] S. S. Roy, S. A. Shahriyar, M. Asaf-Uddowla, K. M. R. Alam, and Y. Morimoto, "A novel encryption model for text messages using delayed chaotic neural network and DNA cryptography," in 2017 20th International Conference of Computer and Information Technology (ICCIT), 2017, pp. 1-6: IEEE.
- [9] N. H. UbaidurRahman, C. Balamurugan, and R. Mariappan, "A novel DNA computing based encryption and decryption algorithm," *Procedia Computer Science*, vol. 46, pp. 463-475, 2015.
- [10] Y. Niu, K. Zhao, X. Zhang, and G. Cui, "Review on DNA Cryptography," in *International Conference on Bio-Inspired Computing: Theories and Applications*, 2019, pp. 134-148: Springer.
- [11] M. R. Biswas, K. M. R. Alam, S. Tamura, and Y. Morimoto, "A technique for DNA cryptography based on dynamic mechanisms," *Journal of Information Security and Applications*, vol. 48, p. 102363, 2019.
- [12] F. E. Ibrahim, H. Abdalkader, and M. Moussa, "Enhancing the security of data hiding using double DNA sequences," in *Industry Academia Collaboration Conference (IAC)*, 2015, pp. 6-8.
- [13] A. Hazra, C. Lenka, A. Jha, and M. Younus, "A Novel Two Layer Encryption Algorithm Using One-Time Pad and DNA Cryptography," in *Innovations in Computer Science and Engineering: Springer, Singapore*, 2020, pp. 297-309.
- [14] M. R. Biswas, K. M. R. Alam, A. Akber, and Y. Morimoto, "A DNA cryptographic technique based on dynamic DNA encoding and asymmetric cryptosystem," in 2017 4th International Conference on Networking, Systems and Security (NSysS), 2017, pp. 1-8: IEEE.
- [15] A. S. Al-Wattar, R. Mahmood, Z. A. Zukarnain, and N. I. Udzir, "Generating a new S-Box inspired by biological DNA," *International Journal of Computer Science and Application*, vol. 4, no. 1, pp. 32-42, 2015.
- [16] D. A. Zebari, H. Haron, S. R. Zeebaree, and D. Q. Zeebaree, "Multi-Level of DNA Encryption Technique Based on DNA Arithmetic and Biological Operations," in 2018 International Conference on Advanced Science and Engineering (ICOASE), 2018, pp. 312-317: IEEE.
- [17] G. Ye, C. Pan, X. Huang, Z. Zhao, and J. He, "A chaotic image encryption algorithm based on information entropy," *International Journal of Bifurcation and Chaos*, vol. 28, no. 01, p. 1850010, 2018.
- [18] H. Othman, Y. Hassoun, and M. Owayjan, "Entropy model for symmetric key cryptography algorithms based on numerical methods,"

- in 2015 International Conference on Applied Research in Computer Science and Engineering (ICAR), 2015, pp. 1-2: IEEE.
- [19] H. Shi, Y. Deng, and Y. Guan, "Analysis of the avalanche effect of the AES S box," in 2011 2nd International Conference on Artificial Intelligence, Management Science and Electronic Commerce (AIMSEC), 2011, pp. 5425-5428: IEEE.
- [20] C. P. Dewangan, S. Agrawal, A. K. Mandal, and A. Tiwari, "Study of avalanche effect in AES using binary codes," in 2012 IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT), 2012, pp. 183-187: IEEE.
- [21] H. Agrawal and M. Sharma, "Implementation and analysis of various symmetric cryptosystems," Indian Journal of science and Technology, vol. 3, no. 12, pp. 1173-1176, 2010.
- [22] S. Ramanujam and M. Karuppiyah, "Designing an algorithm with high Avalanche Effect," IJCSNS International Journal of Computer Science and Network Security, vol. 11, no. 1, pp. 106-111, 2011.
- [23] S. Vyakaranal and S. Kengond, "Performance analysis of symmetric key cryptographic algorithms," in 2018 International Conference on Communication and Signal Processing (ICCSP), 2018, pp. 0411-0415: IEEE.
- [24] K. D. Muthavhine and M. Sumbwanyambe, "An analysis and a comparative study of cryptographic algorithms used on the Internet of Things (IoT) based on avalanche effect," in 2018 International Conference on Information and Communications Technology (ICOIACT), 2018, pp. 114-119: IEEE.
- [25] S. T. Nadu, "A block cipher algorithm to enhance the avalanche effect using dynamic key-dependent S-box and genetic operations," International Journal of Pure and Applied Mathematics, vol. 119, no. 10, pp. 399-418, 2018.
- [26] X. Chai, Z. Gan, Y. Lu, Y. Chen, and D. Han, "A novel image encryption algorithm based on the chaotic system and DNA computing," International Journal of Modern Physics C, vol. 28, no. 05, p. 1750069, 2017.
- [27] M. Imdad, S. N. Ramli, H. Mahdin, B. U. Mouni, and S. Sahar, "An Enhanced DNA Sequence Table for Improved Security and Reduced Computational Complexity of DNA Cryptography," in EAI International Conference on Body Area Networks, 2020, pp. 106-120: Springer.
- [28] A. Sharaieh, A. Edinat, and S. AlFarraji, "An enhanced polyalphabetic algorithm on vigenerecipher with DNA-based cryptography," in 2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA), 2018, pp. 1-6: IEEE.

# Multistage Sentiment Classification Model using Malaysia Political Ontology

Nur Farhana Ismail, Nur Atiqah Sia Abdullah\*, Zainura Idrus

Faculty of Computer and Mathematical Sciences  
Universiti Teknologi MARA  
40450 Shah Alam, Selangor, Malaysia

**Abstract**—Now-a-days, people use social media platforms such as Facebook, Twitter, and Instagram to share their opinions on particular entities or services. The sentiment analysis can get the polarity of these opinions, especially in the political domain. However, in Malaysia, current sentiment analysis can be inaccurate when the netizen tempts to use the combination of Malay words in their comments. It is due to the insufficient Malay corpus and sentiment analysis tools. Therefore, this study aims to construct a multistage sentiment classification model based on Malaysia Political Ontology and Malay Political Corpus. The reviews are carried out in sentiment analysis, classification techniques, Malay sentiment analysis, and sentiment analysis on politics. It starts with the data preparation for Malay tweets to produce tokenized Malay words and then, the construction of corpus using corpus filtering, web search, and filtering using linguistic patterns before enhancing with political lexicons. The process continues with the classifier construction. It started with a generic ontology with Malaysia's political context. Lastly, twelve features are identified. Then the extracted features are tested using different classifiers. As a result, Linear Support Vector Machine yields an accuracy of 86.4% for the classification. It proved that the multistage sentiment classification model improved the Malay tweets classification in the political domain.

**Keywords**—Malay corpus; political ontology; sentiment analysis; sentiment classification; social media

## I. INTRODUCTION

Social media is a common platform for internet users. Netizens can spread and viral issues quickly via social media like Facebook, Twitter, Blog, Instagram, and online platforms. Social media allows people to voice opinions freely on current matters. Their opinions are beneficial, especially for the business, marketing strategies, and policymakers include government. Sentiment analysis tools can analyze their comments into exploitable information.

The existing sentimental analysis classifiers manage to analyze different languages such as English, French, Indian, Arabic, and Chinese. However, it has yet insufficiently in analyzing the Malay language accurately. Each comment containing Malay words will be classified as neutral in most of the social media monitoring tools. It is one of the reasons for the Malay sentiment classifier to support the research on classifying the Malay language, which use lexicon and k-nearest neighbor [1], lexicon [2] and other classification

methods [3]. Besides, there is lacking Malay sentiment analysis that covers the political domain [4].

The author in [4] has conducted a study on the political inclination classifier model for Malay text in social media data. This study focuses on Malay sentiment analysis in the political domain. However, it needs to be improved to get a more accurate sentiment classification. Besides, some corpora are for the abbreviations [5] and hadith [6]. However, there is a need to create a corpus in the political domain.

Currently, most of the agencies use social media monitoring tools to extract comments for strategic planning in marketing, customer behavior, political inclination, and etc. However, the comments that contain Malay words are classified as neutral. This shortage motivates this research to improve the sentiment classification. It sets the interest to investigate the sentiment classification in the political domain due to the political scenario in Malaysia.

The main idea of this study is to propose a multistage sentiment classification model using Malaysia Political Ontology and Malay Political Corpus. This model aims to increase the sentiment classification by adding the entity classification to the existing process. Besides, new features are suggested based on the entity classification. By using this model, the analysis and monitoring process of social media can speed up. Besides, this research helps to expand the knowledge in this field to get better accuracy of sentiment. This paper continues with Section II explains the related works. Section III presents the methods and processes. Section IV and Section V contain the results and discussions. Finally, Section VI concludes the research.

## II. RELATED WORK

### A. Sentiment Analysis

Sentiment analysis is known as opinion mining where the purpose is to determine people's opinion towards certain entities such as an event, product, management, politician, and government issues [7]. Some studies on Malay sentiment analysis use different approaches to construct the Malay sentiment classifiers. Previous studies use the machine learning approaches for sentiment classification include machine learning [8-10], immune network [11], artificial immune network [12] and hybrid approaches [1, 6, 13].

\*Corresponding Author

Sponsor by Ministry of High Education (MOHE) Malaysia, under the Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/UITM/02/9).

TABLE I. MALAY SENTIMENT ANALYSIS

Author	Content of Article			
	Approach	Dataset	Politic	Ontology
[10]	Machine Learning	Newspaper	No	No
[11]	Machine Learning	Newspaper	No	No
[12]	Machine Learning	Newspaper	No	No
[8]	Machine Learning	Online Review	No	No
[9]	Machine Learning	Online Review	No	No
[2]	Lexicon based	Facebook Twitter	No	No
[1]	Hybrid	Online Review	No	No
[4]	Hybrid	Twitter	Yes	No
[13]	Hybrid	Article	No	Yes

Other than that, a lexicon-based approach is used to perform classification [2]. Although the machine learning approaches are used for Malay sentiment analysis, it does not mean this approach is the only one to perform Malay sentiment classification. Reference [13] proved that the hybrid approach gets the highest accuracy in the sentiment classification, which is better than previous studies.

Table I shows the Malay sentiment analysis in terms of approach, types of datasets, political domain, and application on ontology. Three major approaches are machine learning, lexicon-based, and hybrid approach used in Malay sentiment analysis.

From Table I, the study [13] improved the accuracy in sentiment analysis for the Malay language. It deals with informal language style and multilingualism that has become the norm of communication in social media. It used a hybrid approach, which is a combination of machine learning and a knowledge base. The ontology helps to get the more accurate sentiment with 94.34%. The polarities are positive, negative, neutral, and mixed. However, it is not in the political domain. Hence, it is a motivation for sentiment analysis on the political domain of other countries to find out the workflow in political sentiment classification.

### B. Sentiment Analysis in Political Domain

Some approaches that classify the sentiment in the political domain are the machine learning approach, lexicon-based approach, ensemble approach, and multistage classification approach. Table II shows the sentiment analysis in the political domain in various countries use mostly tweets as the dataset.

Two studies [14-15] performed sentiment classification using the machine learning approach. The researchers use tweets as the dataset in Egypt and Indonesia. The lexicon-based approaches in [16-17] used online news and tweets that related to Indonesia and Turkey political context. The research [4, 18] performed sentiment classification using a hybrid approach. These two researches used tweets and corpus-based approach in Malaysia and India. Lastly, the research [19] used a multistage classification approach to get higher accuracy. The study was carried out in United States by using hybrid approach.

TABLE II. SENTIMENT ANALYSIS IN POLITICAL DOMAIN

Author	Content of Article			
	Approach	Dataset	Corpus	Country
[14]	Machine Learning	Tweets	No	Egypt
[15]	Machine Learning	Tweets	No	Indonesia
[16]	Lexicon based	Online News	Yes	Indonesia
[17]	Lexicon based	Tweets	Yes	Turkey
[4]	Hybrid	Tweets	Yes	Malaysia
[18]	Hybrid	Tweets	Yes	India
[19]	Hybrid	Tweets	No	United States

From Table II, the researchers [19] predicted the presidential election of the United States using Twitter sentiment analysis. The multistage classification approach classified the tweets of Donald Trump and Hillary Clinton. The accuracy of sentiment classification for Donald Trump and Hillary Clinton is 0.99% and 0.98%. From the reviews on the sentiment analysis in political domain, the studies [16, 19] become the anchors to construct a Malay sentiment classifier in this study.

### C. Ontology

In [16], the ontology in a sentiment classifier helps to analyze social media content and gets an accurate sentiment. Ontology is a set of concepts related to entities, and the ontological hierarchy is constructed from the relations between concepts of entities.

There is still a lack of political ontology for the political domain in Malaysia. The construction of Malay political ontology (MPO) is adapted from [20]. Reference [20] constructed Australian politic ontology uses BBC politic ontology. There are four main concepts in BBC political ontology, which are person, place, organization, and event.

However, Australian politicians and parties are the main concepts in the ontology because it focuses on the election. These concepts with 53 instances for politicians, and 4 instances for parties. The Australian political structure is similar to Malaysian. Therefore, this study becomes another reference model to construct Malaysia Political Ontology (MPO).

### D. Multistage Classification

The study [19] identified the winner from the election of the United States. The study proposed a multistage classification to classify the entity and sentiment of the tweets. The first stage of classification, the classifier called as entity classifier that classifies a general stream data into the respective entities. The classifier is trained with the entire dataset labelled by the entities. For the next stage of classification, the classifier called a sentiment classifier that classifies the sentiment of the tweets written refer to that particular candidate. Therefore, each candidate has a classifier associated with him or her. The classifier is trained with a dataset that pertaining to only its candidate.

Hybrid approach is used to perform the multistage classification [19]. The hybrid approach combines the machine learning with knowledge-based approach to improve the accuracy of sentiment analysis. The postings are classified into positive, negative or neutral. The result from [19] shows the accuracy of 94.34%, which is better than Naïve Bayes (NB), k-nearest neighbor (kNN) and Support Vector Machine (SVM).

### III. METHODOLOGY

The dataset in this research is obtained from the Centre for Media and Information Warfare Studies (CMIWS) of Universiti Teknologi MARA (UiTM) Malaysia. There is a total of 1207 tweets in the political domain. There are six phases in this research, which are Preliminary Study, Data Pre-processing, Corpus Construction, Entity Construction, Multistage Classification Modelling, and lastly Evaluation.

#### A. Preliminary Study

In the preliminary study phase, literature reviews on articles to identify the research gap of sentiment analysis. It includes sentiment classification techniques, sentiment analysis in the Malay language, and political domain. Besides, it highlights the problem statement, research questions, objectives, scopes, and selected sentiment analysis techniques in the Malay language and political area.

#### B. Data Pre-Processing

This study focuses on Malay tweets. From the tweets collection, 752 Malay tweets are extracted. These tweets are the netizen comments related to political issues and selected politicians in Malaysia. The data pre-processing includes six processes to remove the noisy data. These processes begin with the removal of external links, symbols, and numbers. It continues with the lowercase conversion, abbreviation correction, stop words removal, word stemming, and then tokenization.

The external links, symbols, and numbers in a tweet are removed because these elements do not contain any meaning in classification. This process is similar to the previous studies [4, 15, 17-19]. Then, the remaining words are converted into lowercase to ease the word checking in the sentiment classification process. The abbreviations are converted into formal words as the abbreviations cannot be classified correctly [4].

Then, the process continues with removing the stop words as these words contain no meaning to analyze [14, 16]. The stemming process uses Fatimah stemmer [21] to get the seed words in the Malay language. The last process in the data pre-processing is word tokenization [4, 14] that split the words and store them in the database.

#### C. Corpus Construction

The corpus construction process from [22] is adapted in this research. It contains corpus filtering, web search, and filtering using linguistic patterns and domain-specific polarity lexicon. Our focus is building a Malay Political Corpus.

The corpus filtering contains two processes, which are word extraction and unique word selection. Firstly, 18 political words are extracted as the initial list. Next, the words that are

related to the election are selected. At the end of these processes, it produces a list of five political words that are related uniquely to the election.

After that, these election words are used together with a Linguistic pattern for web search to find more election-related words. There are two patterns in this searching process. In the first pattern, 'Pilihanraya' is used, which represents election in Malay. In the second pattern, it combines 'Pilihanraya' with 'seed words' related to the election.

- Pattern 1: Pilihanraya include(s)\*.
- Pattern 2: Pilihanraya + "seed word".

These unique seed words include 'calon' (candidate), 'kempen' (campaign), 'manifesto' (manifesto), 'parti politik' (political party), and 'pengundi' (voter). Table III contains Malay seed words and sample lexicon related to election. There are 182 lexicons after this searching process.

TABLE III. LIST OF LEXICON

Seed Word	Sample of Lexicon	Total Lexicon
Calon	Wakil, Tanding, Kredibiliti, Khidmat, Pilih	65
Kempen	Strategi, Demokrasi, Lawan, Provokasi, Taktik	48
Manifesto	Subsidi, Janji, Sistematis, Tawar, Bersih, Hapus	15
Parti Politik	Agenda, Bangkang, Kuasa, Propaganda	36
Pengundi	Pangkah, Protes, Daftar, Undi, Sokong, Tolak	18

Then, the process continues with setting the polarity and score for these lexicons. The lexicon is classified into positive, negative, or neutral polarity. The positive word has a score of 1 to 5 based on the meaning of the lexicon. The negative word has a score of -5 to -1, while the neutral word gets 0. At the point, the political corpus is successfully constructed.

#### D. Entity Construction

In this process, the political parties are classified into government or opposition. In the entity construction, the generic ontology construction and instances enrichment from [20] are adapted.

A generic ontology has a set of concepts related to an entity. The relations between these concepts are organized into an ontological hierarchy. The ontology is constructed using Protégé 5.5.0 tool and using OntoGraf for visualizing the relationship in the ontology.

Four main concepts in the ontology include Person, Place, Organization, and Event. The person concept is the class of people in Malaysian political environments like voters and politicians. The place concept is related to the electoral areas such as state and constituency. The organization concept in Malaysian politics includes political parties, government, and council. The event concept relates to Election Day and campaign.

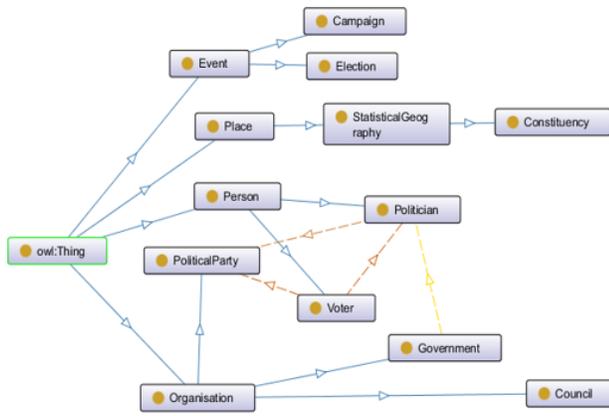


Fig. 1. Main Concept of Malaysian Politic Ontology.

This ontology is not sufficient to classify the entities in the tweets. Therefore, it needs to be enriched with instances before being fully utilized. The Parliament of Malaysia 2021 is referred to assign the instances for a political party and its candidates. We successfully construct the Malaysia Political Ontology (MPO) shown in Fig. 1.

The people and organization concept are used in this study to represent politicians and political parties. This ontology helps to classify the entity in the tweets. For example, with the instances of the political parties in Malaysia, the algorithm is developed to classify the entity into government or opposition. It helps to identify the sentiment towards the political parties in Malaysia. This information is valuable during the election.

E. Multistage Classification Modeling

The multistage classification from [19] is adapted in this model. There are two stages in multistage classification, which are entity classification and sentiment classification.

Entity classification is the classification based on the Malay Political Ontology (MPO). With MPO, the algorithm helps to classify the politicians and political parties into government or opposition. By this entity classification, it helps in the analysis of sentiment, especially during the pre-election. It speeds up the classification and sentiment analysis process based on the politicians and political parties.

TABLE IV. LIST OF ADAPTED FEATURES

Type	Description
F1	Presence of positive words
F2	Presence of negative words
F3	Presence of positive words in proportion to the presence of negative words
F4	Frequency of positive words in proportion to the frequency of negative words
F5	Weighted probabilities of a positive tweet
F6	Weighted probabilities of a negative tweet

Sentiment classification consists of the feature identification, feature extraction, training dataset, and testing dataset using Support Vector Machine (SVM) classifier. The trained dataset needs to be vectorized data. Therefore, it needs to vectorize data through feature extraction. There are twelve identified features in this research. Table IV shows six features adapted from [1].

From Table IV, the six features and descriptions are aimed to cater to the positive and negative words, proportion calculation, and weighted probabilities calculation.

There are six new features (see Table V) in this model that reflect the political domain in Malaysia. These features are used to cater the entity and words in political domain.

TABLE V. LIST OF NEW FEATURES

Type	Description
F7	Presence of domain specific positive words
F8	Presence of domain specific negative words
F9	Presence of domain specific positive words in proportion to the presence of domain specific negative words
F10	Frequency of domain specific positive words in proportion to the frequency of domain specific negative words
F11	Presence of a positive entity
F12	Presence of a negative entity

The feature extraction converts the words into vectors before training and testing. There are twelve sets of the formula, as stated in Table VI.

TABLE VI. FORMULA FOR FEATURES EXTRACTION

Type	Formula	Description
F1	$F1(T) = p$	T is referred to tweet; p is number of positive words in T
F2	$F2(T) = n$	n is number of negative words in T
F3	$F3(T) = p/n$	p is presence of positive words in T; n is presence of negative words in T
F4	$F4(T) = fp/fn$	fp is frequency of positive words in T; fn is frequency of negative words in T
F5	$F5(T) = p*(1-P+)*mp+$	p is number of positive words in T; P+ is probability of seeing positive words in a tweet; mp+ is manually assigned scores for positive score from lexicon
F6	$F6(T) = p*(1-N+)*mn$	n is number of negative words in T; N+ is probability of seeing negative words in a tweet; mn- is manually assigned scores for negative score from lexicon
F7	$F7(T) = dp$	dp is number of domain specific positive words in T
F8	$F8(T) = dn$	dn is number of domain specific positive words in T
F9	$F9(T) = dp/dn$	dp is presence of domain specific positive word in T; dn is presence of domain specific negative word in T
F10	$F10(T) = fdp/fdn$	fdp is frequency of domain specific positive word in T; fdn is frequency of domain specific negative word in T
F11	$F11(T) = pe$	pe is number of positive entities in T
F12	$F12(T) = pn$	pn is number of negative entities in T

After the extraction process, all data become vectorized data and assigned with sentiment polarity. The data is now ready to be trained and tested using MATLAB. 80% of vectorized data train using the Support Vector Machine classifier in MATLAB. The training dataset process runs eight times on different features for each technique in Support Vector Machine. This experiment aims to find the best features that can achieve high accuracy of sentiment.

After the experiments, the Linear Support Vector Machine classifier achieved high accuracy during the training process. A total of 20% of the remaining vectorized data test the Linear SVM classifier. The results are evaluated.

#### F. Evaluation

The result from the testing process was evaluated by the experts using the Delphi technique. Three experts in the political domain have cooperated in the evaluation phase. The experts are given the sample tweets to label the sentiment polarity separately in the first round of the evaluations. The anonymous responses are shared with the group after the first round. The experts are then allowed to adjust their answers in subsequent rounds. The final sentiments by the experts are collected to compare with the multistage sentiment classifier to measure the accuracy of the classifier.

### IV. RESULTS

The main result for this study is the multistage sentiment classification model. It is a combination of entity and sentiment classification. At the first stage, the politicians and political parties are classified into government or opposition using Malaysia Political Ontology (MPO). This knowledge-based technique helps to identify the entity in the tweets. This stage is crucial in sentiment analysis, especially during the pre-election. The data analysts have to analyze the netizens' opinions

quickly to ensure election candidates decide on the pledge to win the election.

The MPO is constructed using the ontology concept and reflect the political entities in Malaysia, which the political parties are classified into government or opposition. With the enrichment of instances from the Parliament of Malaysia 2021, the MPO can be used to classify the political entities into government (positive), and opposition (negative).

At the second stage, the data from the political corpus are used for sentiment classification. This political corpus is specifically constructed based on the election-related words in the Malay language. It follows the processes of corpus filtering, web search, and filtering using linguistic patterns and domain-specific polarity lexicon. At the end of this stage, the lexicons are classified into positive, negative, or neutral polarity with setting of the score. In this entity classification and political corpus, twelve features are identified and extracted using specific formulas to get the vectorized data. Next, the polarity of the data is set before it is classified using SVM. At the end of the processes, the tweets are classified into positive, negative, and neutral.

Fig. 2 shows the multistage sentiment classification model for Malaysia Political Ontology. It illustrates the whole processes for the multistage sentiment classification. The political tweets need to be pre-processed accordingly to form a political corpus. At the same time, the entity classification uses the MPO to classify the polarity of the political parties. Then, it continues with the final sentiment classification using SVM.

The model is executed in a prototype to prove the concept. The experiments are also carried out using MATLAB. The same dataset is used to compare the results with the previous study.

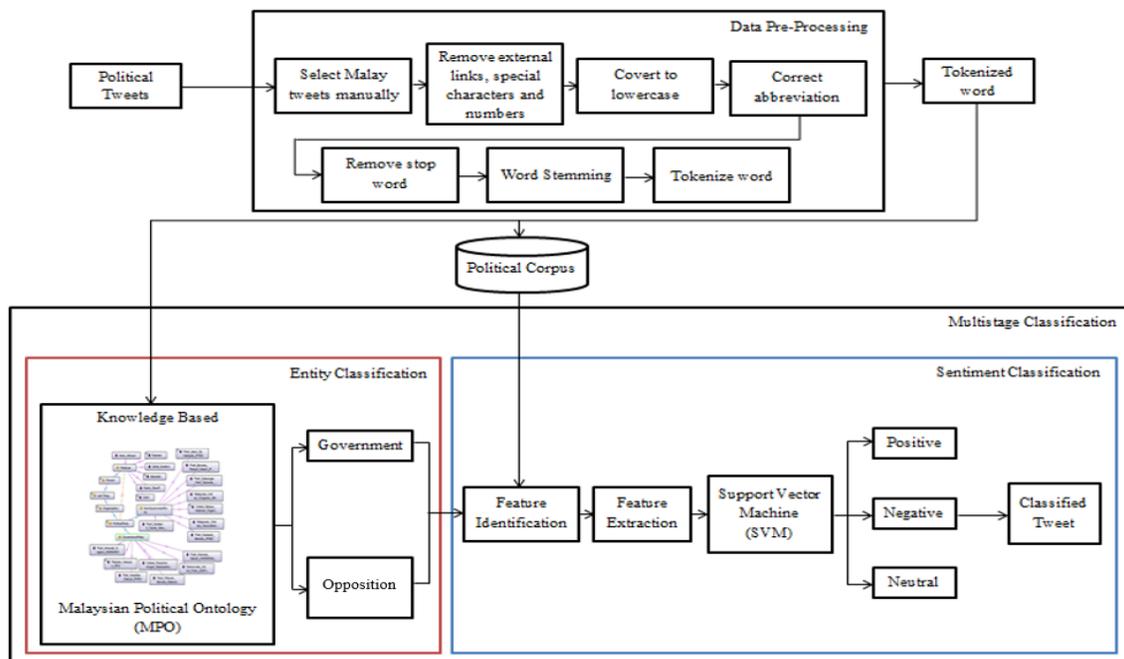


Fig. 2. Multistage Sentiment Classification Model using Malaysia Political Ontology and Malay Political Corpus.

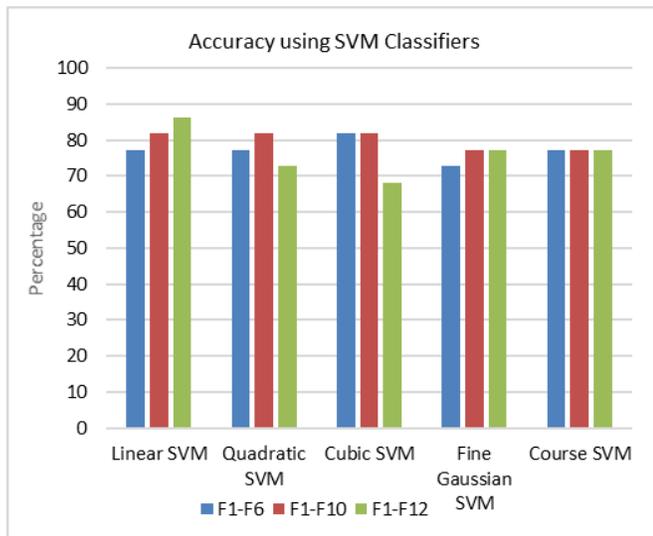


Fig. 3. Accuracy of Classification.

There are five experiments conducted to find the highest accuracy. The classifiers include Linear SVM, Quadratic SVM, Cubic SVM, Fine Gaussian SVM, and Course Gaussian SVM (see Fig. 3).

From Fig. 3, F1-F6 are the features from the existing study. The best accuracy is 81.8% for the F1-F6. The additional features, F7-F12, have improved the accuracy to 86.4% for the classification. The evaluation results show that the 12 features improve the accuracy of the sentiment analysis.

The evaluation of the model is carried out using the Delphi technique. Then, the results between the political experts and the system are compared. We found that the expert results are similar to the results of the experiments.

## V. DISCUSSION

There are few points to discuss from this study. There are available Malay corpora include abbreviation corpus [5] and hadith corpus [6]. However, these corpora are used for the specific domain and are not suitable for the politic. In the political domain, there is a relation between the verb and the candidate or current situation. To ease the classification process, therefore there is a need for specific corpus construction. This study fills the gap by constructing Malay Political Corpus. The terminologies related to the election are the main focus of this study.

The multistage sentiment classification model is successfully constructed in this study. This classification has two stages to classify tweets, which are entity classification and sentiment classification. At the first stage, the politician and party entities are classified as government or opposition using Malaysia Political Ontology (MPO). By classifying the entity, it sentiments the opinions of the netizen towards the politicians and political parties. In the second stage, the classified entity and the political corpus are used for further classification. All data are vectorized using twelve features and finally classifying the polarity of the tweets. The vectorized data are trained and tested using the Support Vector Machine technique. The result

shows that the accuracy is increased by 4.6% compared to the previous study.

However, a few important challenges need to be highlighted in the study. Firstly, the pre-processing process is not covered for negation handling. This negation handling is important to keep the meaning of words. For instance, the word 'tak menang' gives a meaning for 'not winning, with means 'kalah' or lost in English. Thus, the polarity of this word is negative. If there is no negation handling process, the word 'tak' will denote as negative and 'menang' will denote as positive, then the polarity of this word will be neutral. This process affects the accuracy of sentiment.

Secondly, the political corpus in this study is still lacking in lexicon and needs to enrich more political words in future studies. The Malaysia Political Ontology (MPO) only covers person and organization concepts of the political domain. The event and place concepts are out of scope in the study. Therefore, there is a need to covers four main concepts to improve the sentiment analysis in the political domain.

## VI. CONCLUSION

Sentiment analysis tools help to analyze the social media comments into exploitable information for strategic planning in business, marketing, finance, entertainment and politic. The existing sentimental analysis classifiers manage to analyze different languages, but it has yet insufficiently in analyzing the Malay language accurately. Most of the comments that contain Malay words are classified as neutral. This shortage motivates this research to find a better solution for sentiment classification. This research sets the interest to investigate the sentiment classification in the political domain. It is one of the most popular areas due to the political scenario in Malaysia. From the literature, the existing Malay corpora such as abbreviation corpus and hadith corpus are not suitable for the political domain. In the political domain, there is a relation between the verb and the candidate or current politic situation. Therefore, this research constructs Malay Political Corpus, Malaysia Political Ontology, and proposes a multistage classification model. The experiments show the effect of twelve features on the performance of the sentiment classification. The multistage classification model proves that it improves the sentiment classification result by determining the entity in the political domain. The combination of entity classification and sentiment classification in the multistage classification can be a better solution in classifying the sentiments related to the political domain. Besides, the hybrid approach in multistage classification improves accuracy. With the political corpus and the linear SVM, the enhanced features selection increases the accuracy to 86.4%. In the future study, some improvements can be made to the pre-processing, enrich the list of words in the political corpus, and using a larger dataset.

## ACKNOWLEDGMENT

The authors gratefully acknowledge the use of service and facilities of the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA. This study receives funding from the Ministry of High Education (MOHE)

Malaysia, under the Fundamental Research Grant Scheme (FRGS/1/2018/ICT04/UITM/02/9).

REFERENCES

- [1] A. Alsaffar and N. Omar, "Integrating a lexicon based approach and k nearest neighbour for MALAY sentiment analysis," *Journal of Computer Science*, vol. 11, no. 4, pp. 639–644, 2015.
- [2] M. H. Hijazi, L. Libin, R. Alfred, and F. Coenen, "Bias aware Lexicon-based sentiment analysis of Malay dialect on social media data: A study on the SABAH LANGUAGE," *2016 2nd International Conference on Science in Information Technology (ICSITech)*, 2016.
- [3] N. A. Abdullah and N. I. Rusli, "Multilingual sentiment analysis: A systematic literature review," *Pertanika Journal of Science and Technology*, vol. 29, no. 1, 2021.
- [4] N. I. Shaari, "Political Inclination Sentiment Analysis using Lexicon and Support Vector Machine Approaches for Malay Tweets," unpublished.
- [5] N. Omar, A. F. Hamsani, N. A. S. Abdullah, and S. Z. Z. Abidin, "Construction of Malay abbreviation corpus based on social media data," *Journal of Engineering and Applied Sciences*, vol. 12, no. 3, 468–474, 2017.
- [6] S. S. Sazali, N. A. Rahman, and Z. A. Bakar, "Characteristics of malay translated hadith corpus," *Journal of King Saud University - Computer and Information Sciences*, 2020.
- [7] B. Liu, "Sentiment analysis and opinion mining," *Synthesis Lectures on Human Language Technologies*, vol. 5, no. 1, pp. 1–167, 2012.
- [8] T. Al-Moslmi, S. Gaber, A. Al-Shabi, M. Albared, and N. Omar, "Feature selection methods effects on machine learning approaches in Malay sentiment analysis," In Proc. 1st International Conference on Innovation in Science and Technology, 2015, pp. 1-2.
- [9] A. Alsaffar, and N. Omar, "Study on feature selection and machine learning algorithms for Malay sentiment classification," In Proc. IEEE 6th International Conference on Information Technology and Multimedia, 2014, pp. 270-275.
- [10] H. Alshalabi, S. Tiun, N. Omar, and M. Albared, "Experiments on the use of feature selection and machine learning methods in automatic malay text categorization," *Procedia Technology*, vol. 11, pp. 748–754, 2013.
- [11] N. Isa, M. Puteh, and R. M. H. R. Kamarudin, "Sentiment classification of Malay newspaper using immune network," In Proc. of the World Congress on Engineering, 2013, vol. 3, pp. 3-5.
- [12] M. Puteh, N. Isa, S. Puteh, and N. A. Redzuan, "Sentiment mining of Malay newspaper (SAMNews) using artificial immune system," In Proc. of the World Congress on Engineering, 2013, vol. 3, pp. 1498-1503.
- [13] A. A. Sadanandan, A. Osman, H. Saifuddin, M. K. Ahamad, D. N. Pham, and H. Hoe, "Improving accuracy in sentiment analysis for Malay language," In Proc. 4th International Conference on Artificial Intelligence and Computer Science, 2016, pp. 28–29.
- [14] T. Elghazaly, A. Mahmoud, and H. A. Hefny, "Political sentiment analysis using twitter data," In Proc. of the International Conference on Internet of Things and Cloud Computing, 2016, pp.1-5.
- [15] H. T. Gemilang, A. Erwin, and K. I. Eng, "Indonesian President candidates 2014 sentiment analysis by using Twitter data," In Proc. IEEE 2014 International Conference on ICT for Smart Society, 2014, pp. 101–104.
- [16] M. A. F. Yatim, Y. Wardhana, A. Kamal, A. A. Soroinda, F. Rachim, and M. I. Wonggo, "A corpus-based lexicon building in Indonesian political context through Indonesian online news media," In Proc. IEEE 2016 International Conference on Advanced Computer Science and Information Systems, 2016, pp. 347–352.
- [17] E. Uysal, S. Yumusak, K. Oztoprak, and E. Dogdu, "Sentiment analysis for the social media: A case study for Turkish general elections," In Proc. of the South East Conference, 2017, pp. 215-218.
- [18] R. Jose, and V. S. Chooralil, "Prediction of election result by enhanced sentiment analysis on twitter data using classifier ensemble approach," In Proc. IEEE 2016 International Conference on Data Mining and Advanced Computing, 2016, pp. 64–67.
- [19] J. Ramteke, S. Shah, D. Godhia, and A. Shaikh, "Election result prediction using Twitter sentiment analysis," In Proc. IEEE International conference on inventive computation technologies, 2016, vol. 1, pp. 1-5.
- [20] P. Wongthongtham and B. A. Salih, "Ontology-based approach for identifying the CREDIBILITY domain in social big data," *Journal of Organizational Computing and Electronic Commerce*, vol. 28, no. 4, pp. 354–377, 2018.
- [21] S. A. Fadzli, A. K. Norsalehen, I. A. Syarilla, H. Hasni, and M. S. S. Dhalila, "Simple rules malay stemmer," In Proc. International Conference on Informatics and Applications, 2012, pp. 28-35.
- [22] S. S.K.Rastogi, R. Singhal, and A. Kumar, "An improved sentiment classification using lexicon into svm," *International Journal of Computer Applications*, vol. 95, no. 1, pp. 37–42, 2014.

# Factors Impacting Users' Compliance with Information Security Policies: An Empirical Study

Latifa Alzahrani

Department of Management Information Systems  
College of Business Administration, Taif University, Saudi Arabia

**Abstract**—One of the main concerns for organizations in today's connected world is to find out how employees follow the information security policy (ISP), as the internal employee has been identified as the weakest link in all breaches of the security policies. Several studies have examined ISP compliance from a dissuasive perspective; however, the results were mixed. This empirical study analyses the impact of organisational security factors and individual non-compliance on users' intentions toward information security policies. A research model and hypotheses have been developed in this quantitative study. Data from 352 participants was collected through a questionnaire, which then validated the measurement model. The findings revealed that while security system anxiety and non-compliant peer behaviours negatively impact users' compliance intentions, work impediments positively influence these intentions. Security visibility negatively influences users' non-compliance, and security education systems positively impact work impediments. This research will help information security managers address the problem of information security compliance because it provides them with an understanding of one of the many factors underlying employee compliance behaviors.

**Keywords**—Information security; users' compliance; compliance factors; security education systems; information security policies

## I. INTRODUCTION

The COVID-19 pandemic raised a crucial technical issue within many organisations due to a lack of relevant information security protocols [1]. Information security is the process and controls put in place to guarantee data access is protected for reading by authorized personnel only, writing by authorized personnel only, and its readiness is protected when needed by authorized parties, etc. According to Miller [2], even before the virus outbreak, IT threats against organisations increased by 35% in the fourth quarter of 2019 compared to the fourth quarter of 2018. The necessity to transfer IT, users, to remote workplaces opened up a new set of vulnerabilities quickly identified by hackers and scammers who took advantage of the situation [2]. Although the US's Cybersecurity and Infrastructure Security Agency advised preventing cyber-attacks, the need for effective and advanced information security measures remains. Information security is defined as a set of processes and policies that protect information from unauthorised access [3]. There is a significant requirement to analyse the actions of organisations related to higher information security standards (ISS) and protective measures. Now more than ever, during the COVID-19 pandemic, companies' most valuable assets consist of digital data, which

puts them at risk of a set of threats from both inside and outside actors [4]. Any organisation needs to implement strategies to prevent commercial data leaks to their competitors and protect their users' privacy [5]. With an ever-expanding set of information technologies, organisations must explore all possible ways to leak information. The COVID-19 pandemic has caused rapid transformation and increased IT in most organisations in many sectors, including education [6], healthcare [7, 8], business [9], and economics [10]. This recent development has considerably changed critical resources and assets. It is vital to ensure that no information is unintentionally disclosed or altered [11, 12]. To shield resources and safeguard organisations' important data from existing threats, progressive information security plans must be developed to list inappropriate and appropriate ISS activities for IT operators [13]. Information security is a complex issue due to its multidisciplinary nature involving organisational, behavioural, and technical aspects [5, 14, 15] and a holistic method is necessary for information security management (ISM) [16, 17]. Also, Siponen et al. [13] recommended that information security matters be regarded from a management perspective.

Existing studies have indicated that even though scholars in the computer science field have investigated the significant phenomenon of information security [18], most have evaluated the subject from an engineering viewpoint. These researchers have concentrated on expanding technical solutions with limited consideration of security from a behavioural perspective [19]. The existing literature has highlighted that many organisations fail to properly link information security with threats beyond outside IT-related breaches by not taking human error into account. According to Choi et al. [3], "organisations increasingly focus on implementing information security products such as anti-virus, intrusion detection, and prevention systems, total personal computer (PC) security, database/contents security, total security systems and public key infrastructure". It has also been noted that the concept of information security requires a strategy that focuses on different organisational aspects, including structured actions, policy, and governance, to protect organisations' information assets. Governance in an organizational context is the development of a management framework to strategically drive the business processes and support compliance with regulations. Governance is planning for effective management, where management is the application of operational decisions. Information security policies are a necessity for business survival in the new digital world; its main goals are to protect confidentiality, integrity and availability, and it has an essential role in today's organizations. Information security policies

standards are core fundamentals that control the arrangements of information systems. There are multiple standards for addressing information security policies in organizations (COBIT, ISO 27001/2, etc.), and combinations of multiple standards that can help organizations define roles and govern information security. However, the different aspects of information security, such as economic, financial and management are complements to the technical side and not substitutes.

Despite this apparent necessity, Pérez-González et al. [20] observed that the lack of internal protection results in more negative impacts and losses than the security threats posed by outsiders. Pérez-González et al. [20] also stated that “government programs and grants to help companies improve information security focus on supporting companies in purchasing hardware and software technology solutions, without paying attention to organisational issues”. Thus, this study aims to fill the gap between the technical measures of information security and companies’ information security policies for users. Recent research in information security has required the consideration of diverse perspectives by analysing both its technical characteristics and organisational variables and then examining issues linked to conformance with information security principles. It also entails developing systems and information security management models and scrutinising certification procedures [21, 22]. These actions are significant because they must focus on information security related to business procedures and the overall contemplation of information security. The development of information security procedures must begin from the strategic level before advancing to other aspects of an organisation [21-24]. Information Security management roles can be defined as follows:

- Defining security roles, responsibilities and applications: relevant when discussing the accountability of users to specific information security occurrences within organizations.
- Defining goals for security: goals should be built using the business model and defined needs. The classification of systems and data could also come into play when defining the security goals; different organizations with different data will have different security goals.
- Strategies for Security: strategies should comply with business needs. This comes to play when planning the future of business services and legal/regulatory compliance.
- Risk assessment and management: especially useful when policies are being developed, it helps in defining and taking ownership of risks to later define the controls to avoid, mitigate/control, accept or transfer the risks. Risk assessment and controls definition are also highly connected to the asset classification.
- Resource management for security: defining the ISG structure needed is important for running safe operations, achieve information security goals, monitor the security status and respond to threats.

- Compliance with regulations and rules: organizations need to comply with regulations to be able to run their business; compliance is needed to ensure the correct security measures and responsibilities are implemented. Investor relations and communications activity (in relation to security goals).

Consequently, it is particularly significant to recognise the organisational aspects that relate to information security. The mechanisms that categorise the organisational features that may impact information security are modern in their approach. These mechanisms differ in methodology and primarily use theoretical approaches, as well as case studies. They also differ in terms of units of inquiry and present an extensive diversity of elements; thus, it is critical to developing this topic by examining the impacts of these mechanisms on information security organisations.

## II. RELATED WORK

Information security policies are a prime component of almost every modern organization. Information security is a key component of such organizations, and the governance of information security enables organizations to add value to products and services, reduce costs and meet customer requirements. Information security products and technologies cannot defend an organization without the appropriate strategies and policies. Organizational aspects have a direct impact on the behaviour and efficiency of information security policies. However, it is confirmed, but repeatedly forgotten, that security is not principally a technical matter but a management or business issue. Different challenges for information security management are also detailed in von Solms and von Solms [25].

There are different organizational issues that challenge information security management in organizations. For example, Ashenden and Sasse [26] discuss the struggles that Chief Information Security Officers (CISO) face as representative of organizational information security management when dealing with organizational issues. The research focuses on management issues in the context of information security and investigates the factors that most influence CISO success in an organization: enabling or disabling a healthy information security management status through business strategy and compliance, marketing, employees’ engagement, CISO identity in the organization, lack of confidence, effectiveness evaluation, organizational structure, and social responsibility. They also emphasized organizational behaviour, where they prove that employee’s reaction to information security management is positive when well informed and educated; however, this cannot always be true because human behaviour cannot be controlled or predicted. They also indicated that autocratic attitude in an organization is highly damaging to the CISO role and is one of the biggest obstacles [27].

There are many other organizational issues that impact information security management in modern organizations that present serious challenges to the information security status. Information technology and information security’s strategic alignment with business objectives is one that is well documented in the literature. Chang et al. [28] established its

importance by stating that IT systems become more adopted for core modern enterprise activities. Doing so would stabilize systems and smooth operations, enabling better performance. The alignment of the business with IT is also important for external business changes and the introduction of new challenges and business opportunities. That is, rapid technological development can introduce new threats and vulnerabilities to data. The size of the organization is another factor that is documented in the literature to have an impact on the ISM status. Ghobakhloo et al., [29] discuss that organizational size has positive relationship to technological innovation and technology implementation, stating that larger organizations usually have better human, technological and financial resources to better utilize information systems; they are also able to handle information security better with better resources, expertise, and training. In addition, Horvath et al., [30] found that vendors are more willing to cooperate with larger organizations. Industry type has long been used by researchers to investigate quality assurance, information and change management, and using IT systems for competitive behaviour. Johnston et al., found large variations in information security related behaviour in organizations whose type of industry relied more on information security. Hasbini et al., [31] also concluded that financial organizations needed more information security to drive business, and therefore such would have an impact on ISM efforts. IT competencies enable an organization to plan, execute and invest in information security effectively. Various researchers have highlighted the importance of a shared management of IT and ISM between IT professionals and business managers in an organization. While there are a number of researchers who addressed the organizational factors that impact information security management in modern organizations and how these could be developed and maintained, there are few researches focusing on exploring these factors in information security policies. This is an important absence because information security policies are different from information security management. Therefore, such a gap needs to be filled for a better understanding of how organizations can (or should) plan to deal with future information security policies issues.

### III. RESEARCH METHODOLOGY

#### A. Data Collection and Sample

The data was gathered from an educational organisation in Saudi Arabia that had been transformed into an e-learning system during the COVID-19 pandemic. Our study used questionnaires to collect data because this method is appropriate for testing both reliability and validity. The study included approximately 400 respondents. Forty-eight incomplete questionnaires were rejected from the collected replies, leaving 352 fully completed questionnaires for analysis. Of these 352 responses, only usable responses were included and converted into an appropriate sample size. Analysis using AMOS was performed to conduct structural equation modelling (SEM), which assessed the proposed model and the final path prototype.

#### B. Study Instrument

The constructs used in the questionnaire. The survey included a total of 23 items to evaluate the six constructs. All the questions were obtained from preceding studies and incorporated into the research to make them more relatable and logical. Each question that the authors derived from previous studies were altered and attuned to the research framework .A five-point Likert scale has been employed to measure the constructs in the questionnaire, which ranged from “strongly agree” to “strongly disagree”. The respondents were required to select the level that most applied to them while considering each item. The respondents were also asked to provide demographic information.

#### C. Pre-testing the Questionnaire

A complex pilot phase and pre-tests of the procedure were initiated, during which particular e-learning experts and users were consulted. The authors employed 10% of the entire sample size for the pilot study. Selecting the sample size was undertaken with consideration of average research performance. All the questions used in the survey were pre-tested. Forty randomly identified students took part in the pre-testing exercise. The study’s dependability was established using Cronbach’s alpha; the alpha values of all variables surpassed 0.7. Consequently, this study’s questionnaire was highly reliable. The entire group of respondents conceptualised the final questionnaire to increase the overall survey quality and its reliability.

#### D. Students’ Demographic Data

Table I presents the survey respondents’ demographic information; most (approximately 83%) were aged 18–25 years old. The percentage of females (56%) was higher than that of males (44%). Lastly, in terms of internet experience, the highest percentage (52.4%) of respondents had 6–10 years’ experience, followed by 29.1% with 1–5 years.

TABLE I. DEMOGRAPHIC INFORMATION

Variable	Group	Percentage
Age	18–25 years old	83.0
	26–30 years old	14.0
	31–35 years old	3.0
	36–40 years old	0
	Total	100.0
Gender	Male	44.0
	Female	56.0
	Total	100.0
Years of Internet Experience	1–5 years	29.1%
	6–10 years	52.4%
	11–20 years	17.3%
	More than 20 years	1.2%
	Total	100.0

Based on a review of the extant literature, the proposed research model was developed considering both the organisational and individual security factors necessary to reduce the non-compliance of IT users. According to Hwang et al. [5], organisational factors comprise “security systems, security education, and security visibility”. In contrast, individual security factors include the impairment of workflow and peers' negative attitudes towards information security and security system anxiety. In addition, the non-compliance of IT users is an antecedent of increasing the intention to comply with security policy. Fig. 1 illustrates the proposed research model and hypotheses, and the following subsections provide further details on each construct.

### E. Security Education Systems

Organisational factors are major reasons for unintended data exposure due to inadequate security policies and technologies. Ideally, an educational institution should implement a security system that will prevent external attempts to gain unlawful access to information and simultaneously prevent employees from sharing this information [5, 32]. A recent study by Pérez-González et al. [20] demonstrated that students' lack of education about information security standards is a significant source of unintentional data leaks. Hwang et al. [5] also highlighted that it is the responsibility of educational organisations to educate their students about data security as any person with access to the organisation's internal network can be a potential threat. The integrity of a security education system affects all levels of individual compliance; an easy-to-use system reduces employees' anxiety when interacting with it. Based on this, the first hypotheses were developed as follows:

- H1. Security education systems negatively influence work impediments.
- H2. Security education systems negatively influence security system anxiety.
- H3 Security education systems negatively influence non-compliance behaviours.

### F. Information Security Visibility

Another major factor is the visibility of security measures, continuously advertised to remain at the top of students' priorities. Information security visibility refers to the degree that an organisation informs its members about its information security policies [5]. Given these factors, the efforts of each organisation play a crucial role in protecting itself against data breaches. Accordingly, this study proposed the following further hypotheses:

- H4. Security visibility negatively influences work impediments.
- H5. Security visibility negatively influences security system anxiety.
- H6. Security visibility negatively influences non-compliance behaviours.

### G. Work Impediments

In terms of individual non-compliance factors, users may ignore specific security policies when completing their tasks due to their unwieldiness. Work impediments are the adverse impacts of implemented security measures on task completion [5]. Other sources of work impediments can stem from insufficient training or data protection policies. As such, this study proposed the following hypothesis:

- H7: Work impediments negatively influence users' compliance intention.
- H8: Work impediments negatively influence system anxiety.

### H. Security System Anxiety

Security system anxiety may derive from a user's unwillingness to report security incidents due to the fear of punishment. Moreover, such anxiety can materialise due to the complexity of information security systems or users' lack of understanding of their functions [5]. Therefore, this led to the following hypothesis:

- H9: Security system anxiety negatively influences users' compliance intention.

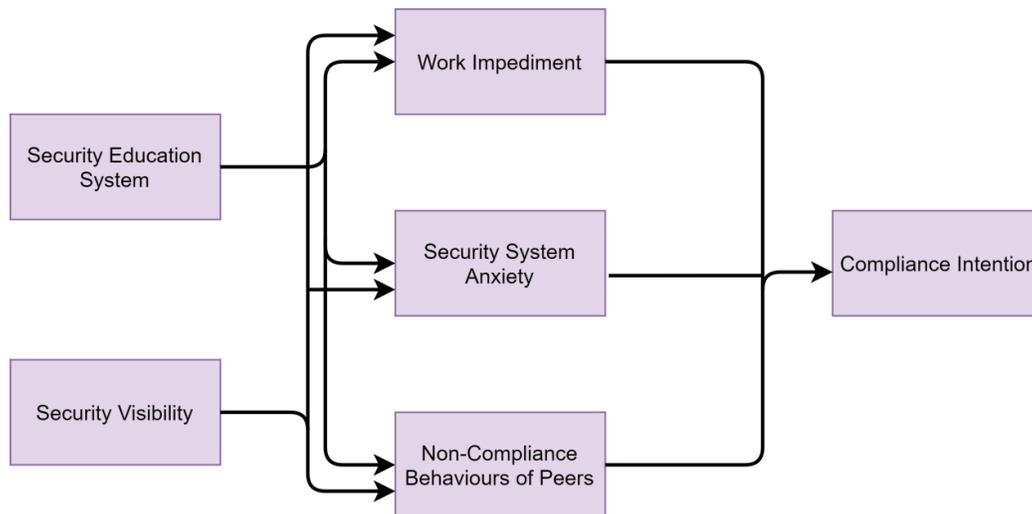


Fig. 1. Proposed Research Model.

I. Non-Compliant Peer Behaviours

The third primary source of non-compliance behaviours is social pressure from others. According to Hwang et al. [5], users' behaviour is affected by peer pressure, including the collective attitude towards information security. Students feel more confident following security instructions when they observe their peers doing the same. Therefore, an institution needs to assess the organisational culture to identify such issues. Accordingly, the present study proposed the following hypothesis:

H10: The non-compliance of peers negatively influences user' compliance.

H11: The non-compliance of peers negatively influences work impediments.

IV. RESULTS

The data analysis was conducted in four steps. First, factor analysis of the collected data was conducted to determine the relationships between the variables. After that, confirmatory factor analysis was performed to confirm the findings. Reliability and validity testing were conducted on the model, followed by SEM. SPSS Statistics 25.0 software was used for factor analysis. SPSS AMOS 22.0 software was used to test the CFA model fit and SEM to estimate the relationships between the independent variables and the dependent variable to accept or reject the proposed hypotheses.

A. Exploratory Factor Analysis

The Kaiser-Meyer-Oklind (KMO) and Bartlett's tests were used to check the suitability of the data for factor analysis. The KMO value was 0.844, exceeding the recommended value of 0.70, and, thus, was considered adequate [33, 34]. Bartlett's test of sphericity reached statistical significance (approximate chi-square 5440.263, df 253 and Sig 0.000), signifying that the data was appropriate for factor analysis. The 23 items were subjected to principal component analysis (PCA), and Varimax Rotation with Kaiser Normalization was used for factor analysis. Any items with a factor loading less than 0.50 were eliminated; however, the factor loadings for each item in the present study's questionnaire were above 0.50, suggesting that the data set was appropriate [35, 36]. Consequently, all 23 items were accepted, and PCA revealed that they were grouped into six components with Eigenvalues exceeding 1 (Table II). The total percentage of variance was 76.825. The individual dimensions of the proposed instrument explained the total variance as exceeding 76%, suggesting the suitability of the process.

B. Confirmatory Factor Analysis

CFA explains the extent to which observed variables are linked to latent factors in a study. CFA postulates the relationships between variables based on theory, empirical research, or both and then statistically tests the hypothesised structure. The present study developed the model based on a priori knowledge, and CFA was used to confirm it, as shown in Fig. 2. The measurement model represents the pattern in which each measure loads on a particular factor. It demonstrates how the measured variables come together to represent the constructs and is used for validation and reliability testing. The

covariance between all the latent variables was significant as the P-value was less than 0.05 (Table III).

TABLE II. FACTOR EXTRACTION RESULTS OF QUESTIONNAIRE ITEMS

Item No.	Component	Eigenvalue
Security System and Security Education		6.999
Sys1	0.755	
Sys2	0.759	
Sys3	0.720	
Edu1	0.774	
Edu2	0.819	
Edu3	0.791	
Edu4	0.802	
Edu5	0.821	
Security Visibility	Component	
Vis1	0.909	4.835
Vis2	0.904	
Work Impediment	Component	Eigenvalue
Imp3	0.808	1.989
Imp4	0.841	
Security System Anxiety	Component	Eigenvalue
Anx1	0.708	1.649
Anx2	0.878	
Anx3	0.882	
Anx4	0.768	
Non-Compliance Behaviour of Peers	Component	Eigenvalue
Peer1	0.845	1.186
Peer2	0.831	
Peer3	0.741	
Compliance Intention	Component	Eigenvalue
Int1	0.840	1.011
Int2	0.846	
Int3	0.911	
Int4	0.894	
Total Variance Explained: 76.825		

TABLE III. COVARIANCE BETWEEN LATENT VARIABLES

			Estimate	S.E.	C.R.	P
Edusys	<-->	Int	0.172	0.025	6.934	***
Edusys	<-->	Anx	-0.060	0.027	-2.178	0.029
Edusys	<-->	Peer	-0.050	0.024	-2.094	0.036
Edusys	<-->	Vis	0.006	0.028	0.200	0.841
Edusys	<-->	Imp	0.065	0.029	2.256	0.024
Int	<-->	Anx	-0.087	0.034	-2.538	0.011
Int	<-->	Peer	-0.064	0.030	-2.149	0.032
Int	<-->	Vis	0.033	0.035	0.948	0.343
Int	<-->	Imp	0.053	0.036	1.481	0.139
Anx	<-->	Peer	0.443	0.054	8.207	***
Anx	<-->	Vis	-0.236	0.052	-4.487	***
Anx	<-->	Imp	0.244	0.051	4.797	***
Peer	<-->	Vis	-0.229	0.046	-4.981	***
Peer	<-->	Imp	0.203	0.043	4.680	***
Vis	<-->	Imp	-0.337	0.058	-5.838	***

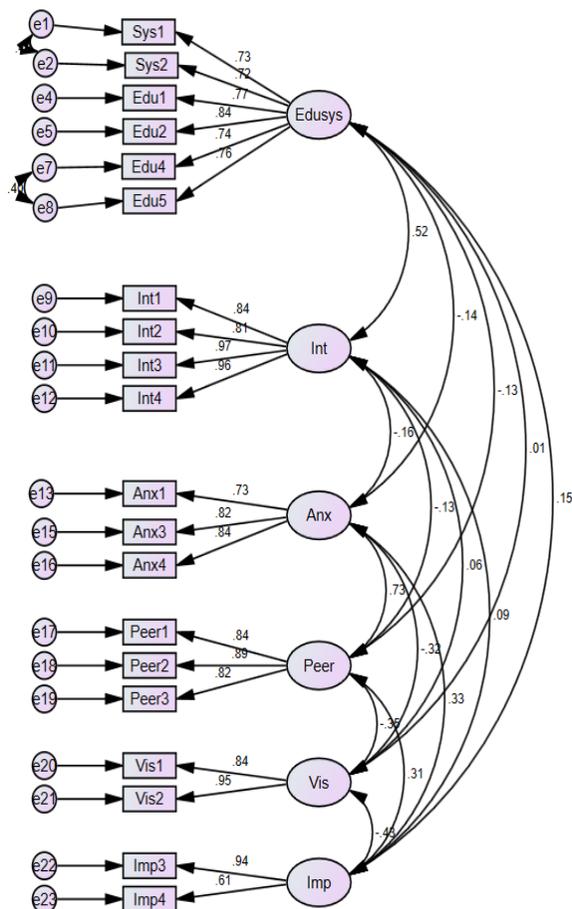


Fig. 2. The Results of Confirmatory Factor Analysis.

There was a high positive correlation of 0.733 between the security system anxiety and peer behaviour variables, followed by security systems and security education and work impediments at 0.522. The correlations between the other variables are shown in Table IV.

TABLE IV. CORRELATION BETWEEN LATENT VARIABLES

			Estimate
Edusys	<-->	Int	0.522
Edusys	<-->	Anx	-0.145
Edusys	<-->	Peer	-0.135
Edusys	<-->	Vis	0.012
Edusys	<-->	Imp	0.146
Int	<-->	Anx	-0.161
Int	<-->	Peer	-0.131
Int	<-->	Vis	0.057
Int	<-->	Imp	0.090
Anx	<-->	Peer	0.733
Anx	<-->	Vis	-0.322
Anx	<-->	Imp	0.335
Peer	<-->	Vis	-0.351
Peer	<-->	Imp	0.311
Vis	<-->	Imp	-0.426

SEM showed that chi-square (CMIN) = 350.635, degree of freedom (DF) = 153, and the probability level was approximately 0.000, evidence that the null hypothesis was not significant at the 0.05 level. CMIN/DF represents the minimum discrepancy, which was 2.292; according to Wheaton et al. [37], a model has a reasonable fit if the minimum discrepancy is less than 5.

Table V shows the values found for each parameter to test the model's fit. In various studies conducted by Bentler and Bonett [38], Jöreskog and Sörbom [39], Bollen's and Bentler [38], it has been suggested that if the index value is greater than 0.9 and if the RMSEA value is less than 0.08, the model has a good fit.

TABLE V. PARAMETER VALUES FOR MODEL FIT

Parameter	Value
Goodness of Fit Index (GFI)	0.906
Comparative Fit Index (CFI)	0.955
Root Mean Square Error of Approximation (RMSEA)	0.064

### C. Reliability and Validity Tests

All the variables had composite reliability greater than 0.7 (Table VI), which indicated good reliability.

TABLE VI. COMPOSITE RELIABILITY TEST

	CR
Edusys	0.893
Int	0.943
Anx	0.839
Peer	0.888
Vis	0.892
Imp	0.761

All the variables had a convergent validity greater than 0.5 (Table VII), indicating good convergent validity.

TABLE VII. CONVERGENT VALIDITY

	AVE
Edusys	0.582
Int	0.805
Anx	0.635
Peer	0.725
Vis	0.805
Imp	0.624

The discriminant value was greater than the corresponding correlation between the variables, indicating good discrimination between the factors in the analysis (see Table VIII).

### D. Structural Equation Modelling

SPSS AMOS 22 software was used to perform CFA via SEM. The model was over-identified, which is a preferable situation for SEM. The path diagram in Fig. 3 specifies the relationship between the observed variables. The model's portion that specifies how the variables are related is

represented by the structural model; the estimates with the largest values represent the most important dimensions in terms of their influence on dependent variables. The findings of the regression weight estimates are summarised in Table IX. P-values demonstrate the significance of estimation: if the P-value is less than 0.05, then the independent variable has a significant effect on the dependent variable (P-values with \*\*\* indicate 0.000). All the impacts were significant except for information security visibility acting on security system anxiety, which did not significantly impact as the p-value was 0.036 (i.e. less than 0.05). Table X presents the results of standardised regression weight estimates.

Table X highlights that both the security education system and system visibility had a significant negative impact on peers' non-compliant behaviour. In addition, this study

highlights that both the security education system and peer' non-compliant behaviour had significant positive impacts on work impediments. In contrast, the system's visibility had a significant negative impact on it. Considering the factors influencing system anxiety, this study highlights that the security education system had a significant negative impact on security system anxiety. In contrast, the work impediments had a significant positive impact of 0.995 on security system anxiety. However, system visibility had no significant impact on security system anxiety. Finally, regarding the compliance intention, the findings of this research present that both security system anxiety and peer' non-compliant behaviour had a significant negative impact on compliance intention. In contrast, work impediments had a significant positive impact on compliance intention.

TABLE VIII. DISCRIMINANT VALIDITY

	Edusys	Int	Anx	Peer	Vis	Imp
Edusys	0.763					
Int	0.522	0.897				
Anx	-0.145	-0.161	0.797			
Peer	-0.135	-0.131	0.733	0.851		
Vis	0.012	0.057	-0.322	-0.351	0.897	
Imp	0.146	0.09	0.335	0.311	-0.426	0.790

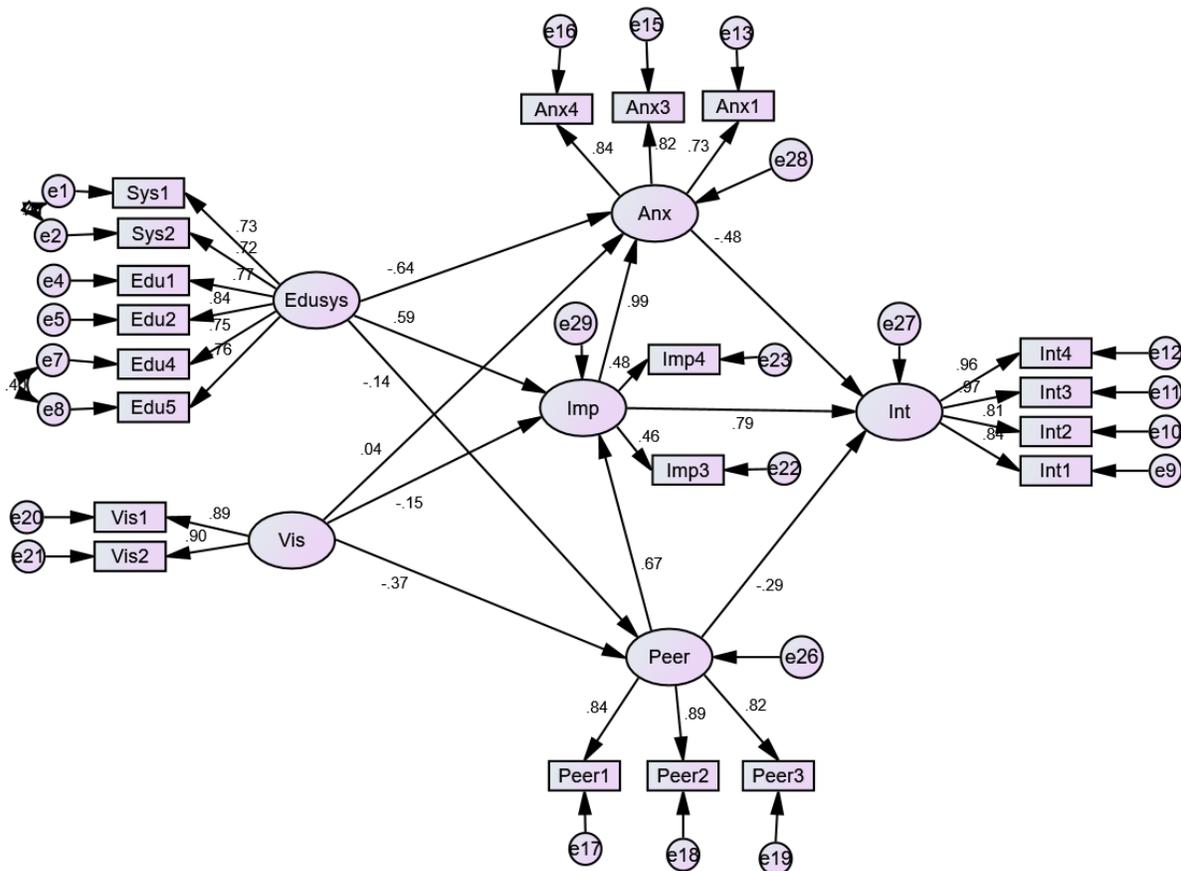


Fig. 3. SEM Path Diagram with Standardised Parameters.

TABLE IX. UNSTANDARDISED REGRESSION WEIGHT ESTIMATES

		Estimate	S.E	C.R.	.P	Supported?
H1	Edusys -> imp	0.516	0.093	5.571	***	Yes
H2	Edusys -> anx	-1.046	0.196	-5.335	***	Yes
H3	Edusys -> peer	-0.207	0.089	-2.333	0.020	Yes
H4	vis-> imp	-0.067	0.032	-2.125	0.034	Yes
H5	vis -> anx	0.031	0.065	0.476	0.634	No
H6	vis -> peer	-0.286	0.049	-5.803	***	Yes
H7	Imp -> int	1.185	0.223	5.309	***	Yes
H8	Imp -> anx	1.847	0.308	5.989	***	Yes
H9	Anx -> int	-0.388	0.119	-3.270	0.001	Yes
H10	Peer -> int	-0.261	0.121	-2.161	0.031	Yes
H11	Peer -> imp	0.397	0.064	6.210	***	Yes

TABLE X. STANDARDISED REGRESSION WEIGHT ESTIMATES

			Estimate	Supported
Peer	<---	Edusys	-0.140	Yes
Peer	<---	Vis	-0.367	Yes
Imp	<---	Edusys	0.587	Yes
Imp	<---	Vis	-0.145	Yes
Imp	<---	Peer	0.667	Yes
Anx	<---	Edusys	-0.641	Yes
Anx	<---	Imp	0.995	Yes
Anx	<---	Vis	0.036	No
Int	<---	Anx	-0.481	Yes
Int	<---	Peer	-0.292	Yes
Int	<---	Imp	0.792	Yes

## V. DISCUSSION

This study analysed the relationship between organisational security factors and users' non-compliance behaviours in one higher education institution's transformation to online systems during the COVID-19 pandemic. A proposed model was developed based on a recent study by Hwang et al. [5]. In total, six constructs were selected for the model: two organisational security factors (security education systems and security visibility), three individual non-compliance causes (work impediments, security system anxiety and the non-compliance behaviours of peers) and compliance intention. The proposed model was tested using SEM. The negative link between study impediments and compliance was significant. This result is similar to previous findings, as work impairments diminish compliance [40, 41]. Users' compliance increases when they identify security actions as impediments to achieving the goals of a distinct task.

The hypothesis that security system anxiety exhibits a significant negative impact on compliance intent was

supported, an outcome that was similar to previous research demonstrating that employees' anxiety decreases their intent to comply [42, 43]. Users' anxiety regarding security systems, triggered by an institution's imprecise security guidelines, thus, has an undesirable effect on their compliance. The hypothesis that peers' non-compliance behaviours have an undesirable impact on compliance intent was also supported. Generally, people tend to follow the behaviours of others if they are in the same group. Consequently, as students working on an online system obey the same security guidelines, there is a higher chance that other individuals in the same group will embrace comparable behavioural patterns. Therefore, information security actions are necessary at a university's personal, departmental, and team levels. Meanwhile, the hypothesis is that security education negatively impacts users' non-compliance with information security policies. This demonstrates limited equivalency with previous findings that security education systems decrease the non-compliance of workforces [12]. Security education systems effectively lessened work impairments and were significant in decreasing non-compliance behaviours and security system anxiety. Lastly, the hypothesis suggesting the negative link between security discernibility and users' non-compliance. This outcome is similar to preceding studies that have demonstrated that security visibility augments employees' compliance intent at work [13]. Security visibility can be heightened by suggesting approaches for security actions and public relations packages, for example, visual advertisements regarding an organisation's information safety requirements.

We previously discussed the importance of users' compliance with information security policies and suggested methods to have that accomplished. Such measures are expected to be even more pressing as information security issues could be the cause of large-scale damage. Users' compliance with policies and regulations is an important matter and a major worry for modern organizations. A different number of challenges could be behind the lack of sufficient users' compliance, also going back to the literature around employee engagement part of an organizational culture. Hu et al. [44] emphasized the critical importance of top management's commitment and participation towards the influence on the organizational compliance culture and shaping the intention of employees to comply with information security policies. Puhakainen and Siponen [45] emphasized the need for the adoption of information security awareness training and continued communication processes to motivate the employees' systematic cognitive processing of the information they receive and achieve the best development of employees' compliance results. Another influencer of employees engagement is their perception of trainings and career development inside the organization, which highly reflect on smart cities requirements which demand smart people, though such cannot be achieved without strong skills development techniques employed in the workplace and presented in different forms of modern training methods like wargames or simulations [46].

## VI. RESEARCH IMPLICATIONS

This study's findings highlight some significant implications for both practitioners and academics. First, the

study confirmed that the intent to comply with an organisation's information security policy is undesirably impacted by the mediators of work impediments, the non-compliance of peers, and security system anxiety. A study impediment denotes the limitations on working processes and activities caused by conforming to established security guidelines. Education processes involve particular tasks, and completing these tasks is a more significant goal than complying with information security guidelines. Each time information security actions impede or conflict with their tasks, students can identify rational reasons for compliance but demonstrate non-compliance intents. Consequently, organisations should convince students that constructive security conduct is among the most important performance elements. Security system anxiety denotes an individual's hesitation or fear regarding information security guidelines. If these guidelines are severe and complex, users can experience anxiety regarding their security behaviours. In various cases, users may comply, although, in reality, they are more prone to non-compliance. Consequently, organisations should offer users support to better comprehend the systems and policies affecting information security. The non-compliance actions of peers encompass the belief that peers do not conform to the organisation's security procedure. Users exhibit tendencies to act like their peers. Comparable tendencies were demonstrated in this study, emphasising the need to promote a security atmosphere that stimulates peer compliance.

Secondly, the study's findings highlight that organisations' security efforts impact users' non-compliance. Security education systems increase work impairments, reducing peers' non-compliance and security system anxiety. Homogeneous security structures increase work impairments; for instance, organisations encourage users to use proficient USB drives and activate cloud-oriented security structures to systemise their safety configurations: security structures and security education system, anxiety, and non-compliant peer behaviour. Comprehensive education on matters linked to security procedures, performance, and behaviours may decrease users' system anxiety concerning required security actions, as well as peers' non-compliance tendencies. Moreover, security visibility was shown to decrease security system anxiety and peers' non-compliance behaviours; therefore, exhaustive promotion of security campaigns and guidelines may decrease these negative outcomes. Information security and protection controls should only be introduced when a risk is confirmed; they need to be cost-effective. Information security roles and responsibilities should be made public to all employees through the utilization of the information security policy. The information/asset owner is responsible for the monitoring and control of the information/asset usage in addition to the authorization of the users. They should also verify compliance with the information security policy and ensure that the system is appropriately secured. Information protection requires a comprehensive approach that follows a system development lifecycle. Information security should be periodically reassessed and verified, based on objectives and requirements. In

addition, information protection is directly impacted by the organizational culture. Information security management should be involved with business units to best understand their needs and determine the solutions that best protect assets.

This research expands the protection motivation model by suggesting discrete non-compliance causes and recommends organisational strategies for universities to help alleviate non-compliance with information security measures. The investigation recommends administrative variables for security improvement, including security education, security systems, and security visibility, as important constituents in reducing students' non-compliance with information security strategies. For establishments in which study impairments are a main cause of non-compliance, the institutions should invest primarily in security structures. In organisations with increased non-compliance levels and security system anxiety, an appropriate assortment of security systems, visibility, and education can result in satisfactory users' compliance.

## VII. CONCLUSION

This study aimed to establish a causal link between organisational security efforts and the reasons for users' non-compliance with information security policy during the COVID-19 pandemic. Specifically, the study scrutinised the influence of organisational countermeasures, including security education systems and security visibility, on the causes of users' non-compliance, including work impairments, security system anxiety, and peers' non-compliance behaviours. SEM was used to test the suggested hypotheses with data collected from students at a business college. The findings showed that users' compliance intent is negatively impacted by the mediators of security system anxiety and the non-compliance of peers, while it is also positively influenced by work impairments. Meanwhile, the independent variables of security education systems and security visibility negatively impact security system anxiety and the non-compliance behaviour of peers. Nevertheless, only security education systems were found to positively impact the work impairment of the identified independent variables. The study's outcomes indicate the significance of security visibility and education in decreasing non-compliance, although security education systems seem to increase it. This study has some limitations. First, it is restricted in that we measured students' reflections on the reasons for individuals' non-compliance and organisational security efforts without discerning real activities. Consequently, future research should observe real behaviours related to information security objectives via controlled research laboratory experiments. Second, this study used SEM to examine the reasons behind users' non-compliance and organisational efforts to alleviate these reasons. In the future, we plan to discover the theoretical factors behind compliance intent that are highlighted by education belief theory and safeguard the motivation model, which can impact the instigators of non-compliance with the data security policy and procedures employed in higher education. Lastly, this study was situated in a precise time and location. It may be reinforced by longitudinal studies that observe diverse nations for a more robust overview of information security outcomes.

REFERENCES

- [1] A. Nasir, K. Shaukat, I. A. Hameed, S. Luo, T. M. Alam, and F. Iqbal, "A Bibliometric Analysis of Corona Pandemic in Social Sciences: A Review of Influential Aspects and Conceptual Structure," *IEEE Access*, vol. 8, pp. 133377-133402, 2020.
- [2] E. A. Miller, "Protecting and improving the lives of older adults in the COVID-19 era," *Journal of Aging & Social Policy*, vol. 32, pp. 297-309, 2020.
- [3] S. Choi, J. T. Martins, and I. Bernik, "Information security: Listening to the perspective of organisational insiders," *Journal of information science*, vol. 44, pp. 752-767, 2018.
- [4] G. D. Moody, M. Siponen, and S. Pahnla, "Toward a unified model of information security policy compliance," *MIS quarterly*, vol. 42, 2018.
- [5] I. Hwang, D. Kim, T. Kim, and S. Kim, "Why not comply with information security? An empirical approach for the causes of non-compliance," *Online Information Review*, 2017.
- [6] T. M. Alam, M. Mushtaq, K. Shaukat, I. A. Hameed, M. Umer Sarwar, and S. Luo, "A Novel Method for Performance Measurement of Public Educational Institutions Using Machine Learning Models," *Applied Sciences*, vol. 11, p. 9296, 2021.
- [7] T.-M. Alam, K. Shaukat, A. Khelifi, W.-A. Khan, H.-M.-E. Raza, M. Idrees, et al., "Disease Diagnosis System Using IoT Empowered with Fuzzy Inference System," *Computers, Materials & Continua*, vol. 70, pp. 5305--5319, 2022.
- [8] S. Shakir, M. S. Asif, A. Talha Mahboob, and R. Zeeshan, "Early Prediction of Malignant Mesothelioma: An Approach towards Non-invasive Method," *Current Bioinformatics*, vol. 16, pp. 1-1, 2021.
- [9] T. M. Alam, K. Shaukat, M. Mushtaq, Y. Ali, M. Khushi, S. Luo, et al., "Corporate bankruptcy prediction: An approach towards better corporate world," *The Computer Journal*.
- [10] K. Shaukat, S. Luo, N. Abbas, T. Mahboob Alam, M. Ehtesham Tahir, and I. A. Hameed, "An analysis of blessed Friday sale at a retail store using classification models," pp. 193-198.
- [11] R. Willison and M. Warkentin, "Beyond deterrence: An expanded view of employee computer abuse," *MIS quarterly*, pp. 1-20, 2013.
- [12] J. D'Arcy, A. Hovav, and D. Galletta, "User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach," *Information systems research*, vol. 20, pp. 79-98, 2009.
- [13] M. Siponen, S. Pahnla, and M. A. Mahmood, "Compliance with information security policies: An empirical investigation," *Computer*, vol. 43, pp. 64-71, 2010.
- [14] N. S. Safa and R. Von Solms, "An information security knowledge sharing model in organizations," *Computers in Human Behavior*, vol. 57, pp. 442-451, 2016.
- [15] W. R. Flores, E. Antonsen, and M. Ekstedt, "Information security knowledge sharing in organizations: Investigating the effect of behavioral information security governance and national culture," *Computers & security*, vol. 43, pp. 90-110, 2014.
- [16] Z. A. Soomro, M. H. Shah, and J. Ahmed, "Information security management needs more holistic approach: A literature review," *International Journal of Information Management*, vol. 36, pp. 215-225, 2016/04/01/ 2016.
- [17] K. Shaukat, F. Iqbal, T. M. Alam, G. K. Aujla, L. Devnath, A. G. Khan, et al., "The Impact of Artificial Intelligence and Robotics on the Future Employment Opportunities," *Trends in Computer Science and Information Technology*, vol. 5, pp. 050-054, 2020.
- [18] L. Alzahrani and K. P. Seth, "The Impact of Organizational Practices on the Information Security Management Performance," vol. 12, p. 398, 2021.
- [19] S. Kwon, S. Jang, J. Lee, and S. Kim, "Common defects in information security management system of Korean companies," *Journal of Systems and Software*, vol. 80, pp. 1631-1638, 2007.
- [20] D. Pérez-González, S. T. Preciado, and P. Solana-Gonzalez, "Organizational practices as antecedents of the information security management performance: An empirical investigation," *Information Technology & People*, 2019.
- [21] J. May and G. Dhillon, "A holistic approach for enriching information security analysis and security policy formation," 2010.
- [22] M. Siponen and R. Willison, "Information security management standards: Problems and solutions," *Information & management*, vol. 46, pp. 267-270, 2009.
- [23] R. Werlinger, K. Hawkey, and K. Beznosov, "An integrated view of human, organizational, and technological challenges of IT security management," *Information Management & Computer Security*, 2009.
- [24] A. N. Singh, M. Gupta, and A. Ojha, "Identifying factors of "organizational information security management"," *Journal of Enterprise Information Management*, 2014.
- [25] B. Von Solms, R. J. C. Von Solms, and security, "The 10 deadly sins of information security management," vol. 23, pp. 371-376, 2004.
- [26] D. Ashenden, A. J. C. Sasse, and Security, "CISOs and organisational culture: Their own worst enemy?," vol. 39, pp. 396-405, 2013.
- [27] I. Javed, X. Tang, K. Shaukat, M. U. Sarwar, T. M. Alam, I. A. Hameed, et al., "V2X-Based Mobile Localization in 3D Wireless Sensor Network," *Security and Communication Networks*, vol. 2021, p. 6677896, 2021/02/11 2021.
- [28] K. Piwowar-Sulej and R. J. I. J. o. C. M. Mroziowski, "MANAGEMENT BY VALUES: A CASE STUDY OF A RECRUITMENT COMPANY," vol. 19, 2020.
- [29] M. Ghobakhloo and M. J. J. o. M. T. M. Fathi, "Corporate survival in Industry 4.0 era: the enabling role of lean-digitized manufacturing," 2019.
- [30] D. Horváth, R. Z. J. T. f. Szabó, and s. change, "Driving forces and barriers of Industry 4.0: Do multinational and small and medium-sized companies have equal opportunities?," vol. 146, pp. 119-132, 2019.
- [31] M. A. Hasbini, T. Eldabi, A. J. W. J. o. E. Aldallal, Management, and S. Development, "Investigating the information security management role in smart city organisations," 2018.
- [32] K. Shaukat, T. M. Alam, M. Ahmed, S. Luo, I. A. Hameed, M. S. Iqbal, et al., "A Model to Enhance Governance Issues through Opinion Extraction," in 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), 2020, pp. 0511-0516.
- [33] B. K. Nkansah, "On the Kaiser-meier-Olkin's measure of sampling adequacy," *Math. Theory Model*, vol. 8, pp. 52-76, 2011.
- [34] T. M. Alam, K. Shaukat, H. Mahboob, M. U. Sarwar, F. Iqbal, A. Nasir, et al., "A Machine Learning Approach for Identification of Malignant Mesothelioma Etiological Factors in an Imbalanced Dataset," *The Computer Journal*.
- [35] D. W. Stewart, "The application and misapplication of factor analysis in marketing research," *Journal of marketing research*, vol. 18, pp. 51-62, 1981.
- [36] T. M. Alam, K. Shaukat, I. A. Hameed, W. A. Khan, M. U. Sarwar, F. Iqbal, et al., "A novel framework for prognostic factors identification of malignant mesothelioma through association rule mining," *Biomedical Signal Processing and Control*, vol. 68, p. 102726, 2021.
- [37] B. Wheaton, B. Muthen, D. F. Alwin, and G. F. Summers, "Assessing reliability and stability in panel models," *Sociological methodology*, vol. 8, pp. 84-136, 1977.
- [38] P. M. Bentler, "Comparative fit indexes in structural models," *Psychological bulletin*, vol. 107, p. 238, 1990.
- [39] K. G. Jöreskog and D. Sörbom, "Recent developments in structural equation modeling," *Journal of marketing research*, vol. 19, pp. 404-416, 1982.
- [40] R. West, "The psychology of security," *Communications of the ACM*, vol. 51, pp. 34-40, 2008.
- [41] B. Bulgurcu, H. Cavusoglu, and I. Benbasat, "Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness," *MIS quarterly*, pp. 523-548, 2010.
- [42] V. Venkatesh, "Determinants of perceived ease of use: Integrating control, intrinsic motivation, and emotion into the technology acceptance model," *Information systems research*, vol. 11, pp. 342-365, 2000.

- [43] T. M. Alam, K. Shaukat, I. A. Hameed, S. Luo, M. U. Sarwar, S. Shabbir, et al., "An investigation of credit card default prediction in the imbalanced datasets," *IEEE Access*, vol. 8, pp. 201173-201198, 2020.
- [44] Q. Hu, T. Dinev, P. Hart, and D. J. D. S. Cooke, "Managing employee compliance with information security policies: The critical role of top management and organizational culture," vol. 43, pp. 615-660, 2012.
- [45] P. Puhakainen and M. J. M. q. Siponen, "Improving employees' compliance through information systems security training: an action research study," pp. 757-778, 2010.
- [46] S. N. A. Hamid and K. K. Yahya, "Relationship between person-job fit and person-organization fit on employees' work engagement: A study among engineers in semiconductor companies in Malaysia," in *Annual Conference on Innovations in Business and Management London*, 2011, pp. 1-30.

# The Application of Image Processing in Liver Cancer Detection

Meenu Sharma\*, Rafat Parveen  
Dept. of Computer Science, Jamia Millia Islamia  
New Delhi, India

**Abstract**—Hepatic cancer is caused by the uncontrolled growth of liver cells, an HCC is the most common form of malignant liver cancer, accounting for 75 percent of cases. This tumor is difficult to diagnose, and it is often discovered at an advanced stage, posing a life-threatening danger. As a result, early diagnosis of liver cancer increases life expectancy. So, using a digital image processing method, we suggest an automated computer-aided diagnosis of liver tumors from MRI images. Magnetic Resonance Imaging (MRI) images are used to identify liver tumors in this case. The image goes through image preprocessing, image segmentation, and feature extraction, all of which are done within the layers of an Artificial Neural Network, making it an automated operation. To make the edge continuous, this operation combines two processes: edge and manual labeling. On the basis of statistical characteristics, tumors are often divided into four categories: cyst, adenoma, hemangioma, and malignant liver tumor. The aim of this proposed technique is to automatically highlight and categorize tumor regions in Magnetic Resonance Imaging images without the need for a medical practitioner.

**Keywords**—Liver cancer; digital image processing; magnetic resonance imaging; early stage

## I. INTRODUCTION

Every day, billions of cells in our body multiply to create new cells. The newly created cells take up the area previously occupied by dead cells. Cells primarily combine to form tissues, which then combine to form organs [1]. As a result, in some abnormal cases, cells divide faster than the body requires, resulting in lumps or growths that are commonly referred to as tumors [2]. Tumors are irregular tissue growth caused by uncontrolled cell proliferation. They serve no physiological purpose and may be cancerous (malignant or metastases) or non-cancerous (benign) [3]. A benign tumor does not have the ability to spread to other areas of the body, while a malignant tumor does. Malignant tumor begins in the liver and grows on the surface or inside the liver. Primary cancer is described as cancer that begins in a tissue or organ, and primary liver cancer refers to tumors that occur from the liver itself. Hepatocellular Carcinomas is the most common form of malignant liver cancer [4]. We proposed a simple cancer detection approach based on digital image processing in this research paper.

Digital image processing is the method of processing images using computers and the necessary algorithms. Image processing is an evolving and growing industry of medical applications. The tumor area is detected using a computed tomography (CT) scan and a magnetic resonance imaging (MRI) scan image of liver cancer. Magnetic resonance imaging

(MRI) is a much safer technique than CT scan for avoiding ionizing radiation while still providing a better visualization picture of soft tissue. Detecting and analyzing tumors will assist doctors in providing better care to patients and reducing mortality rates [5]. There are three major stages in detecting liver cancer. Image preprocessing, image segmentation, and tumor area highlighting are all part of the process. Image resizing, image contrast enhancement, noise removal filters, and image imperfections are all examples of image preprocessing. This phase is critical in cancer detection because even a slight deviation caused by imperfections or noise can have a significant detection impact [2]. In a decision-oriented application for image segmentation, pixels of an image are correctly categorized. Image segmentation techniques include threshold-based, edge-based, clustering-based, neural network-based, and others. Image segmentation aims to make an image's representation more relevant and easier to analyze by simplifying or tuning it [6]. In conventional clinical practice, 3-D organ analysis is done manually, which takes a long time. Automated methods have a number of benefits over manual or interactive approaches. Automated methods are more efficient and do not necessitate the intervention of a person [3]. We used the Artificial Neural Network (ANN) algorithm to automate the tumor detection process in this study.

Artificial neural networks are a form of computation inspired by the human brain and nervous system (ANNs). ANNs have been used to perform cognitive tasks usually done by the brain, such as facial recognition, learning to speak and understand a language, recognizing handwritten characters, and determining if the same object is a target viewed from different angles. However, the number of applications for ANNs is the, and they have recently been used successfully in digital image processing [7].

In this analysis, we expect to segment a tumor into a liver, making it easier for the surgeon to see the tumor and treat it. The MRI images are taken in this analysis, and then the segmentation processes are applied to the liver image in order to locate, extract, and further identify liver disease [8]- [10]. We also show how to use image processing to automatically segment CT liver images and remove tumors, as well as categorize tumors into four groups: liver cancer (hepatoma), adenoma, cyst, and hemangioma, with analysis focused on statistical features without the intervention of humans, though keeping in mind that the manual method of testing data sets is time consuming and less accurate than computer-based analysis, and cost is also a consideration [11] – [20].

\*Corresponding Author.  
e-mail:- meenusharma2275@gmail.com

The following is how the paper is organized: Section 2 contains a detailed description of the proposed methodology. Section 3 discusses the findings and their discussion, and Section 4 concludes.

## II. MATERIALS AND METHOD

The aim of this study is to process and analyze MRI scan images in order to determine if they contain cancer cells or not, and if they do, which type of cancer cells they are. These images come from the Cancer Genome Atlas (TCGA) database, which is open to the public. To process the files, the experimentation procedure employs the MATLAB R2018 program. The segmentation and extraction process depicted in Fig 1 elucidates the overall methodology.

The dataset for this study includes MRI scan images of liver cancer, as well as five images of adenoma, cyst, and hemangioma. Image preprocessing was performed because the images framed by the MRI scan have some noise and discrepancy. The picture is normalized in this step by

minimizing noise, changing contrast and scale, and eliminating blurriness all at once. The image's noise and blurriness will slow down the process.

Since the cancer cell is now considered a region of concern, segmenting the liver alone from an abdominal MRI image is complicated since the image contains other organs such as the kidney, spleen, and pancreas that are very close to the liver and have similar intensities. The experiment uses image segmentation based on edge to collect only the liver component and examine the cancer cell. To make the edge continuous, manual labeling is performed. The segmented image, which depicts the extracted liver with cancer cell, is now used to detect cancer cells. The function is extracted by cropping the region of interest, and the k-means algorithm is used to evaluate and judge if the given image is cancer cell or not. Table 1 shows the clusters formed as a result of the above-mentioned procedure. The number of pixels must be calculated for statistical analysis of the affected portion, which is done using MATLAB software.

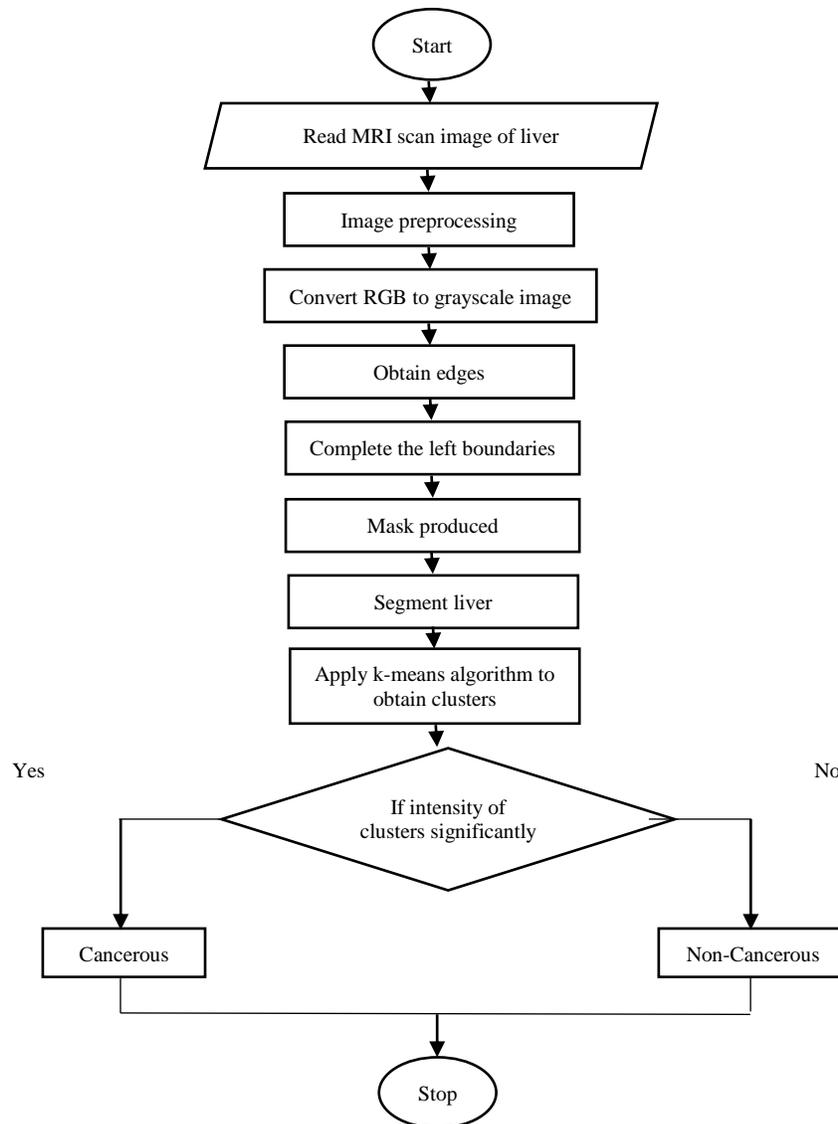
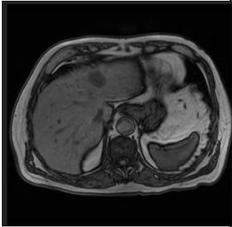
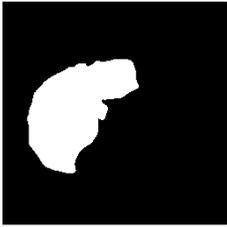
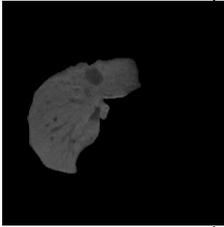
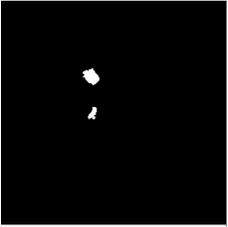
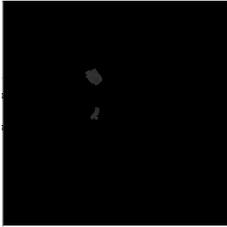
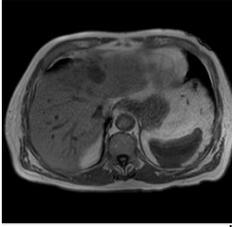
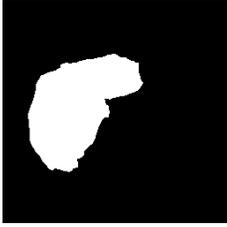
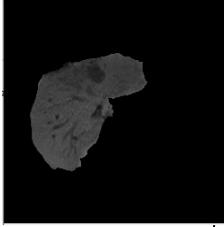
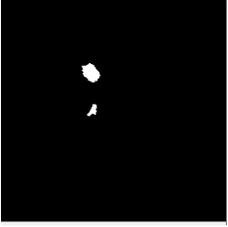
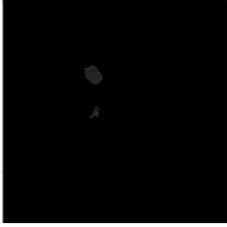
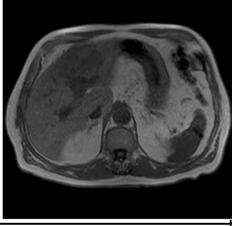
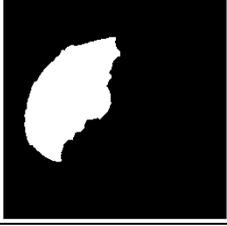
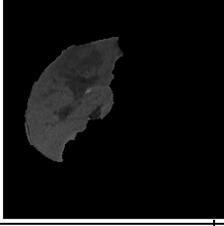
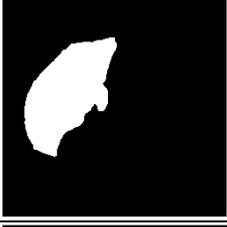
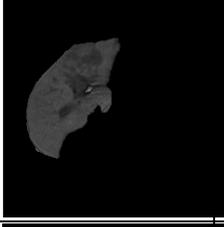
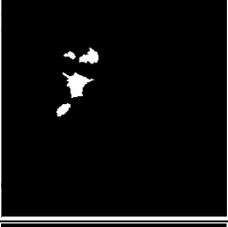
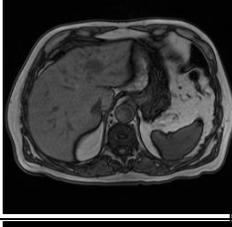
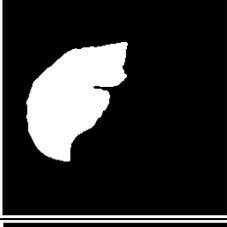
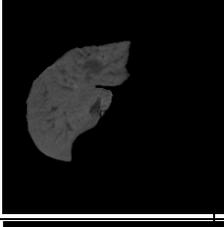
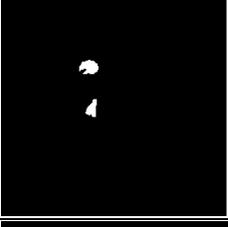
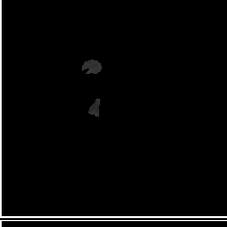
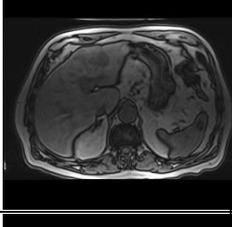
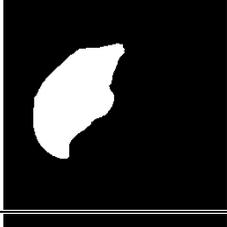
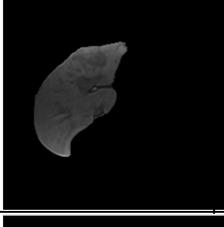
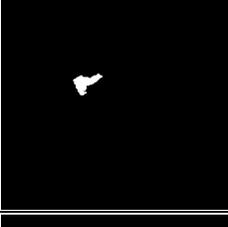
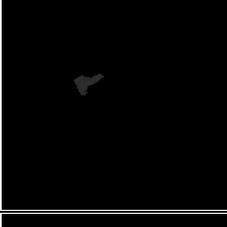
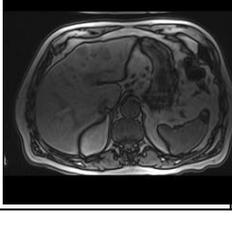
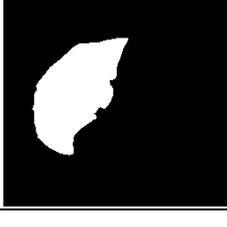
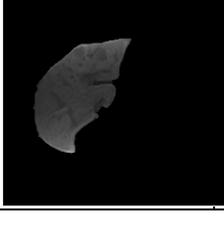
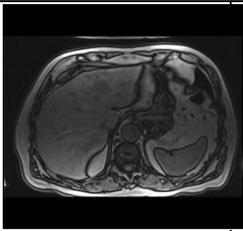
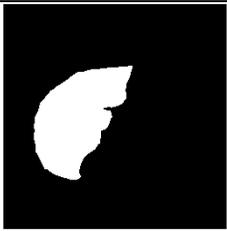
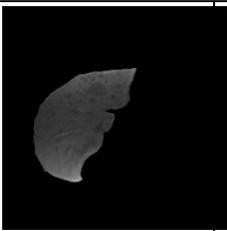
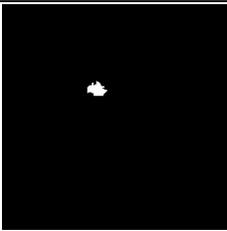
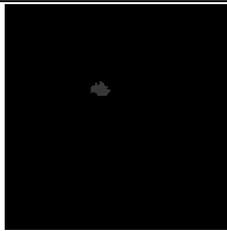
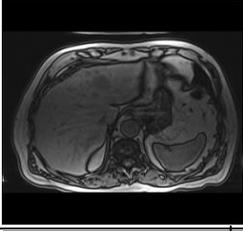
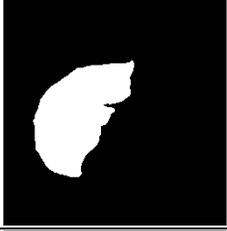
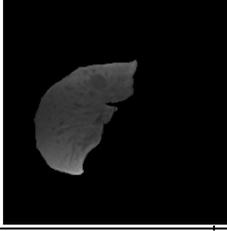
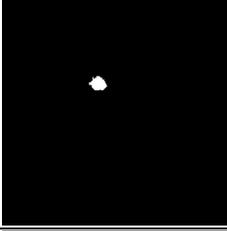
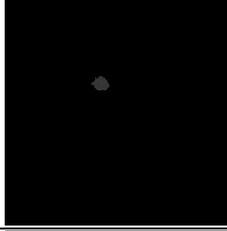
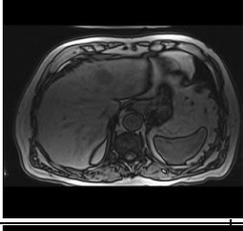
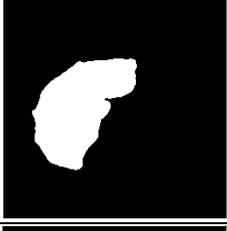
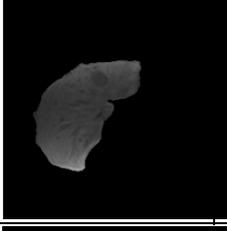
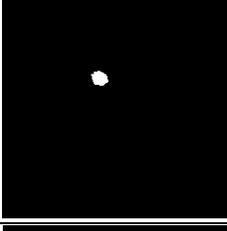
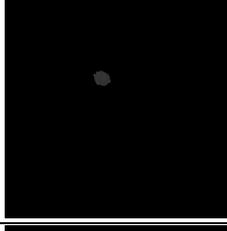
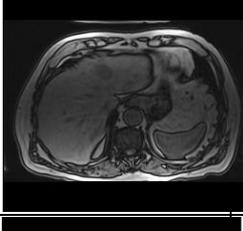
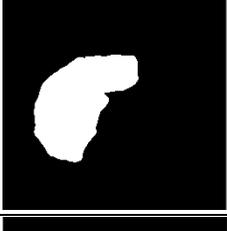
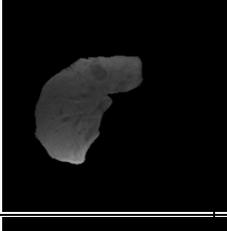
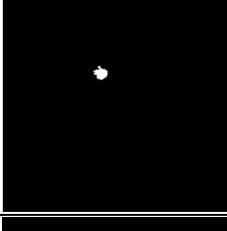
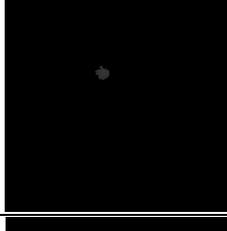
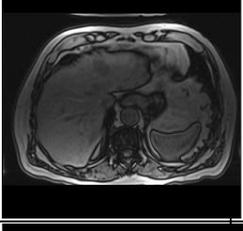
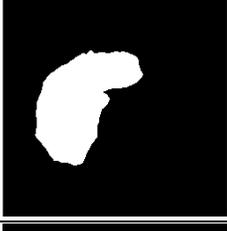
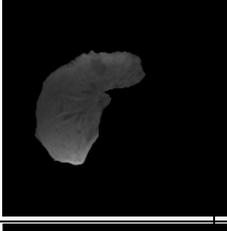
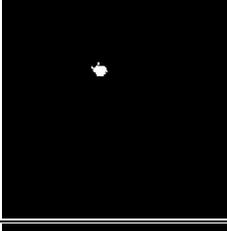
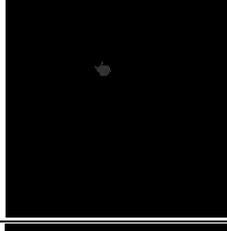
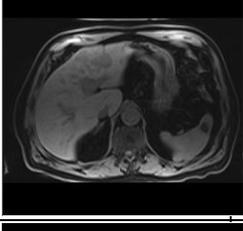
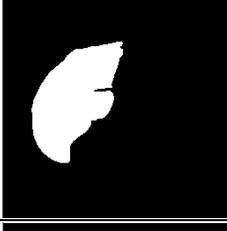
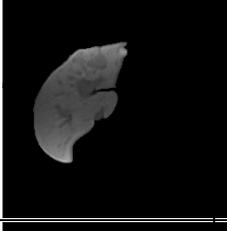
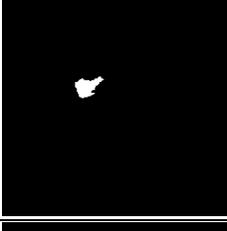
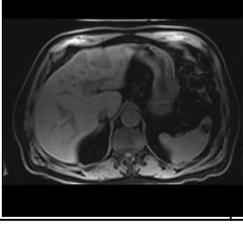
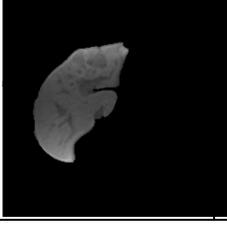
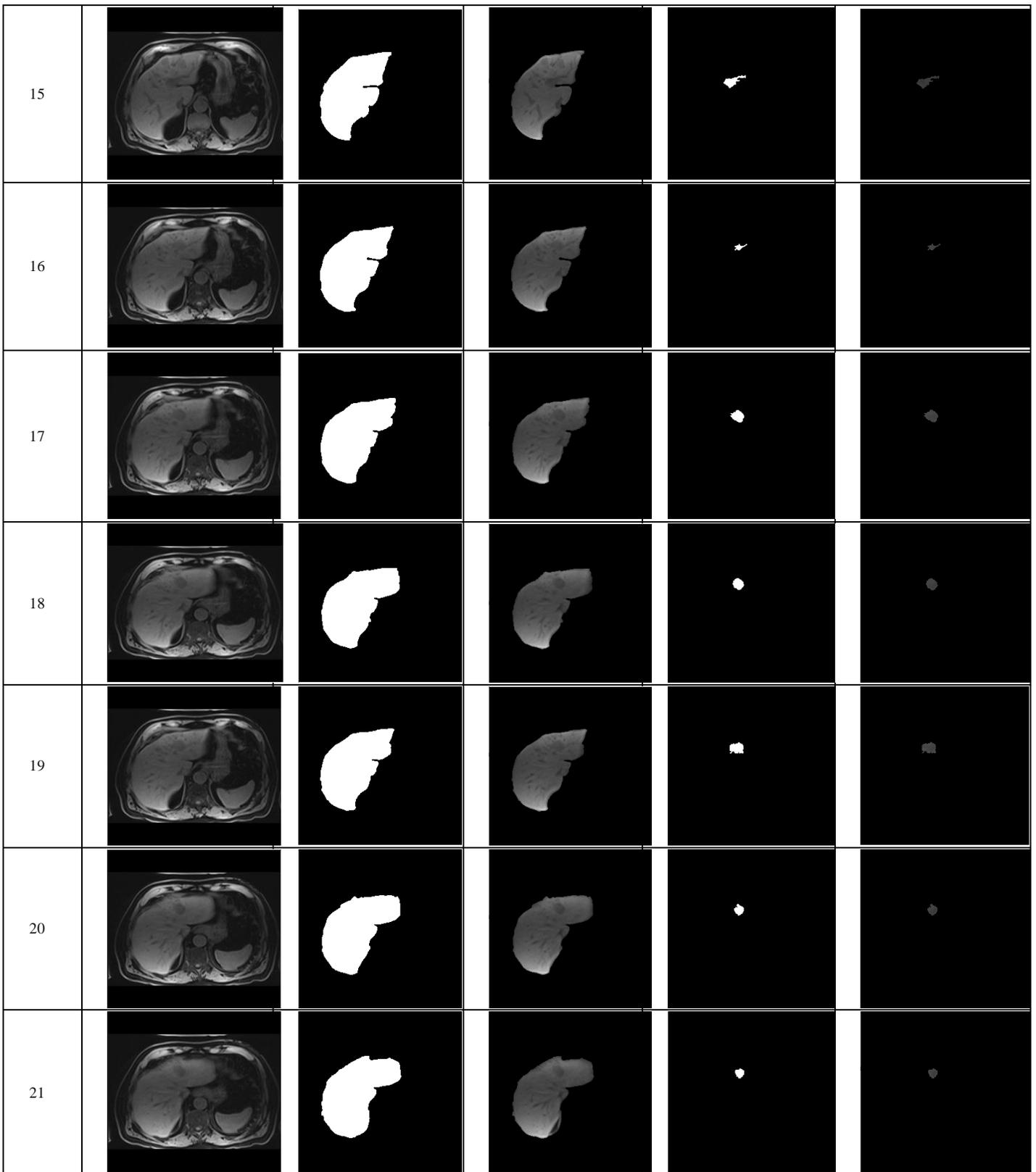


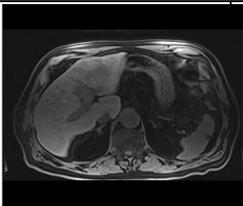
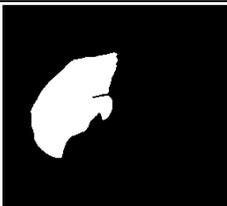
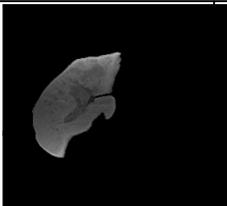
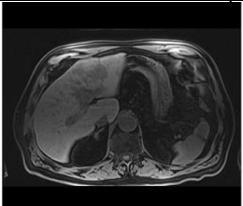
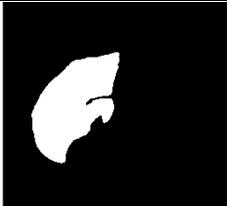
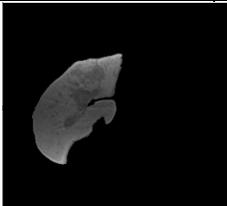
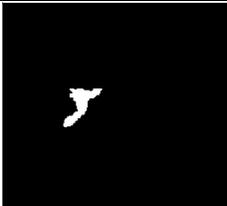
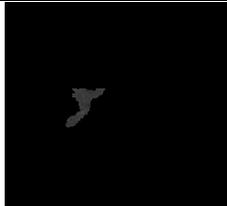
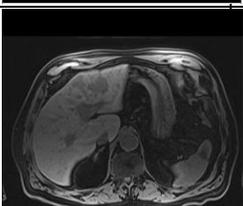
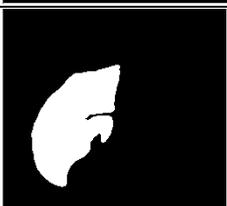
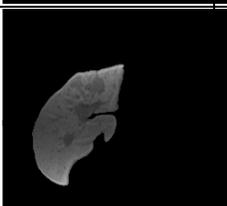
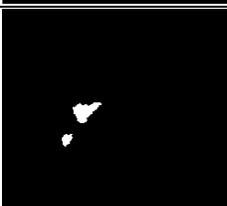
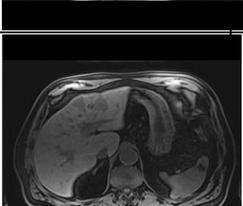
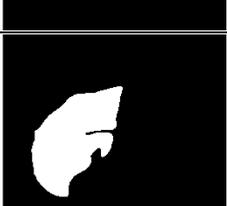
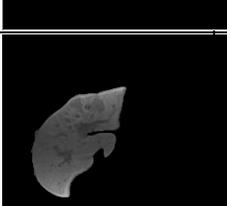
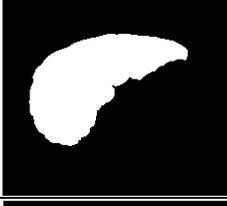
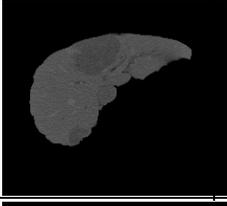
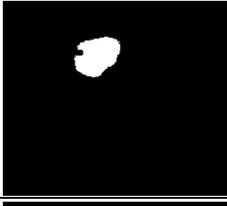
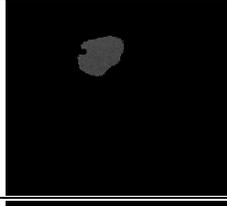
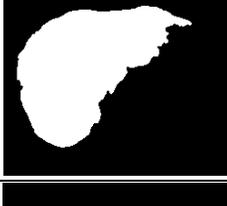
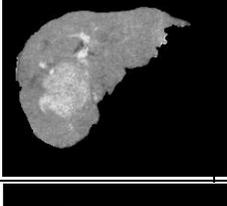
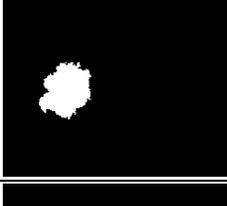
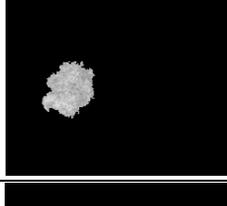
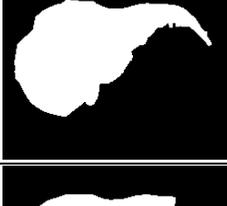
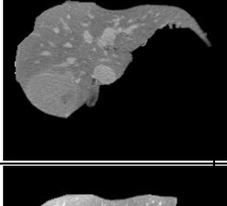
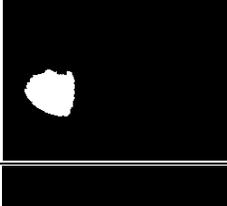
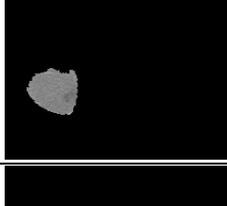
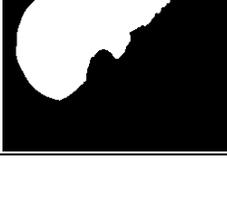
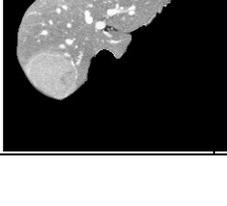
Fig. 1. Proposed Methodology Employed to Segmentation and Tumor Extraction.

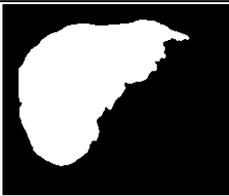
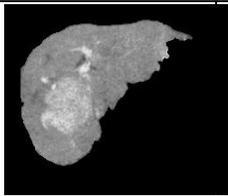
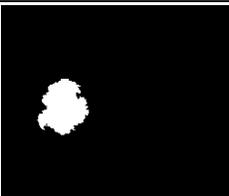
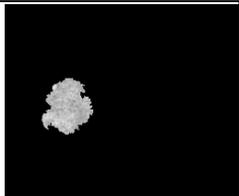
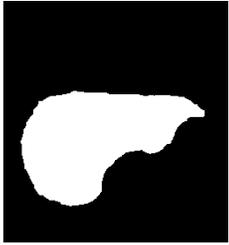
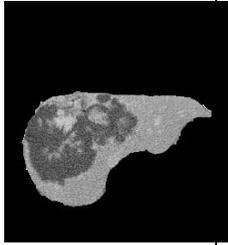
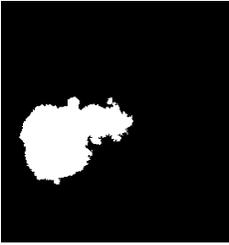
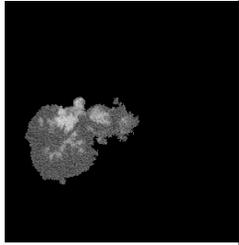
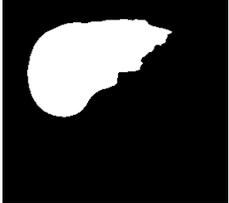
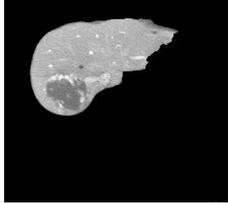
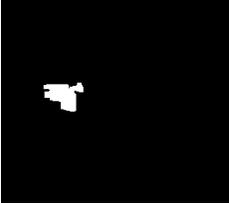
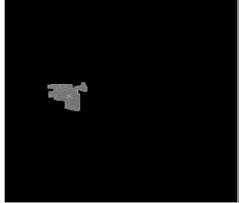
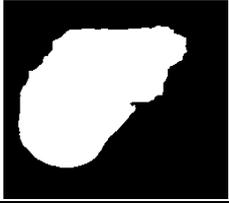
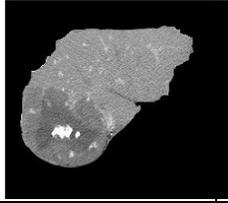
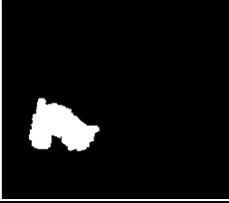
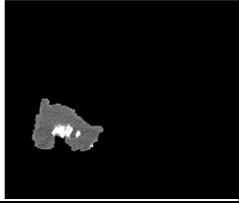
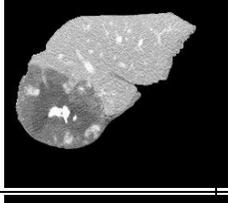
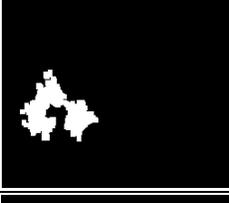
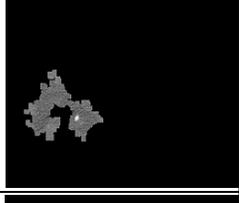
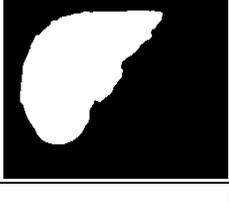
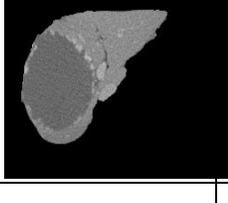
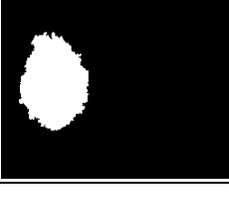
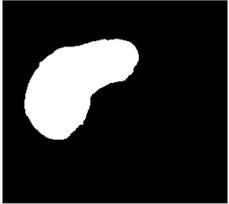
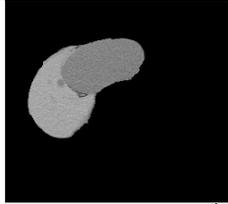
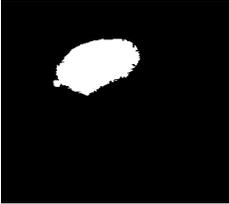
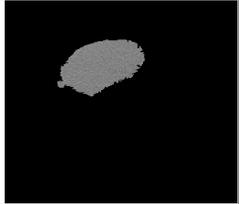
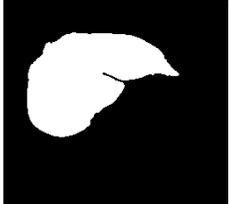
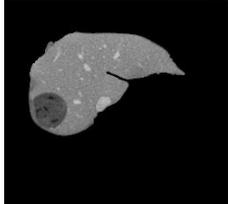
TABLE I. SHOWS THE SEGMENTATION RESULT

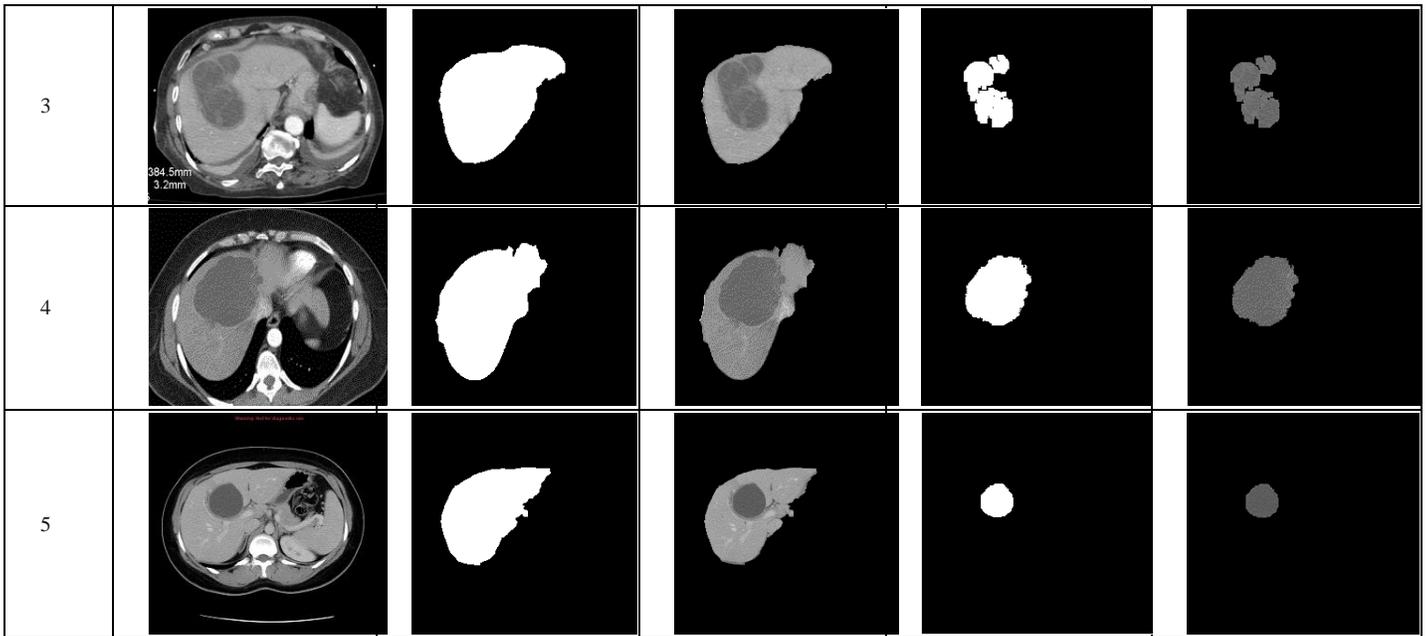
Sr. No	Original Image	Mask	Liver	k-means segmentation	Extracted feature
1					
2					
3					
4					
5					
6					
7					

8					
9					
10					
11					
12					
13					
14					



22					
23					
24					
25					
	<b>Adenoma</b>				
1					
2					
3					
4					

5					
<b>Hemangioma</b>					
1					
2					
3					
4					
5					
<b>Cyst</b>					
1					
2					



Artificial neural networks are used to automate cancer cell identification and further categorization in liver cancer, cyst, hemangioma, and adenoma. Artificial neural networks (ANNs), also known as neural networks (NNs), are computer structures that are loosely based on the biological neural networks that make up animal brains. The artificial neural network feedforward neural network was used in this study. It is made up of layers of neurons (nodes), such as input, hidden, and output layers. Nodes in neighboring layers have connections or edges connecting them. The input layer is made up of input nodes that provide information from the outside world to the network. This layer includes an MRI scan that is analyzed to determine if it contains cancerous cells and, if so, further categorization. There are no direct relations between the hidden nodes and the outside world.

They perform calculations and send data from the input nodes to the output nodes. While a feedforward network can

only have one input layer and one output layer, a hidden layer is formed by a group of hidden nodes. A feedforward network may have zero or several hidden layers. Different masks are saved as hidden nodes in different hidden layers, and the expected edge is compared to all the masks stored in hidden layers, with the highest matching being chosen. The output nodes, collectively known as the “output layer”, are in charge of computing and distributing network information to the outside world. As seen in Fig 2, this layer automatically generates the segmented liver.

Then, on a segmented liver, use the k-means clustering algorithm to predict the cancer-affected area. As shown in Fig 3, tumor analysis and categorization were performed on the basis of statistical features into four categories: cyst, liver cancer, adenoma, and hemangioma.



Fig. 2. Automate Segmentation.

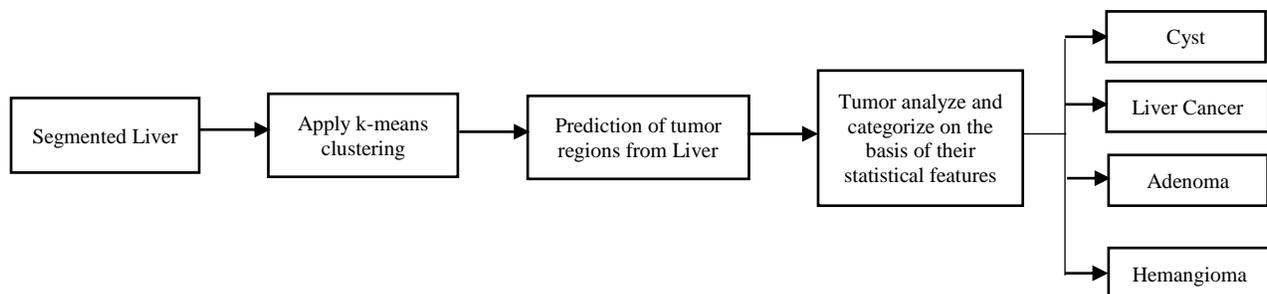


Fig. 3. Categorization of Tumors on the basis of Statistical Features.

### III. RESULTS AND DISCUSSION

One of the most difficult challenges confronting today's researchers is cancer detection. Despite extensive study, there is still a lack of an accurate model since detection is a multidisciplinary role that depends on a variety of parameters. The advancement of accurate cancer detection techniques at an earlier stage has been the subject of extensive research. This paper proposed a novel method for the early detection of cancer that is comparatively precise, less time consuming, and simple to calculate.

From the TCGA database, an MRI scan dataset was downloaded. After the liver segmentation preprocessing is completed, a mask for all images is generated. All of these masks are held in a hidden layer at various nodes. This mask was created using an edge, and since it is discontinuous, manual marking was used to make it continuous. To distinguish cancerous from non-cancerous regions, the Kmeans clustering algorithm was used, followed by statistical analysis. Skewness, Kurtosis, Energy, Entropy, Standard deviation, Eccentricity, and Circularity are used in statistical analysis.

When all of the image's textures were analyzed, the average value was determined for all cases of liver cancer, adenoma, hemangioma, and cyst, and then the calculation of the average was obvious by looking at the data in the form of tables. The Hemangioma has the highest values for Skewness, Entropy, and standard deviation, as can be seen in the table. Also, in the Hemangioma case, the energy and circularity are at their lowest levels as compared to other cases. The cancer of the liver has the highest energy value, indicating that it is mild and has less gray color. Since entropy is inversely proportional to energy, liver cancer has the highest energy value. As a result, it has the lowest entropy value.

The skewness gives a visual representation of the textural symmetry. As a result, the Adenoma has the smallest value, and the texture has the least symmetry. This means the texture is irregular and non-homogeneous, much like kurtosis. When it

comes to circularity, only a circle has a circularity of one, while every other form has different value than one. The cyst has the highest circularity value, because its form is more circular, while the Hemangioma has a lower circularity value. If the eccentricity value is one, the shape appears to be a line segment, and if it is less than one, the shape becomes more inclined toward a circle. Liver cancer has the highest Eccentricity value, indicating that its shape is more like a line section, while Adenoma has the lowest Eccentricity value, indicating that its shape is more like a circle.

The artificial neural network algorithm is used in the following research to do automatic tumor prediction in an image. Real-time MRI scans, used to determine whether a tumor area exists or not, were obtained from patients and fed into the first layer of an artificial neural network for liver segmentation after preprocessing. In addition, the mask is being prepared for real-time MRI. Then compare the masks saved in the hidden layer with the masks from the real-time MRI. After that, the liver is segmented using the mask with the best match. We get segmented liver in the output layer. To distinguish cancerous from non-cancerous regions, the K-means clustering algorithm was used.

The artificial neural network model is trained using all MRI scan images of liver cancer. A total of ten MRI scan images are used in the testing. The classification using an artificial neural network yielded an average result of 0.9 percent; the annotated result is shown in Fig 4.

The working of the proposed technique is depicted in this research paper on a single MRI scan, with measured attribute values of Eccentricity 0.7924, Circularity 0.7314, Skewness 0.3816, Kurtosis 1.9987, Energy 0.0049, Entropy 0.0415, and Standard deviation 0.0034 after study. When the computed attributes were compared to the average value of all the features (as shown in Table 2), this MRI scan was classified as Liver cancer, which it actually is. Figure 4 depicts the contrast of a real-time MRI scan's discontinuous mask with a mask stored in hidden layer.

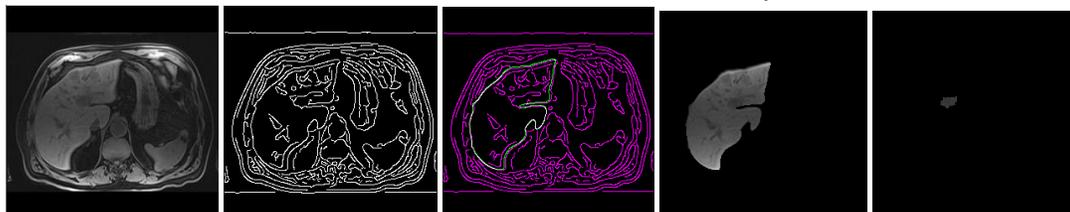


Fig. 4. Shows the Working of our Proposed Method.

TABLE II. AVERAGE VALUE OF FEATURES FOR ALL CASES

Name	Skewness	Kurtosis	Energy	Entropy	Standard deviation	Eccentricity	Circularity
Liver Cancer	0.5149	3.3062	0.005583	0.0531	0.00454	0.7223	0.6545
Adenoma	0.4326	1.4709	0.000497	0.4588	0.05064	0.5867	0.5932
Hemangioma	0.6852	2.6214	0.000446	0.7261	0.05382	0.6932	0.3868
Cyst	0.4234	1.2686	0.000589	0.4413	0.0386	0.5945	0.6883

#### IV. CONCLUSION

Liver segmentation is a difficult task, and automating it is even more difficult, as it involves several steps such as preprocessing, segmentation, and classification. The analogous intensities of other organs such as the spleen, flesh, and muscles are all considered during preprocessing. The artificial neural network algorithm aids in the solution of this problem, automating it through the use of edge and manual marking to create a continuous edge system. The average accuracy rate of the whole liver segmentation using the artificial neural network algorithm is 0.9 percent. Furthermore, an automated method is being developed to identify tumors as benign or malignant, as well as a method to classify perpetual objects using features. It is self-evident that an automated method for classifying tumors as benign or malignant can be useful in object recognition, especially when dealing with medical imaging issues. In addition, a new classification for liver tumors is being considered, which includes more forms of benign liver lesions such as hemangioma, cyst, and adenoma.

#### ACKNOWLEDGEMENT

I am thankful to the Indian Council of Medical Research (ICMR), New Delhi, India for providing me funds for doing this research.

#### REFERENCES

- [1] A. Sharma and P. Kaur, "Optimized Liver Tumor Detection and Segmentation Using Neural Network," no. 5, pp. 7–10, 2013.
- [2] R. Aarthi, S. Nivetha, and P. Vikashini, "LIVER CANCER DETECTION USING IMAGE PROCESSING," pp. 1425–1429, 2020.
- [3] A. Raj and M. Jayasree, "Automated Liver Tumor Detection Using Markov Random Field Segmentation," *Procedia Technol.*, vol. 24, pp. 1305–1310, 2016, doi: 10.1016/j.protcy.2016.05.126.
- [4] A. Krishan, "Detection and Classification of Liver Cancer using CT Images," no. May, pp. 93–98, 2015.
- [5] M. Phil, M. P. Rani, C. Science, and M. Teresa, "Research Article Liver Tumour Detection for Ct Images using Image Processing Techniques Saranya," no. 2015, 2016.
- [6] N. Dhanachandra and Y. J. Chanu, "Image Segmentation Method using K-means Clustering Algorithm for Color Image," vol. 2, no. 11, pp. 68–72, 2015.
- [7] G. Rajesh and A. Muthukumaravel, "Role of Artificial Neural Networks ( ANN )," no. Figure 1, pp. 14509–14516, 2016, doi: 10.15680/IJIRCCE.2016.
- [8] A. H. Ali and E. M. Hadi, "Diagnosis of Liver Tumor from CT Images using Digital Image Processing," vol. 6, no. 1, pp. 685–689, 2015.
- [9] J. Ferlay et al., "Cancer incidence and mortality worldwide : Sources , methods and major patterns in GLOBOCAN 2012," vol. 386, 2015, doi: 10.1002/ijc.29210.
- [10] K. Ahmed, A.-A.-E. Abdullah-Al-Emran, T. Jesmin, R. F. Mukti, M. Z. Rahman, and F. Ahmed, "Early Detection of Lung Cancer Risk Using Data Mining," *Asian Pacific J. Cancer Prev.*, vol. 14, no. 1, pp. 595–598, 2013, doi: 10.7314/APJCP.2013.14.1.595.
- [11] M. Sharma and R. Parveen, "A Complete Summary of Non-Parametric Statistical Methods Used For Biological Microarray Data," no. 4, pp. 4995–5002, 2019, doi: 10.35940/ijrte.D8127.118419.
- [12] M. Sharma, "A Comparative Study of Data Mining , Digital Image Processing and Genetical Approach for Early Detection of Liver Cancer," pp. 687–692, 2020.
- [13] M. Sharma, "A Novel Digital Image Processing based Mechanism for Liver Tumor Diagnosis," 2021, pp. 58–62.
- [14] M. Sharma and R. Parveen, "A Survey on Early Detection of Liver Cancer for Preventive Health Care using Image Processing," vol. 5, pp. 168–173, 2017.
- [15] M. Sharma and R. Parveen, "Prior Detection of a Person ' s Risk Level of Getting Suffered from Liver Cancer," no. 1, pp. 629–637, 2019, doi: 10.35940/ijrtee.A4505.119119.
- [16] D. Sharma and G. Jindal, "Identifying Lung Cancer Using Image Processing Techniques," *Int. Conf. Comput. Tech. Artif. Intell.*, pp. 115–120, 2011.
- [17] Y. A. Deore, "Efficient Image Processing Based Liver Cancer Detection Method," vol. 3, no. 3, 2014.
- [18] A. Verma and G. Khanna, "A Survey on Digital Image Processing Techniques for Tumor Detection," vol. 9, no. April, pp. 1–15, 2016, doi: 10.17485/ijst/2016/v9i14/84976.
- [19] W. Wang and C. Wei, "Advances in the early diagnosis of hepatocellular carcinoma," *Genes Dis.*, vol. 7, no. 3, pp. 308–319, 2020, doi: 10.1016/j.gendis.2020.01.014.
- [20] L. Ali et al., "Intelligent Image Processing Techniques for Cancer Progression Detection, Recognition and Prediction in the Human Liver."

# Automating Time Series Forecasting on Crime Data using RNN-LSTM

J Vimala Devi<sup>1</sup>

Department of CSE  
Cambridge Institute of Technology  
Bengaluru, India

Dr K S Kavitha<sup>2</sup>

Department of CSE  
Dayananda Sagar College of Engineering  
Bengaluru, India

**Abstract**—Criminal activities, be it violent or non-violent are major threats to the safety and security of people. Frequent Crimes are the extreme hindrance to the sustainable development of a nation and thus need to be controlled. Often Police personnel seek the computational solution and tools to realize impending crimes and to perform crime analytics. The developed and developing countries experimenting their trust with predictive policing in the recent times. With the advent of advanced machine and deep learning algorithms, Time series analysis and building a forecasting model on crime data sets has become feasible. Time series analysis is preferred on this data set as the crime events are recorded with respect to time as significant component. The objective of this paper is to mechanize and automate time series forecasting using a pure DL model. N-Beats Recurrent Neural Networks (RNN) are the proven ensemble models for time series forecasting. Herein, we had foreseen future trends with better accuracy by building a model using NBeats algorithm on Sacramento crime data set. This study applied detailed data pre-processing steps, presented an extensive set of visualizations and involved hyperparameter tuning. The current study has been compared with the other similar works and had been proved as a better forecasting model. This study varied from the other research studies in the data visualization with the enhanced accuracy.

**Keywords**—Time series analysis; deep learning; RNN; forecasting; crime data; predictive policing; machine learning

## I. INTRODUCTION

Time series analysis and forecasting[7][17] has always been crucial in the aspects of many research applications such as stock prediction, weather forecasting, supply chain management etc., So why not time series forecasting on crime data?

A time series [5] is a set of numerical values of the same entity taken at equally spaced intervals over time. A time series dataset can be collected yearly, monthly, quarterly and daily etc., any time series analysis can be explained with the help of three components such as

- Trend – Overall long-time direction of series (May be upward or downtrend trend).
- Seasonality – Repeated behaviour at fixed intervals of time.
- Cycles – Occurs when it follows up or down pattern that is not seasonal and can be of varying length.

Conventionally time series analysis has been implemented using linear methods such as AR models, ETS etc., and these methods are simple and effective in implementation for smaller datasets. Machine learning [8] and Deep learning algorithms on the other hand are able to learn the temporal dependencies among the features and do forecasting with more accuracies. Also, deep learning algorithms automatically learn features and build model whereas manual feature extraction is required. The major challenge of this research is to handle the growing volumes of crime data and to build a predictive model with improved accuracy.

This paper is intended to build a better performing forecasting model [4][6] on the crime data. The objective of the current study is to gage the forecasting capacity of the NBeats model [1] on crime data, which is a hybrid of RNN-LSTM [4]. This model will aid police personnel in optimal decision-making and resource management. This work has been compared with the previous works done in this domain and the results are tabulated.

The rest of the paper is organized into the following segments. Section II introduces the existing methodologies. Section III deliberates the proposed approach with flowchart to build a model, discusses the techniques to prepare the dataset suitable for time series analysis and also presents a wide array of data visualization. In Section IV, the outcomes of the forecasting model and measures to calculate its error percentage are presented.

## II. EXISTING METHODOLOGIES

Below is the detailed discussion of the existing methodologies used for forecasting. There are additive models, auto regression models[14][16], machine learning[8][15] and deep learning models[6][12] that are used to foretell about the trend or pattern of the crimes.

### A. Exponential Smoothing (ETS Models)

These ETS models[10] use weighted average of past observations. The components of the model are error, trend and seasonality. Each component can be applied either additively or multiplicatively. Additive methods are useful when the trend and seasonal variations remain constant over time whereas multiplicative methods are applicable when trend and seasonality decrease or increases in magnitude over time.

There are four ETS models:

- Simple exponential smoothing method - In simple exponential method, forecast has been measured as follows.  $Forecast = weight_t y_t + weight_{t-1} y_{t-1} + weight_{t-2} y_{t-2} + \dots + (1-\alpha)_n y_n$ , where  $t$  is the number of periods before the most recent period and  $y_t$  is the target value of time series in 't' and ' $\alpha$ ' is the smoothing parameter.
- Holt's linear trend method - The simple exponential method was expanded to include forecasting data with a trend known as double exponential method or Holt's linear trend methods. This method builds off simple exponential smoothing method not only the level but also trend in its calculation. Trend in this method is always applied in a linear or additive fashion and this method is great and suitable for non-seasonal data.
- Exponential trend method - A variation of Holt's linear trend method is the exponential trend method. It uses the same components (Level and trend) but they are applied multiplicatively. This method is great for non-seasonal time series analysis.
- Holt-winters seasonal method - This method models all the three components such as level, trend and seasonality of time series analysis. It can be either implemented as additive or multiplicative model. The additive method is used in which seasonal fluctuation does not change in time whereas in the multiplicative method, seasonal fluctuation changes in time.

### B. ARIMA Model

ARIMA[11] stands for auto regressive integrated moving average. It is of two types: Seasonal and Non-seasonal. Non seasonal models is built on three components: AR(p), I(d) and MA(q). (p,d,q) represents the amount of time periods to lag for in ARIMA calculation.

- p - refers to the previous periods or the number of lag observations.
- d - refers to differencing term and the number of transformations used in the process of transforming a series into non stationary one.
- q - refers to moving average.

### C. Recurrent Neural Networks(RNN)

Neural networks(NN)[6] in general are simple and great for classification problems by assigning labels and for regression problems in which a continuous value can be predicted. The disadvantage with this kind of NN is that its tendency to forget what it learned or what happened in the past. When it comes to sequential data or ordered data in which data points are interdependent, these NN are a greater disadvantage. Here RNN[4] come into picture which could be imagined as they have a sense of memory to remember what happened in the past. Hence RNN is best suited for time series analysis.

## III. PROPOSED APPROACH

This section introduces dataset and its attributes, data pre-processing steps, smoothing and normalization techniques,

proposed architecture, an algorithm to build a model and evaluation of a model using error accuracy measures such as MAE and Smape.

### A. Dataset

The data used in this paper are real time dataset which was collected from the Sacramento police Open Data portal <https://data.cityofsacramento.org/search> (2014-2021). The dataset contains attributes such as FID, RecordId, Offense Code, Offense\_Extension, Offense Category, Description, Police District, Beat, Grid, occurrence Timestamp. Each instance of the dataset is a crime record with date and timestamp. There are totally 66 unique crime categories. The data set is a collation of the past seven years data and contains a total of 2,72,333 records approximately.

The geographical locations[9] of city of Sacramento have been divided into six districts. Each district is divided into beats and there are a total of 21 prominent beats, beats further split in to grids for better patrolling and surveillance. The dataset reports 66 unique categories of offenses such as trespass, weapon offense, petty theft, burglary, DUI alcohol, owning or possessing ammuniton, conspired crime, vehicle theft, false personation etc.,

### B. Proposed Architecture

In Fig. 1, a flow chart is depicted that explains the proposed methodology step by step.

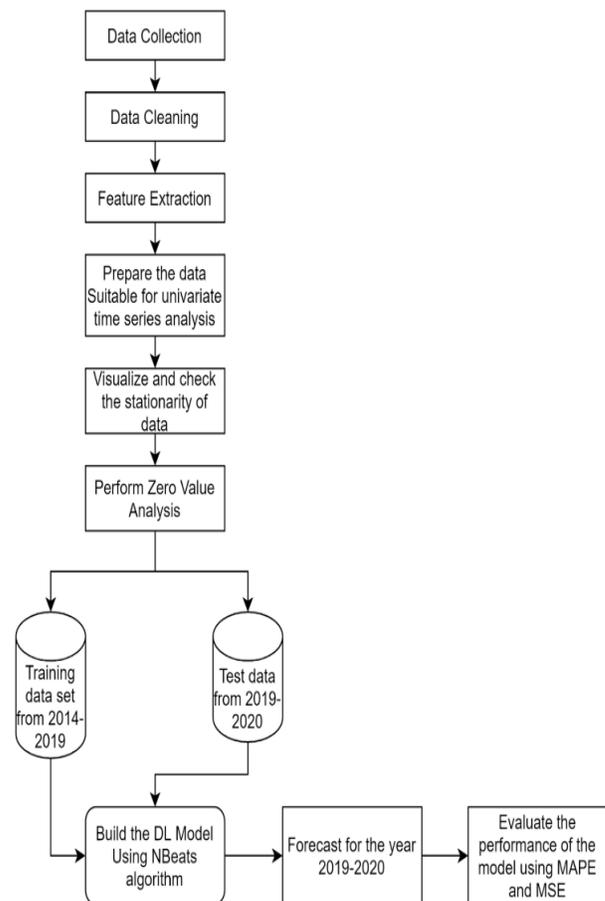


Fig. 1. Proposed Flow of this Work.

It begins with data collection, cleaning and extracting the appropriate features that suit to the requirement of time series analysis. Later, the dataset was tested to realize whether it is stationary or not. Smoothing and normalization techniques had been applied to understand their necessity. Then the dataset was divided into testing and training sets. The model had been trained on 2014 – 2020 data and was tested and forecasted on for the next year 2020-2021 data. The accuracy of the model was measured using MAE and sMAPE.

C. Data Preparation

The real time dataset has to be modified to suit Univariate time series analysis[13][17]. The dataset is cleaned by removing duplicate entries and the rows that contain null values. Less than 1% of rows are found dirty and removed. The instances in the dataset are grouped by Beat and the crime count is calculated for each day beat wise as given in Fig. 2. The zeroth row displays two crimes recorded on 01<sup>st</sup> January 2014, ten crimes recorded on 02<sup>nd</sup> January 2014 and so on in the beat ‘1A’.

For better performance of the model and to achieve uniformity in timeline across the Beats, the period from 2014-12-31 till 2020-12-31 have been considered and the rest of the days are ignored. To do forecasting, measurement of data should be sequential and equal with utmost one data point. For each day within the stipulated time period, the number of crimes is counted.

D. Checking the Stationerity of Series

To check the stationerity of time series, a histogram had been plotted for the 500 days from 1<sup>st</sup> of January 2014 against crime count. Since the distribution of data across the plot did not follow Gaussian distribution and it looked like the distribution is squashed as given in Fig. 3, it may be concluded that the mean and variance is not the same thereby, the given time series data is not stationerity dataset.

E. Zero Value Analysis

Zero value analysis is one of the smoothing techniques. With respect to our time series forecasting, zero value analysis is finding the count of days within the given period for each Beat whose crime count is nil for the day. The sample result is given in Fig. 4.

	Beat	Occurence_Date	Record_ID
0	1A	2014-01-01	2
1	1A	2014-01-02	10
2	1A	2014-01-03	8
3	1A	2014-01-04	6
4	1A	2014-01-05	11
...	...	...	...
57625	UI	2021-02-10	2
57626	UI	2021-02-11	2

Fig. 2. Snapshot that Shows Count of Crimes Day-wise for Every Beat.

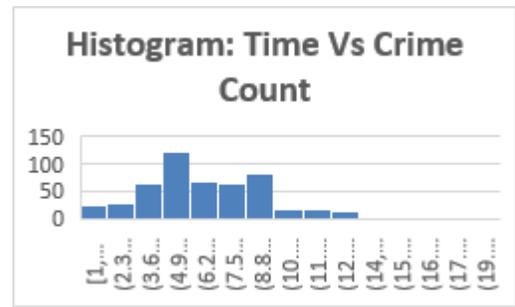


Fig. 3. A Plot to Understand the Distribution of Crime Count.

```

for the beat : ( 1A ) of 1day interval with zero crimes: 5
-----
for the beat : ( 1B ) of 1day interval with zero crimes: 42
-----
for the beat : ( 1C ) of 1day interval with zero crimes: 77
-----
for the beat : ( 2A ) of 1day interval with zero crimes: 5
-----
for the beat : ( 2B ) of 1day interval with zero crimes: 6
-----
for the beat : ( 2C ) of 1day interval with zero crimes: 1
-----
for the beat : ( 3A ) of 1day interval with zero crimes: 12
-----
for the beat : ( 3B ) of 1day interval with zero crimes: 2
-----
for the beat : ( 3M ) of 1day interval with zero crimes: 26
-----
for the beat : ( 4A ) of 1day interval with zero crimes: 17
-----
    
```

Fig. 4. Snapshot Displays Count of Days with Zero Crimes, Beatwise.

For a total of 2,192 days, a time series analysis[13][17] graph with the number of days on the X axis and the count of occurrences of crime on the Y-axis has been plotted for every Beat. Below are the snapshots starting from Fig. 5 till Fig. 13.

For each Beat, a time series graph has been plotted with the incrementing number of days on x-axis and count of crimes on y-axis. From the graphs, it is obvious that the given data set is not a stationary dataset as it exhibits strong seasonality and also there is no obvious upward or downward trend.

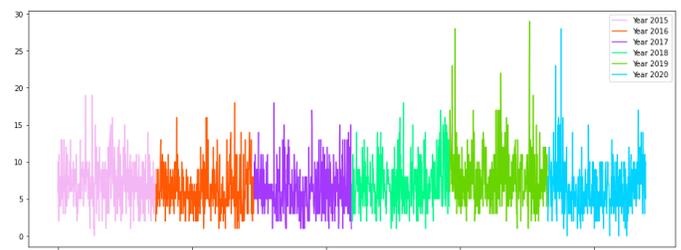


Fig. 5. Time Series Plot for Beat 1A.

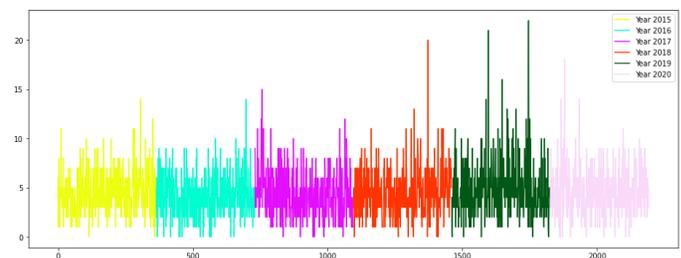


Fig. 6. Time Series Plot for Beat 1B.

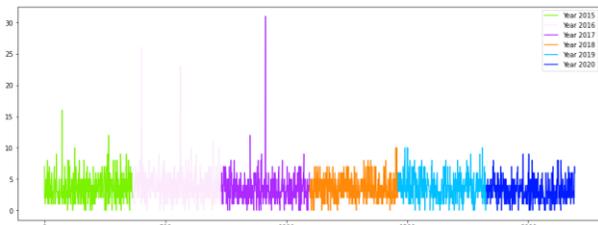


Fig. 7. Time Series Plot for Beat 1C.

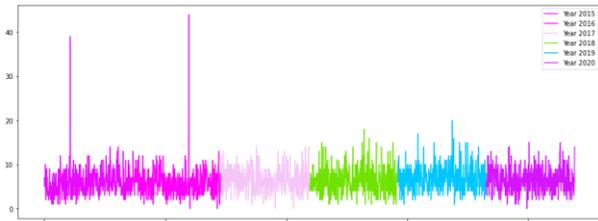


Fig. 8. Time Series Plot for Beat 2A.

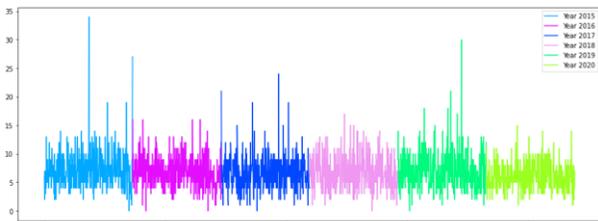


Fig. 9. Time Series Plot for Beat 2B.

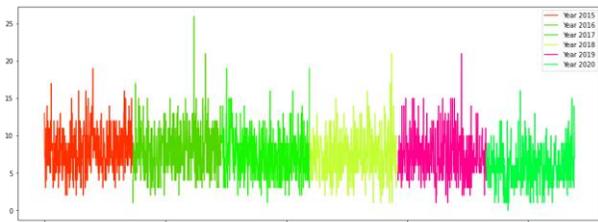


Fig. 10. Time Series Plot for Beat 2C.

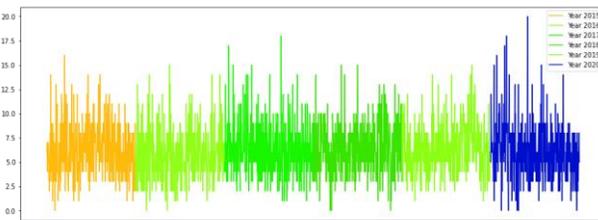


Fig. 11. Time Series Plot for Beat 3A.

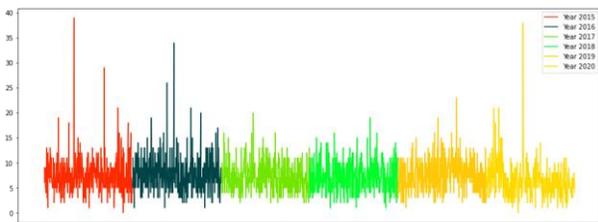


Fig. 12. Time Series Plot for Beat 3B.

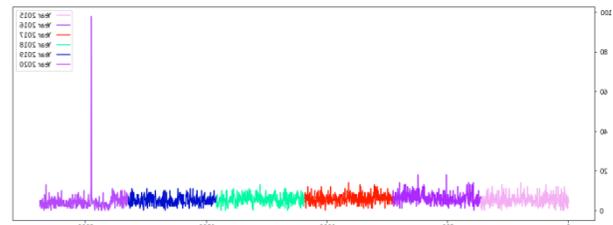


Fig. 13. Time Series Plot for Beat 3M.

Some Beats (geographical locations) recorded the highest number of crimes whereas some Beats such as Beat 3M as in Fig. 13 showed a smaller number of crimes reporting on a daily basis. Most of the Beats exhibited repeating patterns at fixed intervals of time is said to have seasonality. In most of the plots, there is a display for the presence of noise with extraordinary spikes in the growth of crimes.

A normalization technique has been applied to the feature ‘count of crimes’. The count of crimes for every day has been normalized in the range of 0 to 1. The rationale behind this normalization is that in general, deep Learning algorithms that suffer from vanishing and exploding gradient descent problems. In order to overcome these problems, data normalizing have been applied.

#### F. Algorithm

N-Beats – Neural basis expansion analysis for interpretable time series forecasting [1][2] is a block based deep neural architecture suitable for Univariate time series analysis. It is chosen to build a pure deep learning model for forecasting based on time series that can take non stationary data with long term trends and seasonality and excels the accuracy of existing models such as ETS, ARIMA and Holt Winters, etc.

NBeats[1][2] is a hybrid model of RNN and LSTM that takes an entire window of past values and computes many forecast time point values in a single pass. For doing so, the architecture uses fully connected layers containing several blocks connected in a residual way. The first block models the past data(backcast) and predicts the future, then the second block models only the residual error from the previous block and improves the forecast values based on this error and continues to repeat.

Hence it is a residual architecture wherein multiple blocks are stacked together to avoid the risk of gradient vanishing which is common in deep learning algorithms and also has the advantages of ensembling technique. Hence the forecast value is the sum of predictions of several blocks and keeps improving based on residual errors calculated in the other blocks.

Advantages of using N-BEATS RNN over several traditional approaches:

- As all operations are parallelized, it supports quicker training of networks.
- Stacked blocks are much configurable thereby light weight networks.
- Fully Configurable Backcast and Forecast.

This model in Fig. 14 takes time series data upto  $Y_t$ , where  $y =$  datapoints upto time 't' as its input and predict future  $Y_{t+l}$  where  $l =$  length of forecast window. Let us consider  $t = 90$  days and  $l = 30$  days. The size of the input is always  $x \cdot H$  where  $x$  refers to features and  $x = 1$ , also known as Lookback Period. During this period, our time series model learns the behavior in the past and tries to predict the behavior of  $H$  data points which is known as Forecast period. In our case, it is for one day.

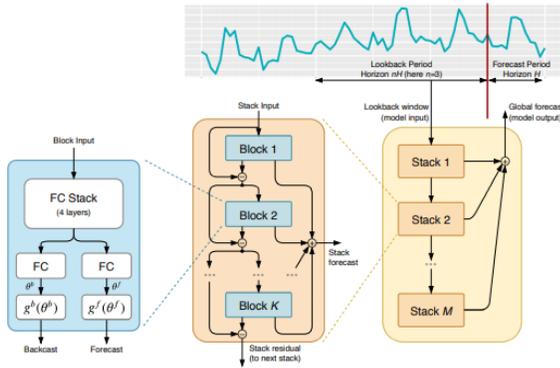


Fig. 14. NBeats Deep Layered Architecture [1].

NBeats architecture takes time series data for the lookback period of 90 days as input to stack 1, and each stack in turn is made up of multiple blocks and it is necessary to understand the structure of basic block as given below.

1) *Basic blocks*: A lookback period of 90 days is given as input to the stack that passes through every block and a forecast period is set for the next 30 days. The input passes through a set of 4 connected layered(FC + Relu) stack and then divided into two outputs. Each output is further passed through FC and finally we receive two outputs such as

- 90-dimension vector as backcast, (X).
- 30-dimension vector as forecast., (FC).

2) *Stacking of blocks*: Each stack consists of multiple basic blocks, arranged in a double residual manner. For each block,

- A vector  $X(x_1, x_2, x_3, \dots, x_{90})$  is given as input to the first block and every block.
- The first block gives two vectors as outputs ie. BC\_1(Backcast of block 1) and FC\_1
- The input of 2<sup>nd</sup>, 3<sup>rd</sup>, and so on blocks is calculated as  $(X - BC_1)$ .
- The backcast output (BC\_n) of nth block is the final stack output.
- The forecast output of stack is calculated as  $\sum_{k=1}^n FC_k$  where n is the number of blocks in a stack.

#### IV. RESULT AND DISCUSSION

Any deep learning neural network is trained using stochastic gradient descent algorithm. The purpose of this algorithm is to optimize the model by updating the weights

during training based on error gradient measures. The rate at which the weights are getting updated during training of a model are referred to as learning rate. A plot for tuning the hyperparameter 'Learning rate' is given in Fig. 15.

Training of any neural network involves the challenge of identifying the hyperparameter 'learning rate'. Estimating the optimal training rate is crucial to train a neural network, since learning rate describes how quickly a model is adapted to the given dataset and problem. Learning rate is a highly tunable parameter that calculates the number of weights needed to be updated so that the loss is reduced each time. The calculated learning rate is 0.000562341325190349.

The error measure of this N-Beats baseline model has been measured using mean and SMape(Symmetric Mean absolute percentage error) [3] and displayed in Table I. There are many error metrics such as MAE, MAPE, sMAPE, etc. available.

Mean absolute Error (MAE) is defined as the average of forecast errors  $e_t$ , where  $e_t = F_t - A_t$ .

$$MAE = 1/n \sum_{t=1}^n |e_t| \tag{1}$$

Symmetric Mean absolute Percentage error(sMAPE) is chosen over MAPE for the reason that MAPE behaves extremely undefined for actual zero values. The prediction or the future values are calculated based on the recent known values. But the resulting SMAPE measure is disappointing and the error percentage is 0.5219. Hence the optimal learning rate to train the RNN is calculated as 10<sup>-4</sup> approximately. After training the model, the error in the model has been reduced and calculated as 0.2922. The smaller the sMAPE value, the greater is the prediction accuracy.

$$sMAPE = 1/v \sum_{i=1}^n |(F_i - A_i)| / (F_i + A_i) / 2 \tag{2}$$

#### A. Comparison with Previous Works

The novelty about our work is the in-depth statistical analysis on the data set and converting it into univariate time series data set suiting to model building, thereby pruning the other dimensions. Here is the tabulation of results of this paper with recently published works given in Table II.

Different data sets have been compared in the above table that are using RNN model and their performance measures have been tabulated.

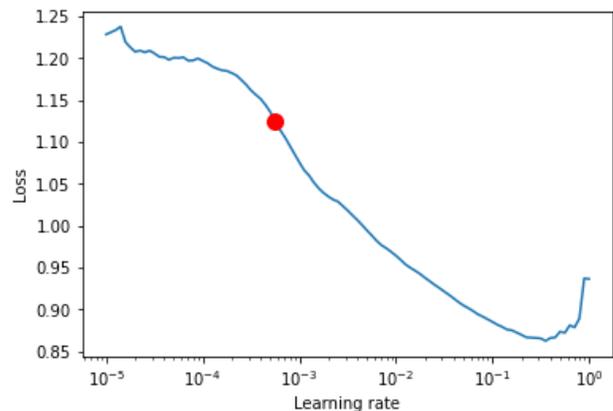


Fig. 15. Plot for Hyperparameter Tuning.

TABLE I. ERROR ACCURACY MEASURES

Error Measures	Before training	After training with optimal learning rate	
		SMApe	MAE
Validation set	0.4314	-	0.1932
Test set	0.5219	0.3922	0.1407

TABLE II. COMPARITIVE ANALYSIS

References	Model	Accuracy Measures
Haseeb Tariq, Muhammad Kashif Hani, Muhammad Umer Sarwar, Sabeen Bari, Muhammad Shahzad Sarfraz, and Rozita Jamili Oskouei [4]	RNN-LSTM model	MAPE = 13.42
Wajiha Safat, Sohail Asghar, (Member, IEEE) and Saira Andleeb Gillani[6]	RNN	RNN-LSTM model for Chicago dataset, MAE = 11.6 RNN-LSTM model for Los Angeles dataset, MAE = 6.0
Current study	RNN-LSTM Model	MAE = 0.1407

## V. CONCLUSION

It is understood that RNN-LSTM model implemented on our univariate data set displayed better performance based on MAE measure(refer in Table II) than the other works in time series forecasting. In general, error accuracy measures vary depending on the context, size of training set and the number of features. In this table, we have used MAE as performance metric. The innovation of this work lies in the systematic way of statistical analysis thereby extracting and understanding the deep insights of the data and converting the dataset suitable for univariate analysis before building a model on the data compared to the other works.

## VI. FUTURE ENHANCEMENTS

In future, a hybrid model could be a better choice for building a forecasting model on this crime data and the accuracy of the mentioned model may be improved by exploring and tuning the other hyperparameters as well. This paper considered the features such as date and time and the number of occurrences of crime per day. In future, the attributes with respect to location that is geospatial coordinates can also be considered to build and improvise the model.

## REFERENCES

- [1] Attilio Sbrana, André Luis Debiasso Rossi, Murilo Coelho Naldi, "N-BEATS-RNN: deep learning for time series forecasting," 19th IEEE International Conference on Machine Learning and Applications (ICMLA), , 978-1-7281-8470-8/20/\$31.00 ©2020 IEEE.
- [2] Boris N.Oreshkin, Dmitri Carpov, Nicolahpados, Yoshua Bengio, "N-BEATS: Neural basis expansion analysis for interpretable time series forecasting," [1905.10437] N-BEATS: Neural basis expansion analysis for interpretable time series forecasting (arxiv.org).
- [3] Choosing the correct error metric: MAPE vs. SMAPE | by Eryk Lewinson | Towards Data Science.
- [4] Haseeb Tariq, Muhammad Kashif Hanif , Muhammad Umer Sarwar, Sabeen Bari, Muhammad Shahzad Sarfraz, and Rozita Jamili Oskouei, "Research Article Employing Deep Learning and Time Series Analysis to Tackle the Accuracy and Robustness of the Forecasting Problem", Hindawi Security and Communication Networks Volume 2021, Article ID 5587511, 10 pages <https://doi.org/10.1155/2021/5587511>.

- [5] Neil Shah , Nandish Bhagat and Manan Shah, Shah et al. "Crime forecasting: a machine learning and computer vision approach to crime prediction and prevention", Visual Computing for Industry, Biomedicine, and Art (2021) 4:9pages.
- [6] Wajiha Safat, Sohail Asghar , (Member, IEEE), and Saira Andleeb Gillani, "Empirical Analysis for Crime Prediction and Forecasting Using Machine Learning and Deep Learning Techniques" in IEEE Access, Received April 24, 2021, accepted May 2, 2021, date of publication May 6, 2021, date of current version May 17, 2021. Digital Object Identifier 10.1109/ACCESS.2021.3078117.
- [7] J Vimala Devi and Dr K S Kavitha, "Time Series Analysis and Forecasting on Crime data" in Press.
- [8] Raza Ul Mustafa, M. Saqib Nawaz, M. Ikram Ullah Lali, Tehseen Zia, Waqar Mehmood, "Predicting The Cricket Match Outcome Using Crowd Opinions On Social Networks: A Comparative Study Of Machine learning Methods" in Malaysian Journal of Computer Science, Mar 1, 2017.
- [9] S. Palaniappan, T.V.Rajinikanth and A. Govardhan "Enhancement of effective spatial data analysis using R in Indian Journal of Science and Technology, Vol 9(21),DOI:10.17485/ijst/2016/v9i21/95149, June 2016.
- [10] J Vimala Devi, Pooja P and Dr K S Kavitha, "Time Series Analysis and Sacramento Crime Data Forecasting", Journal of Huazhong University of Science and Technology, ISSN-1671-451.
- [11] Peng Chen, Hongyong Yuan, Xueming Shu," Forecasting Crime Using the ARIMA Model", IEEE Fifth International Conference on Fuzzy Systems and Knowledge Discovery,vol.5, 2008, pp. 627-630.
- [12] Manal Almuammar, Maria Fasli,"Deep learning for Non-Stationery multivariate time series forecasting", 2019 IEEE International Conference on Big Data (Big Data).
- [13] Jesia Quader Yuki, Md.Mahfil Quader Sakib, Zaisha Zamal, Khan Mohammad Habibullah, "Predicting crime using Time and Location data", ICCCM 2019, July 27-29, 2019, Bangkok, Thailand© 2019 Association for Computing Machinery. ACM ISBN 978-1-4503-7195-7/19/07.
- [14] Roomika yadav, Savita Kumari Sheoran "Crime Prediction using Auto Regression Techniques for Time series data", 3rd International Conference and Workshops on Recent Advances and Innovations in Engineering, 22-25 November 2018.
- [15] Suhong Kim, Param Joshi, Parminder Singh Kalsi and Pooya Taheri, "Crime Analysis through Machine Learning" , 978-5386-7266-2/18/ ©2018 IEEE.
- [16] E. Cesario, C. Catlett, and D. Talia, "Forecasting crimes using autoregressive models", in IEEE 14th Intl Conf on Dependable, Autonomic and Secure Computing, Aug 2016, pp. 795- 802.
- [17] Marzan, C. S., Baculo, M. J. C., de Dios Bulos, R., & Ruiz, C. , " Time Series Analysis and Crime Pattern Forecasting of City Crime Data", Proceedings of the International Conference on Algorithms, Computing and Systems - ICACS '17.

## AUTHORS' PROFILE

**J Vimala Devi** is a B.E graduate in Computer Science and Engineering from Bharathidasan University, M.Tech in Computer Science and Engineering from Satyabama University, Chennai and currently pursuing my Ph.D in Visveswrajs Technology University. She has 13 years of Experience in Teaching. She is a life member of CSI and ISTE. She published a paper titled "Fraud detection in Credit Card Transactions by using Classification Algorithms " in IEEE conference. She is doing a lot of projects on title "Descriptive analytics". She is currently working as Associate Professor, Department of CSE in Cambridge Institute of Technology, Bangalore.

**Dr Kavitha K S** completed BE computer science and Engineering from SIT Tumkur, MTECH from BMSCE Bangalore and PhD from Anna University, Chennai. She is having 22 years of experience in engineering colleges and has worked in various capacities. Around 40 research papers under her credit. Currently she is supervising 6 research scholars. Her areas of interest are Data mining, Machine Learning, Algorithms and Programming etc. Currently she is serving as Professor in the Department of CSE, Global Academy of Technology, Bangalore. She is a life time member of professional bodies such as CSI and IEEE.

# Level Transducer Circuit Implemented by Ultrasonic Sensor and Controlled with Arduino Nano for its Application in a Water Tank of a Fire System

Omar Chamorro-Atalaya<sup>1</sup>, Dora Arce-Santillan<sup>2</sup>  
Faculty of Engineering and Management  
Technological University of Lima Sur (UNTELS)  
Lima - Perú

César León-Velarde<sup>7</sup>  
Universidad Tecnológica del Perú (UTP)  
Department of Humanities  
Lima - Perú

Guillermo Morales-Romero<sup>3</sup>, Adrián Quispe-Andía<sup>4</sup>  
Nicéforo Trinidad-Loli<sup>5</sup>, Elizabeth Auqui-Ramos<sup>6</sup>  
Universidad Nacional de Educación Enrique Guzmán y  
Valle (UNE), Lima - Perú

Edith Gutiérrez-Zubieta<sup>8</sup>  
Universidad de San Martín de Porres (USMP)  
Lima - Perú

**Abstract**—This article aims to describe the design of a circuit of a level transducer implemented by means of an ultrasonic sensor and controlled by Arduino Nano, applied to a water tank of a firefighting system. Initially, the integration of the Siemens 1212C programmable logic controller is described, in the connection between the sensor, the controller and the interfaces that allow to generate the monitoring, control and data recording, conditioned by a PWM pulse width modulated signal controlled by Arduino Nano. When developing the research and performing an analysis of the linear regression model, it is established that the behavior of the controlled variable with respect to time, generates a linear voltage response in the range of 0 to 10 volts; expressing in terms of correlational relationship a factor of R2 equal to 0.997, thus establishing that the designed transducer does not show susceptibility to noise or disturbances in the start-up of the firefighting system.

**Keywords**—Level transducer; ultrasonic sensor; Arduino Nano; control; pulse width

## I. INTRODUCTION

A control system essentially seeks to increase the efficiency of the entire process by maintaining the main variables of the system, within the pre-established range as optimal for the process [1]. Control systems seek to reduce the errors or margins of error typical of non-automated systems, reducing the risks of the plant or process working in unstable conditions [2], [3]. In the same line of opinion in [4], the author points out that control systems are implemented with the purpose of controlling the drive of machines or actuators, seeking to reduce the probability of failures and maintaining certain values of variables at determined intervals.

Under the above, and focusing on industrial systems that rely on fluid fill level control mechanisms. In [5], [6] the authors point out that in the industrial field there are several variables that intervene in the control of the altitude level of some type of fluid on tanks or reservoirs, which makes it essential to control with devices capable of monitoring and

controlling permanent variable tank fill level. Also in [7] the author points out that liquid level system represents a concrete example of control systems with wide diffusion in industrial settings. And it is that any process that needs to store substances in any of their states requires records on the level of deposit of the same in order to make timely and appropriate decisions in search of ensuring the sustainability of the production process [8].

In the search for quality in the production process, guaranteeing liquid level and flow control in tanks is a common problem in industrial processes [9]. Increasing globalization, quality standards and high production standards are the main foundations for specialists to intensify the study of automatic control strategies [10]. In this sense, the study and analysis of variables that intervene in the behavior of related systems in production processes is important and necessary [11]. In this regard in [12]-[14], the authors point out that taking into account technical aspects for the functioning and operation of the sensors and actuators on which the automation and control technology is based. The level control is intended to keep the level of the liquid or fluid within a predetermined value [15]. The inspection of the level height of a fluid by ultrasound encompasses a family of methods based on the transmission of a high frequency wave [16]-[18]. The level sensor detects the surface echo and sends it back to the microprocessor for a digital representation of the distance between the sensor and the surface level [19]-[21].

Low intensity ultrasound signals or, in other words, high frequency signals provide relevant and appropriate information regarding the characterization of liquids or fluids, being able to penetrate containers and chamber walls without significant degradation [22]-[24]. These signals are waves that can propagate through different media such as liquid, solid and gas [25]. In this regard, in [26], [27], the authors point out that the speed with which ultrasound signals propagate and its effects depend mainly on the density and viscosity of the medium

through which they travel, which is why they are They use these signals in industrial and measurement applications.

The electronic instrumentation used to measure the level of liquids works by measuring the height of liquids above a reference line on the one hand, or by measuring the hydrostatic pressure or by using other phenomena. This is the case of ultrasonic sensors, which incorporate an analog signal converter, a processor and input and output interfaces [28]. In this sense, the functionality of embedded systems built from Arduino technology is highlighted, which under its integrated environment seeks to facilitate the use of electronics in multidisciplinary projects [29]-[32].

In this sense, this article aims to describe the circuit of a level transducer implemented by means of an ultrasonic sensor and controlled by Arduino Nano, applied to a water tank of a firefighting system, for which i will initially proceed to specify the connection logic between the sensor, the controller and the interfaces that allow generating the monitoring, control and data recording of the variable under analysis. Finally, an analysis of the dispersion model of the collected data will be carried out in order to establish the behavior of the controlled variable with respect to time.

## II. RESEARCH METHODOLOGY

### A. Design and Research Level

The research method is quantitative, because the filling level of the tank of the firefighting system will be measured with respect to the voltage provided by the transducer output, likewise, the response of the controlled variable is evaluated, in this case the relationship that exists between the altitude measured by the sensor in response to the activation of the fire system.

The research level is descriptive-correlational; it is descriptive because the behavior of the collected data is detailed through statistics in relation to the indicators of the variable under analysis. In addition, it is correlational because it seeks to establish the level of association or relationship between the indicators under analysis in the firefighting system, in order to determine the dispersion model that best describes the data collected by the level transducer circuit.

### B. Data Collection Technique and Instrument

In this research, the technique used for data collection was observation, which was put into practice once the level transducer circuit was implemented and was used on the tank of the firefighting system. Likewise, the data collection technique used was the technical report, the same one that was validated in relation to the data collected through Cronbach's Alpha, and whose value turned out to be equal to 0.7349, evidencing a degree of reliability from moderate to optimal.

## III. DESCRIPTION AND DEVELOPMENT

### A. Description and Development of the Circuit

The control process responds to the use of a level transducer circuit implemented by means of an ultrasonic sensor and controlled with Arduino Nano to maintain the filling level of a tank of a firefighting system within the optimal parameters established for correct operation, as well as the sensors and actuators of the tank's water filling system, it is carried out through a Siemens 1212C programmable logic controller, which requires a conditioning circuit that represents the interface between the Arduino Nano controller and the logic controller programmable. In Fig. 1, the block diagram of the entire system is shown, in order to highlight the integration of the elements and the importance of the signal conditioning, to achieve optimal communication between the two controllers.

The level transducer is made up of an ultrasonic sensor plus an Arduino Nano controller, in which the controller has a PWM (pulse width modulation) output signal with a range of 0 to 5 volts, then we will amplify it with a TL081CP integrated circuit, so that the PWM signal converts it from 0 to 10 volts, Fig. 2 shows the connection architecture, highlighting the integration and synergy of the ultrasonic sensor and the Arduino Nano controller.

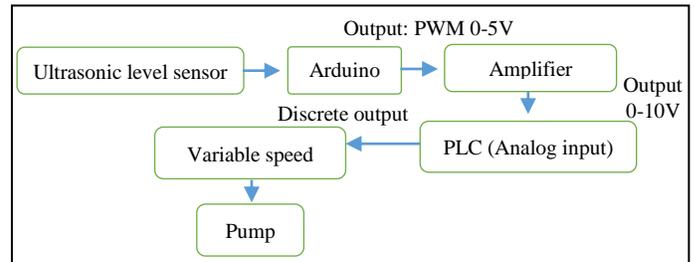


Fig. 1. Controllers Communication System Block Diagram.

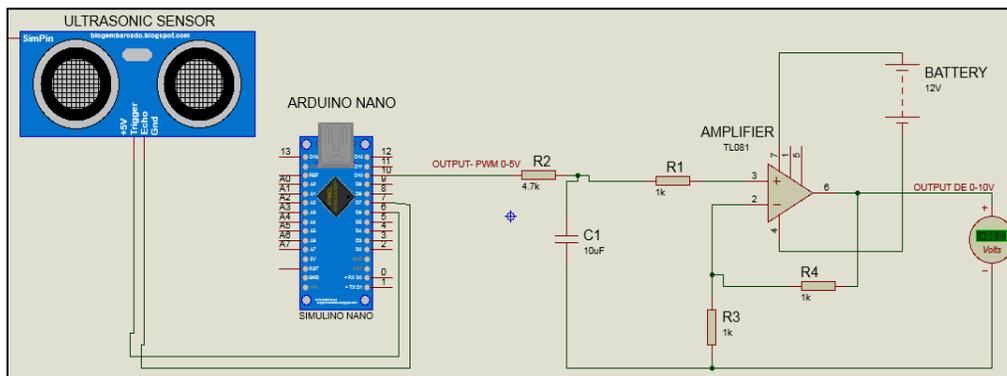


Fig. 2. Connection Architecture of the Arduino Nano and the Ultrasonic Sensor.

Once the connection architecture was defined, the Arduino Nano controller programming relationship was carried out, for which three real type variables (float) are declared, the same one that is linked to the input addresses of the Arduino Nano, these are: trigger (terminal 6), echo (terminal 7) and analog (terminal 10), these variables declared with floating point will be used to carry out the respective calculations in the programming, whose indicators to obtain will be time and distance. The setup function is used to declare the variables to know who will be the inputs and outputs on the Arduino Nano, likewise, the loop function is linked to the trigger variable, it is written in two states at a low level for two 2 seconds, then it is written at a high level for 10 seconds, the response time of the sensor is a function of the variable "echo" (when it is at high level) since it is part of the mathematical operation, thus also the variable "distance" of the sensor is the product of the variable "timeult" (which is the response of the variable echo at high level), between the two constants 2 and 29.15, (this constant is by default). It is important to bear in mind that the value of the variable "outputult" is obtained from the product of the variable "distance" by the constant, whose value is 7.5 (it is specified that how the value of the constant 7.5 is obtained, in the next paragraph).

As the purpose is to obtain an analog signal, it has to be converted to a PWM signal, the equivalent of 0 to 5 volts, but the Arduino Nano works with digitization's from 0 to 255 bits, since the test was carried out with a tank that has a distance of 32 cm, the following calculations are made. The analysis begins considering that 2 times the calibration constant of the distance variable (x) is equal to a digitization of 0 (zero), this due to a possible false alarm that the Arduino Nano controller may generate, thus, 32 is also considered by the calibration constant of the distance variable (x), this because it represents the register that the ultrasonic sensor provided to the tank with a digitization of 255 bits. From the conditions x is obtained, the same that is required, it will help to establish the calibration of the sensor with respect to the distance variable. Adding the two considerations, we have that "34x" is equal to 255, there it is obtained that the value of the calibration constant is 7.5. Adding the two equations, it is determined that the calibration constant of the variable distance (x) is equal to 7.5.

This constant is used to program the Arduino Nano controller. Thus, in Fig. 3, the programming code is shown, in which "analogwrite" is required depending on the operation obtained in the "outputult" variable, in this way we will obtain PWM from 0 to 5 volts.

Another aspect to consider is the amplification stage of the Arduino PWM output from 0 to 5 Volts and from 0 to 10 volts. To achieve such electronic conditioning, the PWM signal from the Arduino Nano was passed through the 4.7 KΩ resistor (R5) and through the 10 uF ceramic capacitor (C1), the sending time of the PWM signal was reduced, this conditioned signal then passes through the 1KΩ resistor (R2) and then connects to terminal 3 of the amplifier. Thus also in terminal 2 of the amplifier the 1KΩ resistor (R3) and the 1KΩ resistor (R4) are placed, in order to achieve a balance of the impedances. Terminals 4 and 7 with 12 volts power the amplifier, and terminals 1 and 5 for the intended purpose will not be used. Terminal 6 is the amplified PWM output of the Arduino Nano,

which is now 0-10 volts, in Fig. 4, the connection architecture of the TL081 operational amplifier is shown.

### B. Description of PLC Programming

To control the system, the system-M0.0 mark is created, which will be enabled by the start-I0.0 button, while the stop-I0.1 button is used to turn off the entire system (Fig. 5). Once the M0.0 mark is turned on, the level sensor programming is activated, for this a normalization is carried out with a digitization of 0-27648 of the Level sensor-IW0 (integer variable) so that a real variable is output with the name of level sensor norm-MD2, this real variable is scaled with a range of 0-35Liters to give us another real variable but already scaled (Level Sensor Output - MD6), as shown in Fig. 6.

```
ULTRASONIC_TRANSMITTER $
int trigger=6;
int echo=7;
int analog=10;
float timeult,distance;
float outputult;

void setup()
{
  Serial.begin(9600);
  pinMode(trigger,OUTPUT);
  pinMode(echo,INPUT);
}

void loop()
{
  digitalWrite(trigger,LOW);
  delayMicroseconds(2);
  digitalWrite(trigger,HIGH);
  delayMicroseconds(10);
  digitalWrite(trigger,LOW);

  timeult=pulseIn(echo,HIGH);
  distance=(timeult/2)/29.15;
  outputult=distance*7.5;
  analogWrite(analog,outputult);
  Serial.print(distance);
  Serial.println("cm");
  delay(100);
}
```

Fig. 3. Arduino Nano Controller Programming Code.

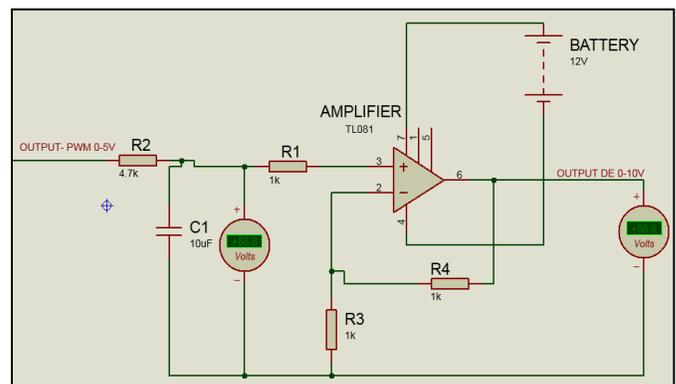


Fig. 4. TL081 op Amp Connection Architecture.

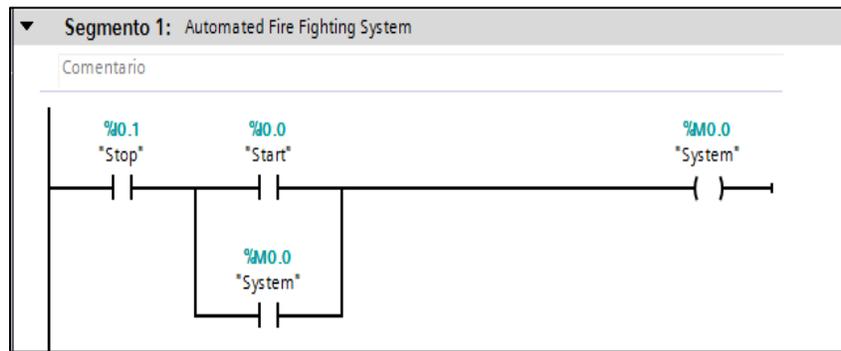


Fig. 5. Automated Fire Fighting System.

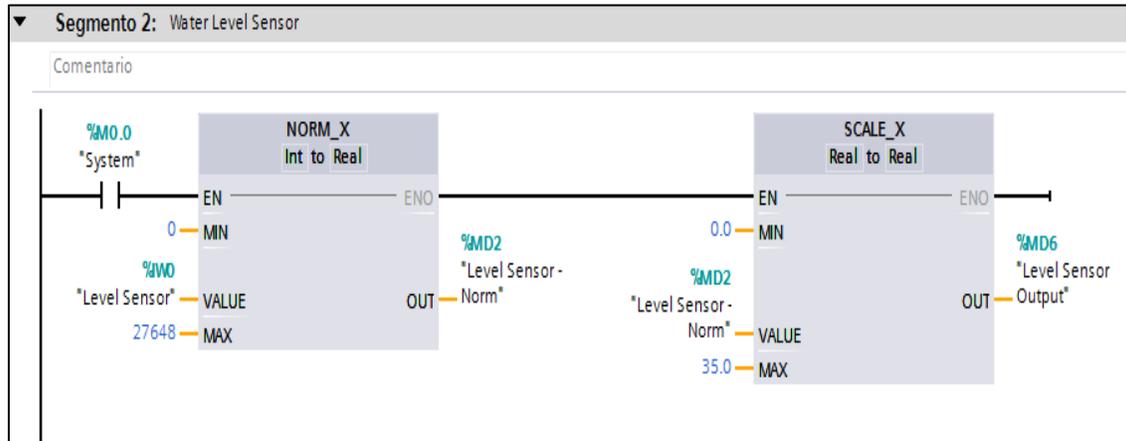


Fig. 6. Water Level Sensor.

Once the M0.0 mark is lit, the pressure sensor programming is activated. A normalization is carried out with a digitization of 0-27648 of the Pressure sensor-IW2 (integer variable) so that a real variable with the name of Pressure sensor norm-MD10 is output, this real variable is scaled with a range of 0-2 Bar which its value of the real variable but already scaled (Pressure Sensor Output - MD14) (Fig. 7).

Once the M0.0 mark is lit, the flow sensor programming is activated. A normalization is carried out with a digitization of 0-27648 of the Flow sensor-IW4 (integer variable) so that a real variable with the name of Flow Sensor Norm-MD18 is output, this real variable is scaled with a range of 0-4 L / min which its value of the real variable but already scaled (Flow Sensor Output - MD22).

When the system is on, the water pump works at a low speed Q0.0 (low speed output), the pump will stop working when the level sensor (Level Sensor output-MD6) reads less than 27L, at that point it will start other speed. The closed outputs Q0.2, Q0.1 and, Q.0.0 are security variables (that is, they are responsible for not letting work at another speed, other than the programmed one).

In the same way, when the level sensor (Level Sensor output-MD6) reads 26L the pump will work at an average speed Q0.1 (Average Speed output), the pump will stop working when the level sensor (Level Sensor output- MD6) dial less than 16L.

Finally, once the level sensor (Level Sensor output-MD6) reads 15L the pump will work at a high speed Q0.2 (Average Speed output), the pump will stop working when the level sensor (Level Sensor output-MD6) mark less than 2L (when it is at 1L), and in this way the process will be completed. In Fig. 8 the programming of the described is shown.

### C. Description of Programming in HMI

When the button I0.2 is pressed, the water pump starts with a low speed of 30 RPM, the level sensor shows a value of 30 liters, the pressure sensor will be at 0.7 Bar and the flow sensor will be at 2.5 L / min., the other speeds will be off. This speed will stop working when the level sensor comparator is less than 27L, which is where the average speed will begin. In Fig. 9 the HMI programming - Low speed is shown.

When the level sensor shows 26L, the water pump starts with an average speed of 45 RPM, the level sensor shows a value of 26 liters, pressure sensor 1 bar and flow rate 3.2 L / min. This speed will stop working when the level sensor comparator is less than 16 L, which will start the low speed. The described is visualized in Fig. 10.

Finally, when the level sensor reads 15L, the water pump turns on with a high speed of 45 RPM, the pressure sensor will read 1.2 bar and the flow rate 3.6 L / min. This speed will stop working when the level sensor comparator is less than 2 L, thereby causing the system to turn off.

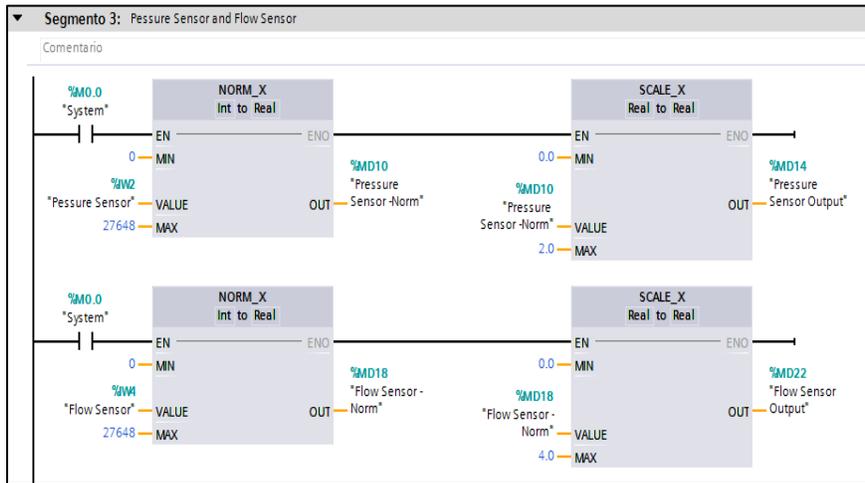


Fig. 7. Pressure Sensor and Flow Sensor.

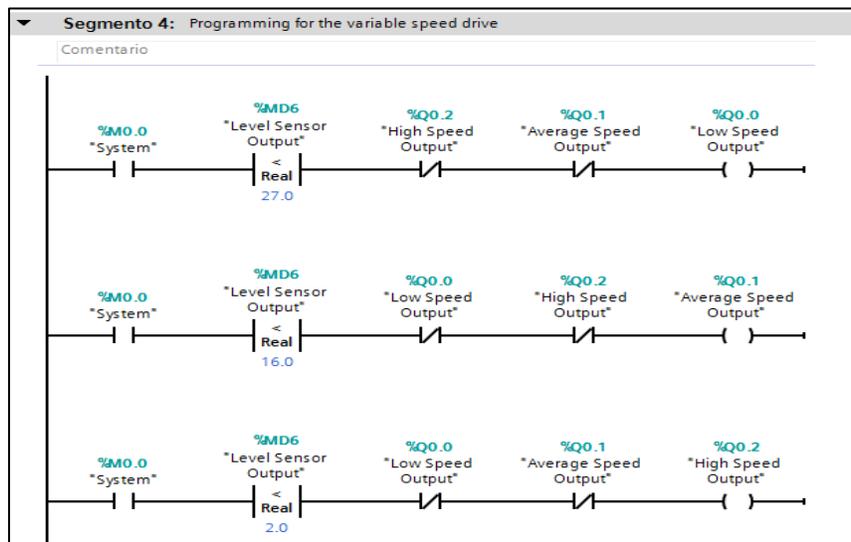


Fig. 8. Programming for the Variable Speed Drive.

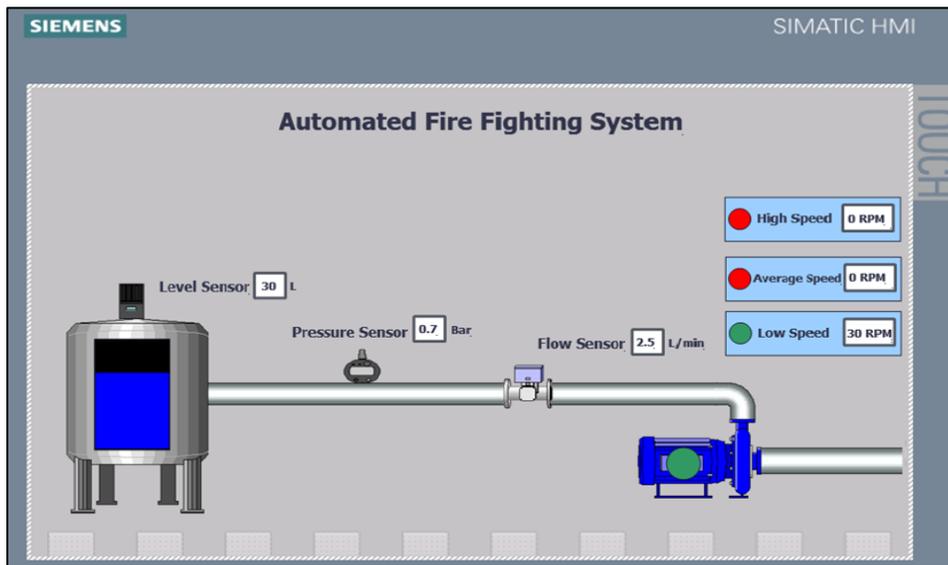


Fig. 9. HMI Programming - Low Speed.

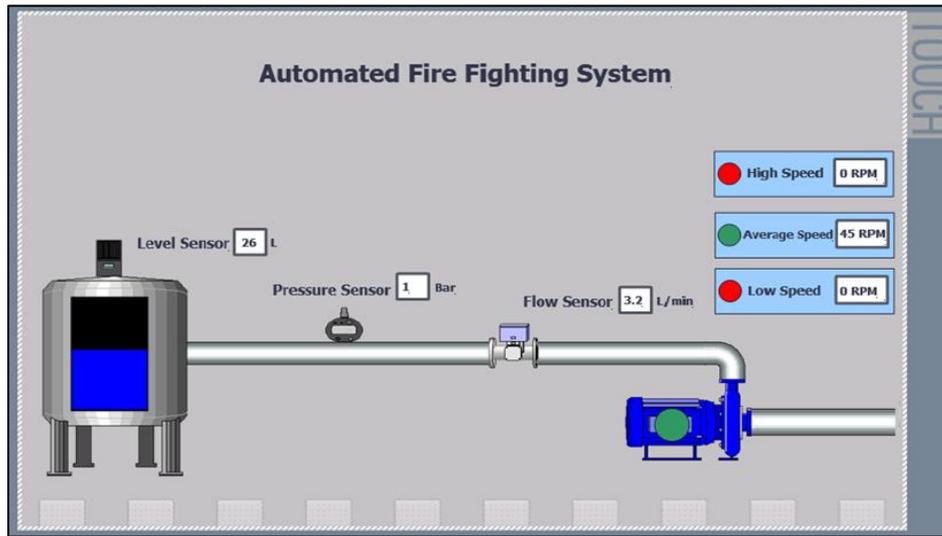


Fig. 10. HMI Programming - Average Speed.

#### IV. RESULTS AND DISCUSSION

##### A. Results

Likewise, the filling level of the tank of the firefighting system was measured with respect to the voltage provided by the transducer output. Using the curvilinear estimation analysis through the SPSS software, the determination factor  $R^2$  for a linear behavior was found to be 0.997, which shows that there is a level of linear scaling of the designed transducer; thus evidencing its optimal performance. It is necessary to indicate that the linear regression model was used because it is the one that provides us with a greater determining factor or  $R^2$ . In Fig. 11, the data dispersion model is shown, highlighting that it responds to a linear behavior.

In Table I, a detail of the estimate that defines the behavior of the output data of the transducer is shown, with respect to the input voltages, the value of  $R^2$  and the constants that show the relationship between voltage and distance are observed.

##### B. Discussion

According to the findings obtained, it was possible to develop the level transducer, from the use of an Arduino controller and an ultrasonic sensor, guaranteeing the linearity of the results obtained, that is, the response of the sensor whose input signal is the filling level of water from the tank of the firefighting system, allows the conversion or transformation of the physical magnitude into an electrical signal in the range of 0 to 10 volts. In this regard, in [18], [8] and [15], they point out that the integration of the ultrasonic sensor, linked to an Arduino controller, turned out to work correctly in remote decision systems, although they emphasize that although they are susceptible to noise, these were not evidenced at the time of their operation. From my point of view, this scenario manifests itself due to the conditions and processes to which the ultrasonic sensor and the Arduino controller are being subjected, since it can change in other contexts.

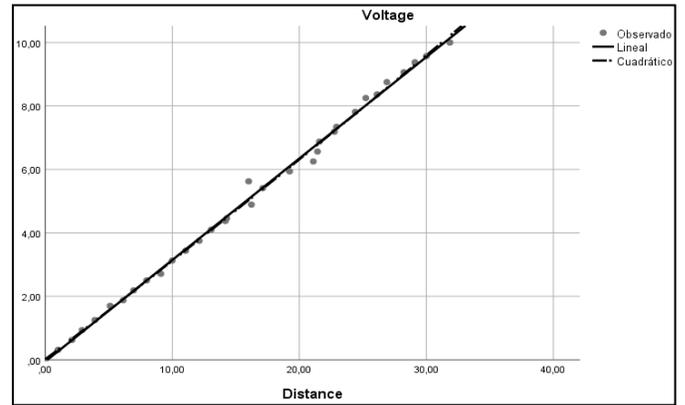


Fig. 11. Curvilinear Estimation of the Response of Data Generated by the Transducer.

TABLE I. RESULT OF THE  $R^2$  CURVILINEAR ESTIMATION TEST

Equation	Model Summary					Parameter estimates		
	$R^2$	$F$	$gl_1$	$gl_2$	Sig.	Constant	$b1$	$b2$
Lineal	0.997	10258.110	1	31	0.000	-0.053	0.320	0.000

Thus, in the analysis of the results, an almost linear behavior is obtained between the variables under analysis (tank filling level and transducer response voltage), in this regard, in [19], [28], [33] and [34] they point out that it is optimal to apply devices such as the Arduino controller to a filling level control system, because they show a linear behavior in their processed data. They do not specify the determining factor of the curvilinear estimate, however they do require that its implementation and assembly were optimal, and these appraisals coincide with the findings obtained in my research, since my determination factor turned out to be 0.997, for a curvilinear estimate.

As indicated in [35] the implementation of the pump alternators system was carried out without major inconvenience when performing the unification of a PLC and Arduino. Both solutions controlled the discrete event system according to the operating requirements set by GRAFCET. The main reasons for using Arduino in automation projects lie in the capabilities of the hardware and its costs. High-end Arduino are known to have superior processing capabilities than many nano PLCs, while PLCs have a high number of inputs and outputs sufficient to automate processes, as well as supporting a large number of open communication protocols.

## V. CONCLUSION

As part of the conclusions to be specified, in relation to the findings obtained, the following is specified:

It is concluded that the proposed integration between the ultrasonic sensor, the Arduino Nano controller and the Siemens 1212C programmable logic controller was viable, this thanks to the conditioning of the PWM modulated signals from 0 to 5 volts to 0 to 10 volts through the TL081 operational amplifier, thus achieving a synergy between all these devices, and achieving the purpose that is the capture of data on the tank filling level through the transducer designed and described in this article.

Finally, it is concluded that the process of converting the physical magnitude to the electrical signal was not affected by noise or external disturbances in the context of the process (tank used for firefighting systems), since when subjected to operations in the same process of detection and fire showed a linear behavior, that is to say, almost devoid of noise effects. This allows it to be concluded that its application to this type of process is useful.

Regarding future plans, remote monitoring, supervision and control strategies should be considered; as well as mechanisms for the detection of fire to be reported to a reception equipment in the 4G or 5G band, through a GPRS communication interface module.

## REFERENCES

- [1] L. Barik, "IoT based temperature and humidity controlling using Arduino and Raspberry Pi," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, pp. 494-502, 2019. DOI: 10.14569/IJACSA.2019.0100966.
- [2] E. Feki, M. A. Zermani and A. Mami, "GPC temperature control of a simulation model infant-incubator and practice with arduino board," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 8, pp. 46-59, 2017. DOI: 10.14569/IJACSA.2017.080607.
- [3] O. Chamorro-Atalaya, J. Yataco-Yataco and D. Arce-Santillan, "Industrial network for the control and supervision of the acetic acid dispatch process, and its influence on the reduction of chemical contaminants for operators," *Advances in Science, Technology and Engineering Systems*, vol. 5, pp. 13-20, 2020. DOI: 10.25046/aj050103.
- [4] Z. Zheng, Y. Yao, S. Yonghai and J. Yeow, "Development of a highly sensitive humidity sensor based on the capacitive micromachined ultrasonic transducer," *Sensors and Actuators B: Chemical*, vol. 286, pp. 39-45, 2019. <https://doi.org/10.1016/j.snb.2019.01.097>.
- [5] O. Chamorro, D. Arce, and M. Diaz, "Comparative Analysis between a Photovoltaic System with Two-Axis Solar Tracker and One with a Fixed Base," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, pp. 124-129, 2019. DOI: 10.14569/IJACSA.2019.0101018.

- [6] K. Arsalan, B. Farzana, D. Muhammad, S. Ahmed, Z. Ullah and H. Ali, "Accident Detection and Smart Rescue System using Android Smartphone with Real-Time Location Tracking," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, pp. 341-355, 2018. DOI: 10.14569/IJACSA.2018.090648.
- [7] D. Wang, S. Masroor and M. Shafiq, "Attitude and Altitude Control of Trirotor UAV by Using Adaptive Hybrid Controller," *Journal of Control Science and Engineering*, vol. 2016, pp. 1-12, 2016. DOI:10.1155/2016/6459891.
- [8] Y. Sang, L. Shi and Y. Liu, "Micro hand gesture recognition system using ultrasonic active sensing," *Journal IEEE Access*, vol. 6, pp. 493-501, 2018. doi: 10.1109/ACCESS.2018.2868268.
- [9] J. Natividad and J. Mendez, "Flood monitoring and early warning system using ultrasonic sensor," *Journal IOP: Material Science and Engineering*, vol. 325, pp. 341-349, 2018. DOI: 10.1088/1757-899X/325/1/012020.
- [10] K. Arsalan, B. Farzana, D. Muhammad, S. Ahmed, Z. Ullah and H. Ali, "Accident Detection and Smart Rescue System using Android Smartphone with Real-Time Location Tracking," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, pp. 341-355, 2018. DOI: 10.14569/IJACSA.2018.090648.
- [11] C. Fayçal, T. Rachid, B. Abderrahmen and B. Mohammed, "The application of fuzzy control in water tank level using Arduino," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 7, pp. 261-265, 2016. DOI: 10.14569/IJACSA.2016.070432.
- [12] P. Shah, A. Patil and S. Ingleshwar, "IoT based smart water tank with android application", *IEEE-International Conference on I-SMAC*, vol. 34, pp. 412-421, 2017. DOI: 10.1109/I-SMAC.2017.8058250.
- [13] O. Atalaya, D. Santillan, and M. Choque, "Fire system for an automated electrical substation via programmable logic controller," *Advances in Science, Technology and Engineering Systems*, vol. 4, pp. 353-359, 2019. DOI: 10.25046/aj040645.
- [14] W. Indrasari, B.Heru and M. Andayani, "Early Warning System of Flood Disaster Based on Ultrasonic Sensors and Wireless Technology," *IOP Conference Series Materials Science and Engineering*, vol. 335, pp. 531-540, 2018. DOI: 10.1088/1757-899X/335/1/012005.
- [15] O. Chamorro-Atalaya, D. Arce-Santillan, T. Diaz-Leyva and M. Diaz-Choque, "Supervision and control by SCADA of an automated fire system," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, pp. 92-100, 2021. <http://doi.org/10.11591/ijeecs.v21.i1.pp92-100>.
- [16] C. Baldeon-Perez, B. Meneses-Claudio and A. Delgado, "Water level monitoring and control system in elevated tanks to prevent water leaks," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 12, pp. 437-442, 2021. DOI: 10.14569/IJACSA.2021.0120255.
- [17] M. Aliff, M. Yusof, N. Samsiah and A. Zainal, "Development of fire fighting robot (QRob)," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 10, pp. 147-142, 2019. DOI: 10.14569/IJACSA.2019.0100118.
- [18] C. Hernández, "Implementation of an absolute location system for mobile robotic platforms using ultrasonic sensors," Thesis, Technological University of Havana, Cuba, 2017.
- [19] J. Hyo and J. Seo, "Low-Cost curb detection and localization system using multiple ultrasonic sensors," *Journal Sensors*, vol. 19, pp. 123-132, 2019. <https://doi.org/10.3390/s19061389>.
- [20] O. Chamorro-Atalaya, D. Goicochea-Vilela, D. Arce-Santillan, M. Diaz-Choque and T. Diaz-Leyva, "Automation of the burner of a piro tubular boiler to improve the efficiency in the generation of steam," *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 21, pp. 101-109, 2021. DOI: 10.11591/ijeecs.v21.i1.pp101-109.
- [21] B. Zhang, et al., "A Novel Ultrasonic Method for Liquid Level Measurement Based on the Balance of Echo Energy," *Journal Sensors*, vol. 17, pp. 706-715, 2017. <https://doi.org/10.3390/s17040706>.
- [22] B. Zhang, et al., "A Liquid Level Measurement Technique Outside a Sealed Metal Container Based on Ultrasonic Impedance and Echo Energy," *Journal Sensors*, vol.17, pp. 185-193, 2017. DOI: 10.3390/s17010185.

- [23] F. Hashim, R. Mohamad, M. Kassim, S. Suliman, N. Mohamad and A. Abu, "Implementation of embedded real-time monitoring temperature and humidity system," Indonesian Journal of Electrical Engineering and Computer Science, vol. 16, pp. 184-190, 2019. DOI: 10.11591/ijeecs.v16.i1.pp184-190.
- [24] A. Roslan and R. Baharom, "Advanced gas leakage, fire and power supply failure monitoring system," Indonesian Journal of Electrical Engineering and Computer Science, vol. 17, pp. 222-227, 2020. DOI: 10.11591/ijeecs.v17.i1.pp222-227.
- [25] C. Moscoso, "Application of the ultrasound technique to experimentally determine the velocity profile of particles contained in pulps or emulsions," Thesis, Federico Santa María Technical University, Chile, 2018.
- [26] D. Ascencios, K. Meza, J. Lluen and G. Simon, "Calibration, validation and automation of the underground drip irrigation system using an Arduino microcontroller," High Andean Research Journal, vol. 22, pp.95-105, 2020. <http://dx.doi.org/10.18271/ria.2020.540>.
- [27] O. Chamorro-Atalaya and D. Arce-Santillan, "Fire alert system through text messages, with arduino mega technology and GSM SIM 900 module," Indonesian Journal of Electrical Engineering and Computer Science, vol. 18, pp. 1215-1221, 2020. <http://doi.org/10.11591/ijeecs.v18.i3.pp1215-1221>.
- [28] J. Moposita, "Control and alert system for the water purification tank in the Ecoagua purification plant," Thesis, Technical University of Ambato, Ecuador, 2018.
- [29] A. Roslan and R. Baharom, "Advanced gas leakage, fire and power supply failure monitoring system," Indonesian Journal of Electrical Engineering and Computer Science, vol. 17, pp. 222-227, 2020. DOI: 10.11591/ijeecs.v17.i1.pp222-227.
- [30] B. Mohd, S. Jong, "Automatic smoke detection system with favoriot platform using internet of things (IoT)," International Journal of Research in Engineering and Technology, vol. 15, pp. 1102-1108, 2019. DOI: 10.11591/ijeecs.v15.i2.pp1102-1108.
- [31] S. Varun, K. Ashok, R. Chowdary, and C. Raju, "Water Level Management Using Ultrasonic Sensor," International Journal of Computer Sciences and Engineering, vol. 6, pp. 799-804, 2014. <https://doi.org/10.26438/ijcse/v6i6.799804>.
- [32] D. Alzate, "Liquid level control and measurement with ultrasound signals," Thesis, Technological University of Pereira, Colombia, 2015.
- [33] M. Reza, S. Sambasri, F. Fitriansyah and H. Rusiana, "Soft Water Tank Level Monitoring System Using Ultrasonic HC-SR04 Sensor Based on ATmega 328 Microcontroller," 2019 IEEE 5th International Conference on Wireless and Telematics, vol. 21, pp. 98-107, 2019. DOI: 10.1109/ICWT47785.2019.8978229.
- [34] L. Restrepo and J. Cardona, "Design of a level control system for the preparation of dialysate liquids based on ultrasonic signals," Thesis, Technological University of Pereira, Colombia, 2015.
- [35] L. Murillo-Soto, "Automation of small-scale with Open Hardware," Technology on the Move, vol. 28, pp. 15-23, 2015.

# Improvement of Deep Learning-based Human Detection using Dynamic Thresholding for Intelligent Surveillance System

Wahyono<sup>1\*</sup>, Moh. Edi Wibowo<sup>2</sup>, Ahmad Ashari<sup>3</sup>, Muhammad Pajar Kharisma Putra<sup>4</sup>  
Department of Computer Science and Electronics, Universitas Gadjah Mada, Yogyakarta Indonesia<sup>1,2,3</sup>  
Faculty of Engineering and Computer Science, Universitas Teknokrat Indonesia, Lampung, Indonesia<sup>4</sup>

**Abstract**—Human detection plays an important role in many applications of the intelligent surveillance system (ISS), such as person re-identification, human tracking, people counting, etc. On the other hand, the use of deep learning in human detection has provided excellent accuracy. Unfortunately, the deep-learning method is sometimes unable to detect objects that are too far from the camera. It is because the threshold selection for confidence value is statically determined at the decision stage. This paper proposes a new strategy for using dynamic thresholding based on geometry in the images. The proposed method is evaluated using the dataset we created. The experiment found that the use of dynamic thresholding provides an increase in F-measure of 0.11 while reducing false positives by 0.18. This shows that the proposed strategy effectively detects human objects, which is applied to the ISS.

**Keywords**—Human detection; YOLO; dynamic thresholding; intelligent surveillance system

## I. INTRODUCTION

Currently, the use of cameras as surveillance media is growing very fast. Usually, cameras are widely used for security purposes in public areas such as schools, offices, stations, airports, highways, and even private homes. Supported by artificial intelligence (AI) development, surveillance with cameras is no longer carried out manually by officers who have many drawbacks such as fatigue, limited staff, etc. Instead, camera-based surveillance allows it to be carried out automatically by utilizing AI-based modules, known as the Intelligent Surveillance System (ISS) [1].

Human detection plays an important role in many applications of ISS, such as person re-identification [2], human tracking [3], people counting [4], human action recognition [5], unattended baggage detection [1], etc. Even though many studies have been carried out for human detection, research on this topic still faces many challenges to overcome real problems constantly changing. One of the popular studies on human detection is the Histogram of Oriented Gradient (HOG), which was first proposed by Dalal [6]. In this study, the gradient in the image is extracted using the Sobel operator, and then histograms are formed. This method is straightforward but produces very good accuracy. Unfortunately, this method cannot handle various kinds of human poses and requires long processing times. Therefore, many new techniques have been

proposed to improve HOG, such as HOG+LBP [7] for handling occlusion, efficient HOG [8], SHOG [9], Rotation-Invariant HOG [10], etc.

The development of deep learning also has a good effect on human detection research. Because of this, many methods for human detection are based on deep learning [11][12]. Martinson and Yalla proposed to use CNN for human detection in mobile robots [11]. Kim and Moon proposed to use deep convolutional neural networks (DCNNs) for human detection on Doppler radar [12]. The use of deep learning provides a significant increase in accuracy compared to handcrafted methods such as HOG. If we assume humans as objects, then many deep-learning-based object detection methods can be used to detect humans. One of the popular deep learning-based methods is YOLO [13]. YOLO produces high accuracy in detecting various kinds of objects, one of which is human objects, and also won the Real-Time Object Detection on PASCAL VOC 2007 competition. Unfortunately, the deep-learning method is sometimes unable to detect objects that are too far from the camera. Thus, this paper proposes to solve this issue.

In many cases, human detection is used at an early stage and significantly affects the accuracy of ISS applications [1-5]. If the human detection accuracy is good, these applications will also produce a good performance and vice versa. Therefore, a reliable human detection module is needed. One method that produces good accuracy is based on deep learning, namely the YOLO Network. However, selecting the confidence value threshold produced by deep learning in the decision stage is very challenging. Using a large threshold will cause human objects far from the camera not to be detected correctly. Conversely, if we use a small threshold, it will result in a lot of false positives. In this study, we propose a new strategy using dynamic thresholding based on the location of potential objects that have been detected. Thus, it is expected to be able to detect small objects while reducing false positives.

Overall, this paper provides the following major contributions: (1) Utilize deep learning for the human detection method. (2) Propose a new strategy to use dynamic thresholding in the decision stage of human detection. (3) Provide a more detailed investigation regarding the effect of threshold selection.

\*Corresponding Author.

## II. THE PROPOSED STRATEGY

### A. Data Collection

In this research, we use the open images dataset v4<sup>1</sup> for training purposes. This dataset contains more than 9 million images with unified annotations for image classification, object detection, and visual relationship detection [14]. We only used person images with object detection annotations. The example of the open images dataset is shown in Fig. 1. We used two CCTV videos from FMIPA Universitas Gadjah Mada, one CCTV video from traffic, and two random CCTV videos for testing purposes. The examples of a testing video are shown in Fig. 2. Table 1 shows the characteristics of video data for evaluation with the various scenario.

### B. Data Labeling and Preprocessing

For testing purposes, the ground truth labeling process starts automatically and then manually verifies using labeling software LabelImg<sup>2</sup>. The annotation process is carried out by following procedure:

- 1) The automatic labeling process is repeated until the best results are obtained subjectively assessed by the annotator.
- 2) The image and label, which is the output of the previous process, will be loaded on the labelImg application.
- 3) The validation process is conducted manually by the annotator.
- 4) If there are wrong or missing bounding boxes, the annotator can add them.

Every second of the video will be divided into twelve images then the coordinates of the bounding box of each image will be saved in a CSV file. The example of a saved bounding box is shown in Fig. 3.

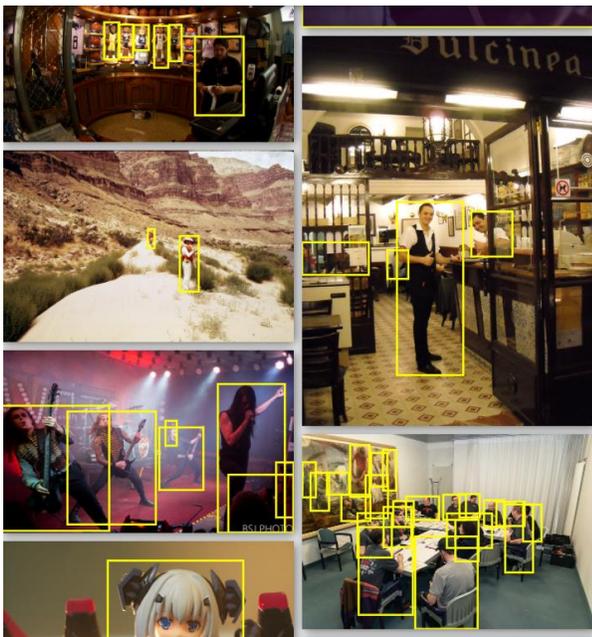


Fig. 1. Several Sample of Open Image Dataset for Training.



Fig. 2. Sample Image of Testing Data.

TABLE I. TESTING VIDEO DATA CHARACTERISTICS

No	Dataset	Duration	FPS	Scenario
1	MIPA 1	01:14	30	Indoor
2	MIPA 2	01:12	30	Indoor
3	MIPA 3	00:28	30	Indoor
4	Office	00:12	30	Indoor
5	Traffic	00:12	30	Outdoor
6	Kitchen	00:12	30	Indoor
7	School	00:13	30	Outdoor

```
1 frame,x1,y1,x2,y2
2 1.0,740,482,818,664
3 1.0,878,465,942,626
4 1.0,977,453,1047,612
5 1.0,814,451,877,612
6 1.0,393,269,414,336
7 1.0,365,277,384,331
8 1.0,518,316,546,413
9 2.0,740,485,822,666
```

Fig. 3. Saved Bounding Box for Testing Data.

### C. Detection Strategy using the Dynamic Thresholding

As shown in Fig. 4, the proposed method starts with extracting human candidate regions using a deep learning model and is then followed by the validation stage using thresholding. The basic method we use in detecting humans is by using YOLO. YOLO network will generate candidate regions of objects with certain confidence values. If the confidence value exceeds the threshold, we will classify this object as human and vice versa. However, selecting the threshold of confidence is very challenging. Using a large threshold will cause human objects far from the camera not to be detected properly. Conversely, if we use a small threshold, it will result in a lot of false positives. To solve this problem, we propose using dynamic thresholding for verifying the human region based on the object's position in the vertical direction, as shown in Fig. 5. The closer the object's position to the top, the smaller the object's threshold score will be and vice versa. This strategy is applied with the assumption that objects close to the top are far from the camera. Objects far from the camera will have faint details, so we use a small threshold so that the object can still be detected. However, if this small threshold is applied to objects close to the camera, it can be false positive.

<sup>1</sup> <https://opensource.google/projects/open-images-dataset>.

<sup>2</sup> <https://github.com/tzatalin/labelImg>.

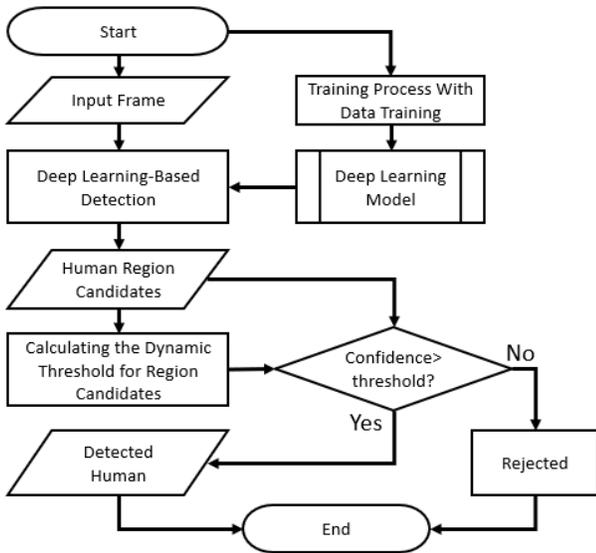


Fig. 4. The Flowchart of the Proposed Method.



Fig. 5. Illustration of Calculating the Object Vertical Position.

We determine the threshold with the following strategy. First, we scale the object's vertical position by dividing the object's vertical center point by the image height ( $H$ ). This value will be used to obtain a threshold on a scale of 0.5 to 1 using the following equation:

$$y' = \frac{y}{H} \quad (1)$$

$$t = y' \times (t_{max} - t_{min}) + t_{min} \quad (2)$$

### III. EXPERIMENT AND RESULTS

This section presents the evaluation protocol used in the experiment and the result of the proposed method with a comparison to the YOLO method. In addition, a discussion of the effectiveness of the proposed method is also presented.

#### A. Evaluation Protocol

We will compare performance and processing time between the basic YOLO method and the YOLO + dynamic threshold in the testing stage. Thus, it can be seen whether the

dynamic threshold process will significantly affect the accuracy and processing time. We use hardware with the following specifications: Processor AMD Ryzen 9 3900x, VGA Nvidia RTX 2080 Ti, RAM 64 Gb with Ubuntu 20.04 operating system.

There are seven videos from different CCTV as test objects. The evaluation process will calculate the IoU value between the detected bounding box and ground truth for each CCTV video frame. Intersection over Union (IoU) is the value based on the statistical similarity and diversity of the sample set whose purpose is to evaluate the area of overlap between the two bounding boxes, namely the predicted bounding box and the ground truth bounding box [15]. IoU can be found using the following equation:

$$IoU = \frac{A \cap B}{A \cup B} \quad (3)$$

We use 0.5 as a threshold for the IoU value. That means any detected object with an IoU value greater than the threshold will be considered true positives (TP). In contrast, if the IoU value is less than the threshold, it will be considered as false positive (FP), and any undetected object will be considered as false negative (FN). To evaluate the method's performance, we use precision, recall, and f-measure [16]. These metrics are used to evaluate the prediction of each frame. To evaluate the model, the precision, recall, and f-measure of all the frames are calculated.

$$Precision = \frac{TP}{TP+FP} \quad (4)$$

$$Recall = \frac{TP}{TP+FN} \quad (5)$$

$$FMeasure = \frac{2 \times precision \times recall}{precision + recall} \quad (6)$$

#### B. Comparison Results

Based on the testing results using seven different datasets, the following results were obtained in Table 2. It can be seen that in all datasets, the proposed strategy achieves 0.89, 0.95, and 0.91 in precision, recall, and f-measure, respectively, for detecting the human object on the video. These results are better than the YOLO method, which only archives 0.71, 0.94, and 0.80 in precision, recall, and f-measure, respectively. Furthermore, applying our strategy could increase the f-measure of human detection by around 0.11. Thus, it proved that the proposed approach is effective for increasing accuracy and reducing the false positive.

#### C. Discussion

In general, for each data test, it can be seen that the recall value tends to be higher than the precision value for both YOLO and the proposed method. This indicates that both methods are weak against false positives or often detect other objects as human objects. Some examples of test results for each datatest are shown in the image below. The blue box shows the results of YOLO detection, while the red boxes show the results of YOLO detection and the proposed method.

TABLE II. COMPARISON RESULTS THE PROPOSED METHOD AND YOLO

No	Datatest	Method					
		YOLO [13]			Proposed Method		
		Precision	Recall	F-Measure	Precision	Recall	F-Measure
1	MIPA 1	0.67	0.92	0.78	0.83	0.91	0.87
2	MIPA 2	0.73	0.97	0.83	0.95	0.99	0.97
3	MIPA 3	0.84	1.00	0.91	0.95	1.00	0.97
4	Office	0.56	0.92	0.70	0.81	0.88	0.84
5	Traffic	0.47	0.87	0.62	0.81	0.86	0.84
6	Kitchen	0.98	1.00	0.98	0.99	1.00	0.99
7	School	0.72	0.92	0.81	0.87	0.93	0.90
<b>AVERAGE</b>		<b>0.71</b>	<b>0.94</b>	<b>0.80</b>	<b>0.89</b>	<b>0.95</b>	<b>0.91</b>

In video 1, the proposed method almost always succeeds in detecting human objects without errors. Still, there are false positives in the YOLO method by detecting the announcement box as a human object, as shown in Fig. 6(a). According to the YOLO network, the announcement box has a confidence value of 0.3, as it is close to the top area. The proposed dynamic thresholding process has eliminated the announcement box because it has a confidence value that does not meet the threshold. Same as in the first video, in video 2, the YOLO method is still wrong in detecting the announcement box as a human object, as shown in Fig. 6(b). However, it can be seen if the human object in front of the announcement box can be detected correctly by both methods.

In video 3, although the camera angle is the same as videos 1 and 2, there is a false positive for another object, namely the trash box, when detected using the YOLO method, as shown in Fig. 6(c). While in the proposed method, there are no errors. In video 4, there are false negatives if detected using the proposed method, as shown in Fig. 6(d). False negatives occur when there is an occlusion of a human object. Occlusion makes the object's confidence value low due to the lack of features that can be extracted due to some features covered by other objects. There were many false positives when testing on video 5 using the YOLO method by detecting road cones as humans, as shown in Fig. 6(e)-(g). At the same time, the proposed method is still able to detect well every human object.

Both YOLO and the proposed method can detect human objects well because the distance of the camera to the object is still quite ideal so that the details of the object are quite clear and there is no occlusion on the object. Therefore, it can be concluded that the proposed method has better performance than the YOLO method, as shown in Table 2. In the example of the detection results, it can also be seen that there are errors in the YOLO method in detecting objects. Overall, both YOLO and the proposed method can almost always detect human objects but still often detect other objects as human objects. This is indicated by the recall value, which is higher than the precision value.

Nevertheless, the proposed method fails to detect objects that are very far from the camera because the details of the object are not clear, so that there are not many features that can be extracted. It makes the object's confidence value below the threshold. To solve this problem, we may improve the selection of dynamic threshold by considering the distance between the candidate object and the vanishing point. In this case, we should integrate the vanishing point detection [17] [18]. Another solution is by utilizing the super-resolution method for very far objects [19]. However, this solution may require a long processing time.



(a) Detection Sample from Video 1.



(b) Detection Sample from video 2.

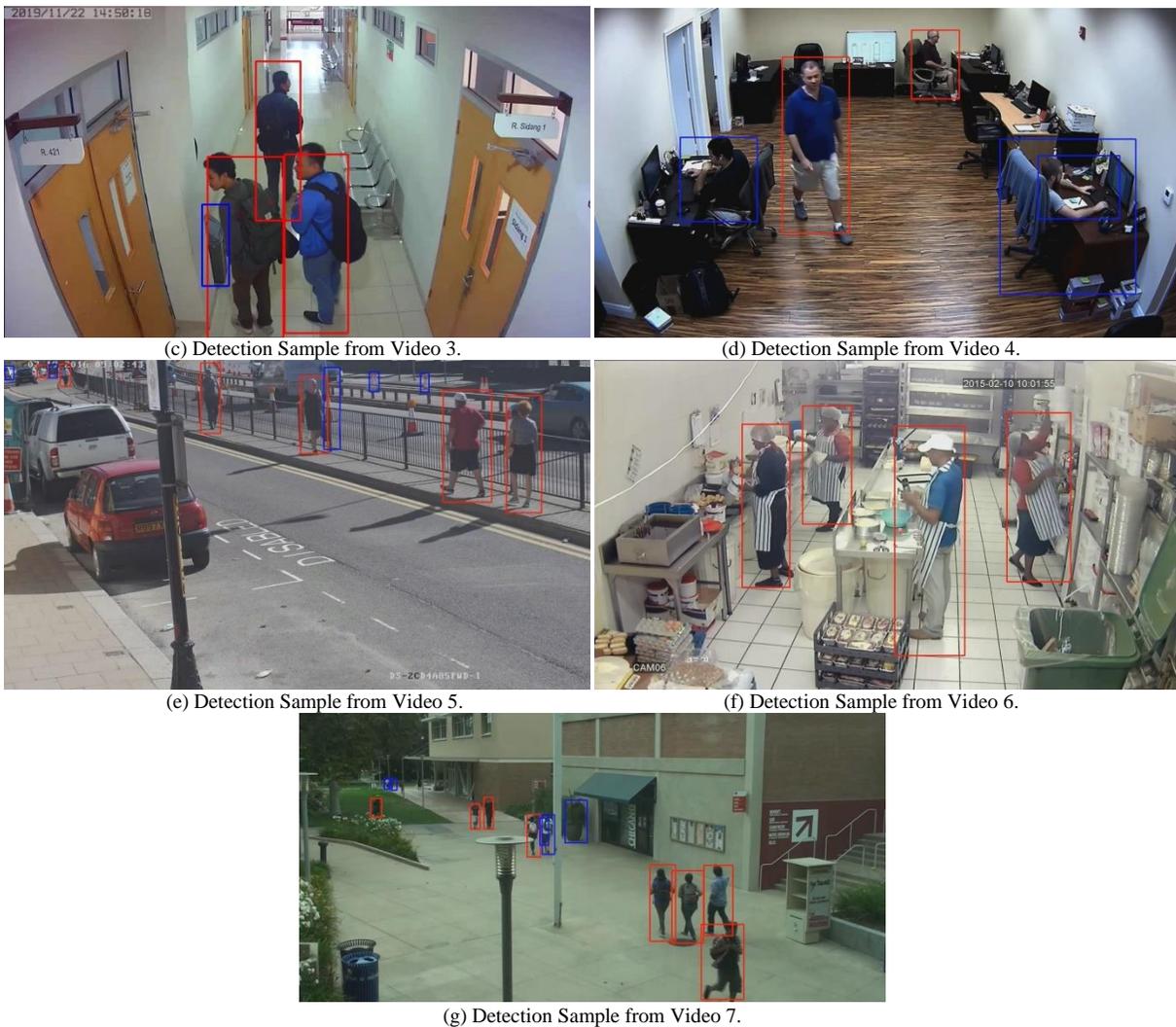


Fig. 6. Detected Sample for Video 1 until Video 7 with various conditions.

#### IV. CONCLUSION

The use of deep learning in human detection provides fairly good accuracy. However, this result is still influenced by selecting the threshold for the confidence value in the decision stage. The use of a static threshold is still not optimal in detecting objects that are far from the camera. This paper has succeeded in proposing the use of a dynamic threshold which is proven to provide a fairly good increase in f-measure, which is around 11% compared to the use of YOLO without a dynamic threshold. It should be noted that the use of dynamic thresholding can be used not only in YOLO but also in other deep-learning architectures. Even so, the dynamic threshold is still possible to be improved by considering the vanishing point in the image or super-resolution image [20].

#### V. ACKNOWLEDGMENT

This research was supported by 2021 Penelitian Dasar Unggulan Perguruan Tinggi-PDUPT (*College Excellence Basic Research*), funded by the Ministry of Education, Culture, Research and Technology, the Republic of Indonesia with

Grant Number 6/E1/KP.PTNBH/2021 and 1691/UN1/DITLIT/DIT-LIT/PT/2021.

#### REFERENCES

- [1] Wahyono, A Filonenko, KH Jo, "Unattended Object Identification for Intelligent Surveillance Systems Using Sequence of Dual Background Difference", *IEEE Transactions on Industrial Informatics* vol. 12, no. 6, 2247-2255, 2016, doi: 10.1109/TII.2016.2605582.
- [2] M. P. Kharisma and Wahyono, "A Novel Method for Handling Partial Occlusion on Person Re-Identification Using Partial Siamese Network", *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 7, pp. 313-321, 2021, doi: 10.14569/IJACSA.2021.0120735.
- [3] E.U. Haq, H. Jianjun, K. Li, and H.U Haq, "Human detection and tracking with deep convolutional neural networks under the constrained of noise and occluded scenes", *Multimedia Tools and Applications*, vol. 79, pp. 30685-30708, 2020, doi: 10.1007/s11042-020-09579-x.
- [4] M. Padmashini, R. Manjusha, L. Parameswaran, "Vision Based Algorithm for People Counting Using Deep Learning", *International Journal of Engineering and Technology*, vol. 7, no. 3, 2018, doi: 10.14419/ijet.v7i3.6.14942.
- [5] N. A. Simanjuntak, J. Hendarto, and Wahyono, "The Effect of Image Preprocessing Techniques on Convolutional Neural Network-Based Human Action Recognition", *Journal of Theoretical and Applied Information Technology*, vol. 98, no. 16, pp. 3364-3374, 2020.

- [6] N. Dalal, B. Triggs, "Histograms of oriented gradients for human detection", 2005 IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR'05), 20-25 Juni 2015, doi: 10.1109/CVPR.2005.177.
- [7] X. Wang, T.X. Han, S. Yan, "An HOG-LBP human detector with partial occlusion handling", 2009 IEEE 12th International Conference on Computer Vision, doi: 10.1109/ICCV.2009.5459207.
- [8] Y. Pang, Y. Yuan, X. Li, and J. Pan, "Efficient HOG human detection", *Signal Processing*, vol. 91, no. 4, April 2011, pp. 773-781, doi: 10.1016/j.sigpro.2010.08.010.
- [9] H. Skibbe, M. Reiser, and H. Burkhardt, "SHOG - Spherical HOG Descriptors for Rotation Invariant 3D Object Detection", Mester R., Felsberg M. (eds) *Pattern Recognition. DAGM 2011. Lecture Notes in Computer Science*, Springer, Berlin, Heidelberg, vol 6835, pp. 142-151, 2011, doi: 10.1007/978-3-642-23123-0\_15.
- [10] K Liu, H Skibbe, T Schmidt, T Blein, K Palme, T Brox, O Ronneberger, "Rotation-invariant HOG descriptors using Fourier analysis in polar and spherical coordinates", *International Journal of Computer Vision* vol. 106, no. 3, pp. 342-364, 2014.
- [11] E. Martinson, V. Yalla, "Real-time human detection for robots using CNN with a feature-based layered pre-filter", 2016 25th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN), 26-31 Aug. 2016, doi:10.1109/ROMAN.2016.7745248.
- [12] Y. Kim, T. Moon, "Human Detection and Activity Classification Based on Micro-Doppler Signatures Using Deep Convolutional Neural Networks", *IEEE Geoscience and Remote Sensing Letters*, vol. 13, no. 1, pp. 8-12, doi: 10.1109/LGRS.2015.2491329.
- [13] J. Redmon, S. Divvala, R. Girshick, A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection", *Conference on Computer Vision and Pattern Recognition*, 27-30 June 2016, doi: 10.1109/CVPR.2016.91.
- [14] A. Kuznetsova, et al., "The Open Images Dataset V4: Unified Image Classification, Object Detection, and Visual Relationship Detection at Scale", *International Journal of Computer Vision* vol. 128, pp.1956-1981, 2020, 10.1007/s11263-020-01316-z.
- [15] H. Rezaatofghi, et al., "Generalized Intersection over Union: A Metric and A Loss for Bounding Box Regression", 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), doi: 10.1109/CVPR.2019.00075.
- [16] C. Goutte, E. Gaussier, Probabilistic Interpretation of Precision, Recall and F-Score, with Implication for Evaluation. In: Losada D.E., Fernández-Luna J.M. (eds) *Advances in Information Retrieval. ECIR 2005. Lecture Notes in Computer Science*, vol 3408. Springer, Berlin, Heidelberg. [https://doi.org/10.1007/978-3-540-31865-1\\_25](https://doi.org/10.1007/978-3-540-31865-1_25).
- [17] J. Kim, "Efficient Vanishing Point Detection for Driving Assistance Based on Visual Saliency Map and Image Segmentation from a Vehicle Black-Box Camera", *Symmetry*, vol. 11, no. 12, pp.1492, 2019; doi: 10.3390/sym11121492.
- [18] A. Tai, J. Kittler, M. Petrou, and T. Winder, Vanishing point detection, *Image and Vision Computing*, vol. 11, no. 4, May 1993, pp.240-245, doi: 10.1016/0262-8856(93)90042-F.
- [19] S.-J. Park, H. Son, S.Cho, K.-S. Hong, and S. Lee, "SRFeat: Single Image Super-Resolution with Feature Discrimination", *The 2018 European Conference on Computer Vision*, doi: 10.1007/978-3-030-01270-0\_27.
- [20] Z. Wang, J. Chen, and S.C.H. Hoi, Deep Learning for Image Super-Resolution: A Survey, *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 43, pp. 3365-3387, Oct 2021, doi: 10.1109/TPAMI.2020.2982166.

# Forecast Breast Cancer Cells from Microscopic Biopsy Images using Big Transfer (BiT): A Deep Learning Approach

Md. Ashiqul Islam<sup>1,\*,#</sup>, Dhonita Tripura<sup>2,#</sup>, Mithun Dutta<sup>3</sup>, Md. Nymur Rahman Shuvo<sup>4</sup>, Wasik Ahmmed Fahim<sup>5</sup>  
Puza Rani Sarkar<sup>6</sup>, Tania Khatun<sup>7</sup>

Dept. of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh<sup>1, 4, 5, 6, 7</sup>

Dept. of Computer Science and Engineering, Rangamati Science and Technology University, Rangamati, Bangladesh<sup>2, 3</sup>

**Abstract**—Now-a-days, breast cancer is the most crucial problem amongst men and women. A massive number of people are invaded with breast cancer all over the world. An early diagnosis can help to save lives with proper treatment. Recently, computer-aided diagnosis is becoming more popular in medical science as well as in cancer cell identification. Deep learning models achieve excessive attention because of their performance in identifying cancer cells. Mammography is a significant creation for detecting breast cancer. However, due to its complex structure, it is challenging for doctors to identify. This study provides a convolutional neural network (CNN) approach to detecting cancer cells early. Dividing benign and malignant mammography images can significantly improve detection and accuracy levels. The BreakHis 400X dataset is collected from Kaggle and DenseNet-201, NasNet-Large, Inception ResNet-V3, Big Transfer (M-r101x1x1); these architectures show impressive performance. Among them, M-r101x1x1 provides the highest accuracy of 90%. The main priority for this research work is to classify breast cancer with the highest accuracy with selected neural networks. This study can improve the systematic way of early-stage breast cancer detection and help physicians' decision-making.

**Keywords**—Convolutional neural network (CNN); breast cancer; Big Transfer (BiT); densenet-201; NasNet-Large; Inception-Resnet-v3; mammography

## I. INTRODUCTION

Breast cancer is the second crucial illness worldwide [1]. In 184 significant countries, breast cancer is most common in 140 (70%) countries and a frequent cause of cancer mortality in 101 (55%) countries. Compared to other diseases, the ratio of breast cancer in women is higher in more developed countries and increases rapidly. The swift advancement of new technology is helping the doctor to identify the breast cancer cells in the inflammation stage with the help of Artificial Intelligence. Deep learning models aided in the prognosis of cancer cells and took the necessary steps.

Almost every woman is fearful if they feel something abnormal in their breasts. Moreover, they become much seared when they lump their breast [2]. However, most of them are not aware of the thing that all lump is not cancer. Furthermore, there is a thing if a women lumps in her breast she cannot even ignore this. Because according to DRHC (STYLE YOUR HEALTH), one out of four women has a complaint about their

breast at one time, and one-quarter of those patients who complain about their breast has cancer. It is considered one of the most severe and petrified diseases in women.

There are many issues affecting breast cancer. A woman can be affected by breast cancer if she gets it from an inherited genetic mutation. The main risk factor for breast cancer is being women and getting older. According to the CDC (Centers for Disease Control and Prevention), most breast cancer patients are found in a woman whose age is 50 years or more than 50 years [3]. These factors cause breast cancer, but they also have other factors that can because breast cancer. Reproducing history is another serious risk factor. In this factor, a woman who has menstrual periods before age 12 and menopause after age 55. This risk factor raises the risk of getting breast cancer. Some other factors like having dense breasts, previous treatment using radiation therapy, women who took the drug diethylstilbestrol (DES) can cause breast cancer.

Breast cancer disease has two advanced primary detections: early detection and screening [4]. Detecting early age mammography is the best technique for doctors. For being a most sensitive technique, a significant fraction of patients are referred for biopsy. As a reason, mammography findings do not have a fatality. However, a specific biopsy is an expensive, presumptuous, emotionally disturbing procedure for women.

At present, researchers are mainly working on deep learning, which performs well in image processing. Out of all deep learning, artificial neural network is the most popular, whereas Convolutional neural network is an extended version of it [5]. CNN is a robust algorithm that can extract features from raw input. CNN performs better than any other in image segmentation and achieves better accuracy.

Cancer tumors generally happen when the cells of breast ducts are overgrown from normal cells. A study shows that when diagnosing breast cancer, microscopic images are ubiquitous. Breast tissue can provide important microscopic level images to the pathologist for access. From the analysis, a pathologist can identify the tissue as normal tissue, benign or malignant tissue. If a patient has a benign tumor, cells form a lump and grow abnormally, but it does not spread to other body parts [6].

\*Corresponding author.

# Both authors contributed equally.

On the other hand, an untreated malignant tumor can spear any part of the body. Here, it is crucial to identify types of tumors from the beginning. It can easily save a women's life as well as the precious time of the doctors.

This decade, machine learning algorithms have been proposed for cancer diagnosis from microscopic biopsy images [14]. Neural network algorithm-based intelligent systems are proposed to be a part of the systematic diagnosis process. Artificial intelligence (AI) can impact the ratio of early-stage cancer cell identification with its immense power and growing improvements.

## II. LITERATURE REVIEW

Cancer is currently a dire thread for women, especially for elders. Breast cancer is the second most cancerous disease in the world right now. As a result, many works have been done on breast cancer. Deep learning plays an essential role in medical science. With the help of deep learning algorithms, people can predict different diseases from very early stages, significantly reducing the suffering of patients and doctors.

Yadavendra discussed the detection of benign and malignant tumors in the breast using machine learning and deep learning algorithms [3]. They used almost 2lakhs color patches sized 50×50. For the library, the author implemented sci-kit, Keras, and tensor flow with CNN based classifier. For training, testing and validation, sigmoid activation provided output in malignant and benign classes. CNN-based classifier outperformed all other machine learning algorithms.

Preprocessing is very important for removing noises, artifacts, and muscle regions as they increase the probability of false-positive values. As a result, Luqman Ahmed proposed a method of fine-tuning and preprocessing to decrease the probability of false-positive rates [4]. The datasets were collected from mammographic image analysis society digital mammogram database (MIAS) and Curated Breast Imaging (Digital Database for Screening Mammography). The author said that for handling big data vast amount of memory resources is required; here, the author used a method of converting data in small patches for batch training. ResNet is 152 layer CNN. The limitation of this method is that the cancerous region is irregular in shape and border, affecting calculation and resulting in a drop in precision. Authors [7] apply machine learning-based classification to determine the risk factor and prognosis of the CKD disease.

ZHIWEN HUANG said a hybrid neural network is better than other CNN classifiers in accuracy, sensitivity, specificity [8]. The author here presents a hybrid model based on DenseNet and PCANet. For learning about the dataset, he used a kernel of modified PCANet. However, the DenseNet is used for high-level image classification and constructing dense blocks or transition blocks. The method uses the same number of feature map outputs in transition block input. The global pooling technique was implemented for blocking a large number of weights in the network.

Data augmentation increases the image dataset ten times with original quality with random geometric image transformations, flipping, rotating, scaling, and shifting. The

proposed models by Li-Qiang Zhou were trained with Keras 2.2.0 and Tensor Flow [2] and the weight of the pre-trained model on ImageNet. Feature visualization methods can increase the predictive ability of deep learning networks. The author also shows that his model performs better than the radiologist's inaccuracy.

Deep Convolutional Neural Network is a robust deep learning algorithm [9]. It is pretty used in breast cancer segmentation and detection. Author Md Zahangir Alom compared the existing algorithms concerning image, patch, image-level, and patient-level classification. For the implementation, he used Keras and Tensorflow frameworks. Here, the author mentioned the eight types of breast cancer with image level and patient-level performance classification. The image-wise and patch-wise classification was discussed for better understanding. Researchers [10] evaluated the papaya disease classification using a Convolutional Neural Network.

Convolutional Neural Network outperformed any other algorithms in image recognition [6]. The author gives an example of ResNet outperforming human participants with an error rate of 3.6%. Different dataset types were used in the proposed model, and it seemed like the performance was varying with different datasets. The model successfully predicts 12 types of skin tumors. For improving the performance, it is crucial to add standardized diagnostics images.

Vikas Chaurasia described the 10-fold cross-validation for measuring the performance of the models [11]. The author used prediction models for malignant and benign parameters, represented by "1" for malignant and "0" for benign.

The author presents a framework of unsupervised feature learning by integrating principal components [12]. DEJUN ZHANG aimed to merge feature selection and feature extraction in a deep learning algorithm. For tackling overfitting, he implemented some scarcity penalties in hidden layers. Elu was introduced for speeding up the training process in the deep neural network.

The study [13] proposed a deep learning model with Convolutional layers for breast cancer classification to extract visual features. First, the author implies a preprocessing method to transform images into common space or variances for improving detection performance. They discussed the effectiveness of data augmentation for increasing training data. Also, multiple deep Convolutional networks can improve the performance significantly with a tensor flow machine learning system. Extracted features were used to boost the framework.

The paper proposed an approach of DenseNet deep learning based on CNN for multiclass classification [14]. DenseNet uses a transition layer to reduce the size of the dataset. The author applied dropout and batch operation for optimization—transfer learning, fine-tuning pre-trained CNN models from natural to medical images. The advantage of using DenseNet is feature concatenation that helps to learn features without compression from any stages. Furthermore, the DenseNet model shows that the deep learning model can obtain good performance from natural images.

Author Angel Cruz-Roa said the main objective of their proposed work is to identify tumors from digital images with deep learning [15]. They show the experimental result of the method that can detect breast cancer regions. Five cohorts were used to train, test and validation. With the help of the dice coefficient, the performed evaluation shows positive predictive value, negative predictive value, true positive rate, true negative rate, and false positive and false negative rate all over the test slides.

The workflow of computer vision-based breast cancer cell detection primarily focused on the supervised learning-based system rather than the semi-supervised or unsupervised system. For the most part, the authors depend on hybrid neural network architectures like ResNet, DenseNet, and Inception. During the neural network-based models training and validation of the trained models, many different sources of public datasets took part as raw input data. Recent researches contain pre-trained weights from Keras deep learning models. Using pre-trained weights initiated by the ImageNet dataset has validated the models [26] [31]. To enrich the good prediction ability of models, researchers mainly focused on data preprocessing stages. Data augmentation has taken part for a smaller dataset, and a different cross-validation process follows through some research.

### III. PROPOSED SYSTEM

This study presents quantitative research on deep learning models based on Convolutional Neural Network (CNN). CNN is applying in the breast mammography dataset to prognosis the breast cancer disease in the human breast cell [16][17]. In this study, four deep learning algorithms (NasNet-Large, Inception ResNet-V3, DenseNet-201, and Big Transfer) are applied to achieve better accuracy from the prediction model [18][9][19]. In the beginning, data are acquisition and preprocessed with different parameters to split the dataset. Various preprocessing techniques such as zoom, rotation, rescaling, flip, shuffle are used to improve the data quality [20][18]. The preprocessed images go through the deep convolutional neural network. Convolutional blocks of the models extract the main features from the input images [21]. For training and testing the splits, the pre-trained model is customized with fully connected layers. The parameter of resizing is (224 x 224), (331 x 331), and the rescaling technique (0-1) is applied to split the data. In fine-tuning, selected convolutional layers are responsible for extracting feature extraction with fully connected layers [11]. This process changed the pre-trained model weights and evaluated the testing data for comparative analysis. Fig.1 visualizes the entire workflow of the proposed system.

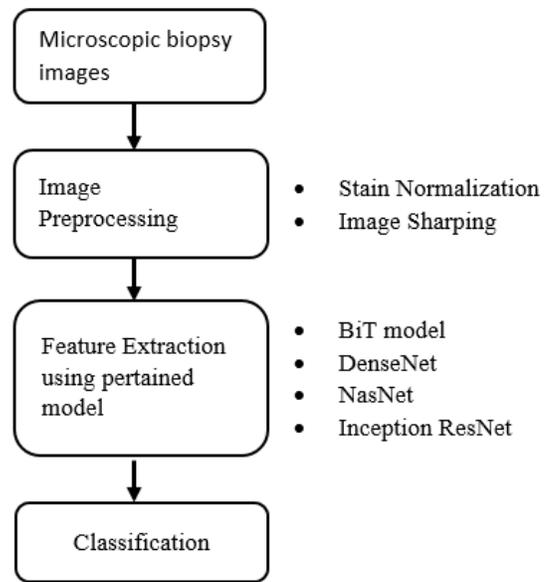


Fig. 1. Process Diagram of the Entire System.

### IV. DATASET DESCRIPTION

Benign and malignant breast cancer is microscopically imaged. Benign and malignant breast cancer is microscopically imaged. Table 1(I, II) provide general information about the dataset. The dataset is divided into two sections, Data for training and testing. In training data, benign and malignant directories contain 436 and 918 image data, respectively. On the other hand, test data is also divided into benign and malignant directories [22]. In testing, the benign directory has 111 files, and the malignant directory has 228 files.

TABLE I. (I): DATASET DESCRIPTION

Dataset features	Parameters
Total instance	1693
Total training data	1354
Total testing data	339
Number of classes	2

(II): DATASET DESCRIPTION

Breast Cancer classification	Number of Images	Number of Images Used for Train and Validation	Number of Images used for Test
Benign	547	436	111
Malignant	1146	918	228
<b>Total</b>	1693	1354	339

This breast cell microscopic biopsy patient's images were gathered from Kaggle [23]. Fig.2 visualize the microscopic images of a cluster of cells. The cluster of cells is called a tumor in medical science, and it is an abnormal growth of the cell. General tumors without invading the nearby area are categorized as benign, Fig.2 (a). A tumor with vast and uncontrollable speed is mentioned as malignant, as shown in Fig.2 (b).

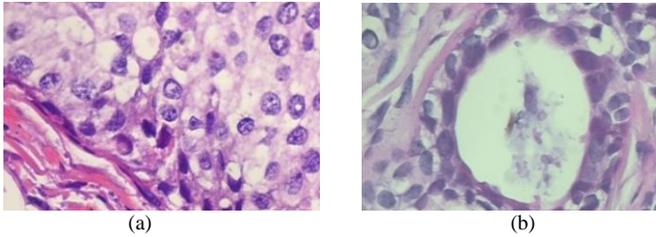


Fig. 2. Microscopic Biopsy Images of a Cluster of Cells from the Selected Dataset [23]. Noncancerous and Cancerous Tumors are Mentioned as Benign (a) and Malignant (b), Respectively.

### A. Data Preprocessing

The dataset contains a variety of image types. The dimensions are as follows: 1500x750, 1254x836, 1024x768, 800x533, 220x230, 100x100, and 61x159. Due to the different image sizes, classification becomes difficult without a fixed image size. As a result, a proposed method used the 200x200 shape as an input shape function. This dataset must contain RGB images. Stain normalization and sharpening the edges of image contents taken part.

## V. MODEL DESCRIPTION

### A. Big Transfer

A BiT, also known as Big Transfer, is a recipe for an image classification model used for pre-training on large supervised datasets [19]. This algorithm has excellent fine-tuning efficiency on the given task. It can provide fantabulous performance on different tasks. R101x1 architecture is implemented in this model; as a result, it can execute multi-label classification on an ImageNet-21k dataset which can contain 14 million images. The output can detect the existence and lack of multiple classes of objects. There are two features in Big Transfer, one is the fine-tuning, and the second one is the BiT collection. Fine-tuning refers to the exact adjustment of parameters in a model. BiT uses a recipe, aka BiT Hyper Rule, for fine-tuning the parameters. This fine-tuning protocol is applied on many down-streaming tasks. BiT collections are used for performing multi-label classification on legit ImageNet-21k datasets. For classifying, it needs an imagenet21k\_classification model. For up streaming pre-trained data scale is essential because it can transfer to tasks with few data points. Residual block showed in Fig. 3 used in M r-101 model with minor changes in the normalization process.

**Residual Block:** Generally, the residual block is a layer stack where the preceding output feeds to the block's deeper layer [24]. For addressing the degradation problem of a complex function, a simpler function should be a subset which is the main idea of the residual block. I consider an input as  $x$  and desired mapping from input as  $g(x)$  then the simpler

function will be  $f(x) = g(x) - x$ . On the other hand, optimization of residual can compromise the dreaded identity mapping in a deep network. When the identity mapping is optimal, the optimization will carry out the weights of residual function to zero.

### B. NasNet Large

NasNet search space is known as Neural Architecture Search, which is used to find convolutional architecture from a dataset. In this search space, a Recurrent Neural Network controller is used to sample different architectures of a child network. Fig. 4 shows the neural architecture generation and selection process of the NasNet model. The child network is trained on a validation set to achieve some accuracy. These accuracies update the controller so that it can generate improved architecture with time. Policy gradient updates the weights of the controller. There are two types of cells named Normal cell and Reduction cell. The average cell returns the feature map's exact dimension, and the Reduction cell returns the reduced feature map (reduced by height and width by factor two). All convolutional cells have two striding for reducing the height width. NasNet can be forced as a hierarchical structure for asserting a well-designed network. For finding optimal architecture:

$$J(\theta_c) = E_{p(a_{1:T}; \theta_c)}[R] \quad (1)$$

Where  $\theta_c$  controller RNN,  $a_{1:T}$  list of actions.

For updating  $\theta_c$  policy gradient method of REINFORCE rule is:

$$\nabla J(\theta_c) = \sum_{t=1}^T E_{P(a_{1:T}; \theta_c)} [\nabla \theta \log P(a_t[a_{(t-1):1}; \theta_c]) R] \quad (2)$$

Where R is non-differentiable.

To overcome unbiased estimation and for reducing variance here need baseline function:

$$\frac{1}{m} \sum_{k=1}^m \sum_{t=1}^T \nabla \theta \log P(a_t[a_{(t-1):1}; \theta_c]) (R_k - b) \quad (3)$$

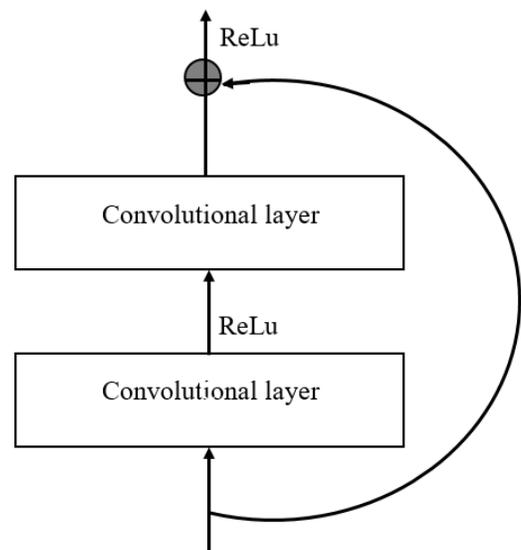


Fig. 3. Basic Residual Blocks of ResNet Architecture [27]. ResNet Architecture is at the Core of BiT Models.

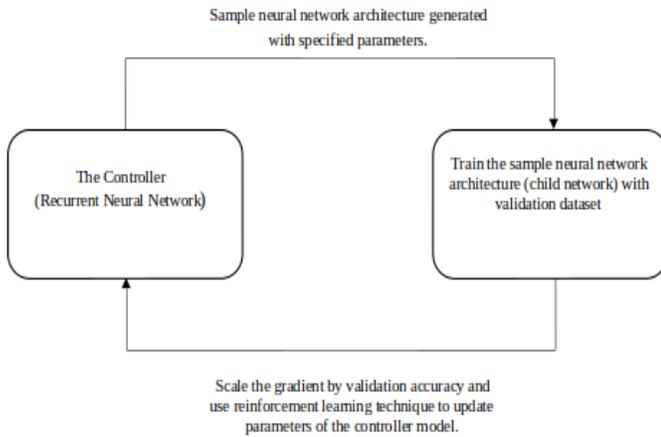


Fig. 4. NasNet Models Process Diagram [28]. The Controller Network is taken Part in Selecting the most efficient Neural Parameters for a Specific Dataset.

Here  $m$  is the number of various architectures,  $T$  is the number of hyper parameters. The validation accuracy of the  $k$ -th neural network after training a dataset is  $R_k$ . If  $b$  doesn't depend on current action then the function is unbiased gradient estimation.

**NasNet Controller Architecture:** On Neural Architecture Search, a controller is being used by us for creating architectural hyperparameters for neural networks [25]. The controller is mainly prepared as a recurrent neural network. Fig. 5 visualize the internal architecture of the NasNet controller. For predicting feed-forward neural networks with convolutional layers, the controller provides hyperparameters as tokens. The generating process of architecture is halted when the layer exceeds a particular value. For sampling convolutional network RNN anticipates filter height-width, stride height-width, and filter numbers for one or more layers. A Softmax classifier makes each prediction, and then the output is fed into the next step.

C. DenseNet-201

Considering CNN, DenseNet contains fewer perimeters than most conventional models [9]. A DenseNet architecture visualizes in Fig. 7. It contains sense built-in blocks with steam and transactional neural blocks. This architecture is not needed necessary to learn redundant feature maps. DenseNet can add a small set of new features because the layers it is narrow. To train intense networks, it has to face problems due to alluded flow of information and gradients. It can solve the problems by DenseNet. Cause each layer of this algorithm has direct access to gradients from the loss function.

Equations of DenseNet would be:

$$X_L = H_L(X_{L-1}) \tag{4}$$

For including skip connection ResNet extends the behavior by reformulating the equation:

$$X_L = H_L(X_{L-1}) + X_{L-1} \tag{5}$$

In this algorithm, the incoming feature maps don't sum up the output of the feature maps layer. So, the final equation is:

$$X_L = H_L([X_0, X_1, \dots, X_{L-1}]) \tag{6}$$

This thing makes the main difference between ResNet and DenseNet.

Using convolutional neural networks in a systematic flow for a specific task is known as blocks of CNN. Dense Block (showed in Fig. 6) is a benchmark model for specific feature extraction purposes. This module connects all matched feature maps (layers) with other available layers. For retraining from all feed forward quality each layer gets extra inputs from all foregoing and leaves them to subsequent layers. On DenseNet features are concatenated and the  $l^{th}$  layer has 1 input which consists of feature maps of previous convolutional blocks and its feature maps are left for  $L-l$  subsequent layers. For traditional dense connectivity, this layer implemented  $\frac{L(L+1)}{2}$  instead of doing  $L$ . The networks defined  $L$  as layers, and  $H_l(\cdot)$  is non-linear transformation,  $x_l$  is the output of the  $l^{th}$  layer.

The convolutional block is consists of two or more convolutional layers with essential activation functions. Fig. shows that every convolutional layer receives direct input from preceding layers. The transition layer mainly does the work of pooling and convolution, which is used in batch normalization with 1x1 convolution and 2x2 pooling. Input feature maps first go to batch normalization and standardize input data. After completing each convolution, the number of channels shows the growth rate of a block by remaining the same as before. After mapping out the feature, the output sends to all of the layer blocks. For extracting features from input data, activation function and convolutional layer are used. VGG-16 networks hold 16 convolutional layers with the same kernel.

D. Inception ResNet-V3

Inception networks interrupt the same filter size concept in a block [16][30]. A single built-in block searches for a different convolutional layer with different shapes shown in Fig. 8. Multiple layers subsist in parallel in a block and concatenate each sequence of layers. 1x1 convolutional layer at the beginning reduces the dimensionality of a sequence. Multilevel feature extraction is expedited by concatenating various filter-sized sequences. Res-Net passes the output of a convolutional layer typically.

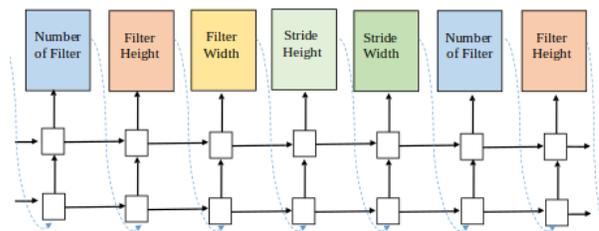


Fig. 5. NasNet Model Controller Architecture [28] based on Recurrent Neural Network (RNN).

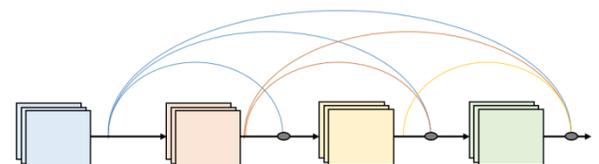


Fig. 6. 4-Layer Dense Block with Growth Rate (Number of Channel in Layer) of 3.

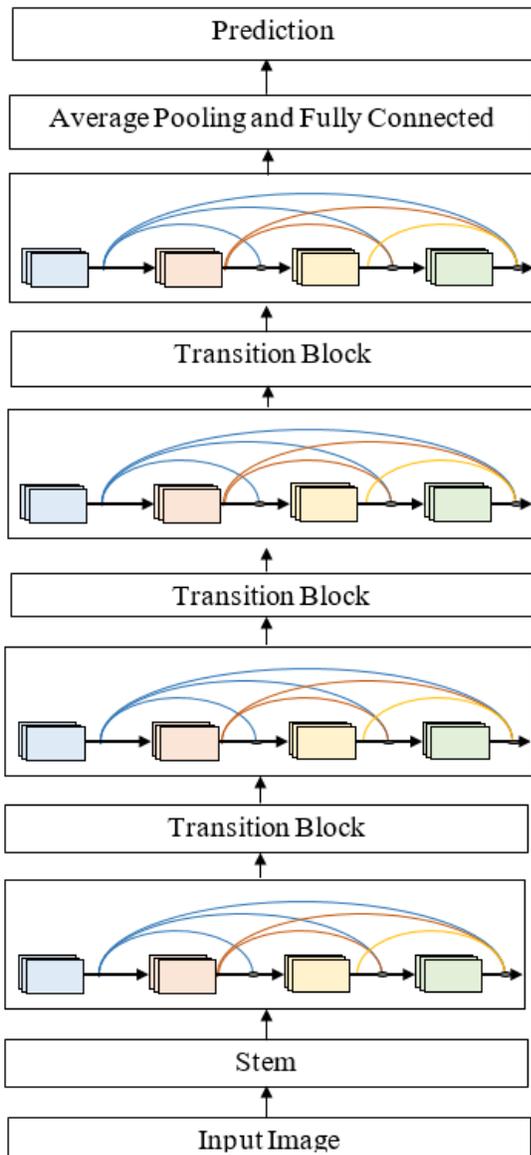


Fig. 7. DenseNet201 Model Architecture [29].

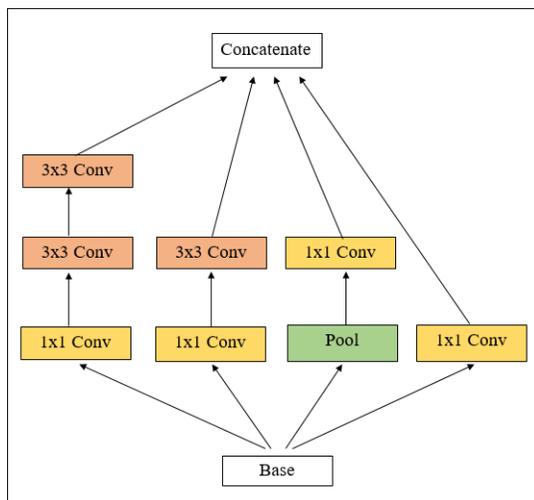


Fig. 8. Basic Inception Built-in Block [30].

## VI. SYSTEM OPERATION

Much work has been done on breast cancer using different types of machine learning and deep learning algorithms. This paper made a complete guideline to classify breast cancer-affected patients by following a flowchart given in Fig. 1. In this flowchart, after acquiring affected people's images, it needs to process those images. In this step, the machine takes the images from the dataset as input. In processing, the system split a dataset into two parts train data and test data. The system uses 80% of data for training and 20% of data for testing. This train data has to go through different processing techniques (rotates, room, flip and shuffle). This process improves the data quality by enhancing image features essential for the next training part of the process [22]. On the other side, in training data, the system applied resizing (224×224) and rescaling (0-1). Only the standard processes are applied between training and testing data.

Then these processed images have to go through the deep convolutional neural network. It is a feed-forward artificial neural network and has taken the role of feature extraction [12]. It is a fully connected layer containing multiple nodes, and every node is connected to the subsequent nodes with the next layer. Pre-trained weights can be changed by training procedure [15]. For comparative analysis, trained models are evaluated by testing data split.

## VII. RESULT ANALYSIS

This analysis was performed on four different types of deep learning algorithms. Table 2 contains the performance summary of selected models. The selected architecture's performance was promising. This study includes NasNet-Large, DenseNet-201, Inception-ResNet-V3, and Big Transfer, with a total of 1693 instances in the dataset. From here, 1354 were used in training and 339 instances in testing. The dataset contains two classes: Malignant and Benign. Out of 1693 selected datasets has 547 images in Benign and 1146 images in Malignant. Again 434 Benign images were used in training, and 111 were in testing.

On the other hand, 918 malignant images were used in the training phase and 228 in the testing phase. After analyzing the training and testing phase, Big Transfer achieved the highest accuracy of 90%, whereas DenseNet-201 has 89%, Inception-ResNet-V3 has 86%, and NasNet Large 81%. One of the great features of this study is that the applied algorithm will take the highest accuracy from 200 epochs intelligently, whereas other typical algorithms take values from predefined epochs [17] (Fig. 9). Table 3(I, II, III, IV) contains the performance measurement of the models with different classes of data. Here support is 111 for Benign and 228 for Malignant for each algorithm.

TABLE II. PERFORMANCES OF SELECTED MODELS

Models	Accuracy
NasNet Large	0.8183
DenseNet-201	0.8917
Inception-ResNet-V3	0.8642
Big Transfer	0.9000

NasNet Large: For Benign class NasNet has 0.31 precision with 0.29 Recall, 0.30 F1 Score. For Malignant class algorithm has 0.67 precision with 0.70 Recall, 0.68 F1 Score.

TABLE III (I): THE PERFORMANCE SCORE FOR EACH CLASS OF NASNET LARGE MODEL

Classes	Precision	Recall	F1 Score	Support
Benign	0.31	0.29	0.30	111
Malignant	0.67	0.70	0.68	228

DenseNet-201: For Benign class DenseNet has 0.28 precision, 0.27 Recall, 0.27 F1 Score and for Malignant class the precision is 0.66, Recall & F1 Score 0.67.

TABLE III (II): THE PERFORMANCE SCORE FOR EACH CLASS OF DENSENET-201 MODEL

Classes	Precision	Recall	F1 Score	Support
Benign	0.28	0.27	0.27	111
Malignant	0.66	0.67	0.67	230

Big Transfer: For the Benign class Big Transfer has 0.29 precision with 0.27 Recall, 0.28 F1 Score. For the Malignant class, the algorithm has 0.66 precision with 0.68 Recall, 0.67 F1 Score.

TABLE III (III): THE PERFORMANCE SCORE FOR EACH CLASS OF THE BIG TRANSFER MODEL

Classes	Precision	Recall	F1 Score	Support
Benign	0.29	0.27	0.28	111
Malignant	0.66	0.68	0.67	228

Inception-ResNet-V3: For Benign class Inception-ResNet-V3 has 0.31 precision, 0.31 Recall, 0.31 F1 Score and for Malignant class the precision, Recall & F1 Score is 0.67.

TABLE III (IV): THE PERFORMANCE SCORE FOR EACH CLASS OF THE INCEPTION-RESNET-V3 MODEL

Classes	Precision	Recall	F1 Score	Support
Benign	0.31	0.31	0.31	111
Malignant	0.67	0.67	0.67	228

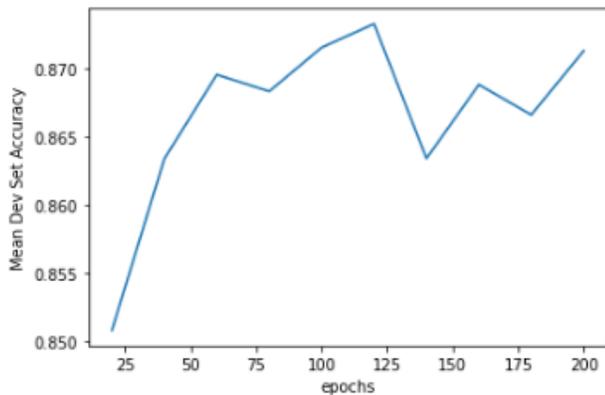


Fig. 9. Best Epochs Selection between 20 and 200.

Training and validation are a significant part of deep learning. If the algorithm is well trained and validated, it can perform better in higher accuracy output. Fig. 10 shows that the dataset was well trained. The training accuracy was almost 0.98 with a standard deviation of 0.0258021, and the highest epoch generated was 120.

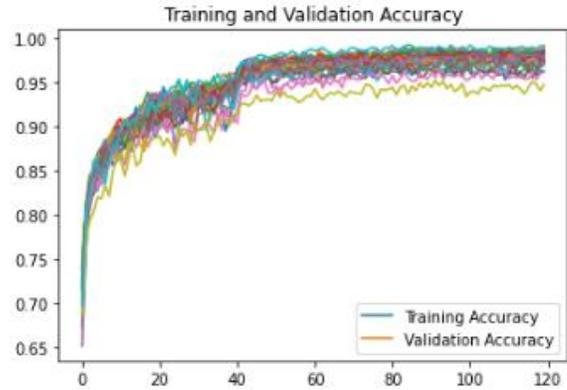


Fig. 10. Training & Validation Accuracy.

Fig. 11 shows that the number of accuracies repeated while performing accuracy with algorithms. Here 0.90 and 0.89 were achieved once. 0.86 accuracy was achieved two times, accuracy between 0.86 and 0.87 was achieved three times. 0.87 And 0.88 were achieved six times. The highest repeated number is 8. It was between 0.87 and 0.88.

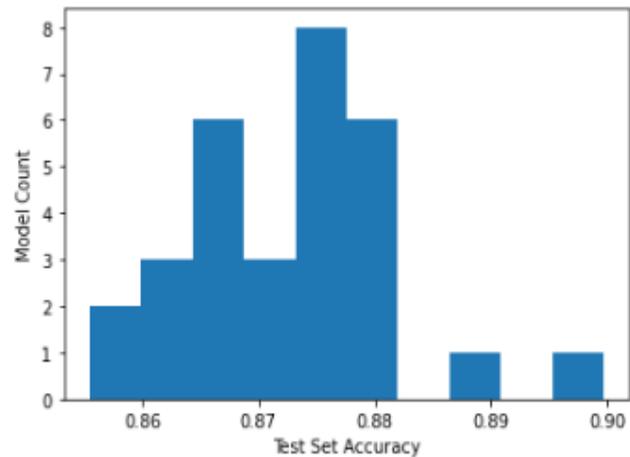


Fig. 11. Multiple Test Accuracy Bar Chart.

Dropout is the method of removing random neurons from the network while training. As a result, the activity of the downstream neurons is temporarily removed from the forward pass, and weight changes do not apply to the backward pass [14]. L2 rate means that it will reduce overfitting with the small size of weight and biases. After analyzing Fig. 12, the best L2 rate was 1.47, and the best dropout was 0.45.

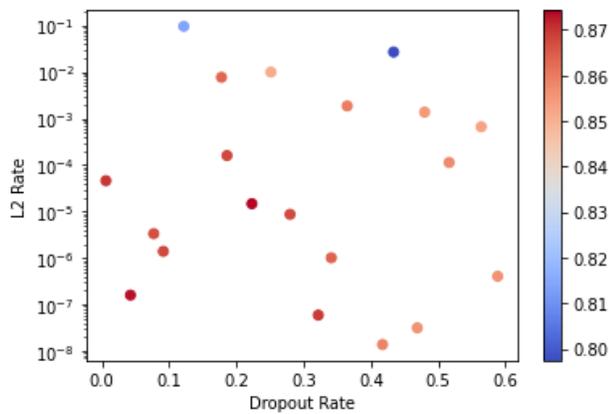


Fig. 12. Networks Dropout Rate Selection.

### VIII. DISCUSSION

Breast cancer is very deadly for women, especially older. Scientists are working very hard to find easy and practical solutions. With the help of modern technology, people are different types of deep learning or machine learning algorithms in medical science. This technology dramatically improves medical treatments as it is very effective, low on cost, and saves much time for doctors and patients.

This paper aims to identify breast cancer from images by using four deep learning algorithms. Those algorithms are NasNet Large, DenseNet-201, Inception-ResNet-V3, and Big Transfer. All of the experimented algorithms provide promising results. The dataset was collected from Kaggle. We worked with total 1693 instance divided into two classes named Malignant and Benign, from here 1354 was used in training, and 339 instances were used in testing. For all the algorithms, the total support instance was 339.

NasNet-Large is a convolutional neural network with more than 1 million images trained from the ImageNet database [28]. Input image size was 331\*331. This analysis shows it obtained 81% of accuracy, which is the lowest out of 4 algorithms.

DenseNet-201[29] is a convolutional neural network with 201 layers. It can add a pre-trained network trained on the ImageNet database. The input image size was 224\*224. This algorithm achieved 89% of accuracy, which is the 2nd highest.

Inception-ResNet-V3 is the descendant from the Inception family [30]. It has some improvements in Label Smoothing, 7\*7 factorized convolutions, and the use of an auxiliary classifier for propagating label information. Here input size was 299\*299. The algorithm provides the third-highest accuracy of 86%.

Significant Transfer is one of the newest in deep learning algorithms [19]. Although it is new, the performance of this algorithm is awe-inspiring. On current analysis, Big Transfer owned first place with 90% accuracy.

### IX. CONCLUSION

This study worked with deep learning methods to predict breast cancer. The proposed method goes through image data selection and preprocessing the data for focusing on the prime

features. DenseNet, NasNet Large, Inception ResNet (v3), m-r101x1x1 (BiT) neural architecture are selected for this study. The architecture selection process was based on their architectural variety and their efficiency in the computer vision sector. The selected public microscopic biopsy dataset is split into two parts for training and testing purposes, where 20% of the data is reserved for evaluating the trained neural network models. This study use pre-trained weights for the benchmark architectures from Keras. This study applies necessary modification in the tail order layers of benchmark models, customizes the neural models for forecasting breast cancer from histological images. Thirty evolution cases occurred for each trained model to finalize the reliable performance rate. The best accuracy of 90% was found once in the thirty evaluations from BiT based m-r101x1x1 architecture which contains 101 layers of neural network. The average accuracy of the Bit based model was found at 87.51%, which is higher than the average accuracy of comparative models. This inaugural work exhibit the probability and promise of working with large data set with more accuracy and larger multicenter studies for ulterior appraise the methods and findings.

### REFERENCES

- [1] M. H. Yap et al., "Breast ultrasound region of interest detection and lesion localisation," *Artif. Intell. Med.*, vol. 107, p. 101880, 2020.
- [2] L.-Q. Zhou et al., "Lymph node metastasis prediction from primary breast cancer US images using deep learning," *Radiology*, vol. 294, no. 1, pp. 19–28, 2020.
- [3] S. Chand, "A comparative study of breast cancer tumour classification by classical machine learning methods and deep learning method," *Mach. Vis. Appl.*, vol. 31, no. 6, pp. 1–10, 2020.
- [4] L. Ahmed, M. M. Iqbal, H. Aldabbas, S. Khalid, Y. Saleem, and S. Saeed, "Images data practices for semantic segmentation of breast cancer using deep neural network," *J. Ambient Intell. Humaniz. Comput.*, pp. 1–17, 2020.
- [5] K. N. Ramanto and A. A. Parikesit, "The usage of deep learning algorithm in medical diagnostic of breast cancer," *Malaysian J. Fundam Appl Sci*, vol. 15, no. 2, pp. 274–281, 2019.
- [6] V. Chaurasia, S. Pal, and B. B. Tiwari, "Prediction of benign and malignant breast cancer using data mining techniques," *J. Algorithm. Comput. Technol.*, vol. 12, no. 2, pp. 119–126, 2018.
- [7] M. A. Islam, S. Akter, M. S. Hossen, S. A. Keya, S. A. Tisha, and S. Hossain, "Risk Factor Prediction of Chronic Kidney Disease based on Machine Learning Algorithms," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 2020, pp. 952–957.
- [8] Z. Huang, X. Zhu, M. Ding, and X. Zhang, "Medical image classification using a light-weighted hybrid neural network based on PCANet and DenseNet," *IEEE Access*, vol. 8, pp. 24697–24712, 2020.
- [9] J. Hai et al., "Fully convolutional densenet with multiscale context for automated breast tumour segmentation," *J. Healthc. Eng.*, vol. 2019, 2019.
- [10] M. S. Hossen, I. Haque, M. S. Islam, M. T. Ahmed, M. J. Nime, and M. A. Islam, "Deep Learning based Classification of Papaya Disease Recognition," in *2020 3rd International Conference on Intelligent Sustainable Systems (ICISS)*, 2020, pp. 945–951.
- [11] D. Zhang, L. Zou, X. Zhou, and F. He, "Integrating feature selection and feature extraction methods with deep learning to predict clinical outcome of breast cancer," *IEEE Access*, vol. 6, pp. 28936–28944, 2018.
- [12] F. M. Alakwaa, K. Chaudhary, and L. X. Garmire, "Deep learning accurately predicts estrogen receptor status in breast cancer metabolomics data," *J. Proteome Res.*, vol. 17, no. 1, pp. 337–347, 2018.
- [13] M. Nawaz, A. A. Sewissy, and T. H. A. Soliman, "Multi-class breast cancer classification using deep learning convolutional neural network," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 6, pp. 316–332, 2018.

- [14] R. Platania, S. Shams, S. Yang, J. Zhang, K. Lee, and S.-J. Park, "Automated breast cancer diagnosis using deep learning and region of interest detection (bc-droid)," in Proceedings of the 8th ACM international conference on bioinformatics, computational biology, and health informatics, 2017, pp. 536–543.
- [15] A. Cruz-Roa et al., "Accurate and reproducible invasive breast cancer detection in whole-slide images: A Deep Learning approach for quantifying tumour extent," *Sci. Rep.*, vol. 7, no. 1, pp. 1–14, 2017.
- [16] L. Tsochatzidis, L. Costaridou, and I. Pratikakis, "Deep learning for breast cancer diagnosis from mammograms—a comparative study," *J. Imaging*, vol. 5, no. 3, p. 37, 2019.
- [17] S. Ray, A. AlGhamdi, K. Alshouli, and D. P. Agrawal, "Selecting Features for Breast Cancer Analysis and Prediction," in 2020 International Conference on Advances in Computing and Communication Engineering (ICACCE), 2020, pp. 1–6.
- [18] M. Z. Alom, C. Yakopcic, M. S. Nasrin, T. M. Taha, and V. K. Asari, "Breast cancer classification from histopathological images with inception recurrent residual convolutional neural network," *J. Digit. Imaging*, vol. 32, no. 4, pp. 605–617, 2019.
- [19] A. Kolesnikov et al., "Big transfer (bit): General visual representation learning," in Computer Vision—ECCV 2020: 16th European Conference, Glasgow, UK, August 23–28, 2020, Proceedings, Part V 16, 2020, pp. 491–507.
- [20] M. N. R. Shuvo, S. Akter, M. A. Islam, S. Hasan, M. Shamsojjaman, and T. Khatun, "Recognizing Human Emotions from Eyes and Surrounding Features: A Deep Learning Approach."
- [21] A. Islam, N. Rahman Shuvo, M. Shamsojjaman, S. Hasan, S. Hossain, and T. Khatun, "An Automated Convolutional Neural Network Based Approach for Paddy Leaf Disease Detection," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 1, pp. 280–288, 2021, doi: 10.14569/IJACSA.2021.0120134.
- [22] D. M. Vo, N.-Q. Nguyen, and S.-W. Lee, "Classification of breast cancer histology images using incremental boosting convolution networks," *Inf. Sci. (Ny)*, vol. 482, pp. 123–138, 2019.
- [23] F. A. Spanhol, L. S. Oliveira, C. Petitjean, and L. Heutte, "A dataset for breast cancer histopathological image classification," *Ieee Trans. Biomed. Eng.*, vol. 63, no. 7, pp. 1455–1462, 2015.
- [24] S. S. Han, M. S. Kim, W. Lim, G. H. Park, I. Park, and S. E. Chang, "Classification of the clinical images for benign and malignant cutaneous tumours using a deep learning algorithm," *J. Invest. Dermatol.*, vol. 138, no. 7, pp. 1529–1538, 2018.
- [25] M. Chung, J. Lee, M. Lee, J. Lee, and Y.-G. Shin, "Deeply self-supervised contour embedded neural network applied to liver segmentation," *Comput. Methods Programs Biomed.*, vol. 192, p. 105447, 2020.
- [26] A. Yala, C. Lehman, T. Schuster, T. Portnoi, and R. Barzilay, "A deep learning mammography-based model for improved breast cancer risk prediction," *Radiology*, vol. 292, no. 1, pp. 60–66, 2019.
- [27] K. He, X. Zhang, S. Ren and J. Sun, "Deep Residual Learning for Image Recognition," 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016, pp. 770–778, doi: 10.1109/CVPR.2016.90.
- [28] B. Zoph, V. Vasudevan, J. Shlens and Q. V. Le, "Learning Transferable Architectures for Scalable Image Recognition," 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2018, pp. 8697–8710, doi: 10.1109/CVPR.2018.00907.
- [29] G. Huang, Z. Liu, L. Van Der Maaten and K. Q. Weinberger, "Densely Connected Convolutional Networks," 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017, pp. 2261–2269, doi: 10.1109/CVPR.2017.243.
- [30] Szegedy, C., Ioffe, S., Vanhoucke, V., & Alemi, A. (2017). Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning. In Proceedings of the Thirty-First AAAI Conference on Artificial Intelligence (pp. 4278–4284). AAAI Press.
- [31] Tsochatzidis, L.; Costaridou, L.; Pratikakis, I. Deep Learning for Breast Cancer Diagnosis from Mammograms—A Comparative Study. *J. Imaging* 2019, 5, 37. <https://doi.org/10.3390/jimaging5030037>.

# Mobile Application with Augmented Reality to Improve Learning in Science and Technology

Miriam Gamboa-Ramos<sup>1</sup>, Ricardo Gómez-Noa<sup>2</sup>, Orlando Iparraguirre-Villanueva<sup>3</sup>  
Michael Cabanillas-Carbonell<sup>4</sup>, José Luis Herrera Salazar<sup>5</sup>

Facultad de Ingeniería y Arquitectura, Universidad Autónoma del Perú, Lima, Perú<sup>1, 2, 3</sup>  
Facultad de Ingeniería, Universidad Privada del Norte, Lima, Perú<sup>4</sup>  
Facultad de Ingeniería y Negocios, Universidad Norbert Wiener, Lima, Perú<sup>5</sup>

**Abstract**—Education has taken a big turn due to the current health situation, and as a result the use of technology has become a great ally of education, achieving important benefits. Augmented reality is being used by teachers and students especially in distance and/or face-to-face learning through didactic learning, self-instruction and the promotion of research. This article shows the development and influence of a mobile application with augmented reality that serves as a reinforcement for the learning of Science and Technology in students of sixth grade of Primary and first year of Secondary School. The Mobile D methodology is used during the development process of the application, the research design is Pre-Experimental since the Pre-Test and Post-Test tests are performed to a single group of students being the total of 30, obtaining as final result the increase in the level of interest of the students to 100%, in the level of understanding there was an improvement of 50% and the level of satisfaction is maintained in a range of 40% satisfaction and very satisfied of 60%, which implies that the application helps them to improve their learning.

**Keywords**—Augmented reality; learning; mobile application; Mobile D methodology

## I. INTRODUCTION

In this sense, the Program for International Student Assessment (PISA) of the Organización para la Cooperación y el Desarrollo (OCDE), which is carried out every 3 years, evaluates 15-year-old students in the areas of reading, mathematics and science, contributing to systematically assess the knowledge of young people [1].

According to OECD results [2], the 10 countries evaluated in Latin America are below average in Reading and Mathematics, with Peru being one of the countries that is showing small growth. In 2018, Peru participated voluntarily with 342 schools and a total of 8028 students (6086 of whom took the cognitive competency and 1942 took the Financial Education competency) [3], 70% of which were state schools and 30% private schools. According to the results obtained by PISA in 2018, the average obtained by Peru were the following: reading comprehension of 401, mathematics of 400 and science of 404 placing it in 64th place out of 77 countries, although in some points a slight improvement has been achieved but it is still worrisome.

In the national evaluations of learning achievements carried out in 2019 [4], [5] where students at 1st secondary school were evaluated, to test if the learning obtained are those

expected by the National Curriculum of Basic Education (CNEB), the national results exposed in Table I were obtained, making a comparison of the national results of the year 2018 and 2019. It was identified that we remain in "Level in process", where the student managed to partially learn the expected learning, but still shows difficulties, since the academic performance that students are obtaining is very low compared to other countries.

One of the ways to establish improvements in the educational world is using technological tools [6], [7], these can be used by teachers and students especially in remote and/or face-to-face learning by combining traditional teaching with technology. One of them being Augmented Reality (AR), which consists of the overprinting of one or more virtual elements in real time [8], this is given thanks to the mobile camera being an appropriate means of entertainment for educational purposes.

What we want to achieve in this research is to provide a technological proposal, which will serve to improve the learning of students in the Science and Technology course, thus showing a significant increase in their level of interest in the course, their understanding of the information they are being taught and an increase in their level of satisfaction using the mobile application with reality, thus achieving a dynamic learning.

TABLE I. NATIONAL RESULTS BETWEEN 2018 AND 2019

Areas evaluated	Average Mean (MP)	
	2018	2019
Reading	571	567
Mathematics	560	567
Science and Technology	500	501

## II. BIBLIOGRAPHIC STUDY

The accelerated advance of technology together with mobile devices has led us to redefine current teaching and communication methods. A lot of research has conducted studies on the impact of Information and Communication Technologies (ICTs) both in everyday life and in specific areas such as education [9]-[11], aiming to demonstrate the results focused on the skills acquired by students. This technological development can use new technologies as an aid in the teaching and learning process for both teachers and students

[12]. Adolescents are during these changes and usually make use of the artifacts and technologies that are being incorporated into our daily lives [13], familiarizing themselves with them and allowing them to take advantage of them in a way that contributes to their intellectual development, aiming to achieve an education based on results.

This section presents a review of the latest research conducted regarding the topic in common, to show the benefits and effects achieved from AR implemented in education. Articles from academic journals and academic research databases between the years 2016-2021 were considered, presenting a summarized analysis of studies.

In the research [14], an application was proposed for learning the Quechua language with augmented reality in pre-school students, serving as support as teaching material inside and outside the classroom. The activities developed within the application were adapted by means of written and audiovisual comprehension, showing favorable results within the population. A 30% improvement in the students' performance was evidenced after being used in the classes as a support tool.

In the research work [15] proposes a mobile application called GEO+. The application would be used by elementary school students allowing them to have a better acquisition of knowledge based on the geometry course, making use of augmented reality, and generating a greater interest in the course. The effectiveness of learning was measured through post-test and pre-test evaluations, finally the results obtained were effective regarding the increase of satisfaction and learning before and after the implementation of the application, allowing them the ease of use of technology and achieving autonomous learning.

Finally, the present research [16], shows an application to demonstrate particle physics experiments using AR and the Kinest sensor to create an experience that immerses users in the subject. The results obtained were profitable, according to the qualitative analysis 85% of the participants were satisfied and recommended the application.

The studies shown allow us to identify how AR has made a great contribution to education.

### III. METHODOLOGY

The Mobile-D Methodology is used for a collaborative work to deliver a ready product within a maximum of ten weeks by a team of no more than ten developers, including test-driven development, continuous integration, and refactoring, as well as software process improvement tasks [17]. The Mobile-D methodology has 5 phases: Exploration, Initialization, Production, Stabilization and System Testing.

#### A. Exploration

At this stage the Stakeholders were established.

- Interest Group: Companies focused on the education sector.
- Application User: (30) Students of 6th Grade of Primary and 1st Grade of Secondary.

- Developers: Researchers/Developers of the present project.

#### B. Initialization

In this phase, the technological resources (hardware and software) for the development of the research project are established.

Hardware:

- 2 laptops with 4-core processor or more, 8 GB RAM.
- Samsung A20S mobile device.

Software:

- Unity: This is a video game development tool that also serves to create interactive experiences in Virtual or Augmented Reality [18], being processed, rendered, and displayed in real time.
- Blender: A software capable of creating new 3d visualizations [19] (still images, animations, video editions, etc.), it has a high-quality architecture, allowing an optimal workflow.
- Vuforia: Vuforia is an augmented and mixed reality application development tool, oriented for the Unity engine [20]. Offering text recognition, image recognition, tracking, target detection.
- Visual Studio: is an integrated development environment (IDE) being a program that has several features around software development [21].

#### C. Production

In this phase the ideas are organized, and the functions of the application are prototyped. Fig. 1 shows the general architecture of the application called ARST.

Through the mobile device captures the scene taken through the camera and the Vuforia SDK will create frames of the captured scene converting the image to a different resolution for the proper processing of the tracker. The Vuforia SDK will analyze the images through the tracker looking for similarities in the database that is composed of the targets, and then the application verifies the status of the targets to update the logic programmed in Unity, and finally present the virtual content on the screen of the device to be observed in augmented reality.

#### D. Stabilization

In this stage, the development of the components and the integration between them is carried out.

1) *Application prototypes*: Fig. 2 (a) shows the design of the main menu of the application, with its respective options where students can interact, then Fig. 2 (b) shows the initial interface of the presentation of the topic to be performed with its respective classification, in Fig. 2 (c), the interface of the ARST Application quiz is shown, finally in Fig. 2 (d), shows the application questionnaire where students interact by asking questions about the topic, giving a score.

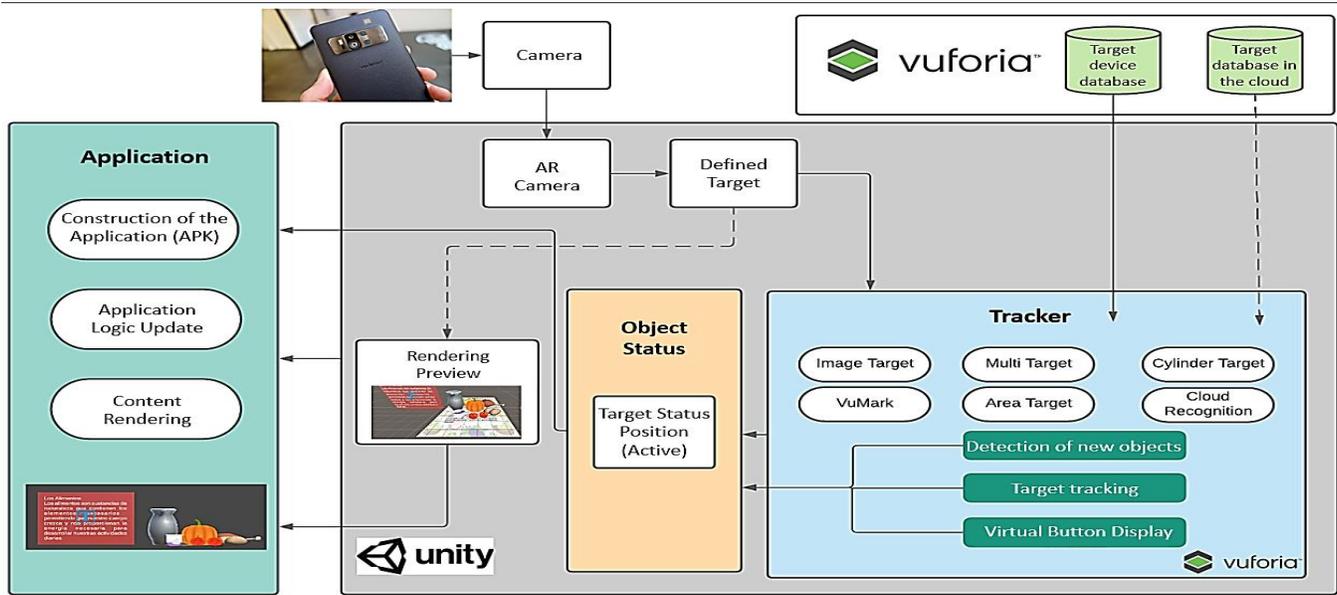


Fig. 1. Project Architecture.

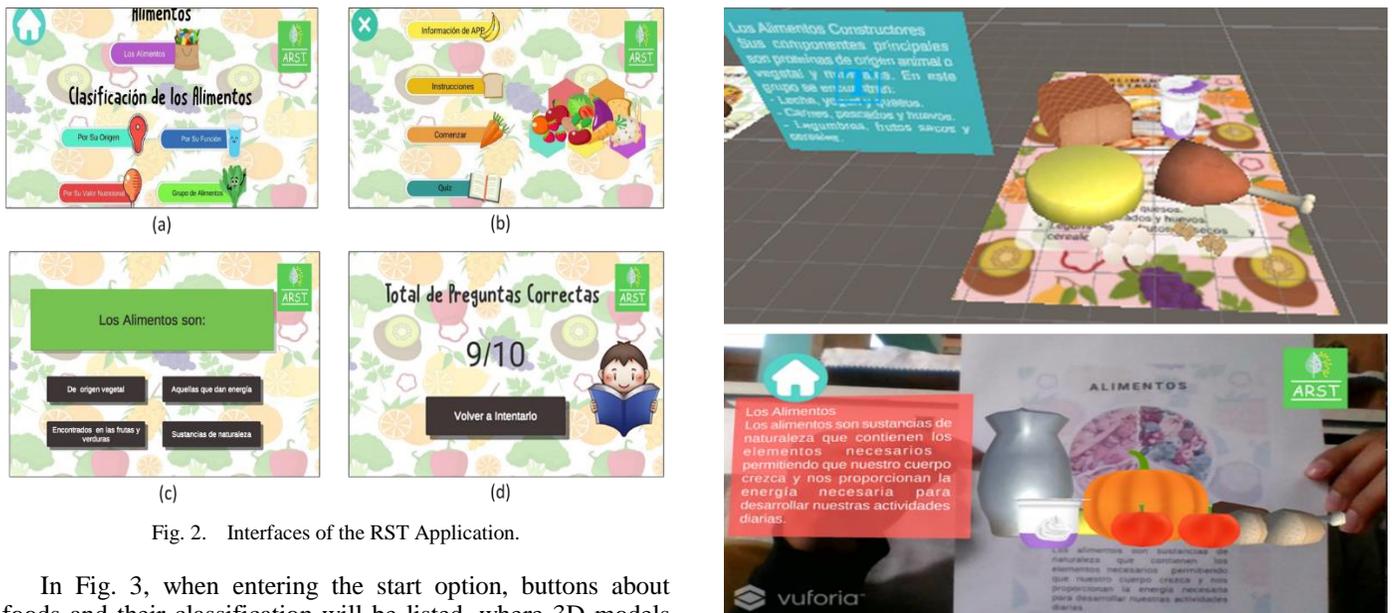


Fig. 2. Interfaces of the RST Application.

Fig. 3. Visualization of 3D Models of Foodstuffs by means of Targets.

In Fig. 3, when entering the start option, buttons about foods and their classification will be listed, where 3D models of foods and their classification are visualized by means of targets. For example, the food with a brief information, the classification of food (by origin, by nutritional value).

E. Test

For this research, the population will be made up of 30 students from I.E.P. Magister in the city of Lima, district of Villa María del Triunfo. It is applied to students in 6th grade of Primary and 1st Grade of Secondary. The design used was pre-experimental, with a pre-test and a post-test since the online method was used (1). Table II shows the definition of the items.

TABLE II. DESCRIPTION OF PRE-EXPERIMENTAL ELEMENTS

Elements (I)	Description
Ge	Experimental Group
O1	Level of learning before applying the system. (Pre-test)
X	Mobile application with augmented reality
O2	Level of learning applied to the system (Post-test)

$Ge \ O_1 \ X \ O_2$  (1)

IV. RESULTS

The objective of this research is to determine to what extent the mobile application with augmented reality will improve learning in the Science and Technology course. For this purpose, the first tests were conducted on one of the most touched topics of the course "Food and its classification", considering the following criteria: The level of interest (KPI-1), the level of understanding (KPI-2) and the level of satisfaction (KPI-3). The information was collected by means of a survey through the Google Forms platform and the results were analyzed with the SPSS tool. The results are shown in Table III.

The first indicator of level of student interest is measured on a Yes/No scale, the second indicator of level of understanding is evaluated on a scale of Beginning to Outstanding Achievement, and the third indicator of level of satisfaction is evaluated on a scale of Very Dissatisfied to Very Satisfied.

1) *KPI-1*: Level of student interest: Fig. 4 shows the results obtained from the experimental group with respect to the Pre-Test and Post-Test, it is observed that the level of interest of the students increases by 30% over the interest they have during the development of the Science and Technology course.

In Fig. 5, the KPI-1 summary report on the level of interest after implementation of the application is shown, which obtained the following results: About 20% of students do not feel a level of interest and 80% do with respect to the science and technology course, also through a 95% confidence interval for the mean, 2 limits 0.61 and 0.99 were obtained.

TABLE III. TEST RESULTS: PRE AND POST

Indicators	Group	Pre-Test	Post-Test
Level of Interest	Experimental	78%	100%
Level of Understanding	Experimental	30%	50%
Satisfaction Level	Experimental	Very Satisfied	Satisfied

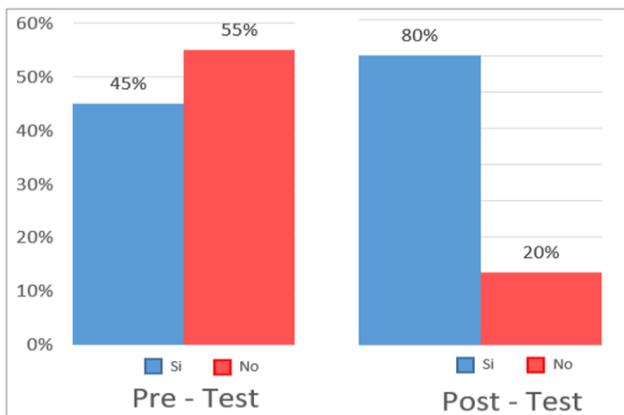


Fig. 4. Pre-Test and Post-Test of Students' Level of Interest.

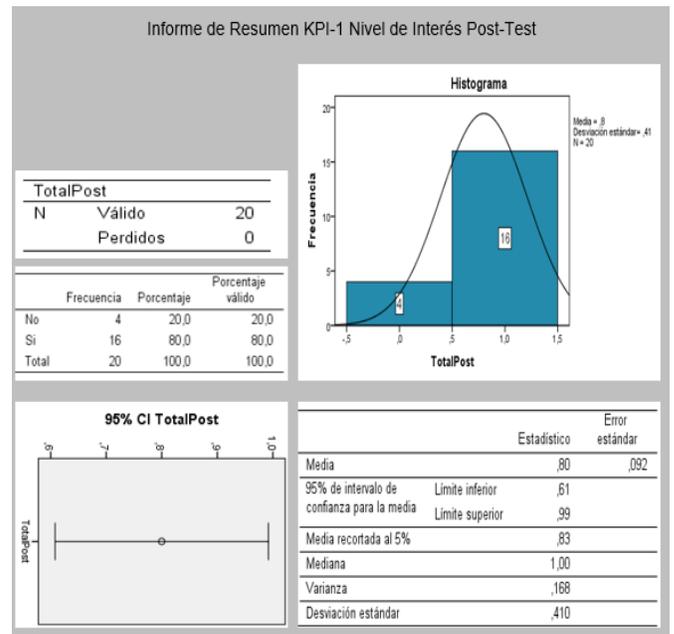


Fig. 5. KPI-1 Summary Report Post-Test Level of Interest.

2) *KPI-2*: Students' level of understanding: Fig. 6 shows the results obtained by the experimental group with respect to the Pre-Test and Post-Test, showing that the level of understanding of the students has increased by 50%, since half of the students have reached an achievement in their comprehension.

In Fig. 7, the KPI-2 Summary report on the level of understanding after implementation of the application is shown, which obtained the following results: Through the tabulation, 50% in process, 30% in Expected Achievement and 20% in Outstanding Achievement of the students with respect to their level of knowledge and understanding on the topic of Food and its classification of the Science and Technology course, with the use of the mobile application with augmented reality.

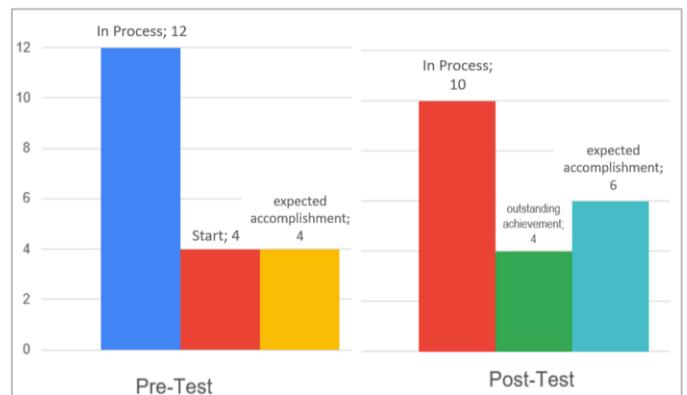


Fig. 6. Pre-test and Post-test of Students' Level of understanding.

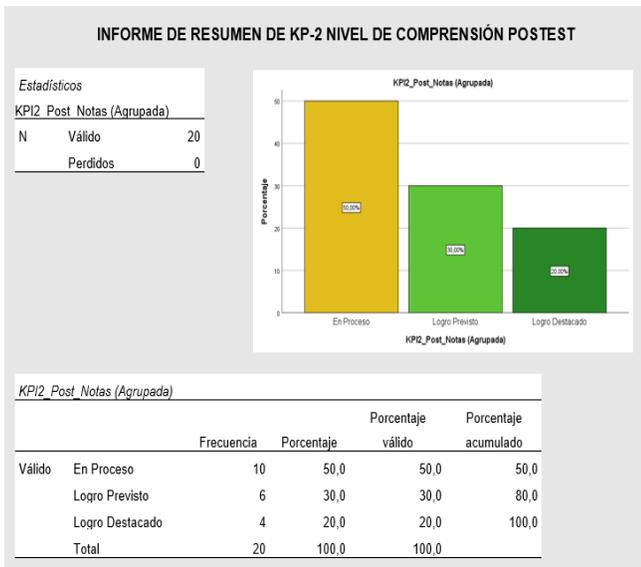


Fig. 7. KPI-2 Post-Test Comprehension Level Summary Report.

3) **KPI-3: Student Satisfaction Level:** Fig. 8 shows the results obtained by the experimental group with respect to the Pre-Test and Post-Test, showing that the level of satisfaction has decreased, but is still maintained in a degree of satisfaction (Very Satisfied and Satisfied) by the students.

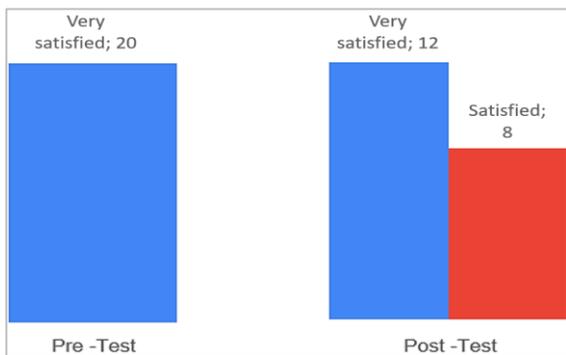


Fig. 8. Pre-test and Post-test of Student Satisfaction Levels.

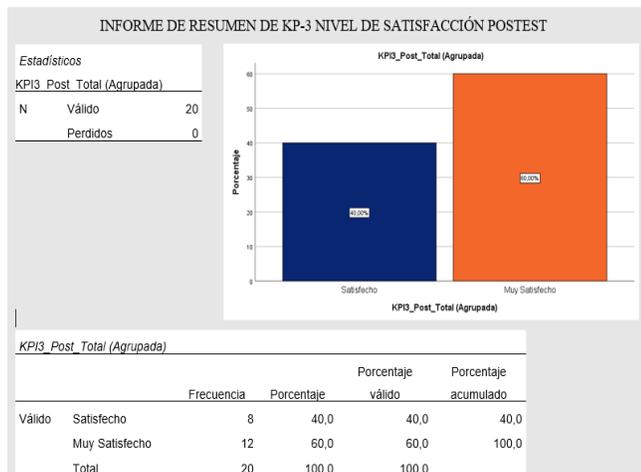


Fig. 9. KPI-3 Post-Test Satisfaction Level Summary Report.

Fig. 9 shows the KPI-3 summary report on the level of satisfaction after implementation of the application, which obtained the following results: Through the tabulation, 40% of the students feel satisfied and 60% of the students feel very satisfied with respect to the application with augmented reality applied during the class with the topic of Food and its Classification in the Science and Technology course.

## V. CONCLUSION

This research article has presented a review of research in recent years regarding the benefits of AR in education, concluding that it contributes greatly to their academic performance, self-learning, and creativity, in addition to increasing their enthusiasm in courses by encouraging research.

An AR application was developed as a tool to improve learning in the science and technology course for regular elementary school students, providing additional didactic information together with questionnaires to measure learning.

It has been observed that the use of a mobile application with augmented reality significantly improves learning in the Science and Technology Course due to the 50% increase in the Comprehension Level (Fig. 4 and Fig. 5), applied in the questionnaire of students in 6th grade of primary education and 1st grade of secondary education (experimental group). There were not many changes in the students' satisfaction (Fig. 6 and Fig. 7), but it remains between the intervals of 40% of Satisfied Students and 60% of Very Satisfied Students. There was an increase of 30% of students who showed interest in the Science and Technology course (Fig. 8 and Fig. 9).

The results showed that the proposed ARST application has succeeded in promoting self-learning, didactic learning, and research. It is recommended for future research to develop more topics applying augmented reality focused on education.

## REFERENCES

- [1] Ministerio de Educación y Formación Profesional and Instituto Nacional de Evaluación Educativa, "PISA", España, 2021.
- [2] Ministerio de Educación (MINEDU), "PISA: Perú sigue siendo el país de América Latina que muestra mayor crecimiento histórico en matemáticas, ciencia y lectura", 2019. <http://umc.minedu.gob.pe/pisa-peru-sigue-siendo-el-pais-de-america-latina-que-muestra-crecimiento-historico-en-matematicas-ciencia-y-lenguaje>.
- [3] Oficina de Medición de la Calidad de los Aprendizajes (UMC) and Ministerio de Educación (MINEDU), "Evaluación PISA 2018," 2018. [http://umc.minedu.gob.pe/wp-content/uploads/2020/10/PPT-PISA-2018\\_Web\\_vf-15-10-20.pdf](http://umc.minedu.gob.pe/wp-content/uploads/2020/10/PPT-PISA-2018_Web_vf-15-10-20.pdf).
- [4] Ministerio de Educación (MINEDU), "Evaluaciones nacionales de logros de aprendizaje. ¿Qué aprendizajes logran nuestros estudiantes?," Perú, 2019. <http://umc.minedu.gob.pe/wp-content/uploads/2020/06/Reporte-Nacional-2019.pdf>.
- [5] Oficina de Medición de la Calidad de los Aprendizajes (UMC) and Ministerio de Educación (MINEDU), "Evaluaciones de logros de aprendizaje. Resultados 2019," 2019. <http://umc.minedu.gob.pe/wp-content/uploads/2020/06/PPT-web-ECE-2019-28.05a.pdf>.
- [6] Saéz Daniela, "La Tecnología e Innovación educativa en el Marco de la pandemia: Lecciones aprendidas," El Diálogo Lidedazgo para las Américas, vol. 1, 2020.
- [7] C. Marín, R. Vallejo, G. Castro, Q. Mendoza, M. G. Castro, and C. Q. Mendoza, "Innovación y tecnología educativa en el contexto actual latinoamericano / Innovation and Educational Technology in the current

- Latin American context,” *Rev. Ciencias Soc.*, vol. 26, 2020, doi: 10.31876/rscs.v26i0.34139.
- [8] A. Blázquez Sevilla, “Realidad Aumentada en Educación,” 2017. [http://oa.upm.es/45985/1/Realidad\\_Aumentada\\_Educacion.pdf](http://oa.upm.es/45985/1/Realidad_Aumentada_Educacion.pdf).
- [9] S. V. Raju, M. S. V. S. B. Raju, G. Abbaiah, and M. Gudavalli, “Role of ICT in Outcome Based Education,” 2016 IEEE 6th Int. Conf. Adv. Comput., pp. 815–819, Feb. 2016, doi: 10.1109/IACC.2016.155.
- [10] P. R. Rajarapolu and S. A. Bhagwatkar, “ICT - An Effective Way for Active and Collaborative Learning Teaching Process in Engineering Education - A Review,” *Int. Conf. Transform. Eng. Educ. ICTEE 2017, Dec. 2018*, doi: 10.1109/ICTEED.2017.8585697.
- [11] J. Gómez Galán, “Innovation and ICT in Education: The Diversity of the 21st Century Classroom,” *River Publ.*, 2021. <https://ieeexplore.ieee.org/document/9494314>.
- [12] G. Á. Calero, J. A. Díaz Quiñones, and P. M. Díaz Martínez, “Adolescencia y tecnologías de la información y comunicaciones. Un reto para la sociedad cubana actual Adolescence and information and communication technologies. A challenge for the current Cuban society,” *Scielo*, pp. 30–40, 2018.
- [13] A. Barquero and F. Calderón, “Influencia de las nuevas tecnologías en el desarrollo adolescente y posibles desajustes,” *Cúpula*, pp. 11–25, 2016. <https://www.binasss.sa.cr/bibliotecas/bhp/cupula/v30n2/art02.pdf>.
- [14] J. Zapata-Paulini, M. Soto-Cordova, and U. Lapa-Asto, “A Mobile Application with Augmented Reality for the Learning of the Quechua Language in Pre-School Children,” in 2019 IEEE 39th Central America and Panama Convention (CONCAPAN XXXIX), Nov. 2020, pp. 1–5, doi: 10.1109/concapanxxxix47272.2019.8976924.
- [15] V. Rossano, R. Lanzilotti, A. Cazzolla, and T. Roselli, “Augmented Reality to Support Geometry Learning,” *IEEE Access*, vol. 8, no. June, pp. 107772–107780, 2020, doi: 10.1109/ACCESS.2020.3000990.
- [16] H. Hyder, G. Baloch, K. Saad, N. Shaikh, A. B. Buriro, and J. Bhatti, “Particle Physics Simulator for Scientific Education using Augmented Reality,” *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 2, pp. 671–681, 2021, doi: 10.14569/IJACSA.2021.0120284.
- [17] J. Gomez and D. Hernandez, “Mobile D (programación dispositivos móviles),” *Universidad del Quindío*, 2016. <https://es.slideshare.net/pipehernandez1020/mobile-d-programacion-dispositivos-moviles>.
- [18] Unity, “Unity - Manual: Manual de Unity,” 2016. <https://docs.unity3d.com/es/530/Manual/UnityManual.html>.
- [19] Blender, “Introducción — Blender Manual.” [https://docs.blender.org/manual/es/2.82/getting\\_started/about/introduction.html](https://docs.blender.org/manual/es/2.82/getting_started/about/introduction.html).
- [20] Unity, “Vuforia - Unity Manual,” 2018. <https://docs.unity3d.com/es/2018.4/Manual/vuforia-sdk-overview.html>.
- [21] Microsoft, “IDE de Visual Studio | Visual Basic,” 2021. <https://docs.microsoft.com/es-es/visualstudio/get-started/visual-basic/visual-studio-ide?view=vs-2019>.

# Learning Pick to Place Objects using Self-supervised Learning with Minimal Training Resources

## Pick-to-Place Objects with Self-supervised Learning

Marwan Qaid Mohammed, Lee Chung Kwek, Shing Chyi Chua

Faculty of Engineering and Technology  
Multimedia University (MMU)  
Melaka, Malaysia

**Abstract**—Grasping objects is a critical but challenging aspect of robotic manipulation. Recent studies have concentrated on complex architectures and large, well-labeled data sets that need extensive computing resources and time to achieve generalization capability. This paper proposes an effective grasp-to-place strategy for manipulating objects in sparse and chaotic environments. A deep Q-network, a model-free deep reinforcement learning method for robotic grasping, is employed in this paper. The proposed approach is remarkable in that it executes both fundamental object pickup and placement actions by utilizing raw RGB-D images through an explicit architecture. Therefore, it needs fewer computing processes, takes less time to complete simulation training, and generalizes effectively across different object types and scenarios. Our approach learns the policies to experience the optimal grasp point via trial-and-error. The fully convolutional network is utilized to map the visual input into pixel-wise Q-value, a motion agnostic representation that reflects the grasp's orientation and pose. In a simulation experiment, a UR5 robotic arm equipped with a Parallel-jaw gripper is used to assess the proposed approach by demonstrating its effectiveness. The experimental outcomes indicate that our approach successfully grasps objects with consuming minimal time and computer resources.

**Keywords**—Self-supervised; pick-to-place; robotics; deep q-network

### I. INTRODUCTION

Dexterous grasping is a crucial ability of robots that enables them to assist and substitute humans in accomplishing various tasks that might be too dangerous or tedious to do. Deep learning (DL) allows computational models composing multiple processing layers to learn data representation with multiple levels of abstraction [1]. On the other hand, Reinforcement learning (RL) relates how software agents learn to take actions in an environment such that some notion of cumulative reward is maximized via a trial-and-error approach [2]. A typical deep reinforcement learning (deep-RL) combines these two machine learning methods [3], which leverages the representation power of deep learning to solve the reinforcement learning problem. When applied to robotic grasping, the robot observes the environment through RGB-D data, and attempts an optimal action the predefined policy. Robotics can be used in nearly every circumstance, but particularly in cluttered environments, where the need for enhanced grasping efficiency demands. Object grasping is a

typical robotics challenge that has made substantial progress in recent years, which is an essential step in many robotic tasks [4]. Objects removal task has been extensively researched in many studies. yet it is a challenging task in robotic manipulation [5].

The process by which a robot learns to grab and remove objects from its workstation is called object removal. Although many studies have focused on learning to grasp a single or multiple objects, some of these studies have examined how to overcome the difficulty of grasping in crowded surroundings where things seem to be stuck together in a pile. The robot must be able to detect and interpret objects and their environment in this situation, as well as effectively remove the objects from the robot's workspace. Recently, a standard Deep-RL has been used in a variety of robotic applications [6], including placement [7], grasping deformable objects [8], and grasping in a cluttered environment [5]. Meanwhile, it has advanced technology by integrating visual and tactile input, particularly in robotic grasping [4]. Additionally, deep-RL has offered great solutions for difficult-to-perform and repeat tasks via the use of end-to-end training. Since robots are usually effective at grabbing a variety of objects, interest in robots with warehouse automation skills has steadily increased in recent years. RGB-D data is increasingly being used to enhance robotic vision-based grasping in cluttered environments. Zeng et al. [9] developed a method that utilizes multi-view RGB-D data in conjunction with self-supervised and data-driven learning.

In [10], the authors utilised a straightforward view-based rendering as a forward-prediction model. To generate reliable dense visualizations of objects from RGB-D data for robotic manipulation, Florence et al. [11] presented the Dense-Object Net using a ResNet architecture. Some studies used only RGB data, obviating the necessity of depth images. The use of depth images was not required in certain studies. For example, [12] proposed GANs that could use a single batch of RGB data to predict a hand's form and location for various object grasping. Kalashnikov et al. [13] employed RL to generate a grasp pose detection dataset from RGB data in cluttered settings. The learned policies were optimized utilizing the aforementioned methods' experience. However, learning typically takes days to acquire enough experience training iterations since it needs significant computing resources to calculate the large quantity of required data. Using a large dataset [14] (e.g., recognizing

graspable poses with RGB-D data [15], point clouds[16], semantic segmentation based grasp[17]) necessitates a large amount of memory and a powerful graphics processor unit (GPU), such as NVidia Drivers, which is currently one of the difficulties in Supervised learning. In this paper, we propose an explicit pick-to-place framework that is less sophisticated than others [18]–[22] and that can be trained with appropriate CPU-Memory or GPU-Memory while taking into account training time and sufficient data for adequate evaluation analysis.

We propose a pick-to-place approach in self-supervised learning, in which RGB-D images are mapped to grasping actions through a fully connected network (FCN). The executed action is evaluated via trial-and-error by maximizing the rewards. The paper's primary contributions are as follows:

- To create an all-inclusive explicit manipulation approach that incorporates both picking and placement activities.
- To minimize the complexity of the model architecture to do training with minimal GPU or CPU resources.
- To increase the chance of robotic grasping in cluttered environment.

The paper is organized as follow: Section 2 discusses related studies, while Section 3 discusses the proposed approach's methodology in detail, including an overview of the strategic approach. The simulation experiment is given in the next section. Section 5 summarizes the findings and discusses them. The conclusion of the paper is presented in Section 6.

## II. RELATED WORK

Several studies have focused on robotic grasping, especially in dense surroundings, and proposed solutions using deep-RL, an efficient method. This area requires further investigation and understanding of the problems. Taking everything from a robot's workplace is part of cleaning up a cluttered environment. The robot must be able to perceive, interpret, and act on its surroundings and objects. When objects are physically close together, the robot's gripper must locate a place for its fingers to grasp. Zeng et al. [9] proposed to train Q-learning on FCNs. The vision system takes RGB-D images from various angles. The robot's workspace collects RGB-D images from 15 to 18 angles. Each RGB image feeds an FCN for 2D object segmentation. The final product is 3D. This data is then combined with an existing 3D model to get the 6d posture. In [13], QT-Opt, an off-policy training technique based on Q-continuous learning's action extension, is proposed. Closed-loop vision-based control is enabled via dynamic manipulation and scalable RL. The robot constantly updates its grab tactic to improve long-horizon grasp success probability.

Florence et. al [11] used the idea of self-supervised learning. The Dense-Object Network is employed, which uses the ResNet model to learn dense visual representations of objects from RGB-D data for robotic grasping in cluttered surroundings. However, it only shows a dense descriptor for three object classes, but more object classes might complicate the descriptor space segregation. Furthermore, mask region-based convolutional neural network (R-CNN) incorporates pixel-wise multi-class instance mask prediction for visible and

occluded area mask segmentation. The [23] proposed learning instances and semantic segmentation for visible and occluded regions. Semantic segmentation utilizes Fully convolutional instance-aware semantic segmentation (FCIS) architecture to estimate position-sensitive masks using multi-class instance masks. It requires a dataset including all of the objects' possible occlusion states, labels, and masks; the amount of effort required to complete this task increases exponentially with the number of items. Those studies seem to be a time-consuming and complicated approach.

Active learning trained an RL framework on the intended neural network (NN) [24]. The grasp space is explored using a set of rules. Weighted retraining reduces the effect of measurement mistakes. The pixel-attentive policy gradient method proposed in [25] uses a single depth image and progressively zooms onto a specific area of the image to estimate the optimum grasp. Using Generative models to arrange multi-finger grasps is more difficult than using parallel-jaw grasps in a cluttered environment. In [26], a real-time deep convolutional encoder-decoder NN for open-loop robotic grasping has been proposed. In their method, UG-Net can estimate the quality and posture of a grip using a depth image. In [10], rendering or simulating future states concerning many possible actions is re-used. As a result, an end-to-end 6-DoF closed-loop grasping model using RL is shown employing a learned value function (Q-value). Also, an RL framework and 3D vision architectures were proposed [27] using hand-mounted RGB-D cameras. However, manipulation with more task-dependent representations must be learned from limited training data. Also, Yang and Shang [28] suggested an attention DQN for robotic grasping in clutter. Whereas, Assembly task to grasp the objects and place in stacking manner has been executed in [29].

In [12], generative adversarial networks (GANs) were introduced to estimate the hand shape and position for multiple item grasping. However, unstable training requires careful hyperparameter tuning. For 6-DoF grasping, the generative attention learning (GenerAL) method [30] has been provided, which uses deep RL to directly output the final position and configuration of the fingers. In another study, a generative grasping GG-CNN is provided [31] to extract the grip quality from a depth image. It also predicts the optimum grip based on the location, angle, and grasping breadth. However, an inaccurate grasp width estimate causes gripper collisions on large and small objects. In cluttered scenes, an end-to-end network (Contact-GraspNet) has been presented [32] to effectively and automatically distribute 6-DoF parallel-jaw grasps using depth data while preventing collisions. The limited grip breadth prevents it from grasping heavy objects. The discontinuous selection boundary makes predictions less trustworthy. Besides, The collision-aware reachability predictor (CARP) approach [33] has been proposed to learn to estimate the probabilities of a collision-free grasp position, thus substantially enhancing the grasping of objects in challenging situations. In addition, Generative deep dexterous grasping in clutters (DDGC) proposed to generate a set of collision-free multi-finger grasps in cluttered scenes. High-quality grasps produced by DDGC do not always give a successful grasp [34].

There are some challenges that arise as a consequence of the training requirements and the time required to complete grasping activities. Certain failure scenarios occur in clutter circumstances due to the clutter being so dense that there is no space for the robot to place its fingers. Additionally, it needs a simulation setup and, in most cases, an extensive parameter search to function well. As a result, it is computationally intensive, taking between tens of seconds and minutes to complete. Similarly, batch training may not be optimal for predictions involving dense clutter. Learning often involves computing a massive quantity of necessary data, which results in a high cost of training setup and a long amount of time required to acquire proficiency. As a result, the majority of studies used sophisticated architectural frameworks that need a powerful graphics processing unit (GPU) to accelerate the training process, which not every academic can afford. Additionally, they focused on executing grasp movements without regard for where the object should be placed after it was grasped. To overcome the aforementioned challenges, we propose a grasp action with a single FCN of posture estimation using an explicit approach that consumes less time while performing efficient grasping. The proposed approach's purpose is to avoid model architectural complexity to enable training to be done with minimal GPU or CPU resources. Additionally, it focuses not just on grasping but also on placing tasks. Accordingly, a complete manipulation system (pick-to-place) is developed, which is learned collaboratively via end-to-end learning.

### III. METHODOLOGY

This section will explain the system's architecture and functions in detail. Then, the grasp and placement actions will be described in terms of how they perform and how they grasp and place actions' rules-based coordination works. The reinforcement learning formula and associated rewards will be explained, as well as how this component contributes to the robot's task learning.

#### A. Approach Overview

The proposed approach is intended to minimize the demands of the computing process, which could have an impact on the cost of time used during operation (Figure 1). The approach architecture is designed to run in a reasonable amount of time on a moderate CPU or GPU. The purpose of this paper is also to create a self-supervised learning

manipulation approach that avoids the inherent complexity of approach architecture.

Firstly, the camera captures the RGB-D images, which then projected to generate the color ( $C_h$ ) and depth ( $D_h$ ) heightmaps. The  $C_h$  and  $D_h$  will be rotated ( $\cup \times N$ ) before being forwarded into the conventional layers (a 2-layer residual networks [35]). The residual networks will reduce the input parameters of DenseNet-121 to be 1024 instead 2048, which can effectively minimize the time-consuming, and run on moderate CPU and GPU. Then, the extracted features are then fed to a DenseNet-121 [36], a pre-trained model on ImageNet [37], to create motion agnostic features. Then, the motion agnostic features are used as inputs by the grasp net  $\phi_g$  followed by bilinear upsampling, which estimates the grasp Q-maps ( $Q_g(s_t, a_t) \in \phi_g$ ). A three-layer residual network is used in the  $\phi_g$ . Finally, the robot executes the predicted best grasp, corresponding to the highest Q-value. Rewards are then assigned automatically depending on the success of grasps. The experience replay [38] is employed, which used to store the agent's experiences at each time step in a data set  $e_t = (s_t, a_t, r_t, s_{t+1})$  that is pooled across many episodes to create a replay memory. Then, like with DQN, we randomly sample the memory for a minibatch of experience and utilize this to train off-policy.

#### B. Q-Learning and Reward Function

The representation image of the environment is viewed as a state ( $s_t$ ) in this article, which is the deep network's input. The output is the action with the highest action-value, and it results in an immediate reward. As a consequence, as demonstrated in Eq. (1) [2], the policy ( $\pi$ ) is reinforced by selecting the action with the highest state-action value. The agent's goal is to select the best action that maximizes the action-value function and the sum of future reward expectation returns. Maximization is accomplished by selecting the optimal value action (among all potential actions).

$$\pi^*(s) = \arg \max_a Q_\pi(s, a). \quad (1)$$

To estimate the optimal grasping action, the approach is trained via Q-learning on FCN. The Q-value is learned in association with the offline policy, as in Eq. (2).

$$Q_{new}(s_t, a_t) \leftarrow Q(s_t, a_t) + \alpha(r_t + \gamma \max_{a'} Q(a', s') - Q(s_t, a_t)) \quad (2)$$

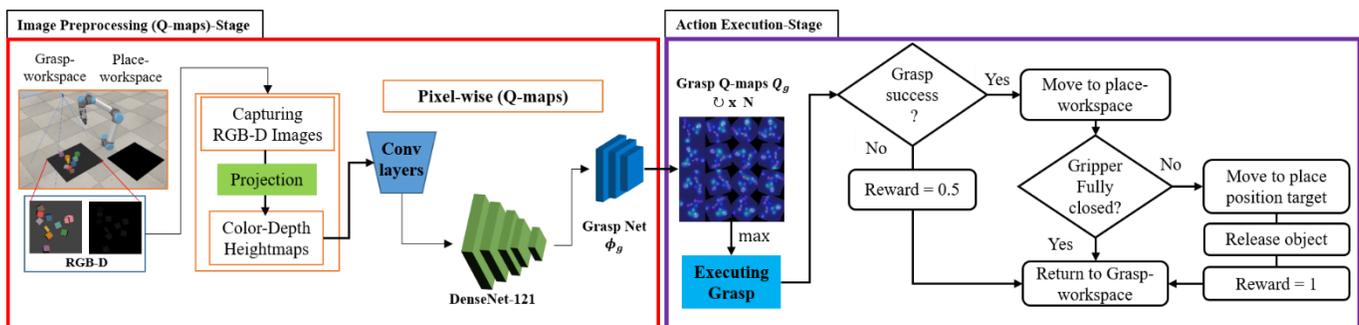


Fig. 1. The Workflow of Proposed Approach based Picking and Placing of Objects.

The  $Q(s_t, a_t)$  parameter represents the current Q-value, which is updated during the training, and the  $(\alpha)$  variable represents the assigned learning rate, which is between 0 and 1. Meanwhile, The discount factor  $(\gamma)$  is set to 0.5. The current reward  $(r_t)$  is received by transitioning from the present state  $(s_t)$  to the future state  $(s' = s_{t+1})$ . The reward is required to inform the robot about which state-action pairs are efficient and which are not. The initial value of  $r_t$  is 0, but it is increased throughout the training process to stimulate the robot to perform grasp tasks and reduce the loss value. The grasp prediction yields the future reward (e.g.  $\max_{a'} Q(a', s')$ ). Since Q-learning is trained on FCN, the learning rate is used in the stochastic gradient descent optimizer's back-propagation, it is no longer essential to include it in the Q-learning equation. After removing the learning rate, the two terms cancel out (as written in Eq. (3)).

$$r_t + \gamma \max_{a'} Q(a', s') \quad (3)$$

Accordingly, we set the reward function as follows:

- $r_g(s_t, s_{t+1}) = 0.0$  for grasp if it fails and gripper never come in contact with the objects,
- $r_g(s_t, s_{t+1}) = 0.5$  for grasp if it fails and gripper come in contact with the objects.
- $r_g(s_t, s_{t+1}) = 1.0$  for successful grasp and place the object.

### C. Grasp and Place Primitive Actions

Each action  $(a_t)$  is represented as a primitive motion  $(\Psi)$  at 3D position  $(P)$ , which is projected from the pixel  $(px)$  of the heightmap image that depicts the state  $(s_t)$ , as shown in Eq. (4).

$$a = (\Psi, P) \mid \Psi \in \{grasp\}, P \rightarrow px \in s_t \quad (4)$$

A gripping action is presented as primitive motion. In one of 16 positions, the grasping motion is executed utilizing the center point within the gripper's parallel-jaw of top-down grasp. The robot moves its gripper's fingers down 3 cm of the expected location before closing its fingers to ensure that it reaches the desired object. The difference between the location of the gripper before and after gripping attempts is compared to its threshold value to detect a grasp action. The distance between the gripper's fingers and the workspace, which is 300 cm, is used as the threshold value. A successful grabbing attempt, on the other hand, is recorded when the fingers are not entirely closed, indicating that the object stays intact within the gripper's fingers until the robot places the object down.

In the next stage, once the robot has gripped an object, the placing operation will be carried out, as shown in Figure 1. The robot arrives at the workplace. The gripper's state is then verified to make sure the object is still in position. The placement process will be interrupted if there is slippage. After then, the robot returns to its starting location for a new iteration. For example, the robot will then place the object into the pre-defined place-workspace if it has been successfully grabbed. If the robot's gripper is not fully closed during a placement job, it implies that the object is within the gripper's fingers, allowing the robot to continue placing the object;

otherwise, the robot will interrupt and resume grasping instead of placing the object.

## IV. SIMULATION EXPERIMENT

In this paper, V-REP [39] is used to simulate an experiment using a UR5 robot equipped with a parallel jaw gripper. The robot uses an RGB-D camera to observe its environment. The color and depth images are captured at a 640 by 480-pixel resolution. A 3.7 GHz Intel Core i7-8700HQ CPU and an NVIDIA 1660Ti GPU power the PyTorch-based prediction network.

### A. Training Session

Self-supervised learning using a simulation platform is used to train the proposed approach. A similar training procedure to that described in [40] is used. For training, a collection of ten objects of different shapes is randomly placed into the robot's workspace. By trial and error, the robot learns to perform picking and a placement action. After clearing the workspace of all objects, another set of 10 objects is dropped for additional training. Continuous data collection occurs until the robot has completed 3K training iterations.

### B. Testing Session

We conducted a series of experiments to determine if the proposed approach is successful at accomplishing the grasping-to-placing task. We validate our approach using scenarios involving randomly cluttered objects with varying degrees of clutter, namely sparsely, medium, and dense clutter levels, as shown in Figure 2.

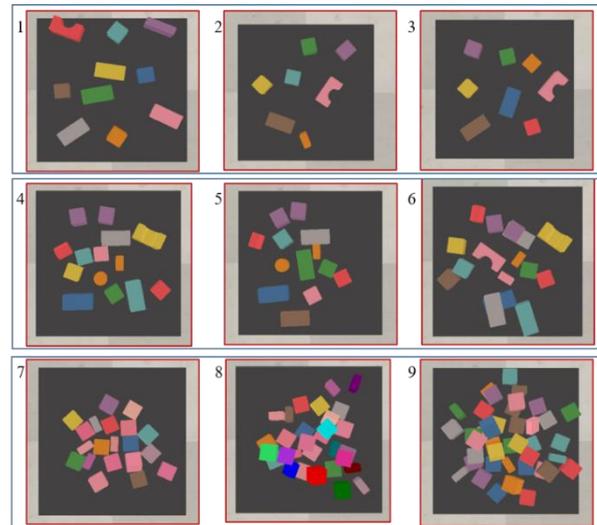


Fig. 2. A Series of Randomly Sparsely, Medium, and Densely Cluttered Object Challenge Scenarios.

- Sparsely cluttered objects scenario (test-cases 1-3): the objects are randomly distributed on the workspace in groups of 6–7.
- Medium cluttered objects scenarios (test-cases 4-6): The objects disperse in a random order of 9–10 objects that are distributed in close contact with one another. They are more challenging to perform than the first type of scenario.

- Densely cluttered objects scenarios (test-cases 20-30): Three scenarios, including a random selection of 20–30 objects, conduct to assess the proposed approach, which implies more challenging than the previous two sorts of scenarios.

### C. Evaluation Metrics

The proposed approach is assessed using the test scenarios described before. The robot must retrieve and clean all objects from the workspace in order to place them into place-workspace. Five test runs (denoted by  $n$ ) are conducted for each test case. The workspace contains between 6 to 40 objects. Three assessment metrics are utilized to evaluate the models' performance. The greater the value for each of these metrics, the better. These are the metrics.

- The grasp success rate: Ratio of the success grasp attempts to the total of executed actions over  $n$  test runs per each test case, and
- The place success rate: ratio of the number of successful place over the number of successful grasp through whole run tests of each case test.
- The completion rate: It's the average of the total number of completed objects divided by the total number of objects. It is used to measure the capability of proposed approach to grasp all objects in each test case without failing for more than five actions consecutively.

## V. RESULT AND DISCUSSION

This section organizes the findings into training and testing sessions. The proposed method's results will be shown throughout the training session via graphs of grasp success rate, which illustrate how the proposed approach performed during the training stage and how fast and effectively it learned. The testing session consists of a sequence of test cases, each of which is conducted five times. The models' performance is assessed using their grasp success, place success and completion rates.

### A. Training Session Outcome

The proposed approach (PA) was trained alongside other baselines utilizing a different training procedure. The grasping performance is evaluated by the proportion of successful grasp attempts made within the last 200 tries ( $m = 200$ ). The percentage is scaled by a factor of  $i/m$  in the earlier training trials, i.e., trials  $i < m$ . Figure 3 illustrates the grasp success rate graphs for 4000 training iterations. In this section, we trained the suggested method using different variables to evaluate whether or not these aspects affect the grasping performance when taken into account.

1) *PA-nodepth*: the proposed approach is trained only on color image data, ignoring depth information. It can be shown that when depth is not included during training, it affects grasp performance, with a grasp rate of almost 73%. Additionally, it requires many trials at the beginning of learning to gain expertise with the environment to boost its performance.

2) *PA-nopretrain*: the proposed approach leverages the use of the DenseNet-121 model, which was pre-trained on

ImageNet. However, we need to evaluate our proposed approach's effectiveness in the absence of ImageNet pre-training. The training session findings show that pre-trained models assist the learning process by improving grasping performance with a minimum number of iterations, in comparison to grasping performance when no pre-training model was used, which struggled for the first 200 iterations of total training iterations, within the range of 65% to 70% grasp success rate.

3) *PA-noER*: In this portion, the proposed approach was trained without using experience replay (ER), which stores the agent's experiences at each time step for use as an off-line policy in subsequent training iterations. The success rate graph indicates that ER has an effect on learning, gradually improving grasping skill in comparison to other factors. The first 500 iterations of a training session achieve a success rate of almost 50%, indicating that the model could be significantly influenced by no experience replay.

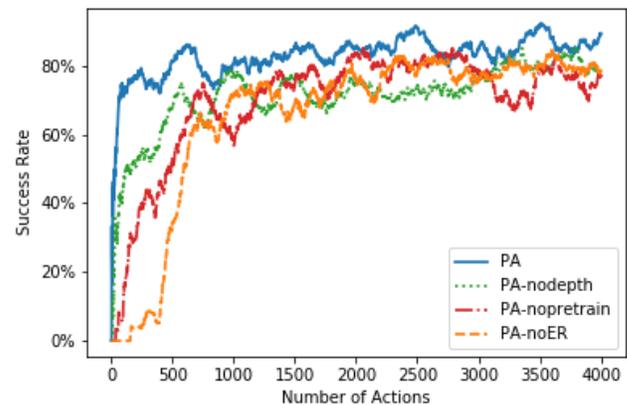


Fig. 3. The Proposed Approach's Performance in Comparison to other Baseline Models in Terms of Grasp Success Rate throughout Training Sessions.

The proposed approach, when combined with pretrain, ER, and RGB-D data, has been demonstrated to significantly improve grasping performance with a success rate of almost 83% and steady learning throughout the training. In term of time-consuming, each iteration takes an average 4 second on the GeForce GTX-1660Ti (6GB) and GeForce GTX 1650 Ti (4GB). We also test the time consuming of the proposed approach on the CPU with RAM of DDR4 (16GB) with 30 seconds. The whole training session for each baseline it takes almost 4-4.5 hours.

### B. Testing Session Outcome

The grasp success, place success, and completion rate are the two evaluation metrics used to assess the performance of the proposed approach. The proposed approach is tested using three scenarios: 1) Sparsely clutter objects, 2) medium clutter objects and 3) densely clutter objects (Figure 2). These type of scenarios are varied in level of clutter challenge with range of objects 6-40 objects.

In Table 1, the results indicate that our approach performed well in more difficult tasks, especially in the first two types of

situations, namely sparsely and moderately cluttered objects, where it achieved a grasp success rate of 93.2 % and 86.1 %, respectively. However, performance degrades as the test scenario becomes more cluttered, with a grasp success rate of 71.7 %. In general, the proposed approach is capable of effectively performing grasping tasks, with a completion rate of about 95% in all scenarios. It implies that it is capable of efficiently moving objects from the robot's workspace to the place workspace.

When we compare our approach to others, many factors must be addressed, as shown in Table II. Interestingly, our approach is capable of grasping with a minimum of time and training resources. In comparison, other approaches need a minimum of ten seconds to complete one iteration. Similarly, if their approaches are carried out on the CPU, they may take

multiple minutes to finish a single iteration due to the complexity of the computing process. On the other hand, our approach is capable of performing grasping tasks on the CPU as well, with each iteration averaging 30 seconds.

TABLE I. ASSESSMENT OF RANDOMLY CLUTTERED OBJECT CHALLENGE SCENARIOS

Metrics (average %)	Test scenarios		
	<i>Sparsely Clutter</i>	<i>Medium Clutter</i>	<i>Densely Clutter</i>
Grasp Success Rate	93.2	86.1	71.7
Place Success Rate	100	95.7	93.8
Completion Rate	100	100	86.1

TABLE II. COMPARISON OF THE PROPOSED APPROACH WITH OTHERS

Method	Training Resources				Time-Consuming	Grasp Success %	Execution action	
	CPU		GPU				Grasp	Place
	RAM-16GB	4GB	6GB	≥ 8GB				
[9]	x	x	x	✓	8-15 seconds	66.7%	✓	x
[18]	x	x	x	✓	10-18 seconds	78%	✓	x
[29]	x	x	x	✓	15-20 Seconds	81.2%	✓	✓
[28]	x	x	x	✓	7-10 seconds	73.5%	✓	x
Ours	✓	✓	✓	✓	4-5 seconds	83.7	✓	✓

## VI. CONCLUSION AND FUTURE WORK

One of the difficulties faced by robots is performing grasping tasks in an unstructured environment. In this paper, the proposed approach, which is based on DQN, showed exceptional grasping performance in a range of test scenarios including randomly cluttered objects. The proposed method has been proven its capability of removing objects from a workspace efficiently. The approach achieves an 83.1 % grasp success rate in cluttered object settings, demonstrating that it is capable of successfully performing a grasping challenge. Additionally, even in challenging circumstances, the proposed approach obtains a high completion rate (96.1 % in all cluttered environment scenarios). In terms of time required, each iteration takes an average of four seconds on the GPU and 30 seconds on the CPU. Significantly, the proposed learning approach proved successful in addressing the aforementioned problems, namely the time and training resources requirements. On the other hand, the proposed approach becomes inefficient as the number of objects increases. This deficiency could well be addressed in the future via the potential merging of grasp and push. Similarly, simulations have been used to assess the proposed approach, which is another possible disadvantage to consider. However, the proposed approach has been evaluated only via simulations, which is a possible drawback to consider. The proposed approach will be implemented on hardware in a future study, giving strong validation for those interested in doing further research.

## ACKNOWLEDGMENT

Authors are thankful to Multimedia University (MMU) for supporting this research. This research is supported by

Multimedia University (MMU) through MMU GRA Scheme (MMUI/190004.02.) and MMU Internal Fund (MMUI/210111).

## REFERENCES

- [1] H. Il Suk, "An Introduction to Neural Networks and Deep Learning," in Deep Learning for Medical Image Analysis, 1st ed., Elsevier Inc., 2017, pp. 3–24.
- [2] R. S. Sutton and A. G. Barto, Reinforcement Learning: An Introduction, 2nd ed. MIT press, 2018.
- [3] V. François-lavet et al., "An Introduction to Deep Reinforcement Learning," Found. Trends® Mach. Learn., vol. 11, no. 3–4, pp. 219–354, 2018.
- [4] Q. M. Marwan, S. C. Chua, and L. C. Kwek, "Comprehensive Review on Reaching and Grasping of Objects in Robotics," Robotica, vol. 39, no. 10, pp. 1849–1882, 2021.
- [5] M. Q. Mohammed, K. L. Chung, and C. S. Chyi, "Review of Deep Reinforcement Learning-Based Object Grasping: Techniques, Open Challenges, and Recommendations," IEEE Access, vol. 8, pp. 178450–178481, 2020.
- [6] J. Andrew Bagnell, "Reinforcement Learning in Robotics: A Survey," Springer Tracts Adv. Robot., vol. 97, pp. 9–67, 2014.
- [7] W. Guo, C. Wang, Y. Fu, and F. Zha, "Deep Reinforcement Learning Algorithm for Object Placement Tasks with Manipulator," in 2018 IEEE International Conference on Intelligence and Safety for Robotics (ISR), 2018, pp. 608–613.
- [8] H. Han, G. Paul, and T. Matsubara, "Model-based reinforcement learning approach for deformable linear object manipulation," in 2017 13th IEEE Conference on Automation Science and Engineering (CASE), 2017, pp. 750–755.
- [9] A. Zeng et al., "Multi-view self-supervised deep learning for 6D pose estimation in the Amazon Picking Challenge," in 2017 IEEE International Conference on Robotics and Automation (ICRA), 2017, pp. 1383–1386.
- [10] S. Song, A. Zeng, J. Lee, and T. Funkhouser, "Grasping in the Wild: Learning 6DoF Closed-Loop Grasping From Low-Cost

- Demonstrations,” *IEEE Robot. Autom. Lett.*, vol. 5, no. 3, pp. 4978–4985, 2020.
- [11] P. R. Florence, L. Manuelli, and R. Tedrake, “Dense Object Nets: Learning Dense Visual Object Descriptors By and For Robotic Manipulation,” arXiv:1806.08756v2, pp. 1–12, 2018.
- [12] E. Corona, A. Pumarola, G. Alenyà, F. Moreno-Noguer, and G. Rogez, “GanHand: Predicting Human Grasp Affordances in Multi-Object Scenes,” in *2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR)*, 2020, pp. 5030–5040.
- [13] D. Kalashnikov et al., “QT-Opt: Scalable Deep Reinforcement Learning for Vision-Based Robotic Manipulation,” arXiv:1806.10293v3, no. L, pp. 1–23, 2018.
- [14] J. Mahler et al., “Dex-Net 2.0: Deep Learning to Plan Robust Grasps with Synthetic Point Clouds and Analytic Grasp Metrics,” arXiv Prepr. arXiv:1703.09312 v3, pp. 1–12, 2017.
- [15] I. Lenz, H. Lee, and A. Saxena, “Deep learning for detecting robotic grasps,” *Int. J. Rob. Res.*, vol. 34, no. 4–5, pp. 705–724, 2015.
- [16] S. Levine, P. Pastor, A. Krizhevsky, J. Ibarz, and D. Quillen, “Learning hand-eye coordination for robotic grasping with deep learning and large-scale data collection,” *Int. J. Rob. Res.*, vol. 37, no. 4–5, pp. 421–436, Apr. 2018.
- [17] M. Q. Mohammed, L. C. Kwek, S. C. Chua, and E. A. Alandoli, “Color Matching Based Approach for Robotic Grasping,” in *2021 International Congress of Advanced Technology and Engineering (ICOTEN)*, 2021, pp. 1–8.
- [18] J. Mahler and K. Goldberg, “Learning Deep Policies for Robot Bin Picking by Simulating Robust Grasping Sequences,” in *Proceedings of the 1st Annual Conference on Robot Learning*, 2017, vol. 78, pp. 515–524.
- [19] M. Q. Mohammed, M. F. Miskon, M. B. Bin Bahar, and S. A. Ali, “Comparative study between quintic and cubic polynomial equations based walking trajectory of exoskeleton system,” *Int. J. Mech. Mechatronics Eng.*, vol. 17, no. 4, pp. 43–51, 2017.
- [20] A. Zeng et al., “Robotic pick-and-place of novel objects in clutter with multi-affordance grasping and cross-domain image matching,” in *IEEE International Conference on Robotics and Automation (ICRA)*, 2019, pp. 3750–3757.
- [21] M. Q. Mohammed, K. L. Chung, and C. S. Chyi, “Pick and Place Objects in a Cluttered Scene Using Deep Reinforcement Learning,” *Int. J. Mech. Mechatronics Eng. IJMME*, vol. 20, no. 04, pp. 50–57, 2020.
- [22] S. A. Ali, M. Fahmi Miskon, A. Zaki Hj Shukor, and M. Qaid Mhoammed, “The Effect of Parameters Variation on Bilateral Controller,” *Int. J. Power Electron. Drive Syst.*, vol. 9, no. 2, p. 648, 2018.
- [23] K. Wada, K. Okada, and M. Inaba, “Joint learning of instance and semantic segmentation for robotic pick-and-place with heavy occlusions in clutter,” in *Proceedings - IEEE International Conference on Robotics and Automation*, 2019, vol. 2019-May, pp. 9558–9564.
- [24] L. Berscheid, T. Rühr, and T. Kröger, “Improving Data Efficiency of Self-supervised Learning for Robotic Grasping,” in *2019 International Conference on Robotics and Automation (ICRA)*, 2019, pp. 2125–2131.
- [25] B. Wu, I. Akinola, and P. K. Allen, “Pixel-Attentive Policy Gradient for Multi-Fingered Grasping in Cluttered Scenes,” in *2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2019, pp. 1789–1796.
- [26] Y. Song, Y. Fei, C. Cheng, X. Li, and C. Yu, “UG-Net for Robotic Grasping using Only Depth Image,” in *2019 IEEE International Conference on Real-time Computing and Robotics (RCAR)*, 2019, pp. 913–918.
- [27] X. Chen et al., “Transferable Active Grasping and Real Embodied Dataset,” in *2020 IEEE International Conference on Robotics and Automation (ICRA)*, 2020, pp. 3611–3618.
- [28] Z. Yang and H. Shang, “Robotic pushing and grasping knowledge learning via attention deep Q-learning network,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12274 LNAI, Academy for Engineering and Technology, Fudan University, Shanghai, China, pp. 223–234, 2020.
- [29] K. Zakka, A. Zeng, J. Lee, and S. Song, “Form2Fit: Learning Shape Priors for Generalizable Assembly from Disassembly,” in *2020 IEEE International Conference on Robotics and Automation (ICRA)*, 2020, pp. 9404–9410.
- [30] B. Wu et al., “Generative Attention Learning: a ‘GenerAL’ framework for high-performance multi-fingered grasping in clutter,” *Auton. Robots*, vol. 44, no. 6, pp. 971–990, Jul. 2020.
- [31] D. Morrison, P. Corke, and J. Leitner, “Learning robust, real-time, reactive robotic grasping,” *Int. J. Rob. Res.*, vol. 39, no. 2–3, pp. 183–201, 2020.
- [32] M. Sundermeyer, A. Mousavian, R. Triebel, and D. Fox, “Contact-GraspNet: Efficient 6-DoF Grasp Generation in Cluttered Scenes,” arXiv:2103.14127v1, pp. 1–7, 2021.
- [33] X. Lou, Y. Yang, and C. Choi, “Collision-Aware Target-Driven Object Grasping in Constrained Environments,” arXiv:2104.00776v1, pp. 1–7, 2021.
- [34] J. Lundell, F. Verdoja, and V. Kyrki, “DDGC: Generative Deep Dexterous Grasping in Clutter,” *IEEE Robot. Autom. Lett.*, vol. 6, no. 4, pp. 6899–6906, 2021.
- [35] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778.
- [36] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, “Densely connected convolutional networks,” in *Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017, pp. 2261–2269.
- [37] L. Fei-Fei, J. Deng, and K. Li, “ImageNet: Constructing a large-scale image database,” in *IEEE Conference on Computer Vision and Pattern Recognition*, 2009, pp. 248–255.
- [38] M. Andrychowicz et al., “Hindsight experience replay,” in *Advances in Neural Information Processing Systems*, 2017, vol. 2017-Decem, pp. 5049–5059.
- [39] E. Rohmer, S. P. N. Singh, and M. Freese, “V-REP: A versatile and scalable robot simulation framework,” in *IEEE International Conference on Intelligent Robots and Systems*, 2013, pp. 1321–1326.
- [40] A. Zeng, S. Song, S. Welker, J. Lee, A. Rodriguez, and T. Funkhouser, “Learning Synergies Between Pushing and Grasping with Self-Supervised Deep Reinforcement Learning,” in *2018 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS)*, 2018, pp. 4238–4245.

# Time Line Correlative Spectral Processing for Stratification of Blood Pressure using Adaptive Signal Conditioning

Santosh Shinde<sup>1</sup>

Research Scholar, Department of Computer Science and Engineering, Koneru Lakshmaiah Education Foundation Vaddeswaram, AP, India-522502

Pothuraju RajaRajeswari<sup>2</sup>

Professor, Department of Computer Science and Engineering Koneru Lakshmaiah Education Foundation Vaddeswaram, AP, India-522502

**Abstract**—Stratification of Blood Pressure is essential input in most of the cardiovascular diseases detection and prediction and is also a great aid to medical practitioners in dealing with Hypertension. Denoising based on spectral coding is developed based on frequency spectral decomposition and a spectral correlative approach based on wavelet transform. The existing approaches perform a standard deviation and mean of peak correlation in signal conditioning. The artifact filtrations were developed based on thresholding. Filtration of coefficients has an impact on accuracy of estimation and hence proper signal conditioning is a primal need. Wherein threshold is measured with discrete monitoring, time line observation could improve the accuracy of filtration efficiency under varying interference condition. Dynamic interference due to capturing or processing source results in jitter type noises which are short period deviations with varying frequency component. Hence a time-frequency analysis for filtration is adapted for filtration. This paper presents an approach of spectral correlation approach for signal condition in stratification of blood pressure under cuff less monitoring. This presented approach operates on the spectral distribution of finer resolution bands for monitoring signal in denoising and decision making. Existing approaches lacks the capability of loss-less denoising which is efficiently worked out in this paper.

**Keywords**—Stratification of blood pressure; discrete wavelet transform; spectral coding; and selective correlative approach

## I. INTRODUCTION

Monitoring of blood pressure is a vital monitoring for automated diagnosis in cardio vascular disease diagnosis. A deflected blood pressure (BP) has a high risk of heart disorderness or heart failure. An early detection and diagnosis is an optimal solution to the asserted risk. The present diagnosis is a cuff based monitoring where the device is interfaced to patient hand to read the mercury level for BP monitoring. The interfacing of such devices is limited to expert personals and not users friendly in handling. With advancement of technology new approaches has evolved in diagnosis, wherein BP monitoring is also improved towards cuff-less measurement. Pulse transient time (PTT) [1-4] is a majorly observed approach in this type of measurement. The analysis presents a good correlation in diagnosis of PTT with BP monitoring. In [5] author interfaced electrocardiograph (ECG) with photoplethysmography (PPG) signals to estimate

the BP level. A correlative approach in measuring mean error (ME) for the measured BP and the actual measurement is evaluated based on standard deviation for the magnitude values. In [6] boosting approach is presented in deriving a more calibrated monitoring of BP using ME. The impact of monitoring is however limited in such approach with the interference of external distortion.

This paper presents a novel Time line correlative spectral processing approach for efficient denoising of Vital Bio-Signals such as PPG, ECG and ABP. It utilizes an adaptive signal conditioning approach. The proposed method results in minimum loss in terms of Frequency components after wavelet computations and hence preserves the significant medical information in the signal.

To present the outlined approach this paper is outlined into seven sections. Section 2 presents the Background work citing the challenges and limitations of existing approaches. Section 3 outlined the existing approach of signal processing and analysis. Section 4 presents the approach of denoising signal in a nonlinear distortion approach. Section 5 outlines the simulation result for the developed approach. Section 6 presents Discussion and Future Work. The conclusion for the developed approach is presented in Section 7. Section 8 is about acknowledgment.

## II. BACKGROUND

The filtration of the distorted signal in BP monitoring were developed in past where a threshold based estimation approach is proposed in [4] for PLI noise elimination. The approach developed a correlative method in minimizing the distortion using spectral energy variation among the normal and effective signal. In [7,8] a wavelet based estimation is proposed based on threshold approach where the signal is processed based on wavelet coefficients and measured threshold value. The correlation performs an elimination of the distortion effect based compared threshold. However it has an elimination of required signal coefficient as well. To eliminate the effect a K-NN based approach was presented in [9]. Varying window of filtration for signal processing is outlined in [10]. The Hilbert transformation approach is developed in signal processing for varying interference. Feature detection based on normalized multi wavelet measure is outlined in [11]. The approach developed evaluate based on Euclidian distance. A simple

segmentation approach for signal processing is outlined in [12], where multiple features based on spectral representation is outlined. The approach works on the geographical feature is presented. A time based estimation where the time parameter of magnitude is outlined in [13, 14]. This approach is developed for a temporal sequence where time based features are used in deriving the observations for the determination of the peak parameter as feature values. The denoising based on DWT is developed based on frequency spectral decomposition and the range of frequency value is considered as the noised element wherein a standard deviation and mean of peak is considered for denoising. However, the decision is developed based on threshold value. The elimination of coefficient has an impact on accuracy of estimation hence threshold valuation is a critical issue. Wherein threshold is measured with discrete monitoring, time line observation could improve the accuracy of threshold detection and denoising efficiency. It is observed that sampling of signal for processing result in jitter [15-18] which are short period variation with different frequency component, which limits the DWT based denoising approach. The assumption of frequency range elimination for denoising leads to information loss and appropriate selection of coefficient could improve the accuracy. We propose to develop a new denoising approach to signal processing by developing time line processing and analysis for threshold computation. Secondly, we propose to integrate the DWT based approach with standard deviation and mean of peak over decomposed Time line (TL) to improve denoising performance. Towards developing a filtration of processing signal for distortion minimization in this work a time line approach for signal denoising using spectral decomposition and spectral correlation is outlined.

Machine Learning and Deep Learning is becoming increasingly popular in health informatics [21], [23-24], [27-29] [31]. Further Compute-Intensive Large Scale Servers and Cloud Storage could optimize the effectiveness in terms of storage and transmission which will be secure for such data systems in future development efforts [19], [20], [22], [25].

### III. PHOTOPLETHYSMOGRAPHY (PPG) SIGNAL ANALYSIS FOR BP STRATIFICATION

Blood pressure is an important physiological parameter in the human body and it is critical indicator of clinical condition in both emergency situations and daily health care basis. In modern society of rich living, high blood pressure is constantly increasing. At the same time, people are more cautious about their health. Blood pressure (BP) is a force in the bloodstream flowing in the blood vessels and chambers of the heart. It is measured as the amount of blood flow in the arterial arteries, which is the main blood vessel that transmits blood from the heart. BP of a person is usually measured as a systolic pressure due to contraction cycle of the heart and as a diastolic pressure during its relaxation state. Average values of healthy people at systole read 80 mm of Hg and 120 mm of Hg diastole at stable condition [1]. Some factors that affect a person's blood pressure are pumping rates, hypertension, immune suppression, and blocks in respiratory airways. Because of various reasons, the average blood pressure is different from each individual. Blood pressure is categorized into five main scope-based on measured values as shown in Table I.

TABLE I. CATEGORIES OF BLOOD PRESSURE [1]

Category	Systolic (mmHg)	Diastolic (mmHG)
Hypotension	<90	<60
Normal	90-120	60-80
Prehypertension	121-139	Or 81-89
Stage 1 Hypertension	140-159	Or 90-99
Stage 2 Hypertension	>160	Or =100

According to the Seventh Report of the Joint National Committee for Prevention, Detection, Evaluation, and High Blood Pressure, hypertension is an elevated blood pressure, which leads to vascular damages of internal organs. It is considered to be a critical issue, as most of the patients do not realize the symptoms of the elevated blood pressure. Hypotension refers to a state of low blood pressure due to inadequate supply of blood to other organs in the body. The drop in blood pressure consequently results in heart attacks, strokes, kidney failure and other more serious complications. The monitoring of cuff less blood pressure is hence a prime need in current health monitoring approach. Blood pressures are monitored via different bio-signals such as ECG, PPG, etc. In our previous work we have developed a Hybrid framework for BP estimation utilizing both ECG and PPG signals [30]. However, the approach of representative features and the quality of signal plays a vital role in making decision. The analysis of PPG is observed to be more effective in BP monitoring due to confined feature representation. In processing of PPG signal, the electrical distortions are the major concern. The distortion has a greater impact in the accuracy of decision and hence need to be removed to the finest level. In PPG signal processing, the 50-60 Hz power line noise are one major source of distortion. This noise is observed stationary and majorly observed in the signal processing. The baseline distortion is considered to be due to respiration artifact is observed to be of low-frequency and the component is effective in time domain due to saturation of analog component in the processing system. The high frequency components are observed to be due to muscular movement in the body. Filtration of such artifacts is of primal need in processing of bio-signal to highest accuracy. Wavelet based spectra coding were observed in recent past for the filtration of noise component and need a finer processing for filtration. The approach of DWT based processing decompose the signal into finer TLs where a low range frequency of 0-0.25 Hz referring to baseline and a higher frequency range of 20-500Hz reflect to power line harmonic and muscular based artifact where zero coefficient are removed. The decomposed coefficient is processed to denoising based on threshold approach. The deviation is measured based on mean peak value used for denoising. The representation of PPG signal is illustrated in "Fig. 1".

The process of Bio-signal processing for BP Stratification is developed in three steps of operations:

- 1) Preprocessing.
- 2) Feature extraction.
- 3) Learning and Decision system.

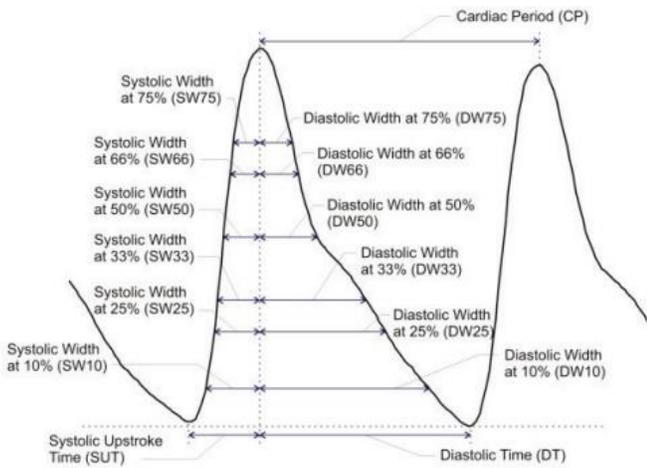


Fig. 1. PPG Signal Representation [3].

Preprocessing is developed for elimination of noise and artifacts in signal captured. In recent, DWT based approach was presented with a specified low and high frequency range for noise suppression. A standard deviation and mean peak based denoising is presented in [1]. Denoising is developed based on threshold limits. The limiting threshold is developed based on discrete magnitude monitoring, which is limited for usage for randomly varying time variant distortions. The sampling process adds jitter noise to the processing signal. The issue of discrete monitoring is focused and a new estimation approach based on time line observation is proposed. This approach develops a denoising threshold based on set of coefficients for a time interval. The process of denoising based on fixed cutoff approach is proposed to improve by a time line monitoring of standard deviation and peak (valley) for decomposed sub frequency bands. The noise parameter is developed for jitter analysis and harmonic content are observed in the processing signal. The decomposed signal is processed with a varying of frequency component is directly extracted and correlated using distortion minimization using spectral coding. The signal analysis is developed for the selection of a spectral power density using correlation approach. The derivative component of the filtration approach is processed for noise reduction in consider to lower magnitude value based on the deviation of the distortion in the signal processing. The processing of signal is divided into decomposed bands which eliminate the basic frequency for the process of no DC component. The process is developed based on the decomposition of processing signal into finer frequency bands and performs an extreme spectral selection. The process of decomposition for a given processing signal  $S(t)$  is represented by the spectral resolution ( $\varphi$ ) and the residual component  $res[i]$  is presented by,

$$S[t] = \sum_{i=1}^K \varphi_j[i] + res[i] \quad (1)$$

The processing bio-signal is recorded as a set of 3 channels data, where the 1st channel represents the PPG signal, 2nd signal represents the arterial blood pressure (ABP), and the 3rd channel represented the ECG signal of monitoring signal. Wherein channel 1 and 3 are the monitoring signal, channel 2

is taken as the baseline representation of the BP signal. In evaluation of the denoising process in this work, 2nd channel signal (ABP) is processed with varying noise levels to evaluate the efficiency of proposed approach. The baseline reference of ABP presents the level of analysis with the noised signal. The proposed approach of spectral correlation filtration approach for the Bio-signal in BP stratification is presented in next section. More noisy situations restricts the real time use of many such and similar systems [26].

#### IV. SELECTIVE TIME LINE SPECTRAL CORRELATIVE PROCESSING (TLSC)

This proposed approach focus in improving the denoising performance by minimizing the interference level and improving the details of representation. The spectral band extraction in time-frequency domain is proposed to represent physiological parameters and spectral parameters for denoising signal. A feature representation and classification process is used as an integral module for learning and decision making. The proposed processing system is for signal conditioning is illustrated in “Fig. 2”.

##### A. Spectral Decomposition Coding

The signal analysis of the processing signal is performed based on the spectral decomposition and correlation process where the following two process were performed,

- 1) Extreme bands decomposition is developed with the successive decomposition of signal using cascaded filters.
- 2) Selecting local minima parameter for noised component based on local maxima of spectral density in spectral bands.

The process of filtration is developed with the normalization of processing signal based on mean parameter given as,

$$m_1 = S(t) - mn_1 \quad (2)$$

The mean normalized signal set the processing signal to mean level, and random glitches are truncated to a mean reference. This normalized signal is then processed for spectral decomposition in denoising operation. The process of denoising is performed using a cascaded filter bank as shown in “Fig. 3”.

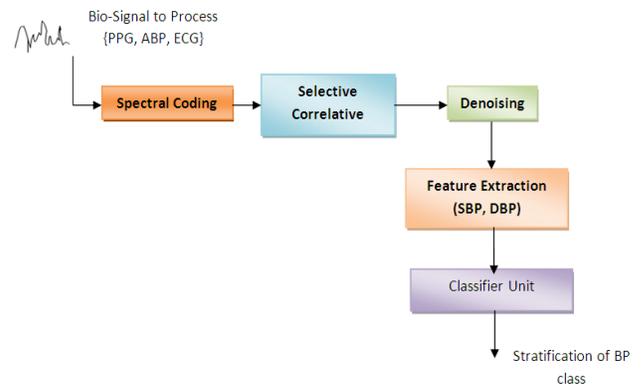


Fig. 2. Proposed Systems for Signal Analysis.

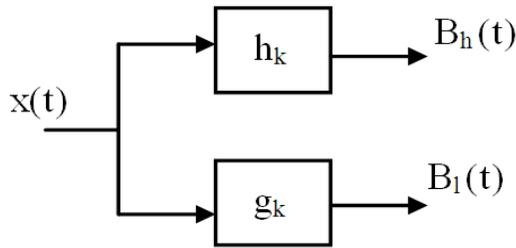


Fig. 3. Decomposition Filter Bank Structure.

The processing signal is represented as in “Fig. 4”,

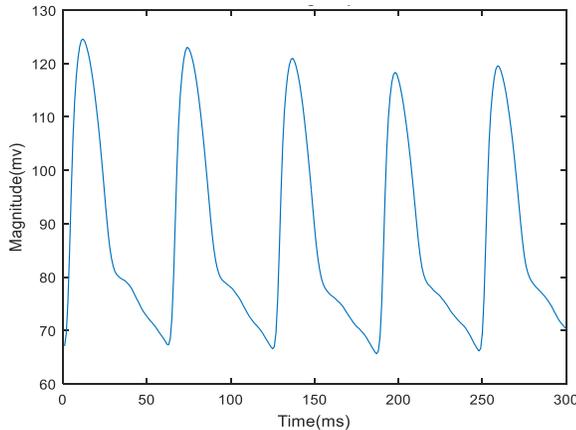


Fig. 4. An ABP Signal Plot for Processing.

The monitoring input to the Decision system is given by the spectral feature developed by band decomposition. A successive integration of filter banks results in a decomposition of signal into finer frequency band. For the realization of such filtration a wavelet based filtration is used. In the process of spectral decomposition approach, successive filter bank architecture is used as shown in “Fig. 5”.

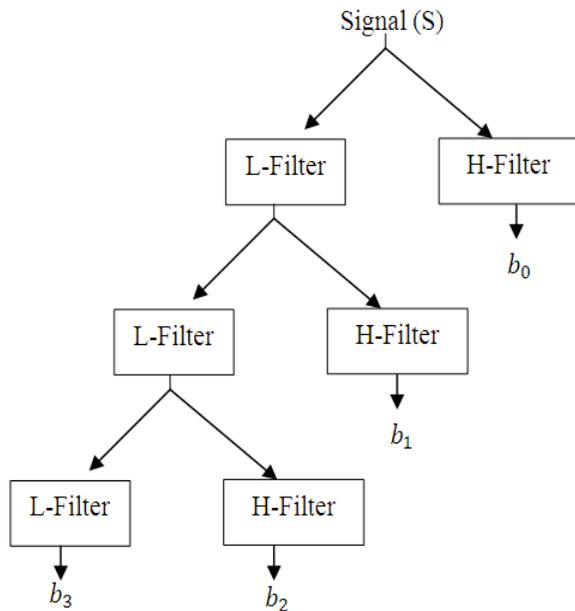


Fig. 5. Hierarchical Filtration Structure for Band Decomposition.

### B. Spectral Correlative Denoising Approach

For spectral denoising each of the signal (S) is processed for B-Bands decomposition which represent a set of decomposed bands  $\{b_0, b_1, b_3 \dots \dots b_n\}$  given as,

$$B = \{b_0, b_1, b_3 \dots \dots b_n\} \in S \quad (3)$$

The filtration of the noise component is developed by the convolution operation of given signal with the selected filtered signal F,

$$B = \text{conv}(S, F) \quad (4)$$

The High pass (HP) and low pass (LP) filter are developed as FIR filter giving the spectral variation of the observing parameter. Information's lower than the threshold is neglected. In this approach by the acquisition of vital parameter coding and normalization process is proposed. The acquisition process converts the vital parameter information into a 1-D plane. The resultant information is then processed for extracting the features based on Wavelet coding. This suggested method improves the selection of feature relevancy, in terms of selectivity. Since, now features are selected based on variation density rather than magnitudes. For the acquisition of the spectral coding curve, a linear sum of the entire vital parameter plane at different Gaussian smoothing factor is taken.

Each decompose band mean spectral density (MSD) is computed given by,

$$MSD = \frac{\sum_{i=1}^n |B^2|}{n} \quad (5)$$

B is the decomposed band for a signal S which reflect the measured parameter for a period 't'.

For each of the band decomposed is given by,

$$MSD(i), \text{ for } i = 1 \text{ to } n. \quad (6)$$

Where n defines the number of decompositions.

For derived MSDi, the maximum MSD is given as,

$$MxPi = \max(MSDi) \quad (7)$$

For  $i=1$  to  $n$

if  $(MSDi \geq (MxPi / 2))$

$sel\_Bi = Bi,$

End

The selected SBSs, 'sel\_Bi' are only considered in processing where other bands are suppressed to zero. An inverse filtration operation with selected band and other band valued to zero is performed using convolution and successive addition process. This process results in de-noised signal with maximum information's suppressing noise distortion.

### V. SIMULATION RESULT

For the Stratification of Blood Pressure using signal processing, a correlative spectral approach is presented. Wherein the existing approach operates on discrete coordinates and a correlation with the threshold is used in decision, the discrete value can be biased due to miss-operation of sensor, or

measuring devices which effect the decision. Hence, a time line continuous monitoring in time-frequency domain result in more decision accuracy compared to discrete monitoring. It is observed that each of the observation has a systolic, Diastolic parameter which is time variant. In the developed approach the processing signal ABP is extracted from the 3 recorded channel and channel 2 is used for the noised component filtration analysis. The processing signal with Gaussian distortion have variance (var)=0.01 is shown in “Fig. 6”.

The noised signal is represented to decomposed sub band which is carried out using ‘db4’ wavelet decomposition to compute the spectral band (SBSs). The 5 sub bands extracted from the processing signal is shown in “Fig. 7”.

The MSD parameter for 4 detail SBSs and 1 residual SBS is illustrate in “Fig. 8”. The decomposed bands are processed for selection based on the magnitudes of these bands.

The representation of correlation of spectral bands with the decomposed band is illustrated in “Fig. 9”. The band with a maximum MSD is selected with other band suppressed to zero.

The inverse process of selected band with other zero suppressed in inverse filtered and successive added to produce de-noised signal. Obtained de-noised signal is shown in “Fig. 10”.

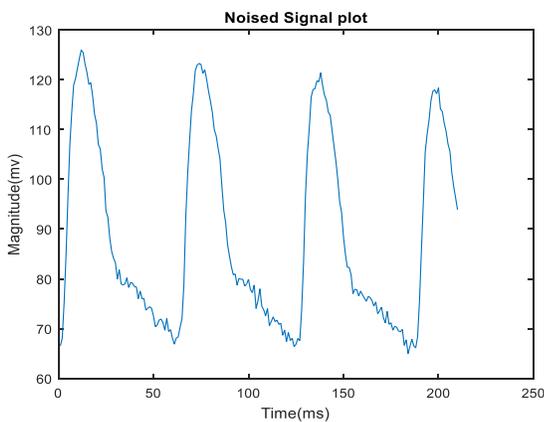


Fig. 6. Noised Signal with Variance (var=0.01).

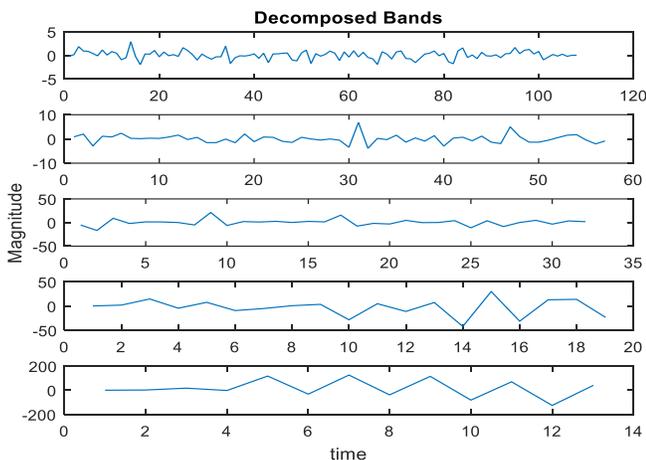


Fig. 7. SBSs Extracted from Processing Signal for Analysis.

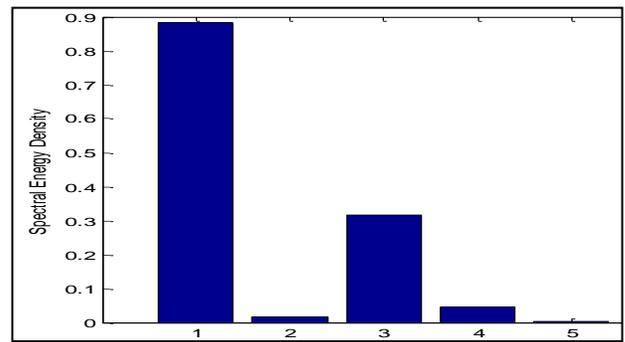


Fig. 8. MSD for the Spectral Bands Decomposed.

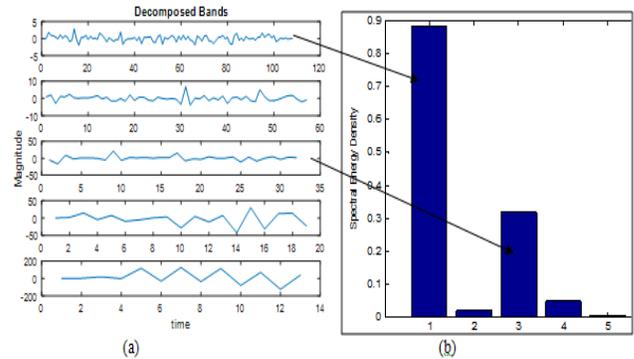


Fig. 9. (a) SBS for the Signal (b) MSD Correlation.

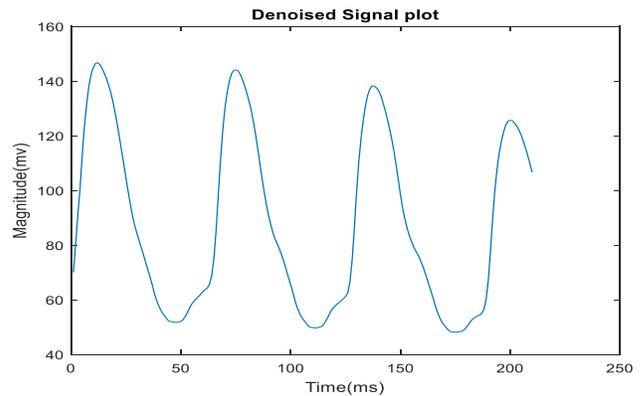


Fig. 10. De-noised Signal.

The de-noised signal is processed for feature extraction where the two extremes SBP and DBP is measured. The detected SBP and DBP detected for the de-noised signal is shown in “Fig. 11”.

The decision system process on the computed DBP and SBP for a period of observation and an average majority of the BP stratification as derived from the condition listed in Table I is made. The decision system generates an alert for the decision made as shown in “Fig. 12”.

A test of 10 iterations with varying Variance value from 0 to 10 is performed. The decision is monitored and an average accuracy is computed. The denoising efficiency is measured by an average Means square error (MSE), Peak signal to noise ratio (PSNR) and Root mean square error (RMSE) values.

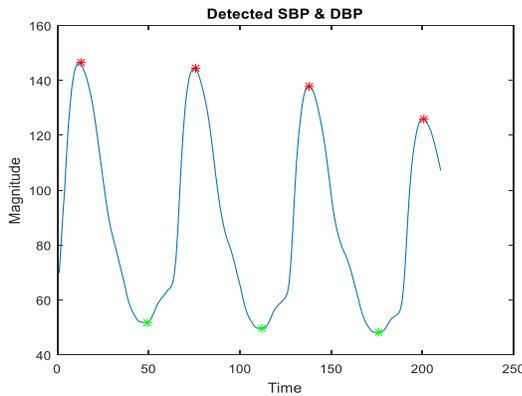


Fig. 11. Detected Peak Points for Decision.

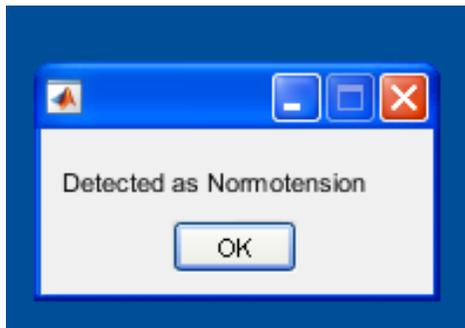


Fig. 12. Detected effect for Test Signal.

The average accuracy is computed given by,

$$Avg Acc = \frac{\text{majority of class detected}}{\text{Total Number of test conducted}} \quad (8)$$

The mean square error is given by,

$$MSE = \frac{\sum_{i=1}^n (x-x')^2}{n} \quad (9)$$

Where  $x$  is the actual signal processing and  $x'$  is the de-noised coefficient.

PSNR is given by,

$$PSNR = \log_{10} \frac{\text{peak}(x')}{\text{peak}(x)} \quad (10)$$

and RMSE is given by,

$$RMSE = \sqrt{MSE} \quad (11)$$

Observations for the developed approach TLSC is compared with the existing approach of temporal spectral coding (SR) [32], and multi information fusion with neural Network (MIF-NN) [1]. The observation of the developed approaches for denoising for different test samples is presented in Table II.

The test observations developed for different test sample illustrates an enhancement of PSNR by 16dB and 5.4dB in comparison to SR and MIF-NN method respectively. The time line coding of signal denoising eliminate distortion using a period of observation, wherein a discrete observation generate filtration for a observing coefficients only which has lower filtration performance; more effective denoising results into an

accurate signal representation. This result into improve the accuracy of detection. The performance of detection for the developed approaches is listed in Table III.

TABLE II. OBSERVATION FOR THE DEVELOPED APPROACH BASED ON TIME LINE SELECTIVE APPROACH

Test sample	Method	MSE	PSNR(dB)	RMSE	Time(Sec)
S1	SR	6.3076	34.9088	2.5115	0.156
	MIF-NN	1.3557	45.4041	1.1643	0.031
	TLSC	1.3821	50.8703	1.1756	0.015
S2	SR	6.2818	34.4641	2.5064	0.175
	MIF -NN	1.3553	45.4121	1.1642	0.029
	TLSC	1.3821	50.8703	1.1756	0.019
S3	SR	6.2378	34.7783	2.4976	0.168
	MIF -NN	1.3557	45.2999	1.1643	0.023
	TLSC	1.3821	50.8703	1.1756	0.011
S4	SR	6.2228	34.3509	2.4945	0.177
	MIF -NN	1.3560	45.4179	1.1645	0.029
	TLSC	1.3821	50.8703	1.1756	0.016

TABLE III. ACCURACY OF DETECTION FOR THE DEVELOPED SYSTEMS

Method of detection	Accuracy (%)
SR	83.25
MIF-NN	91.33
TLSC	94.34

The detection of BP parameters for the estimation accuracy is observed to 94.34% for the proposed time line processing, wherein the existing approach of SR [32] and MIF-NN [1] has 83.25 and 91.33% respectively. A more accurate signal denoising results to an improvement of detection of SBP and DBP parameters improve decision accuracy.

“Fig. 13” shows the Observation for MSE for the proposed method. It outperforms the SR method and is almost as good as MIF-NN method.

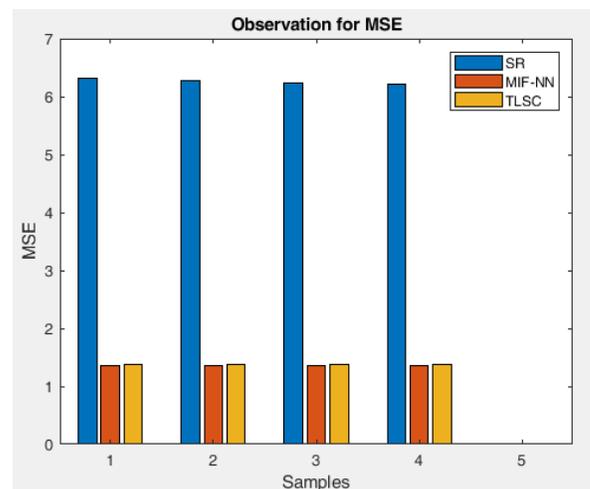


Fig. 13. Observation for MSE Plot.

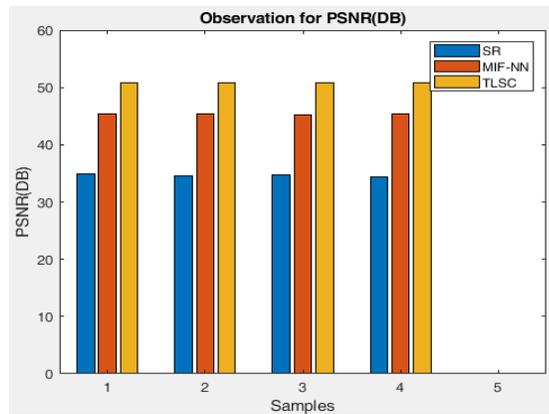


Fig. 14. Observation for PSNR(DB) Plot.

“Fig. 14” shows the Observation for PSNR(DB) plot for the proposed method. The proposed method demonstrates good PSNR values compared with the existing approaches.

“Fig. 15” shows the Observation for RMSE for the proposed method. It outperforms the SR method and is almost as good as MIF-NN method.

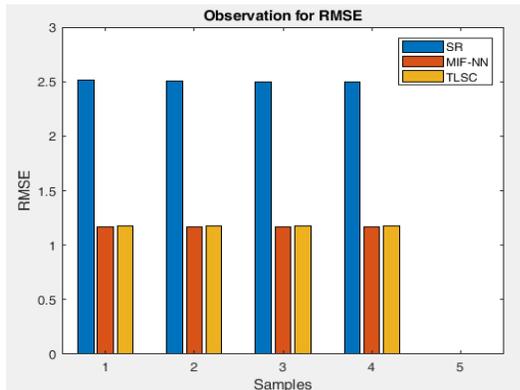


Fig. 15. Observation for RMSE Plot.

## VI. DISCUSSION AND FUTURE WORK

Cuff-Less BP Stratification has gained enormous attention in recent years due to its potential possibility of highly accurate, convenient to use and continuous nature of measurement. However, the accuracy of such measurements largely depends on the quality of captured Vital Bio-Signals used for stratification. Most of the signals are noisy and can lead to problems in BP Stratification. Existing signal denoising and normalization techniques are mostly discarding the wavelet coefficient values above a given threshold, discrete in nature and somewhat lossy. The proposed method in this paper namely Time line correlative spectral processing has demonstrated good results in terms of PSNR values as depicted in the results. It has outperformed the SR and MIF-NN techniques. This will in turn motivate to use this method in practical medical setups for Signal acquisition, filtering and for BP Stratification.

In future we will be using the Time line correlative spectral processing approach for more accurate BP Estimation by processing the PPG Signals by means of optimal feature

extraction, selection and application and invention of efficient machine learning algorithm; also to build a temporal dataset of continuous BP measurements and apply big data analytics for more scientific explorations of Cardiac diseases patterns and Hypertension.

## VII. CONCLUSION

A spectral coding approach based on correlative spectral density to implement cuff less Stratification of BP measurement is developed. The coefficients are represented as a continuous time series of measured parameter and the signals is decomposed using sub band coding. Each of the sub bands outlines a variation in frequency domain and is further processed for selection using mean spectral density (MSD). The proposed approach performs a selection for the required bands discarding less informative bands. Selected coefficients are processed for the detection of SBP and DBP parameter in Stratification of BP. The proposed approach shows an improvement of 11% in average classification accuracy and 16dB in PSNR for different tested samples.

## ACKNOWLEDGMENT

We would like to acknowledge Dr. Ramesh Pokale, Physician, Sidhhivinayak Clinic, Nira, Dist: Pune, India for providing the necessary medical support and required information from time to time.

## REFERENCES

- [1] Wang, Dingliang, Xuezhi Yang, Xuenan Liu, Shuai Fang, Likun Ma, and Longwei Li. "Photoplethysmography Based Stratification of Blood Pressure Using Multi-Information Fusion Artificial Neural Network." In Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops, pp. 276-277. 2020.
- [2] Y. Liang, Z. Chen, R. Ward, and M. Elgendi, "Photoplethysmography and deep learning: Enhancing hypertension risk stratification". Biosensors, 2018.
- [3] W. Liu, X. Fang, Q. Chen, Y. Li, and T. Li. "Reliability analysis of an integrated device of ECG, PPG and pressure pulse wave for cardiovascular disease". Microelectronics Reliability, 87:183-187, 2018.
- [4] I. Pavlidis, J. Dowdall, N. Sun, C. Puri, J. Fei, and M. Garbey. "Interacting with human physiology". Computer Vis. Image Understand, 108(1):150-170, 2017.
- [5] L. Tarassenko, A. Hann, and D. Young, "Integrated monitoring and analysis for early warning of patient deterioration", British Journal of Anaesthesia, May 17, 2006.
- [6] M. Saeed, M. Villarroel, A. T. Reisner, G. Clifford, L. W. Lehman, G. Moody, T. Heldt, T. H. Kyaw, B. Moody, and R. G. Mark. "Multiparameter intelligent monitoring in intensive care ii: A public-access intensive care unit database". Crit. Care Med., 39:952-960, 2011.
- [7] Y. Kurylyak, F. Lamonaca, and D. Grimaldi, "A neural network-based method for continuous blood pressure estimation from a PPG signal", IEEE International Instrumentation and Measurement Technology Conference, pages 280-283, 2013.
- [8] Alvaro Araujo, Jaime Garcia, Javier Blesa, "Wireless Measurement System for Structural Health Monitoring with High Time Synchronization Accuracy", IEEE Transactions on Instrumentation and Measurement, Vol.61, No.3, March 2012.
- [9] M. S. Somayyeh, F. Mohammad, C. Mostafa, H. Mohammad, M. Maryam, and G. Yadollah. "Blood pressure estimation from appropriate and inappropriate PPG signals using a whole-based method". Biomedical Signal Processing and Control, 47:196-206, 2019.
- [10] Alumona T.L, Idigo V.E, and Nnoli, "Remote monitoring of patients health using wireless sensor networks", IPASJ International Journal of Electronics and Communication, vol.2, pp 90-95, Issue 9, September 2014.

- [11] P. Su, X. R. Ding, Y. T. Zhang, J. Liu, F. Miao, and N. Zhao., "Long-term blood pressure prediction with deep recurrent neural networks". In Proceedings of the 2018 IEEE EMBS International Conference on Biomedical and Health Informatics, pages 323–328, 2018.
- [12] Abdelhamid.S Mohamed.S and Ajith Abraham, "A review of ambient intelligence assisted health care monitoring",Computer Information Systems and Industrial Management Applications, Vol.5. pp. 741-750, 2013.
- [13] Nakamura Masayuki, Nakamura Jiro, Lopez Guillaume., "Collaborative processing of wearable and ambient sensor system for blood pressure monitoring", Sensors Journal, ISSN 1424- 8220, June 2011.
- [14] Shahina Begum, Shaibal Barua and Mobyen Uddin Ahmed, "Physiological sensor signals classification for health care using sensor data fusion and case base reasoning", Sensors Journal, 2014.
- [15] Chen Xijun, Max Q-H Meng, Ren Hongliang, "Design of sensor node platform for wireless biomedical sensor networks", Proceedings of IEEE, 2005.
- [16] A. Visvanathan, A. Sinha, and A. Pal., "Estimation of blood pressure levels from reflective photoplethysmograph using smart phones". IEEE 13th International Conference on Bioinformatics and Bioengineering, 2013.
- [17] Tarassenko L, Hann A, Patterson A., "BioSign: multiparameter monitoring for early warning of patient deterioration", Proc 3rd IEEE international Seminar on Medical Applications of Signal Processing, 2005.
- [18] L. Wang, W. Zhou, Y. Xing, and X. Zhou. , "A novel neural network model for blood pressure estimation using photoplethysmography without electrocardiogram, "Journal of Healthcare Engineering", 2018:1–9, 2018.
- [19] Mane, P.M., Sheela Rani, C.M., High data availability with effective data integrity and user revocation using abe scheme for cloud storage, International Journal of Innovative Technology and Exploring Engineering, 2019.
- [20] Mane, S.U., Narsinga Rao, M.R., Large-scale compute-intensive constrained optimization problems: GPGPU-based approach, Advances in Intelligent Systems and Computing,2019.
- [21] Meghana, P., Sagar Imambi, S., Sivateja, P., Sairam, K., international Journal of Innovative Technology and Exploring Engineering, Image recognition for automatic number plate surveillance, 2019.
- [22] Kumar, S.A., Vidyullatha, P., A comparative analysis of parallel and distributed FSM approaches on large-scale graph data, International Journal of Recent Technology and Engineering,2019.
- [23] Sai Meghana, S., Amulya, P., Manisha, A., Rajarajeswari, P., A deep learning approach for brain tumor segmentation using convolution neural network, International Journal of Scientific and Technology Research, 2019.
- [24] Sajana, T., Sai Krishna, K., Dinakar, G., Rajdeep, H. Classifying diabetic retinopathy using deep learning architecture, International Journal of Innovative Technology and Exploring Engineering,2019.
- [25] Balaraju, J., Prasada Rao, P.V.R.D., Innovative Secure Authentication Interface for Hadoop Cluster Using DNA Cryptography: A Practical Study, Advances in Intelligent Systems and Computing,2020.
- [26] Roshini, A., Kiran, K.V.D., Challenges in physiological signal extraction from cognitive radio wireless body area networks for emotion recognition, Advances in Intelligent Systems and Computing,2020.
- [27] Sandhya S Waghare , PothuRaju RajaRajeswari, Design and Implementation of System which efficiently retrieve useful data for Detection of Dementia Disease SPRINGER 2021.
- [28] Somase, K.P., Imambi, S.S., Develop and implement unsupervised learning through hybrid FFPA clustering in large-scale datasets, Soft Computing,2021.
- [29] Anisha, P.R., Vijaya Babu, B., CEBPS: Cluster based effective breast cancer prediction system, International Journal of Recent Technology and Engineering,2019.
- [30] Santosh A. Shinde, Dr. P. Raja Rajeswari, "A Novel Hybrid Framework for Cuff-Less Blood Pressure Estimation based On Vital Bio Signals processing using Machine Learning," International Journal of Advanced Trends in Computer Science and Engineering, Vol.9, Issue 2, March-April 2020, pp. 1556-1561.
- [31] Ms.Bhandare Trupti Vasantrao, Dr. Selvarani Rangasamy, "Review on Heart Disease Diagnosis Using Deep Learning Methods," International Journal of Next-Generation Computing - Special Issue, Vol. 12, No. 2, April 2021, pp. 91-102.
- [32] Sundar, Aditya, Vivek Pahwa, Chinmay Das, Mukund Deshmukh, and Neethu Robinson. "A comprehensive assessment of the performance of modern algorithms for enhancement of digital volume pulse signals." International Journal of Pharma Medicine and Biological Sciences 5, No. 1, 2016.

# SMAD: Text Classification of Arabic Social Media Dataset for News Sources

Amira M. Gaber<sup>1</sup>, Mohamed Nour El-din<sup>2</sup>, Hanan Moussa<sup>3</sup>

Information System Department, Faculty of Computer and Artificial Intelligence, Cairo University, Giza, Egypt<sup>1, 2, 3</sup>  
Higher Institute of Computer Science and Information Systems, Culture and Science City Academy, 6 October-Giza-Egypt<sup>1</sup>

**Abstract**—Due to the advances in technology, social media has become the most popular means for the propagation of news. Many news items are published on social media like Facebook, Twitter, Instagram, etc. but are not categorized into various different domains, such as politics, education, finance, art, sports, and health. Thus, text classification is needed to classify the news into different domains to reduce the huge amount of news available over social media, reduce time and effort for recognizing the category or domain, and present data to improve the searching process. Most existing datasets don't follow pre-processing and filtering processes and aren't organized based on classification standards to be ready for use. Thus, the Arabic Natural Processing Language (ANLP) phases will be used to pre-process, normalize, and categorize the news into the right domain. This paper proposes an Arabic Social Media Dataset (SMAD) for text classification purposes over the social media using ANLP steps. The SMAD dataset consists of 15,240 Arabic news items categorized over the Facebook social network. The experimental results illustrate that the SMAD corpus gives accuracy of about 98% in five domains (Art, Education, Health, Politics, and Sport). The SMAD dataset has been trained tested and is ready for use.

**Keywords**—Text classification; Arabic text classification; Arabic Natural Language Processing (ANLP)

## I. INTRODUCTION

Recently, the news media has transformed from hardcopy like newspapers, radios, and magazines to digital forms integrated with the internet to organize social media platforms like Facebook, Twitter, blogs, channels, and other digital media formats. Online social media has become a great way to connect people with each other around the whole world. Users of social media share news, communicate with other people, and create more posts and tweets related to the news than they consume. Consequently, a huge amount of incredible news is created and propagated through social media, which has a serious impact on society and individuals. Various social media needed to categorize their news into different domains, like politics, education, finance, art, sports, and health. So text classification is used to reduce the huge amount of news available over the social media. It is useful for reducing time and effort for recognizing the category or domain, and the data will be pretreated to improve the searching process and performance of classification.

The online news published on social media propagates over the network in different languages and formats, such as texts, images, videos, and unstructured formats. It is difficult to detect and classify the news and check its veracity, especially in the Arabic language, where it needs human expertise.

However, Arabic Natural Language Processing (ANLP) are computational techniques that can be used for identifying the reality of text news based on facts and handling the Arabic language.

### A. Arabic Language

This work concentrates on Arabic language news. The Arabic language is one of the greatest languages in the world. As this language possesses special spelling, grammatical rules, and punctuation marks. However, the text classification for this language is a challenging task because its structural essentials are complex. In the Arabic language, the text consists of some features which can be classified into external or internal features. The external features do not relate to the content of the text document which includes the author name, publication date, publishing house, etc. In contrast, the internal features relate to the text content and its linguistics features including lexical words and grammatical characteristics [1]. As a result, the following is the characteristics of the Arabic language structure and should be treated and deal with them to classify the news into the correct domain:

- The direction of Arabic language reading and writing from right to left.
- This language possesses 28 letters and there aren't any upper-case letters
- Arabic pronouns can be a singular, dual, or plural; masculine or feminine pronoun.
- Has three grammatical cases: nominative, accusative, and genitive.
- Words are classified into three main parts of speech, nouns, verbs, and particles.
- Nouns include adjectives and adverbs.
- Arabic verbs can have suffixes that change the overall meaning or the tense of the word.
- All verbs and some nouns have morphological rules.
- Arabic sentence can be a noun phrase or verbose phrase in which the verb can be passive.
- The subject pronouns may be removed from the sentence [1] [4].

## B. Arabic Natural Processing Language (ANLP)

Most researchers tend to do and implement a set of tools that can be used in Arabic Natural Language Processing (ANLP) to help in the preparations for the processing structure for it. Because the Arabic language is the widest language due to the number of users using it and according to research introduced in 2015, it is the mother tongue of over 300 million people [2].

There are various developing tools and applications like tokenizers, Part of Speech (POS), Bag of Words (BOW), sentence segmentation, syntactic parsers, Matchers, etc. and various approaches are used for classification such as:

- Lexicon-based approach: The concerned data will be classified into a class or more based on linguistic rules (lexicon-based).
- Machine learning (ML) approach: The classification processes can be supervised, or unsupervised, or semi-supervised learnings. The seven stages of ML classification shown in Fig. 1.
- Hybrid approach: The classification integrates between the rule-based approaches besides the ML-based approach to achieve the optimum performance [3].

This paper presents SMAD dataset, a new Arabic social media dataset built across Facebook social media for news sources using the hybrid approach ANLP standard classification to cover five different domains (Sports, Arts, Health, Education and Political) domains. In addition, several algorithms in the ML approach will be used to help the classification with the principle of ANLP to reach high accuracy classification. The KNN algorithm will be used as a classifier. After the data was assembled and organized, the pre-processing methods and filtering are applied to make the data ready using ANLP.

This paper is organized as follows. Section II introduces the related work for the existing Arabic corpus. Section III presents the text classification methodology. Section IV presents the applied methodology that shows the formation of SMAD corpus, Section V displays the experiment results. Section VI will discuss the proposed methodology with others. Finally, Section VII concludes this work.

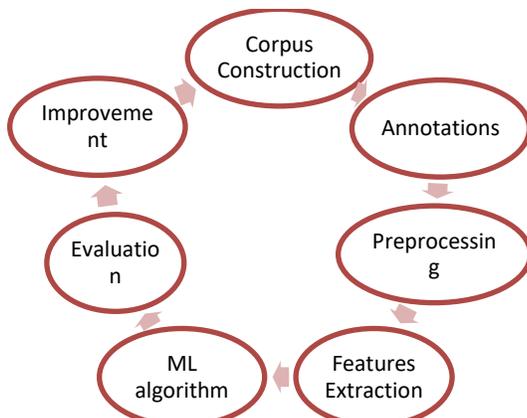


Fig. 1. Arabic Natural Language Processing (ANLP) Stages.

## II. RELATED WORK

There are several studies categorize the text and build datasets tested against the quality measurement metrics. Riyad et al. [4], proposed an Arabic text classifier based on the Document Frequency threshold (DF) besides the Support Vector Machines (SVM) algorithm with a precision of 0.95. The datasets were collected from various Arabic newspaper online websites like Al-Jazeera, Al-Hayat, Al-Ahram, Al-Nahar, and Al-Dostor.

Syiam et al. [5], proposed a new Arabic text classification depending on a Hybrid approach of document frequency. Egyptian newspapers like El-Ahram, El-Akhbar, and El-Gomhoria were used to collect datasets. The used classifiers are the Key Nearest Neighbor (KNN) and Rocchio the classifier performance accuracy was 0.98.

Harrag et al. [6], performed a classification in which data collected from the Arabian scientific encyclopedia. They used the decision tree algorithm with an accuracy of 0.93.

Chantar and Corne [7], applied the Particle Swarm Optimization (PSO) Algorithm with Support Vector Machin (SVM) classifier. Datasets were collected from specialized web sites as Al-Jazeera, Al-Hayat, and Al-Ahram. The result of the classification is more accurate and efficient.

In Saraç and Ayşe Özel [8], they concentrate on web documents they use a Firefly Algorithm and J48 classifier to test data from WebKB and Conference datasets. The applied algorithm returned an accuracy (between 0.56 and 0.93).

Rohaidah et al. [9], introduced a new Sentiment Analysis approach using the k-NN classifier. The dataset was collected from customer review datasets with maximum precision results equal to 0.892.

Guessoum et al. [10], performed a text classification on OSAC3 corpus (Open-Source Arabic Corpora) which was gathered from several different websites (BBC Arabic, CNN Arabic, etc.). It contains 22,429 textual records. Every text document is a part of one of ten separate categories (Economics, History, Religion, Health, Education and Family, Sports, Astronomy, Law, Stories, and Cooking Recipes).

There are number of Arabic datasets like, DAA [11] is a dataset in which nine categories have been processed and standardized with 400 documents for each category, Akhbar-Alkhaleej [12] is a popular Arabic Dataset with 5690 Arabic news documents gathered regularly from the online newspaper "Akhbar-Alkhaleej". It consists of five categories: Alwatan [13] is an Arabic Dataset with 20,291 Arabic news documents collected regularly from its online newspaper, Al-Jazeera-News [14] Arabic Dataset (Alj-News) is an Arabic dataset with 1500 documents. It consists of five categories (Sport, Economy, Science, Politics, and Art), NADA, [11] is an Arabic dataset consists of two corpora OSAC and DAA it used a s (Dewey Decimal Classification scheme (DDC) and Synthetic Minority Over-Sampling Technique (SMOKE) to reprocess and filtering to enhance the results to reach high accuracy.

All previous work concentrated on how to classify the articles using different classifiers which collected its precision and accuracy measurements. All Arabic datasets collected data

from web sources and didn't take into consideration the sources of the news collected from the social media sources. This paper will construct a new dataset collected from different news websites (BBC Arabic, Al-Watan, El-youm7, etc.) to classify the news over the Facebook social media because it is a widest mean for spreading news using the text classification methodology for the Arabic Natural Language Processing (ANLP).

### III. TEXT CLASSIFICATION METHODOLOGY

Text classification is a process of retrieving strong meaningful bulk of text [15] then segmenting them into meaningful sentence, topic, words or character for the text analysis [16]. There are many reasons for using text classification. One of the main reasons is the breaking down the text into smaller give more meaning and contrast than the whole document. Another one is the smaller text useful in accessing and analyzing the text.

#### A. Arabic Text Classification Steps

Fig. 2, shows the text classification process steps which are: 1) stemming, which returns back to the root of the word; 2) stop word removal: it removes unnecessary words, 3) Indexing is the process of creating an internal representation of the documents. It consists of three phases: a) Construction, which builds a vector consisting of all the words that appear in the document; b) Term Selection: choose the main words according to some criteria; c) Term Weighting: count how many occurrences the main word appears; 4) classifier construction, which learns the classifier for each category characteristics by training it on a set of documents to classify correctly; 5) Evaluate Classifier Which Apply a test set to check whether the classification process completed correctly or not [5].

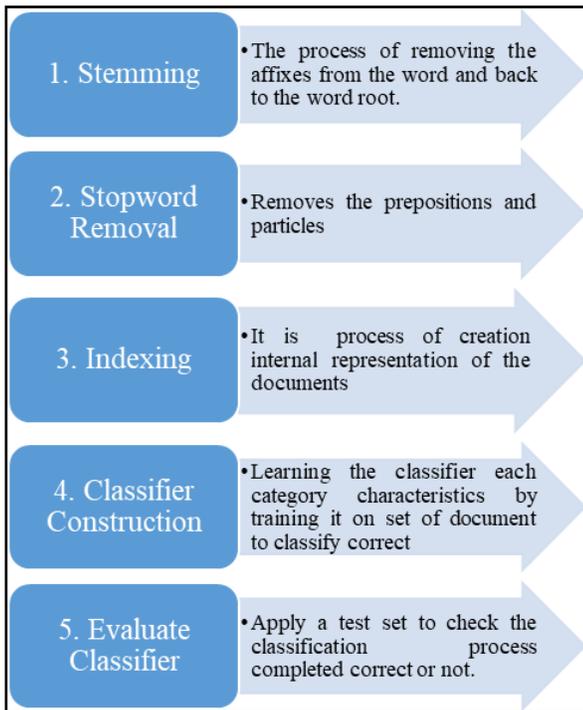


Fig. 2. The Arabic Text Categorization Steps.

### IV. SMAD METHODOLOGY

This work focused on classifying Arabic news into different domains for each news source that published news on Facebook. It can be considered as a new step in classification and detection of content targeted at the Arabic language over Facebook and social media. For this purpose, Arabic Natural Language Processing (ANLP) and machine learning are used, to achieve this purpose. Fig. 3 shows the phases of SMAD formation methodology.



Fig. 3. SMAD Methodology Phases.

#### A. Dataset Collection Phase

Data collection step it is a crucial step to gather the information of the research and it is accuracy depend it for all rest of steps [17]. In this step, the SMAD dataset will be collected. It is new corpora dataset consist of 15,240 textual topic of news collected from (BBC Arabic, Al-Watan, El-youm7, etc.) websites scrapped for five domains: Sports, Art, Education, Health and Political with size 2MB. For our study, the randomly train data about 2000 textual topics in different domain for training phase and about approximately 1000 textual topics news items extracted from Facebook social media for testing phase.

#### B. Dataset Construction Phase

This phase consists of two steps data preprocessing and indexing step.

1) *Data Pre-processing step using ANLP:* Data preprocessing considered as different transformations applied to the data (data gathered from various sources different in style which are not feasible for the analysis) before introducing it to the classification methodology. Data preprocessing is important to raise the efficiency of machine learning algorithms to put the data into a suitable form for the next processing steps [12] to facilitate the analysis of data. the SMAD methodology will follow steps of Arabic text classification explained in details in Section III:

- The Stemming and stop words removal steps, execute the stemming process which includes the stop word process by using the "Root-Based Stemmer" technique to remove the affixes from the word and back to the word root, matches the root word against a set of suggested 67 patterns that represent most of word forms to reduce the number of words used in the indexing step to get more accurate results and finally executes the stop word removal step which removes the prepositions and particles of the word. Fig. 4 will explain the steps applied in this step.
  - Remove all numbers exists in the text.
  - Splits text into words.



$$\text{Sim}(A,B) = \frac{\sum_{i=1}^r w_{ij} \times w_{ik}}{\sqrt{\sum_{i=1}^r w_{ij}^2} \sqrt{\sum_{i=1}^r w_{ik}^2}} \quad (4)$$

Where A and B are the two vectors constructed to get the similarity between them

,i,k are the text representing A and B.

, r is the number of terms in the feature space .

2) *Evaluate classifier*: All the news of the corpus is collected and handled using new corpus using TF-IDF technique, the number of trained texts used about 2000 news items for each domain and now it needs to input test data for the classifier to categorize news to the appropriate classes. The performance metrics are the best indicators to evaluate the classifier. There are four basic quality metrics of any classifier Precision (P), Recall (R), F-measure, and accuracy.

- Precision: it is the answer of the question; what are the of positive identifications were actually correct?
- Recall: it is the answer of the question, what are the actual positives of the data was identified correctly?
- F-score: is the harmonic mean of Precision and Recall, as precision and recall alone cannot provide the best evaluation of the model.
- Accuracy / classification error: is the performance measure, it is a ratio of correctly predicted observation to the total observations.

To calculate each of these measures, it's should define the following:

- TP (true positive) – the set of news that are in the correct category and are predicted truly.
- TN (true negative) – the set of news that are not in the correct category and are predicted to be in a different category.
- FP (false positive) – the set of news that are in a different category and are predicted to be in the correct category.
- FN (false negative) – the set of news that are in a different category and were predicted false category.

These four performance quality metrics are measured by the following equations [21].

- Precision (p) =  $\frac{T_p}{T_p+F_p}$
- Recall (R) =  $\frac{T_p}{T_p+F_n}$
- F-measure =  $\frac{2PR}{(R+P)}$
- accuracy =  $\frac{T_p+T_n}{T_p+T_p+f_p+f_n}$

## V. EXPERIMENTAL RESULTS

In this section, the evaluation and the performance of the proposed methodology is shown using six real datasets. Section A will present experimental setup details, including dataset construction by using the Arabic text categorization steps, and measure its performance by calculating its accuracy and quality metrics measurements. Section B will present the main results of the accuracy and quality metrics (Recall, precision, and F measure) of the SMAD dataset and then compares the performance improvement of the personalized model, with other similarity metrics for baseline datasets in different domains.

### A. Experimental Setup

Datasets: To evaluate our model, experiments were conducted on 15,240 news items collected from the (BBC Arabic, Al-Watan, El-youm7, etc.) website and Facebook in five domains, like sports, political health, art, politics, and education. The dataset was collected at a size of 2 MG with different files. Each file corresponds to one domain generated as a CSV file. The "SMAD" dataset trained on the 2000 news items and tested on a data benchmark of 1000 news item for each domain using the KNN classifier to classify the news into the correct domain at a specific time. Fig. 6 shows the performance of classifying SMAD through the recall, precision, and F1 measure quality metrics.

The proposed model will be compared with other baseline models on these six datasets compared with the previous Arabic datasets OSAC, DAA, Akhbar-Alkhalee, Aljezera, NADA, and Alwatan corpus used in categorizing domains in the Arabic language w.r.t. the recall, precision, and F1 measure quality metrics.

Fig. 7 shows the comparison of accuracy measurement for all datasets, SMAD corpus gives accuracy of about 98% in five domains while accuracy of 98% while the accuracy of NADA is 93.8792%, accuracy of OSAC is 98.1758%, accuracy of DAA is 80.9087%, accuracy of Alj-News is 93.1%, accuracy of Alwatan is 96.1% and the accuracy of AkhbarAlkhaleej is 88.7%.

### B. Main Results

The performance quality measurements of the proposed model will summarize the key observations and show a detailed comparison for the mentioned Arabic datasets with respect to recall, precision, and F-measures. These performance metrics are specialized in different domains and record the weighted average for each domain in each news source shown in Table I.

### C. Methodology Implementation Architecture

Fig. 8 illustrates the Data Flow Diagram (DFD) of the proposed methodology, which shows how the SMAD dataset implemented in the following steps:

- The news source will generate the news on its web page. Then, it publishes a sample of this news on the Facebook page for the interaction.

- The BOW Scrapper will pre-process posts and extract the bag of words (BOW) to train the classifier to choose the correct domain in the future. This step was completed by using Puppeteer library to scrap Facebook data.
- After the classifier extracted the data and is trained on the BOW, the dataset will be built as a Jason file then transform it into CSV files using unicodescv library.
- To evaluate the dataset, the sklearn.metrics library will be used to calculate the model confusion\_matrix (precision – recall – f-measure) and the accuracy\_score for this classifier.

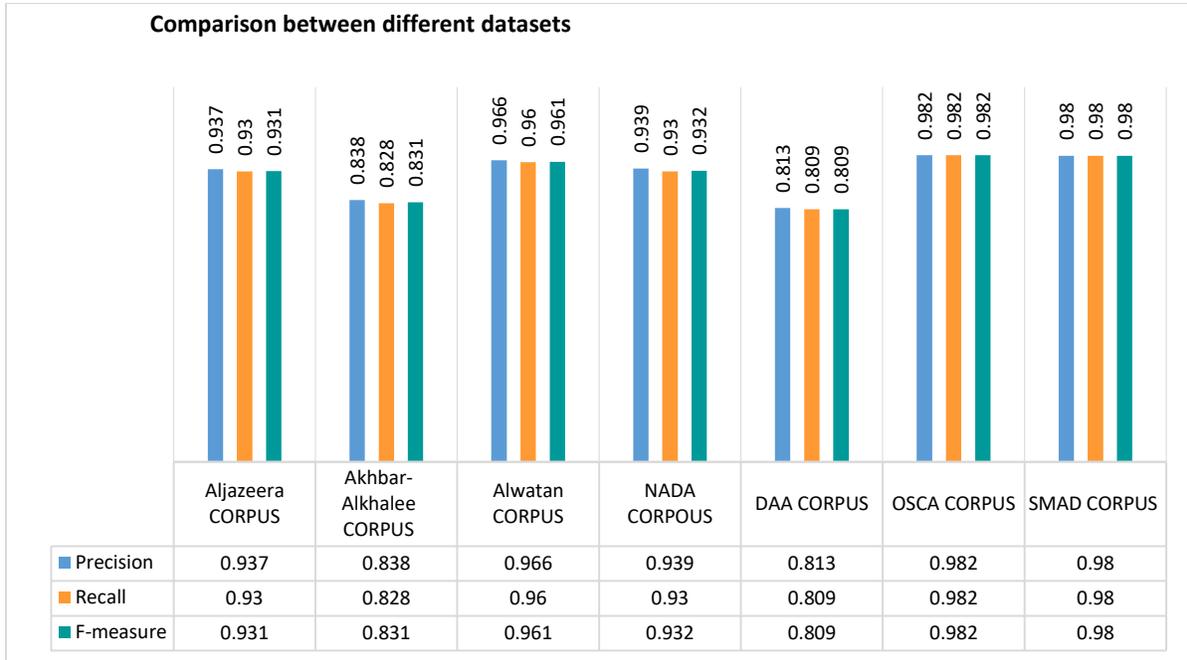


Fig. 6. Performance Quality Metrics Measurements of different Datasets with SMAD Dataset.

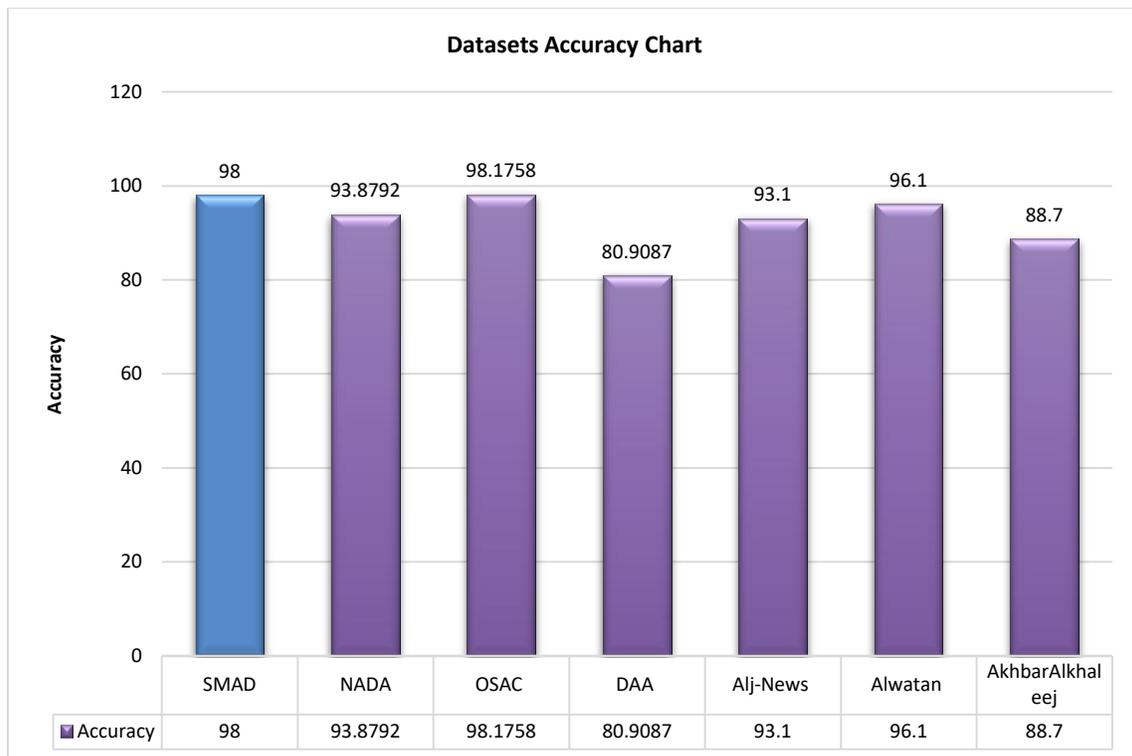


Fig. 7. Accuracy Comparison between SMAD, NADA, OSAC, DAA, Alj-News, AlWatan and Akhbar-Alkhaleej Datasets.

TABLE I. COMPARISON BETWEEN OSAC, DAA, ALJEZZERA, NADA, AKHBAR-ALKHALEE, ALWATAN AND SMAD CORPUS

CORPORA	CLASS	CLASSIFIER	# OF CLASSES	Precision	Recall	F- Measure
Alj-News CORPUS	SPORT	SVM	5	1	0.983	0.992
	ART			0.934	0.95	0.942
	SCIENCE			1	0.933	0.966
	POLITICAL			0.789	0.933	0.855
	ECONOMIC			0.962	0.85	0.903
	<b>Weighted average</b>			0.937	0.93	0.931
Akhbar-Alkhaalee CORPUS	CLASS	SVM	4	Precision	Recall	F- Measure
	Economy			0.821	0.836	0.829
	Int. News			0.98	0.845	0.907
	Local News			0.835	0.917	0.874
	Sport			0.975	0.895	0.933
	<b>Weighted average</b>			0.838	0.828	0.831
Alwatan CORPUS	CLASS	SVM	4	Precision	Recall	F- Measure
	Culture			0.838	1	0.912
	Economy			0.892	0.943	0.946
	Religion			1	0.978	0.989
	Sport			0.991	0.972	0.981
	<b>Weighted average</b>			0.966	0.96	0.961
NADA CORPUS	CLASS	SMOTE	10	Precision	Recall	F- Measure
	Arabic Literature			0.920	0.927	0.926
	Social science - economy			0.908	0.884	0.871
	Social science - politics			0.948	0.950	0.944
	Social science - law			0.887	0.896	0.884
	Sport			0.967	0.964	0.959
	Art-General			0.977	0.973	0.970
	General Religions - Islam			0.918	0.933	0.925
	Applied science – computer science			0.912	0.925	0.917
	Applied and health sciences			0.969	0.964	0.960
	Pure Astronomy Science			0.967	0.973	0.925
	<b>Weighted average</b>			0.939	0.939	0.932
DAA CORPUS	CLASS	TF-IDF	9	Precision	Recall	F- Measure
	أدبيات – الادب العربي			0.770	0.760	0.765
	علوم اجتماعية - اقتصاد			0.675	0.856	0.755
	علوم اجتماعي - سياسة			0.485	0.436	0.459
	علوم اجتماعية قانون			0.783	0.720	0.750
	رياضة			0.970	0.953	0.961
	فنون - علم			0.893	0.917	0.905
	ديانات - اسلام			0.861	0.812	0.836
	علوم بحثة – علوم كمبيوتر			0.863	0.805	0.833
	علوم تطبيقية – علوم صحية			0.789	0.723	0.755
	<b>Weighted average</b>			0.813	0.809	0.809
OSCA CORPUS	CLASS		6	Precision	Recall	F- Measure
	علوم اجتماعية - اقتصاد			0.965	0.985	0.984
	علوم اجتماعية قانون			0.970	0.975	0.984
	رياضة			0.966	0.971	0.965
	ديانات - اسلام			0.958	0.959	0.943
	علوم بحثة – علوم فلك			0.999	0.999	0.997
	علوم تطبيقية – علوم صحية			0.996	0.996	0.996
	<b>Weighted average</b>			0.982	0.982	0.982
SMAD CORPUS	CLASS	KNN	5	Precision	Recall	F- Measure
	SPORTS			0.95	1.00	0.98
	EDUCATION			0.98	1.00	0.99
	ART			1.00	0.96	0.98
	HEALTH			0.99	0.97	0.98
	POLITICAL			0.98	0.97	0.98
<b>Weighted average</b>	0.98	0.98	0.98			

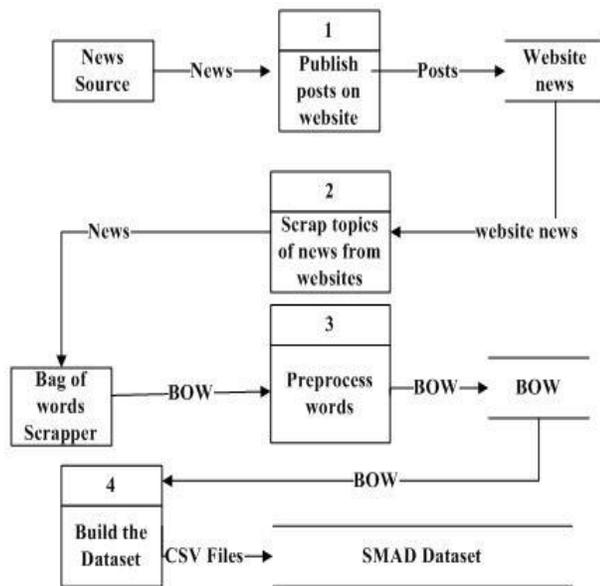


Fig. 8. SMAD Methodology DFD.

## VI. DISCUSSION

All the pervious Arabic datasets [10-14] classify the articles using different classifiers for various purposes. All these Arabic datasets didn't take into consideration the fact that news spread rapidly over social media. Facebook is the widest means of social media as news plays an important role in spreading rapidly on it but is not classified into domains. Thus, the purpose of this paper is to classify the news that is widely spread on Facebook by constructing the SMAD dataset in order to save time and effort in recognizing domain news and to improve the search process for specific news at a specific time. The SMAD corpus was compared with other different datasets according to quality measurement metrics (precision, recall, F-measure, and accuracy). In the sports domain, its precision is 0.95, recall is 1 and the F-measure is 0.98. In the education domain, its precision is 0.98, recall is 1 and the F-measure is 0.99. In the arts domain, its precision is 1, recall is 0.96 and F-measure is 0.98. In the health domain, its precision is 0.99, recall is 0.97 and F-measure is 0.98. Finally, the political domain precision is 0.98, recall is 0.97, and F-measure is 0.98. The accuracy of the SMAD dataset is about 98% in five domains while the accuracy of NADA is 93.8792%, accuracy of OSAC is 98.1758 %, accuracy of DAA is 80.9087 %, accuracy of Alj-News is 93.1 %, accuracy of Alwatan is 96.1 % and the accuracy of Akhbar Alkhaleej is 88.7 %.

## VII. FURTHER WORK

For the future, a news benchmark will be needed for social media from the most credible news sources in a specific domain at a specific period of time to facilitate the searching process to reduce time, effort and checking the veracity of the news from the most credible sources.

## VIII. CONCLUSION

This study was done to construct a new Arabic Dataset corpus built from several websites to classify the news spreads over social media means. Facebook has become one of the

news sources. The Facebook social media's source news is not categorized into any domain; this corpus is composed of five domains (Art-Health-Education-Politics-Sports) and can be extended easily by adding new various domains which can be used for several purposes in the Arabic text classifications. This dataset goes through predefined stages of pre-processing and filtering to eliminate the anomalies of the data, then tested and validated using KNN classifier with four evaluation measures: precision, recall, F-measure, and accuracy for each domain. The experiment results deduced that the new corpus is an efficient dataset for the Arabic classification of news with an accuracy of 98%.

## REFERENCES

- [1] S.L. Marie-Sainte, and N. Alalyani, "Firefly algorithm based feature selection for Arabic text classification", Journal of King Saud University-Computer and Information Sciences, vol:32, No. 3, pp.320-328,2020.
- [2] Y. Jaafar, K. Bouzoubaa, "A survey and comparative study of Arabic NLP architectures", In: Intelligent Natural Language Processing: Trends and Applications, Springer, Cham, pp. 585-610, 2018.
- [3] MA. Omari, M. Al-Hajj, "Classifiers for Arabic NLP: survey", International Journal of Computational Complexity and Intelligent Algorithms", vol:1, No. 3, pp. 231-58.
- [4] R. Al-Shalabi, G. Kanaan, and M. Gharaibeh, "Arabic text categorization using KNN algorithm", In: Proceedings of The 4th International Multiconference on Computer Science and Information Technology, Vol. 4, pp. 5-7, 2006.
- [5] M.M. Syiam, Z.T. Fayed, M.B. and Habib, "An intelligent system for Arabic text categorization", International Journal of Intelligent Computing and Information Sciences", vol. :6, No.1, pp.1-19, 2006.
- [6] F. Harrag, E. El-Qawasmeh and P. Pichappan, P., "Improving Arabic text categorization using decision trees", In: 2009 First International Conference on Networked Digital Technologies, IEEE, pp. 110-115, 2009, July.
- [7] H.K. Chantar and D.W. Corne, "Feature subset selection for Arabic document categorization using BPSO-KNN", In: 2011 Third World Congress on Nature and Biologically Inspired Computing, IEEE, pp. 546-551, 2011, October.
- [8] E. Saraç, and S.A. Özel, "Web page classification using firefly optimization", In :2013 IEEE INISTA, IEEE, pp. 1-5, 2013, June.
- [9] S.R. Ahmad, N.M.M. Yusop, A.A. Bakar and M.R. Yaakub, "Statistical analysis for validating ACO-KNN algorithm as feature selection in sentiment analysis", In: AIP conference proceedings, AIP Publishing LLC. Vol: 1891, No. 1, p. 020018, 2017, October.
- [10] R. Belkebir, and A. Guessoum, "A hybrid BSO-Chi2-SVM approach to Arabic text categorization", In :2013 ACS International Conference on Computer Systems and Applications (AICCSA), IEEE, pp. 1-7, 2013, May.
- [11] N. Alalyani and S. L. Marie-Sainte, "NADA: New Arabic dataset for text classification", "International Journal of Advanced Computer Science and Applications", vol: 9, No.9, 2018.
- [12] M. A. Abdeen, S. AlBouq, A. Elmahalawy and S. Shehata, "A closer look at arabic text classification", International Journal Advanced Computer Science Applications", vol:10, No.11, p.p. 677-688, 2019.
- [13] B. Hawashin, A. Mansour and S. Aljawarneh, "An efficient feature selection method for Arabic text classification", "International journal of computer applications", Vol:83, No. 17, 2013.
- [14] M. M. Al-Tahrawi, "Arabic text categorization using logistic regression", "International Journal of Intelligent Systems and Applications", VOL:7, No.6, p. 71, 2015.
- [15] I. Pak and P.L. Teh, P.L., "Text segmentation techniques: a critical review", Innovative Computing, Optimization and Its Applications", pp.167-181,2018.
- [16] P. Badjatiya, L.J. Kurisinkel, M. Gupta and V. Varma, "Attention-based neural text segmentation", In: European Conference on Information Retrieval, Springer, Cham, pp. 180-193., 2018, March.

- [17] R. Mouty and A. Gazdar, "Survey on Steps of Truth Detection on Arabic Tweets", In: 2018 21st Saudi Computer Society National Computer Conference (NCC), IEEE, p.p. 1-6, 2018, Apr 25.
- [18] J.N. Singh and S.K. Dwivedi, "Comparative analysis of IDF methods to determine word relevance in web document". "International Journal of Computer Science Issues (IJCSI)", Vol:11, No.1, p.59,2014.
- [19] S. Qaiser and R. Ali, "Text Mining: Use of TF-IDF to Examine the Relevance of Words to Documents", "International Journal of Computer Applications," vol. 181, No. 1, pp. 25-29, 2018. Available: 10.5120/ijca2018917395.
- [20] Al-Shalabi, R., Kanaan, G., & Gharaibeh, M. (2006, April). Arabic text categorization using KNN algorithm. In Proceedings of The 4th International Multiconference on Computer Science and Information Technology (Vol. 4, pp. 5-7).
- [21] R. Soleymani, E. Granger and G. Fumera, "F-measure curves: A tool to visualize classifier.

# P Systems Implementation: A Model of Computing for Biological Mitochondrial Rules using Object Oriented Programming

Mohammed M. Nasef<sup>1</sup>

Mathematics and Computer Science Department  
Faculty of Science, Menoufia University  
Shebin El-Koom,32511, Egypt

Bishoy El-Aarag<sup>2</sup>

Biochemistry Division, Chemistry Department  
Faculty of Science, Menoufia University  
Shebin El-Koom,32511, Egypt  
Division of Chemistry and Biotechnology  
Graduate School of Natural Science and Technology  
Okayama University, Okayama 7008530, Japan

Amal Hashim<sup>3</sup>

Mathematics and Computer Science Department  
Faculty of Science, Menoufia University  
Shebin El-Koom,32511  
Information Systems Department  
Higher Institute of Advanced Studies, Haram, Giza, Egypt

Passent M. El Kafrawy<sup>4</sup>

Mathematics and Computer Science Department  
Faculty of Science, Menoufia University  
Shebin El-Koom,32511  
School of Information Technology and Computer Science  
Nile University, Egypt

**Abstract**—Membrane computing is a computational framework that depends on the behavior and structure of living cells. P systems are arising from the biological processes which occur in the living cells' organelles in a non-deterministic and maximally parallel manner. This paper aims to build a powerful computational model that combines the rules of active and mobile membranes, called Mutual Dynamic Membranes (MDM). The proposed model will describe the biological mechanisms of the metabolic regulation of mitochondrial dynamics made by mitochondrial membranes. The behaviors of the proposed model regulate the mitochondrial fusion and fission processes based on the combination of P systems variants. The combination of different variants in our computational model and their high parallelism lead to provide the possibility for solving problems that belong to NP-complete classes in polynomial time in a more efficient way than other conventional methods. To evaluate this model, it was applied to solve the SAT problem and calculate a set of computational complexity results that approved the quality of our model. Another contribution of this paper, the biological models of mitochondrial is presented in the formal class relationship diagrams were designed and illustrated using Unified Modeling Language (UML). This mechanism will be used to define a new specification of membrane processes into Object-Oriented Programming (OOP) to add the functionality of a common programming methodology to solve a large category of NP-hard problems as an interesting initiative of future research.

**Keywords**—Computational biology; P systems; membranes fusion – fission; mitochondria; Mutual Dynamic Membranes (MDM); NP- complete problems

## I. INTRODUCTION

A lot of ideas in Bioinformatics have attracted the attention of researchers. These ideas have been inspired by living cells, their organics, and their membranes that have been used to

compute and model a large number of problems in computational science. Natural Computing is a wide field that describes computational methods and processes inspired by natural environments. The natural computing frameworks that are known to solve computational problems are, for example: DNA computing [1], automata computing [2], quantum computing [3], genetic algorithms [4], and neural networks [5]. Similarly, membrane computing is abstracted to solve hard problems in Artificial Intelligence (AI) [6].

Membrane computing is introduced by Păun in 1998 and was inspired by paradigmatic computation based on the structure, behavior, and functions of living cells [7]. One of such outcomes is the P systems, a category of various biological parallel computing models which can be considered as universal computing paradigms [8]. P systems projected efficient computational models by combining the structural and dynamic properties of biological systems [9]. As a result, many fields such as the formal languages [10], theory of computability [11], and theory of computational complexity [12] with intractable problems were solved by the biological model, called P systems [13].

Some of the biological phenomena of the living cells were incorporated into membrane computing as an influential kind of computational concepts, cell-like P systems. According to these phenomena, the framework of active membranes in polarizationless P systems [14] are developed and evaluated by using rewriting rules [7] which can be merged, divided, separated, or passed through membranes [15]. Another variant of cell-like P system was inspired by cells movement as exocytosis and endocytosis rules that are expressed of the outside and inside processes of neighboring membranes, this variant is called mobile membranes [16].

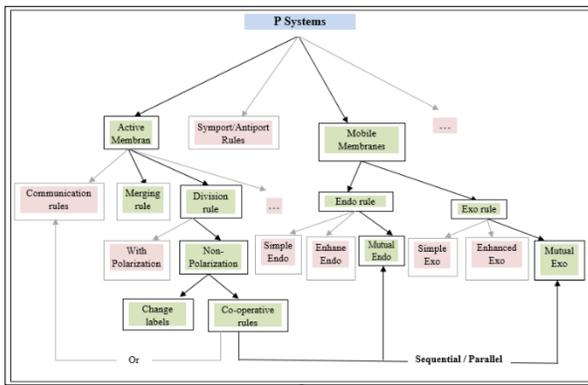


Fig. 1. P Systems Variants.

A general form of cell-like P systems variants is shown in Fig. 1. Each variant has a set of rules describing the basic structure of any model designed to solve computational problems. The main components used in the proposed model are represented by green arrows and compartments in Fig. 1.

The living cells have organelles called mitochondria; mitochondrion is a dynamic organelle capable of interacting with each other. It is responsible for producing energy molecules in the living cell, Adenosine Triphosphate, (ATP) [17]. The function of mitochondria depends on four processes, fusion, fission, motility, and Mitophagy [17]. In the current work, the focus is on the first two operations, fusion and fission that will be introduced in a powerful computational model. The influential division rule is cooperative with mutual exo and mutual endo rules in (MDM) model. All rules are applied in parallel and non-deterministically selecting the membranes, the rules, and the objects. In the case a set of rules can be executed in each step, but no other rules can be added to this set and no membranes and objects can be evolve at the same time; this is indicated to the parallelism mechanism is maximal for a final solution.

The basic idea is to develop a set of rules that will be the bases of a model to solve NP hard problems through the interactions of the objects, those set of rules are an abstraction of the natural biological generation of energy in human cells. From which conclusions can be achieved. The benefit is to develop a new set of AI models that do not need a priori knowledge nor learning, and moreover to model standardization in smart application development.

Our target is to represent the computability and complexity of an unconventional computing system as a theoretical solvent for NP-complete problems in Polynomial/ linear time. In the current work, the combination of variants of P systems in the model, using real operations, leads to solve a number of problems belonging to different classes further than NP in a more efficient manner than other classical computing systems. A semi-uniform linear time solution has been introduced to SAT problem using (MDM), with 3 membranes only as described in the initial configuration of the fission model.

Finally, another side is the need for alternative mechanisms and unconventional methods to describe and illustrate complex biomolecular processes which have actions, behaviors, and functions are vitality to the health of human. Accordingly, to

this aspect, our biological models are considered a computational method for the development of object relationship diagrams. Then the objects structure and their actions are represented by UML diagrams. These diagrams can be implemented using object-oriented programming to be used as an analysis tool for complex data of mitochondria neural diseases to extract the diseases' characteristics, causes, and insights as an initiation in huge applications of data science. The object relationship diagrams will be used to develop machine learning algorithms in the future work.

This paper is organized as follows: Section II introduces the concepts of active and mobile membranes, as well as their basic conceptions of P systems. The third section is dedicated to the elaboration of the related work. The proposed model, (MDM) is introduced and modeled in Section IV. Efficient Solutions to different classes of problems by the proposed model and a semi-uniform linear time solution have been introduced to SAT problem using the proposed model (MDM), with 3 membranes only as presented in the initial configuration of the fission model is explained in Section V. UML diagrams representations will be introduced in Section VI. A final conclusion and some future researches lines are given in Section VII.

## II. DEFINITIONS OF P SYSTEMS WITH ACTIVE AND MOBILE MEMBRANES

The distributed parallel computing models included P systems class arisen from the membrane computing framework. In the present work, the important processes in mitochondria are recruitment. The combination of two important classes of rules described in P systems models, active and mobile membranes are presented as a new model, (MDM).

The first class is the active membranes variant. It has evolution, merging, division, and communication rules. The second class is the mobile membranes variant, which is inspired by biological events such as cell membrane mobility, Endocytosis, and Exocytosis processes. It has four types: simple, enhanced, mutual mobile membranes and mutual mobile membranes with objects on the surface [18]. We will focus on the third type, mutual mobile membranes. It's worth noting that the rules permit a membrane to move independently of the other membranes involved. According to this property, the mutual mobile membrane is completely suitable for fusion and fission mitochondria.

The fundamental notions of P systems with active and mutual mobile membranes are constructed as follows:

$\Pi = (V, H, \mu, W, R, i)$ , where:

- 1)  $V$  is the alphabet (non-empty and finite) objects;
- 2)  $H$  is a finite set of labels for membranes, labeled  $h_1, h_2, \dots, h_n$ ; ( $n \geq 1$  the degree of the system);
- 3)  $\mu$  is the membrane structure, composed of  $n$  membranes;
- 4)  $W$  is string,  $w_1, w_2, \dots, w_n$  on  $V$  which represent the multisets of objects present in regions  $h_1, h_2, \dots, h_n$  of the membrane structure  $\mu$ ;

- 5)  $R$  is finite sets of evolutionary rules related to regions  $h_1, h_2, \dots, h_n$  of membrane structure, for the following forms;  
 6)  $i \in HU \{environment\}$ , is either one of the regions  $h_1, h_2, \dots, h_n$  and the respective region are the output range of the system, or it is  $\emptyset$ , where  $i = environment$ .

Fig. 2 presents the class of P systems with active and mobile membrane rules as follows:

a)  $[a \rightarrow v]_{h_1}$ , where  $a \in V; v \in V^*; h_1 \in H$ .

Object evolution rule; associated with the membrane and depending on the label, but not directly involving the membrane, in the sense that the membrane is neither taking part in the application of this rule nor modified by it [7, 19, and 20].

b)  $a[ ]_{h_1} \rightarrow [ ]_{h_2}$ , where  $a, b \in V; h_1, h_2 \in H$ .

In-Communication rule; an object is sent in the membrane  $h_2$  [7, 19, and 20].

c)  $[ ]_{h_2} \rightarrow a[ ]_{h_1}$ , where  $a, b \in V; h_1, h_2 \in H$ .

Out-Communication rule; an object is sent out of the membrane  $h_2$  [7, 19, and 20].

d)  $[a]_{h_1} \rightarrow [ ]_{h_2} [ ]_{h_3}$ , where  $a, b, c \in V; h_1, h_2, h_3 \in H$ .

Division rule for elementary membrane  $h_1$ ; in reaction with an object  $a$ , the membrane is divided into two new membranes with the different labels  $h_2$  and  $h_3$ , the object specified in the rule is replaced in the two new membranes by possibly new objects  $b$  and  $c$ ; the new objects may evolve in the same step [7, 20]. The object specified in this rule may be replaced in the two new membranes by possibly new objects or they are duplicated and may evolve in the same step by rule of type (a) [7].

e)  $[ ]_{h_2} [ ]_{h_3} \rightarrow [a]_{h_1}$ , where  $a, b, c \in V; h_1, h_2, h_3 \in H$ .

Merging rule for elementary membranes  $h_2$  and  $h_3$ ; in reaction with their objects  $b$  and  $c$ , they are merged into a single membrane  $h_1$ ; the object  $a$  is produced in the new membrane  $h_1$  [7, 20].

f)  $[ ]_{h_1} [a]_{h_2} \rightarrow [ ]_{h_1} [b]_{h_2}$ , where  $a, b \in V; h_1, h_2 \in H$ .

Mutual Endocytosis (mendo): Under the management of object  $a$ , an elementary region labeled  $h_2$  enters the next region named  $h_1$ ; the labels  $h_1$  and  $h_2$  stay the same during this process. But the object  $a$  may be adapted to  $b$  during the process;  $h_1$  isn't always seen as a fundamental region [7, 19].

g)  $[ ]_{h_2} [ ]_{h_1} \rightarrow [ ]_{h_1} [a]_{h_2}$ , where  $a, b \in V; h_1, h_2 \in H$ .

Mutual Exocytosis (mexo): an elementary region labeled  $h_2$  is sent out of a region labeled  $h_1$ , The labels  $h_1$  and  $h_2$  remain unchanged during this procedure, as they are under the control of object  $b$ , however, the object  $b$  may be changed to  $a$  during this operation; region  $h_1$  is not always an elementary region [7, 19].

In [21] one observed that the electrical charges (polarization) are not adapting to biological rules. In fact, using the polarization features with mobile rules as exo and endo rules were not common in membranes systems. Although of that, P systems with mobile membranes have given computational power and universality properties. Their efficiency and ability are used to solve NP-complete problems without using the polarization [22].

The rules of type (a) are applied in parallel (all objects that may be developed by such rules must evolve). However, the rules of types (b) through (g) are implemented in such a way that only one rule of these kinds may be utilized at a time on one membrane. Overall, the rules are applied in a non-deterministic, maximally parallel fashion; all objects and membranes that may evolve should do so. These rules modify the label of the membrane, but they must be implemented in a sequential manner to avoid label conflicts.

Rules (b) and (c) are considered as a simple form without polarization, those two powerful rules are used for in and out communication as illustrated in [23]. Even in the limited instance where no polarization is utilized, membrane labels are modified. While in rules (d) and (e), P systems are used without polarization and the membrane division and merging rules are allowed to change the label of a membrane (Theorem 2 in [21]). This condition is to accomplish P system efficiency and universality without polarization.

Finally, under the control of object  $a$ , the elementary membrane labeled  $h_2$  enters the next membrane named  $h_1$ ; the labels  $h_1$  and  $h_2$  stay unchanged during this operation. Hence, object  $a$  may be changed to  $b$  throughout the endocytosis process, rule (f). Similarly, under the control of object  $b$ , an elementary membrane labeled  $h_2$  is expelling from a membrane labeled  $h_1$ ; the two membranes labels stay the same. However, the object  $b$  from membrane  $h_2$  can be modified throughout the exocytosis process, rule (g).

In all of the variants, the number of membranes can only be reduced during computation by merging membranes as a result of applying evolution rules to the objects represented in the system. A natural possibility is to allow increases in the number of membranes also to increase during a computation. For example, by division, as it is well known in biology. Actually, the membranes from biochemical are not passive. Where, the majority of chemical compound passage across a

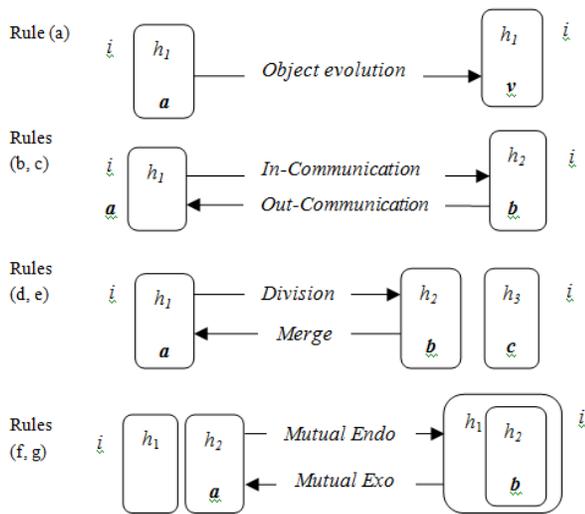


Fig. 2. Membranes Handling Operations.

membrane is accomplished by direct interaction with the membrane itself (through the membrane's so-called protein channels or protein gates). For the duration of this interaction, the chemical compounds that pass during membrane can be modified, while the membrane itself can in this way be modified at least locally.

### III. RELATED WORK

Researches of recent literature are well presented with grateful studies in P systems models that support the computing paradigm known as membrane computing. In addition to simulating the biomolecular processes as fusion and fission of mitochondria as we will introduce in this work the same behavior with P system variants to improve solutions for NP-complete problems. We mention a few reviews of the membrane computing concepts and their notions [24-29]. Membrane computing is similar to quantum computing, is a new unconventional computing model that is applied in linguistics, sociology, optimization design, and a large number of fields [30]. The researcher can read [27, 28, 31, 32, and 19] to cover widely part of P systems variants.

All of the studies are represented and developed to contribute to solving different kinds of problems from formal languages theory [24] to power systems blunder diagnosis [34], passing through a wide range of different research fields as in chemical engineering, scheduling of gasoline blending [35] by membrane computing with its application. Also, in the pattern recognition letters, an automatic clustering algorithm by P systems has been applied [36]. All of the mentioned applications used different P systems models; developed according to the problem nature whether it is theoretical or practical. Here, the focus is on the literary works that addressing computationally NP-complete problems using active and mobile membrane systems and their efficiency and computational power. The efficient variants of Membrane systems and the formal definitions of P systems are investigated from computational complexity theory [34]. Elegant works for NP-complete problems such as Boolean Satisfiability (SAT) problem, has been shown with the polynomial solutions with active membrane principles [26, 16], The Hamiltonian Cycle Problem (HCP) [37], and Travelling Salesman Problem (TSP) [38]. SAT solution is also set by P systems with active membranes by division rule for elementary membranes without dissolution rule. It's verified in [39]. Separation rules are utilized instead of division rules in [40], where it created two new membranes each of them has one new object and the rest of them are replicating. These rules had restrictions that created an exponential workspace in membranes terms in polynomial time, not in objects [41, 42]. The Turing completeness is achieved by using elementary division rules for nine membranes [16, 43].

Regarding the computational complexity of mobile membranes, four mobile membranes are obtained to prove a Turing machine power using evolution rules with exo and endo rules [44].

P automata variant is used to describe a mitochondrial fusion model [45]. It represented the procedure of specific protein production that is necessary for mitochondrial fusion [17]. In [33], Giannakis and Andronikos referred to use six

biological operations described in [46]. The most important process of them is the exocytosis operation used in the mitochondrial fusion model that concerns a mitochondrial fusion mechanism with communication orders and specific actions. The comparison between our model and their study [33] will be introduced in Table I.

All of the studies are represented and developed to contribute to solving different kinds of problems from formal languages theory [24] to power systems blunder diagnosis [34], passing through a wide range of different research fields as in chemical engineering, scheduling of gasoline blending [35] by membrane computing with its application. Also, in the pattern recognition letters, an automatic clustering algorithm by P systems has been applied [36]. All of the mentioned applications used different P systems models; developed according to the problem nature whether it is theoretical or practical. Here, the focus is on the literary works that addressing computationally NP-complete problems using active and mobile membrane systems and their efficiency and computational power. The efficient variants of Membrane systems and the formal definitions of P systems are investigated from computational complexity theory [34]. Elegant works for NP-complete problems such as Boolean Satisfiability (SAT) problem, has been shown with the polynomial solutions with active membrane principles [26, 16], The Hamiltonian Cycle Problem (HCP) [37], and Travelling Salesman Problem (TSP) [38]. SAT solution is also set by P systems with active membranes by division rule for elementary membranes without dissolution rule. It's verified in [39]. Separation rules are utilized instead of division rules in [40], where it created two new membranes each of them has one new object and the rest of them are replicating. These rules had restrictions that created an exponential workspace in membranes terms in polynomial time, not in objects [41, 42]. The Turing completeness is achieved by using elementary division rules for nine membranes [16, 43].

TABLE I. COMPARISON BETWEEN OUR MODEL AND RELATED WORK [33]

Model in [33]	Our Model
Only one operation (fusion operation) is modeled.	Two operations (fusion and fission) are modeled.
Considered that the outer and inner membranes are two individuals in skin membranes; each of them has three nested elementary membranes. This is not matched with the structure of biological model.	Biological model is precisely designed to describe the operations occurred in the two nested mitochondria membranes and regulates the fusion and fission processes.
Depended on Bio Ambients rules with Mobile membranes to design the model.	Depended on combination of active membranes rules with mobile membranes to design the model.
Used an exo behavior to achieve the final configuration.	Used a combination of division, mexo and mendo behaviors to achieve the final configuration.
Proteins have been produced from the outer and inner membranes in the final configuration. This is not matched with mitochondria function and their membranes.	New mitochondria organelles have been produced from fusion and fission processes. These mitochondria organelles are capable to adapt its metabolic and produce ATP molecules.
	Rules of our model have been given computational efficiency for many NP complete problems.

Regarding the computational complexity of mobile membranes, four mobile membranes are obtained to prove a Turing machine power using evolution rules with exo and endo rules [44].

P automata variant is used to describe a mitochondrial fusion model [45]. It represented the procedure of specific protein production that is necessary for mitochondrial fusion [17]. In [33], Giannakis and Andronikos referred to use six biological operations described in [46]. The most important process of them is the exocytosis operation used in the mitochondrial fusion model that concerns a mitochondrial fusion mechanism with communication orders and specific actions. The comparison between our model and their study [33] will be introduced in Table I.

#### IV. PROPOSED MODEL

To present our model, firstly we describe the biological background for mitochondria actions (fusion and fission models), after that we will describe the biological actions by Mutual Dynamic Membranes (MDM) with P Systems.

##### A. Mitochondrial Fusion Model

A mitochondria fusion mechanism includes specific actions and communications motivated by the structure and the functioning of the distribution of mitochondrial fusion in the renewal of the mitochondrial population within an eukaryotic cell.

We will demonstrate the proposed scheme using an actual biochemical model of mitochondrial fusion processes. The proposed model consists of five actual membranes, the cell which acts as an “environment” in the P systems. The skin membrane has two non-elementary membranes called “Outer Membranes” with each one has one elementary membrane called “Inner Membranes”. Both inner and outer membranes have operations “rules” executed by proteins that are considered as “objects” in the P systems. Then, a new mitochondrion is produced in the environment.

1) *Fusion biological model:* As illustrated in Fig. 3, the biological description of a mitochondrial fusion model is designed by Cell Designer software. In the fusion model, the joining of two organelles into one was applied through two basic operations, Outer and Inner membrane fusion.

a) *First operation:* The fusion of outer membrane: There are several proteins involved in the fusion process of the outer membrane such as mitofusin 1 and 2 (MFN1& MFN2). Oxidative stress and the presence of high levels of oxidized glutathione (GSSG) are inducer signals for outer membrane fusion. These signals induced serial of constitutive steps as the following: oxidative stress and the excess formation of glutathione oxidized form (GSSG) induce mitofusins complexes in the outer membrane to act in trans. This induction of trans complexes of mitofusin proteins was mediated by disulfide bonds owing to the binding of organelle and causing fusion of the outer membranes [47].

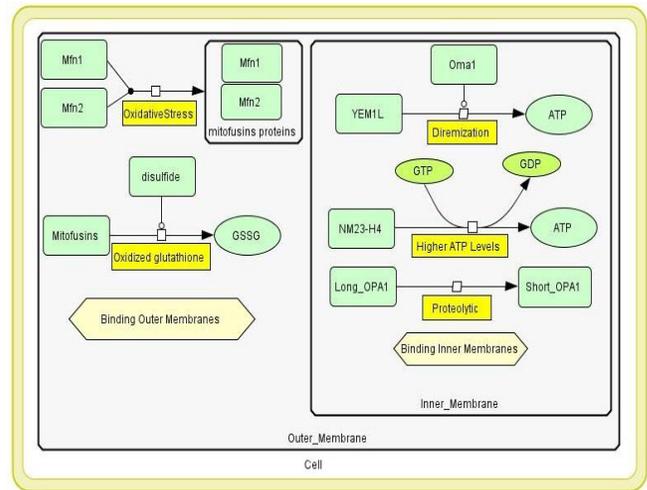


Fig. 3. Fusion Operations for Mitochondria Membranes.

b) *Second operation:* The fusion of inner membrane: A particular protein termed Optic Atrophy 1 (OPA1) has participated in the fusion of the inner membrane. The fusion was initiated by oxidative phosphorylation (OXPHOS) and advanced ATP levels as inducer signals. Concerning to OXPHOS signal these steps have occurred as follows:

- The presence of OXPHOS increases Yme1L metalloprotease. Yme1L and Oma1 activate the Proteolytic processing of Opa1 from the long-form to the soluble short form leading to inner membrane fusion.
- With regards to higher ATP levels, this signal was linked with GTP-loading and hydrolysis by the action of the kinase (NM23-H4) leading to conversion of OPA1 to short-form causing inner membrane fusion [47].

2) *Fusion membranes using Mutual Dynamic Membranes (MDM) with P Systems:* Active and mobile membranes with P systems are used to obtain the behavior of cooperation rules such that using more than one object on the left-hand side of the rule. The biochemical reactions in mitochondria organelles are usually created by the reaction of two or more proteins represented as normal objects that can improve through the computation to get the final configuration.

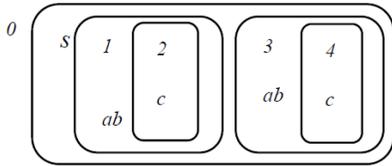
In the following configuration, proteins MFN1, MFN2, and OPA1 are used as “activators” of rules; these proteins are engaged in the fusion process and are important for the regulation of certain chemical processes. These proteins are also responsible for determining which rules apply in each phase leading to a final configuration.

$\Pi_I = (V, H, \mu, W, R, i_0)$  be a P system with the initial degree of the system is  $n = 5$ .

- The system can be viewed as a set of five membranes labeled by elements of  $H = \{s, 1, 2, 3, 4\}$  arranged in a hierarchical structure which including skin membrane ‘s’ contains two non-elementary membranes ‘1’ and ‘3’

each one of them has one elementary membrane, '2' in '1' and '4' in '3'.

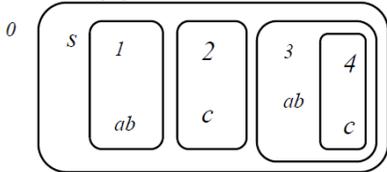
- The initial configuration,  $\mu$  given by  $[[[[]_2]_1[[[]_4]_3]]_s]$
- The finite multisets of objects are represented by  $w_1, w_2, w_3, w_4, w_s$  where  $w_s = \phi$ ,  $w_1=w_3$  have proteins of outer membranes, *MFN1* and *MFN2*. And  $w_2=w_4$  have proteins of inner membranes, *OPA1*. These are placed in membranes of the initial system. For simplicity, we will be considered  $MFN1=a$ ,  $MFN2=b$ ,  $OPA1=c$ ,  $new\_MFN1=a'$ ,  $new\_MFN2=b'$  and  $new\_OPA1=c'$ . Such that,  $a, b, c, a', b', c' \in V$
- $R$  is a finite set of the development rules over  $V$  of the following forms, (**R1**, **R2**, ..., **R6**).
- $i$  is 0, refer to the environment, "cell" in the system.



Initial Configuration

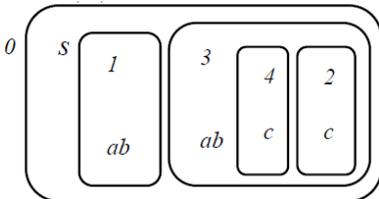
1) Apply mexo rule on membranes 2 and 1.

R1:  $[[ [ a b [ c ]_2 ]_1 [ a b [ c ]_4 ]_3 ]_s \rightarrow [ [ a b ]_1 [ c ]_2 [ a b [ c ]_4 ]_3 ]_s$ , where  $a, b, c \in V$ .



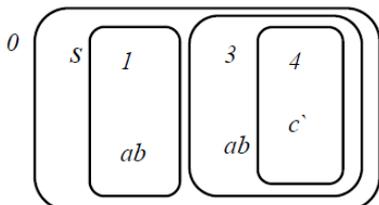
2) Apply mendo rule on membranes 2 and 3.

R2:  $[[ [ a b ]_1 [ c ]_2 [ a b [ c ]_4 ]_3 ]_s \rightarrow [ [ a b ]_1 [ a b [ c ]_4 [ c ]_2 ]_3 ]_s$ , where  $a, b, c \in V$ .



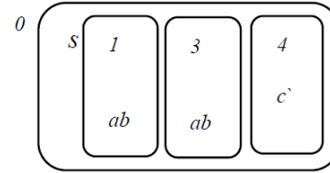
3) Apply merging rule on membranes 2 and 4 (the new membrane has label 4)

R3:  $[[ [ a b ]_1 [ a b [ c ]_4 [ c ]_2 ]_3 ]_s \rightarrow [ [ a b ]_1 [ a b [ c' ]_4 ]_3 ]_s$ , where  $a, b, c, c' \in V$ .



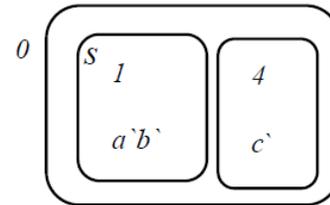
4) Apply mexo rule on membranes 4 and 3

R4:  $[[ [ a b ]_1 [ a b [ c' ]_4 ]_3 ]_s \rightarrow [ [ a b ]_1 [ a b ]_3 [ c' ]_4 ]_s$ , where  $a, b, c, c' \in V$ .



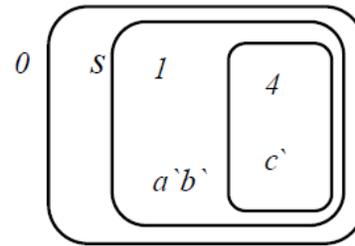
5) Apply merging rule on membranes 1 and 3 (the new membrane has label 1)

R5:  $[[ [ a b ]_1 [ a b ]_3 [ c' ]_4 ]_s \rightarrow [ [ a' b' ]_1 [ c' ]_4 ]_s$ , where  $a, b, a', b', c' \in V$ .



6) Apply mendo rule on membranes 4 and 1

R6:  $[[ [ a' b' ]_1 [ c' ]_4 ]_s \rightarrow [ [ a' b' [ c' ]_4 ]_1 ]_s$ , where  $a', b', c' \in V$ .



Final Configuration

### B. Mitochondrial Fission Model

A mitochondria fission mechanism is described by variants of active and mobile membranes using realistic biological operations. The proposed model consists of three actual membranes, the skin membrane which is a surface membrane, and the cell that acts as an "environment" in the P systems. The skin membrane has one non-elementary "Outer Membrane" that has one "Inner Membrane". Both inner and outer membranes have operations "rules" executed by proteins considered "objects" in the P systems. After that, two mitochondria are produced in the environment.

1) *Fission biological model*: Fig. 4 presented the biological description of mitochondrial fission regulation model. It designed by cell designer software. According to division operation, the fission model was included dividing one mitochondria organelle into two new ones. It should be taken in consideration that a dynamin-related protein 1 (Drp1) is the principal controller protein complicated in fission process. The Drp1 mobilization from cytosol onto the surface of mitochondria is essential and established via many proteins found on the outer membrane of mitochondria. They included

mitochondrial fission factor (Mff) and mitochondrial dynamics proteins 49 and 51 (MiD49 and MiD51). The regulation of fission process is completed by one of the following four basic modes [47]:

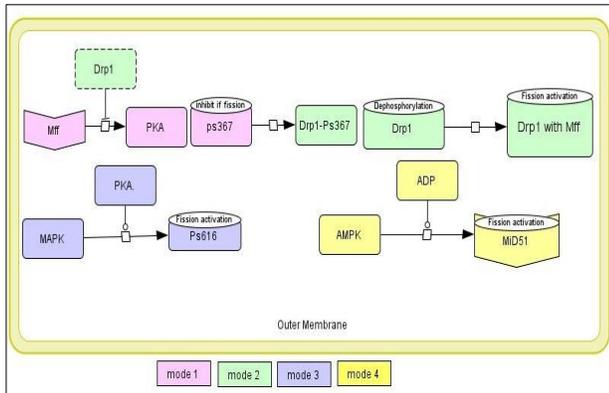


Fig. 4. Fission Operations for Mitochondria Membranes.

Mode (1): showed the inhibition of mitochondrial fission. It induced by signals included exercise and nitrogen starvation. The mode was done through the following sequencing steps:

- 1) Exercise and nitrogen starvation induce protein kinase A (PKA) activation.
- 2) The activated PKA causes phosphorylation of Drp1 at amino acid serine no. 637 (Ser637).
- 3) Phosphorylated Drp1 keep hold of Drp1 in cytosol preventing the fission process.

Mode (2): revealed the induction of mitochondrial fission. It initiated via signals such as metabolic uncoupling of the organelle and calcineurin.

The mode was done through the following sequencing steps:

- 1) Metabolic uncoupling of the organelle activates calcineurin.
- 2) The activated calcineurin dephosphorylates Drp1 at Ser637 (i.e. convert Drp1 from the phosphorylated to dephosphorylated form).
- 3) Dephosphorylated Drp1 allows mobilization of Drp1 to mitochondria resulted in activation of mitochondria fission.

Mode (3): exhibited the induction of mitochondrial fission. It began through signals such as cold exposure and oncogenic RasG12V. The mode was done through the following sequencing steps:

- 1) Cold exposure activates PKA, as well as oncogenic RasG12V activates mitogen-activated protein kinase (MAPK).
- 2) The activated PKA and MAPK phosphorylates Drp1 at Ser616.
- 3) The phosphorylated Drp1 links with both MiD51 and Mff leading to activation of mitochondrial fission.

Mode (4): illustrated the induction of the mitochondrial fission through high adenosine diphosphate (ADP) and adenosine monophosphate (AMP) levels as induction signals.

The following sequencing steps were included in the fission mode.

I- Steps regards to high ADP level signal:

- 1) The presence of high levels of ADP initiates the binding of ADP with MiD51 receptor.
- 2) The bounded ADP with receptor induces MiD51 activation.
- 3) The activated MiD51 associates with Drp1.
- 4) The activated and associated MiD51 with Drp1 causes Drp1 mobilization to mitochondria resulted in activation of mitochondria fission.

II-Steps regards to high AMP level signal:

- 1) The elevated AMP levels are detected by AMP-activated protein kinase (AMPK).
- 2) AMPK causes the phosphorylation of Mff protein receptor.
- 3) The phosphorylated Mff receptor binds to Drp1.
- 4) Drp1 bounded to phosphorylate Mff organizes Drp1 to mitochondria and activates mitochondria fission.

2) *Fission membranes using Mutual Dynamic Membranes (MDM) with P system:* The chemical reactions in mitochondria organelles are mainly caused by the reaction of two or more proteins. These are depicted as normal objects that can evolve by division computation, mexo, and mendo rules to get the final configuration.

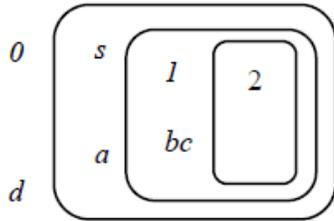
In the following computation, proteins DRP1, MFF, MID51, PKA, Calcineurin, AMPK, and MAPK are used in P systems as “activators” of rules, where proteins are regulated certain biochemical reactions to the fission process occur.

$\Pi_2 = (V, H, \mu, W, R, i)$  be a P system with active and mobile membranes with the initial degree of the system is  $n = 3$ .

- The system can be viewed as a set of three membranes labeled by elements of  $H = \{s, 1, 2\}$  arranged in a hierarchical structure which including the skin membrane ‘s’ contains two nested membranes ‘1’ and ‘2’.
- The initial configuration  $\mu$  given by  $[[[2]1]1]s$ .
- The finite multisets of objects are represented by  $w_0, w_s, w_1, w_2$  where  $w_0$  has proteins of the environment,  $w_s$  has proteins of the surrounding of the outer membrane,  $w_1$  has proteins of an outer membrane and  $w_2$  has proteins of an inner membrane. These are placed in membranes of the initial system. For simplicity, we will be considered  $DRP1=a, DRP1-PS637 = as637, DRP1-PS616 = as616, MFF=b, Phospho-MFF=bp, MID51=c, PKA=d, Calcineurin=e, AMPK=f, MAPK=g$ . Then,  $w_0=d, f, g, w_s=a, e, w_1=b, c$  and  $w_2=\phi$ . Such that,  $a, as637, as616, b, bp, c, d, e, f, g \in V$ .
- $R$  is a finite set of the development rules in  $V$  of the following forms associated with the labels including

evolution, communication, division, mexo, and mendo rules, (R7, R8, ..., R33).

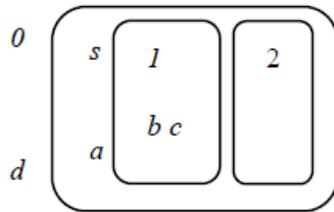
- $i$  is 0, refer to the environment, "cell" in the system.



Initial Configuration of Mode 1

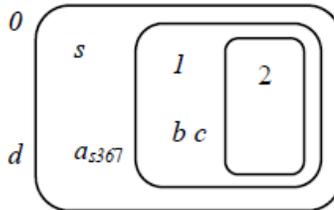
- 1) Apply mexo rule on membranes 2 and 1.

R7:  $d [a [b c [ ]_2 ]_1]_s \rightarrow d [a [b c]_1 [ ]_2]_s$ , where  $a, b, c, d \in V$ .  
(mode1)

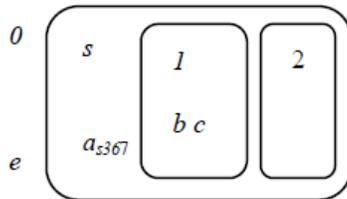


- 2) Apply object evolution rule in the same region [ $a \rightarrow a_{s367}$ ]

R8:  $d [a [b c]_1 [ ]_2]_s \rightarrow d [a_{s367} [b c]_1 [ ]_2]_s$ , where  $a, b, c, d, a_{s367} \in V$



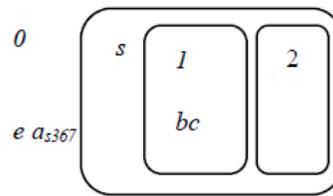
Note:  $a_{s367}$  object leads to inhibition of mitochondrial fission, then it interaction with  $e$  object to activate fission process in mode.



Initial Configuration of Mode 2

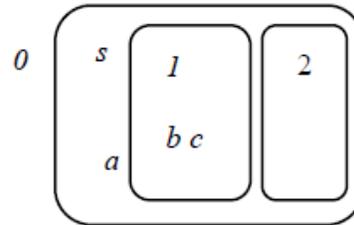
- 3) Apply communication rule;  $a_{s367}$  object is sent out from the skin membrane  $s$ .

R9:  $e [a_{s367} [b c]_1 [ ]_2]_s \rightarrow e a_{s367} [ [b c]_1 [ ]_2]_s$ , where  $a, b, c, e, a_{s367} \in V$ . (mode2)



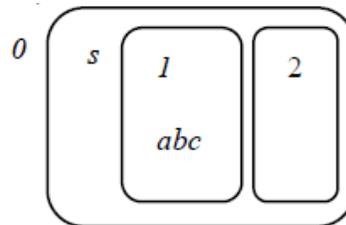
- 4) Apply object evolution rule [ $a_{s367} \rightarrow a$ ]

R10:  $e a_{s367} [ [b c]_1 [ ]_2]_s \rightarrow [a [b c]_1 [ ]_2]_s$ , where  $a, b, c, e, a_{s367} \in V$ .



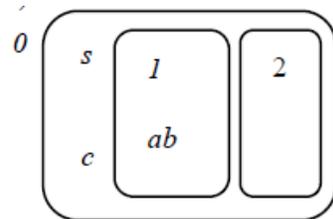
- 5) Apply communication rule;  $a$  object is sent in the membrane 1

R11:  $[a [b c]_1 [ ]_2]_s \rightarrow [ [a b c]_1 [ ]_2]_s$ , where  $a, b, c, e \in V$ .  
(mode2)



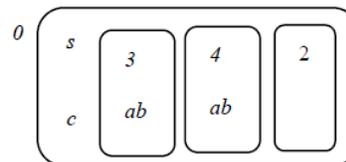
- 6) Apply communication rule;  $c$  object is sent out from the membrane 1

R12:  $[ [a b c]_1 [ ]_2]_s \rightarrow [c [a b]_1 [ ]_2]_s$ , where  $a, b, c, e \in V$ .  
(mode2)



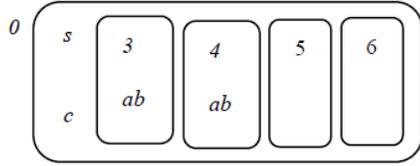
- 7) Apply division rule on membrane 1 (the different membranes labels 3, 4 are results)

R13:  $[c [a b]_1 [ ]_2]_s \rightarrow [c [a b]_3 [a b]_4 [ ]_2]_s$ , where  $a, b, c \in V$ .  
(mode2)



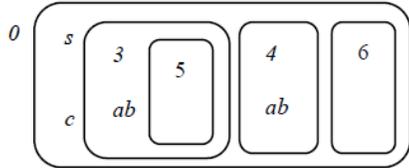
8) Apply division rule on membrane 2 (the different membranes labels 5, 6 are results).

R14:  $[c [a b]_3 [a b]_4 [ ]_2 ]_s \rightarrow [c [a b]_3 [a b]_4 [ ]_5 [ ]_6 ]_s$ , where  $a, b, c \in V$ . (mode2).



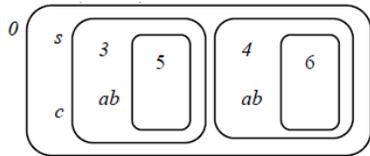
9) Apply mendo rule on membranes 5 and 3.

R15:  $[c [a b]_3 [a b]_4 [ ]_5 [ ]_6 ]_s \rightarrow [c [a b] [ ]_3 [a b]_4 [ ]_6 ]_s$ , where  $a, b, c \in V$ . (mode2)

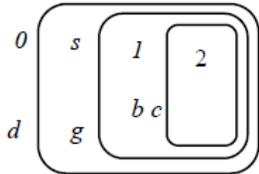


10) Apply mendo rule on membranes 6 and 4.

R16:  $[c [a b] [ ]_5 [a b]_4 [ ]_6 ]_s \rightarrow [c [ab] [ ]_5 [a b] [ ]_6 ]_s$ , where  $a, b, c \in V$ . (mode2)

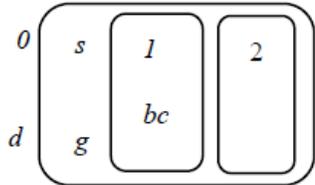


Rules of mode3:



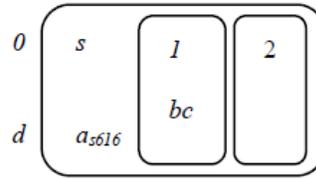
1) Apply mexo rule on membranes 2 and 1

R17:  $d [g [b c] [ ]_2 [ ]_1 ]_s \rightarrow d [g [b c] [ ]_1 [ ]_2 ]_s$ , where  $b, c, d, g \in V$ .



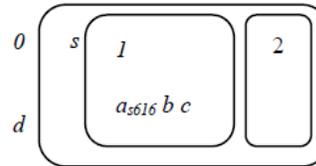
2) Apply object evolution rule in the same region,  $[g \rightarrow a_{s616}]$ .

R18:  $d [g [b c] [ ]_1 [ ]_2 ]_s \rightarrow d [a_{s616} [b c] [ ]_1 [ ]_2 ]_s$ , where  $b, c, d, g, a_{s616} \in V$ .



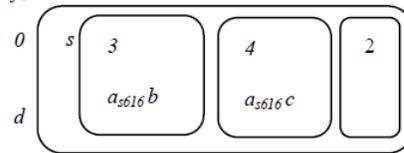
3) Apply communication rule;  $a_{s616}$  sent in the membrane 1,

R19:  $d [a_{s616} [b c] [ ]_1 [ ]_2 ]_s \rightarrow d [ [a_{s616} b c] [ ]_1 [ ]_2 ]_s$ , where  $b, c, d, a_{s616} \in V$ .



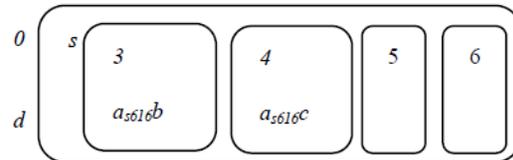
4) Apply division rule on membrane 1 (the different membranes labels 3, 4 are results).

R20:  $d [ [a_{s616} b c] [ ]_1 [ ]_2 ]_s \rightarrow d [ [a_{s616} b]_3 [a_{s616} c]_4 [ ]_2 ]_s$ , where  $b, c, d, a_{s616} \in V$ .



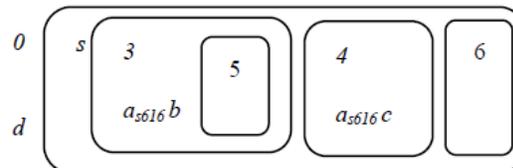
5) Apply division rule on membrane 2 (the different membranes labels 5, 6 are results).

R21:  $d [ [a_{s616} b]_3 [a_{s616} c]_4 [ ]_2 ]_s \rightarrow d [ [a_{s616} b]_3 [a_{s616} c]_4 [ ]_5 [ ]_6 ]_s$ , where  $b, c, d, a_{s616} \in V$ .



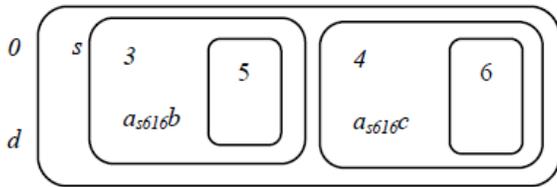
6) Apply mendo rule on membranes 5 and 3

R22:  $d [ [a_{s616} b]_3 [a_{s616} c]_4 [ ]_5 [ ]_6 ]_s \rightarrow d [ [a_{s616} b] [ ]_3 [a_{s616} c]_4 [ ]_6 ]_s$ , where  $b, c, d, a_{s616} \in V$ .



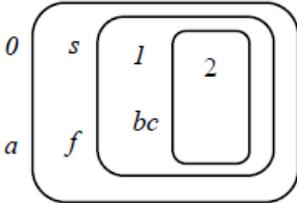
7) Apply mendo rule on membranes 6 and 4

R23:  $d [ [a_{s616} b] [ ]_3 [a_{s616} c]_4 [ ]_6 ]_s \rightarrow d [ [a_{s616} b] [ ]_3 [a_{s616} c] [ ]_4 ]_s$ , where  $b, c, d, a_{s616} \in V$ .



Final Configuration of Mode3

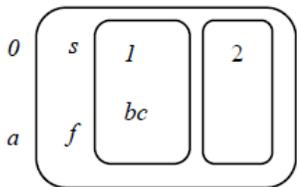
Rules of mode 4:



Initial Configuration of mode 4

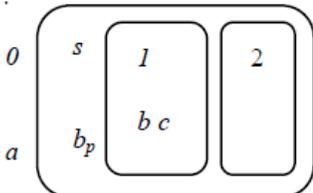
1) Apply mexo rule on membranes 2 and 1.

R24:  $a [f [b c [ ]_2]_1]_s \rightarrow a [f [b c]_1 [ ]_2]_s$ , where  $a, b, c, f \in V$ .



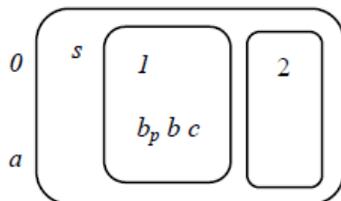
2) Apply object evolution rule,  $[f \rightarrow b_p]$ .

R25:  $a [f [b c]_1 [ ]_2]_s \rightarrow a [b_p [b c]_1 [ ]_2]_s$ , where  $a, b, c, f, b_p \in V$ .



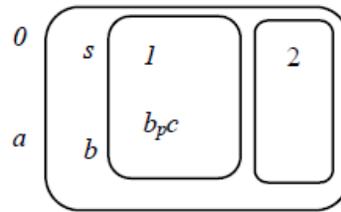
3) Apply communication rule;  $b_p$  object is sent in membrane 1.

R26:  $a [b_p [b c]_1 [ ]_2]_s \rightarrow a [[b_p b c]_1 [ ]_2]_s$ , where  $a, b, c, b_p \in V$ .



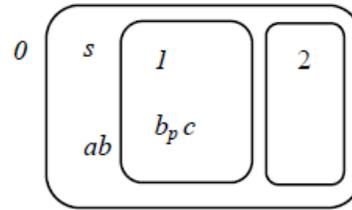
4) Apply communication rule;  $b$  object is sent out from membrane 1.

R27:  $a [[b_p b c]_1 [ ]_2]_s \rightarrow a [b [b_p c]_1 [ ]_2]_s$ , where  $a, b, c, b_p \in V$ .



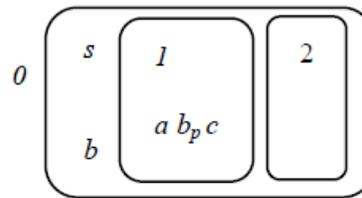
5) Apply communication rule;  $a$  object is sent in skin membrane.

R28:  $a [b [b_p c]_1 [ ]_2]_s \rightarrow [a b [b_p c]_1 [ ]_2]_s$ , where  $a, b, c, b_p \in V$ .



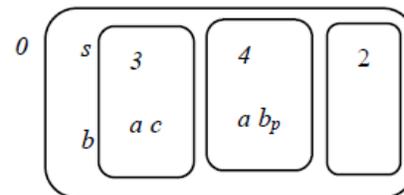
6) Apply communication rule;  $a$  object is sent in membrane 1.

R29:  $[a b [b_p c]_1 [ ]_2]_s \rightarrow [b [a b_p c]_1 [ ]_2]_s$ , where  $a, b, c, b_p \in V$ .



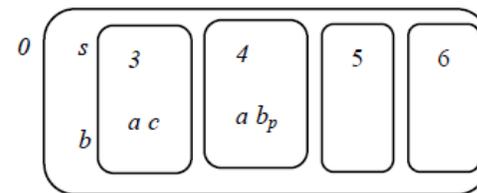
7) Apply division rule on membrane 1 (the different membranes labels 3, 4 are results).

R30:  $[b [a b_p c]_1 [ ]_2]_s \rightarrow [b [a c]_3 [a b_p]_4 [ ]_2]_s$ , where  $a, b, c, b_p \in V$ .



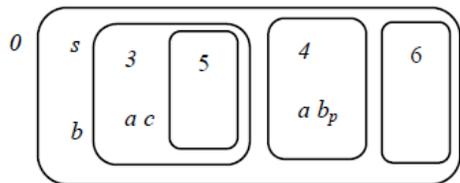
8) Apply division rule on membrane 2 (the different membranes labels 5, 6 are results).

R31:  $[b [a c]_3 [a b_p]_4 [ ]_2]_s \rightarrow [b [a c]_3 [a b_p]_4 [ ]_5 [ ]_6]_s$ , where  $a, b, c, b_p \in V$ .



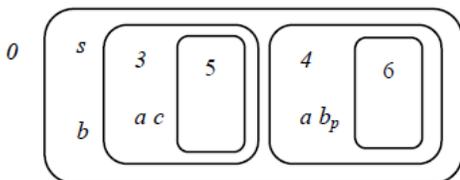
9) Apply mendo rule on membranes 5 and 3.

R32:  $[b [a c]_3 [a b_p]_4 [ ]_5 [ ]_6]_s \rightarrow [b [a c [ ]_5]_3 [a b_p]_4 [ ]_6]_s$ ,  
where  $a, b, c, b_p \in V$ .



10) Apply mendo rule on membranes 6 and 4.

R33:  $[b [a c [ ]_5]_3 [a b_p]_4 [ ]_6]_s \rightarrow [b [a c [ ]_5]_3 [a b_p]_6]_4]_s$ ,  
where  $a, c, b_p \in V$ .



Final Configuration of Mode 4

### C. Computational Properties of Proposed Model

There are several features of our model and are really appropriate for many problems (solvable) that will be discussed:

1) *Distribution*: the behavior of interactive systems in the mitochondrial model depends on nonlinearly results from protein composition to get a new configuration.

2) *Algorithmically*: Our computability model is defined by active and mobile variants, which deal with the Turing machine's computational power or other classic representations of algorithms, making full computational models as decidability devices and efficient algorithms to solve NP-complete problems in polynomial time easy to simulate (and exponential space).

3) *Transparency*: the rules applied in this model are nothing else than reaction equations as illustrated in the previous subsection, biological fusion, and fission models without any mysterious notation and mysterious behavior.

4) *Non-determinism*: our model is viewed as a collection of instructions/rules, with the sole structure being that imposed by membrane localization, but structure inside each membrane consisting of rigid sequences of instructions of programs written in common programming languages.

## V. EFFICIENT SOLUTIONS TO DIFFERENT CLASSES OF PROBLEMS USING PROPOSED MODEL

### A. Computational Complexity Classes with Proposed Model

The types of rules used in the proposed model are shown in the first column of Table II, while the applied rules for each type are listed in the second column. The basic classes of computational complexity problems have been shown in the second row are matched to the set of rules in the third column presenting solvability of each rule type.

TABLE II. COMPUTATIONAL POWER OF RULES RECOGNIZER IN PROPOSED MODEL

Rules Types	Rules Applied in our Models	Classes of Problems		
		P	NP	PSPACE
Evolution rule (a)	R8, R10, R18, R25	√	*	√
In-Communication rule (b)	R11, R19, R26, R28, R29	-	√	√
Out-Communication rule (c)	R9, R12, R27	-	√	√
Membranes Division rule (d)	R13, R14, R20, R21, R30, R31	*	√	√

√ denotes allowed types of rules; \* denotes disallowed types and - Rules with no impact on the computational power

Details of the notations P, NP, and PSPACE with definitions are presented in [48]. P is referred to Problems that had been solved in polynomial time with the evolution and rewriting rules for only one membrane [18, 49, and 50]. For instance, the ranking problem for three numbers had been solved by conventional computers. It has a computational power with P systems with an evolution rule. SUBSET SUM problem is belonging to a class of NP-complete problems that have been solved by division rule for elementary membranes with communication rules. In [51], the efficiency proof of its solution is demonstrated in uniform linear time. The QSAT problem is belonging to a class of PSPACE problems that are called "second class computers". QSAT has been solved by different families of active membranes. PSPACE class has been confirmed as an upper bound of the computations in polynomial time with P systems in [41].

Briefly, Table II is the summary of computational complexity power of rules that belong to active variant and used in this model. Presenting accepted classes of problems in polynomial time. The rules of types from (b, c, and d) can solve NP-complete problems in polynomial time as shown in the fifth column in Table II. Where the division rules for elementary membranes are unrestricted which leads to an increase of computational power [52, 53]. While the rules of types from (a) to (d) are suitable to address PSPACE problems in polynomial time. In [54] highlighted the role of different restrictions/extensions of evolution, communication rules.

### B. Solving SAT Problem using MDM

- The Satisfiability of a propositional logic formula in conjunctive normal form is known as the SAT problem. It is classified as a strong problem in categories of NP-complete problems.
  - For any instance of SAT, Consider the following expression:
 
$$\beta = C_1 \wedge C_2 \wedge \dots \wedge C_m \text{ over } X = \{x_1, x_2, \dots, x_n\} \text{ such } x_i$$
 where  $1 \leq i \leq n$ . In this case,  $(n = 3)$ .
  - For each  $C_i$ ,  $1 \leq i \leq m$ . In this case  $(m=3)$ , a disjunction of the form  $C_i = y_1 y_2 \vee \dots \vee y_r$  ( $r \leq n$ ), where each  $y_j$  indicates to variable  $x_k$  or negation of  $x_k$ ,  $\bar{x}_k$

- The working over the alphabet:  $V = \{z, \bar{z}, q, \bar{q}, g, g_0, \gamma, \bar{\gamma}, \text{yes}, \text{no}, b_i, t_i, f_i, \gamma_i, \bar{\gamma}_i \mid 1 \leq i \leq n\}$
- We construct the system by use the fission model configuration that has MDM rules to generate all potential variables assignments,  $\{x_1, \dots, x_n\}$ . By rules of MDM to solve the SAT problem as follows:

1)  $[b_i]_s \rightarrow [t_i b_{i+1}]_s [f_i b_{i+1}]_s$ , for  $1 \leq i \leq n - 1$  (division rule)

$[b_n]_s \rightarrow [t_n \gamma_1]_s [f_n \gamma_1]_s$  (division rule)

$[g]_1 \rightarrow [ ]_1 [ ]_1$  (division rule)

$[g_0]_1 \rightarrow [\bar{\gamma}_1]_1 [\bar{\gamma}_1]_1$  (division rule)

- $2^n$  membranes are created from the first two rules and labeled by  $s$  contain all potential variables assignments,  $\{x_1, \dots, x_n\}$ . Each membrane labeled by  $s$  is assigned by object  $\gamma_1$ .
- $2^n$  membranes labeled by 1 are created from the following two rules. Each one of them contains object  $\bar{\gamma}_1$ . The correct assignments for  $C_i$  are determined by using symbols  $\gamma_i$  and  $\bar{\gamma}_i$  in two steps.

2)  $[t_j \gamma_i]_s [\bar{\gamma}_i]_1 \rightarrow [[t_j \gamma_i]_s \bar{\gamma}_i]_1$  (mendo)

$[[t_j \gamma_i]_s \bar{\gamma}_i]_1 \rightarrow [t_j \gamma_{i+1}]_s [\bar{\gamma}_{i+1}]_1$  (mexo)

(in case  $C_i$  includes the literal  $x_j$ )

$[f_j \gamma_i]_s [\bar{\gamma}_i]_1 \rightarrow [[f_j \gamma_i]_s \bar{\gamma}_i]_1$  (mendo)

$[[f_j \gamma_i]_s \bar{\gamma}_i]_1 \rightarrow [f_j \gamma_{i+1}]_s [\bar{\gamma}_{i+1}]_1$  (mexo)

(in case  $C_i$  includes the literal  $\neg x_j$ )

$[t_j \gamma_m]_s [\bar{\gamma}_m]_1 \rightarrow [[t_j \gamma_m]_s \bar{\gamma}_m]_1$  (mendo)

$[[t_j \gamma_m]_s \bar{\gamma}_m]_1 \rightarrow [t_j z]_s [\bar{\gamma}_m]_1$  (mexo)

(in case  $C_m$  includes the literal  $x_j$ )

$[f_j \gamma_m]_s [\bar{\gamma}_m]_1 \rightarrow [[f_j \gamma_m]_s \bar{\gamma}_m]_1$  (mendo)

$[[f_j \gamma_m]_s \bar{\gamma}_m]_1 \rightarrow [f_j z]_s [\bar{\gamma}_m]_1$  (mexo)

(in case  $C_m$  includes the literal  $\neg x_j$ )

The objects  $\gamma_i$  from the identical membrane  $s$  are exchanged by  $\gamma_{i+1}$  if the assignments fulfilled the clause  $C_i$ . The assignments from the membranes which contain  $\gamma_{i+1}$  satisfy the clauses  $C_1, \dots, C_i$ , then, the object  $\gamma_{i+1}$  indicate the result in next step the clause  $C_{i+1}$  is checked. If all clauses are satisfied, then the membranes which have these assignments will be marked by object  $\bar{z}$ .

3)  $[c_i \gamma]_2 [\bar{\gamma}]_3 \rightarrow [[c_{i+1} \gamma]_2 \bar{\gamma}]_3$  (mendo)

$[[c_i \gamma]_2 \bar{\gamma}]_3 \rightarrow [c_{i+1} \gamma]_2 [\bar{\gamma}]_3$  (mexo)

$[[c_{n+2m+1} \gamma]_2 \bar{\gamma}]_3 \rightarrow [d \gamma]_2 [\bar{\gamma}]_3$  (mexo)

$[c_{n+2m+1} \gamma]_2 [\bar{\gamma}]_3 \rightarrow [[c_{n+2m+1} \gamma]_2 \bar{\gamma}]_3$  (mendo)

The mentioned rules in (iii) are used to determine the number of steps is applied in rules of type (ii). If the number of

steps is larger than  $n + 2m + 1$ , this is indicated to clauses are not satisfy. Then an object  $q$  is generated, that will create an object **no**. The number  $n + 2m + 1$  correspond to the following steps: generating space in  $n$  steps, validate assignments in  $2m$  steps, generating a **yes** object in one step. Additionally, step can be applied; membrane 2 including the object  $c_{n+2m+1}$  becomes sibling with membrane 3, thus increasing the number of steps needed to generate **d** object to  $n + 2m + 2$ .

4) iv.  $[\bar{z}]_s [z]_4 \rightarrow [[yes]_4]_s$  (mendo)

$[q]_3 [\bar{q}]_4 \rightarrow [[no]_3]_4$  (mendo).

- When membrane 4 enters membrane  $s$  in  $(2m+n+1)$  step, a yes object is created. But a no object is created when no membrane  $s$  contains an object  $q$ . When membrane 3 enters membrane 4, one of these two rules cannot be applied anymore. Finally, the computation result is either a yes or a no object in the system.
- The size of the working alphabet is  $4n+4m+13$ . The number of used rules is computed as follows: the number of rules from type (i) is  $n + 2$ , the number of rules from type (ii) is  $4nm$ , the number of rules from type (iii) is  $n + 2m + 3$  and the number of rules from type (iv) is 2 rules.
- As a result, the size of the computing system to solve SAT is  $O(mn)$ . Because  $n + 2m$  is an odd number, the computation ends in  $n + 2m + 3$ . As a result, we had to do an extra step before obtaining  $q$  object from  $c_{n+2m+1}$ . If  $n+2m$  is an even integer, then after  $n + 2m + 2$  steps,  $q$  object is generated.

## VI. REPRESENTATION MODEL USING UML

Different diagrams of UML are used to analyze the behavior of mitochondria fusion-fission models. The first diagram represents the modality of normal mitochondria organelles in the living cell using an object diagram as shown in Fig. 5.

Fig. 5 revealed that the object diagram is combined from a superclass titled cell that is considered as “environment” in P systems. The super class is consisting of many objects that represent components of a living cell that contains at least two mitochondria. Our proposed design is interested in mitochondria object which is a sub class from the superclass. The mitochondria object has some attributes such as DNA, RNA, and the mitochondria functional operations. The basic operations of mitochondria objects are fusion, fission, motility, and mitophagy, while in the current study, the authors focused on the fusion and fission operations. The outer and inner membranes objects are composited from mitochondria objects, where each mitochondrion has one outer membrane and one inner membrane, and all of them, have some attributes that are represented by proteins that involved in the fusion and fission processes.

Fig. 5 revealed that the object diagram is combined from a superclass titled cell that is considered as “environment” in P systems. The super class is consisting of many objects that represent components of a living cell that contains at least two mitochondria. Our proposed design is interested in

mitochondria object which is a sub class from the superclass. The mitochondria object has some attributes such as DNA, RNA, and the mitochondria functional operations. The basic operations of mitochondria objects are fusion, fission, motility, and mitophagy, while in the current study, the authors focused on the fusion and fission operations. The outer and inner membranes objects are composited from mitochondria objects, where each mitochondrion has one outer membrane and one inner membrane, and all of them, have some attributes that are represented by proteins that involved in the fusion and fission processes.

The diagram is illustrated in Fig. 6, the activity diagram and represents the interactions that occurred in two mitochondria objects to keep their metabolic regulation using fusion operations. The events that occurred to complete fusion operations of the two normal mitochondria organelles were

analyzed in Fig. 6. First, both outer membranes object with their contents such as proteins, enzymes, and ATP molecules are merged by chemical interactions to complete the binding process owing to the formation of a new outer membrane object. Second, both inner membranes object was merged using other chemical operations involved in the binding process followed by the production of a new inner membrane object. Lastly, both objects are joined producing new outer and new inner membranes leading to the production of new mitochondrion object which contains inherits behaviors from the original one. In Fig. 7, actions and events are analyzed to complete fission operations to the one normal mitochondrion organelle. First, the object of Drp1 protein is called to mitochondrion object to interact with proteins in the outer membrane, then one action from four actions will be activated the fission operation according to the required signal. Finally, the mitochondrion divided into two mitochondria organelles.

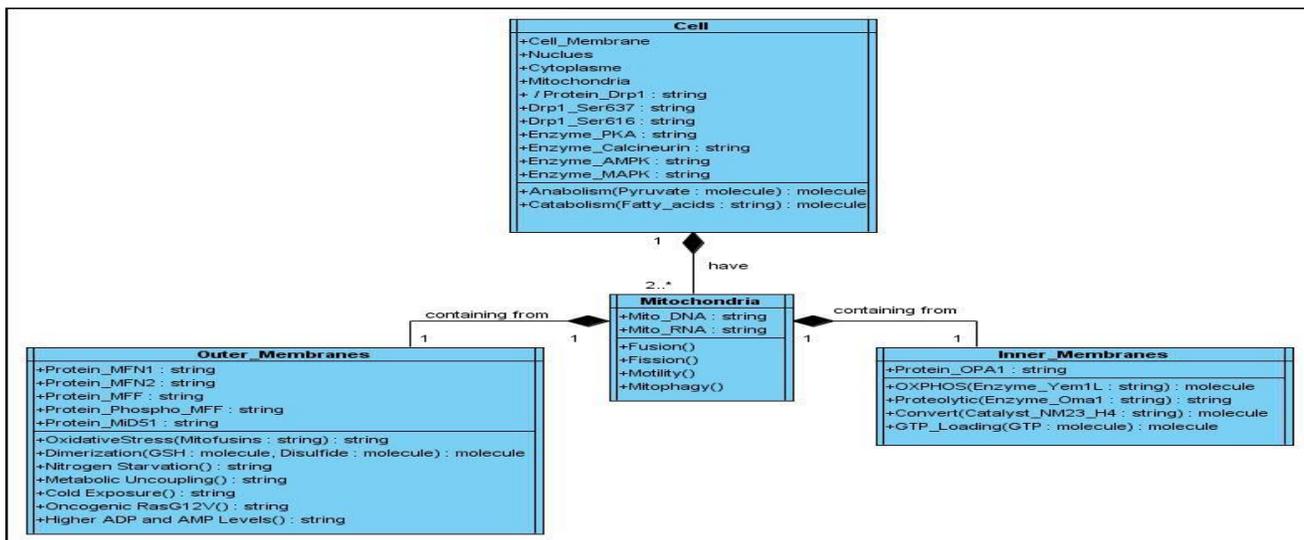


Fig. 5. Object Diagram of Mitochondria Components.

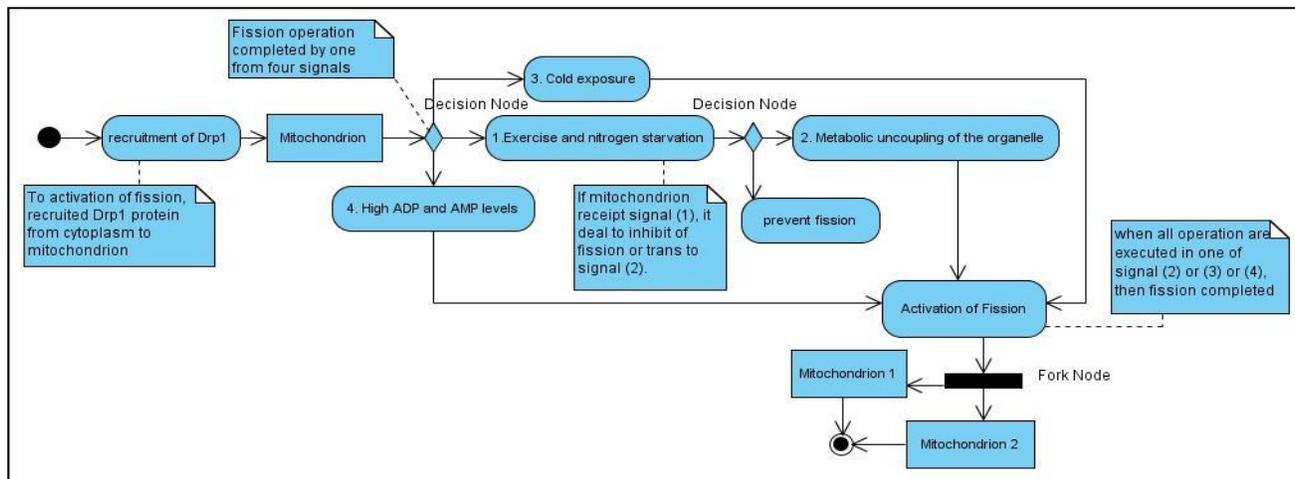


Fig. 6. Activity Diagram for Actions Fusion Model.

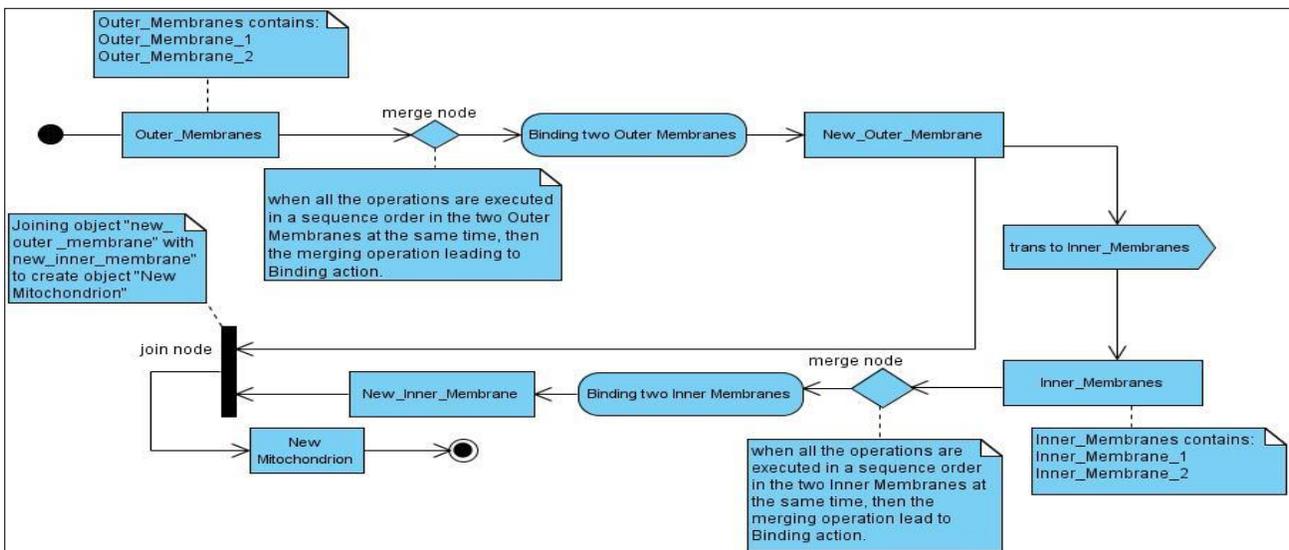


Fig. 7. Activity Diagram for Actions Fission Model.

## VII. CONCLUSION AND FUTURE WORK

P systems can be used to model biological and physiological processes. This paper proposed a model of two actual biological functions of important organelle in a living cell, mitochondria fusion, and fission. This model, MDM, combined a set of rules from different variants of P systems, division rule with mexo and mendo rules that provided higher efficiency in terms of space complexity rather than using rules of active membranes only. The conclusion of this work can be summarized in terms of three aspects. First, P is a computational power set of evolution rules in polynomial time. While a set of PSPACE problems are solved in polynomial time using polynomial uniform of active membranes families with the operation of elementary membrane division. This is one of the most well-studied methods for getting an exponential working space in order to exchange space for time and solve computationally difficult problems (commonly NP-complete problems) in a timely manner (typically polynomial or even linear). Second, this research introduced a semi-uniform linear time solution to SAT problem using MDM rules with 3 membranes. From the results, we proofed that only three membranes suffice in solving the SAT problem. MDM is faster than other models that used 9 membranes to obtain computational universality. Finally, using biological models and development of their object relationship diagrams have been implemented using object-oriented programming (OOP) to be used as an analysis tool for complex data of mitochondria neurodegenerative diseases.

Future research topics may include:

- 1) Understanding of the remaining two operations of mitochondrial regulation (motility and mitophagy) and simulated them by P systems variants.
- 2) Designing a complete model for metabolic regulation of mitochondrial dynamics.
- 3) By different kinds of cell-like P systems.

4) Complete understanding of physiological processes for studying different diseases and malfunctions involved in human neurodegenerative system mediated by irregular mitochondria.

5) Investigating and studying other biological operations for modeling other echo systems using different P systems variants.

6) We hope to define and develop a new strategy in OOP using P systems with active and dynamic rules to solve nondeterministic problems in polynomial time specifically in Machine Learning algorithms.

## REFERENCES

- [1] Paun G, Rozenberg G, Salomaa A. DNA computing: new computing paradigms. Springer Science & Business Media; 2005 Feb 4.
- [2] Román G. Inference of bounded L systems with polymorphic P systems. *Journal of Membrane Computing*. 2019 Mar;1(1):52-7.
- [3] Ambainis A, Yakaryılmaz A. Automata and quantum computing. arXiv preprint arXiv:1507.01988. 2015 Jul 7.
- [4] Haldurai L, Madhubala T, Rajalakshmi R. A study on genetic algorithm and its applications. *International Journal of Computer Sciences and Engineering*. 2016 Oct;4(10):139.
- [5] Albawi S, Mohammed TA, Al-Zawi S. Understanding of a convolutional neural network. In 2017 International Conference on Engineering and Technology (ICET) 2017 Aug 21 (pp. 1-6). IEEE.
- [6] Sempere JM. Modeling of decision trees through P systems. *New Generation Computing*. 2019 Sep;37(3):325-37.
- [7] Ciobanu G, Păun G. Applications of membrane computing. Pérez-Jiménez MJ, editor. Berlin: Springer; 2006 Oct.
- [8] Zhang, Gexiang, et al. "An overview of hardware implementation of membrane computing models." *ACM Computing Surveys (CSUR)* 53.4 (2020): 1-38.
- [9] Song, B., Li, K., Orellana-Martín, D., Valencia-Cabrera, L., & Pérez-Jiménez, M. J. (2020). Cell-like P systems with evolutionary symport/antiport rules and membrane creation. *Information and Computation*, 275, 104542.
- [10] Păun G. Languages in membrane computing: some details for spiking neural p systems. In *International Conference on Developments in Language Theory 2006 Jun 26* (pp. 20-35). Springer, Berlin, Heidelberg.
- [11] Freund R, Păun G. On the number of non-terminal symbols in graph-controlled, programmed and matrix grammars. In *International*

- Conference on Machines, Computations, and Universality 2001 May 23 (pp. 214-225). Springer, Berlin, Heidelberg.
- [12] Jiménez MJ, Jiménez ÁR, Caparrini FS. Complexity classes in models of cellular computing with membranes. *Natural Computing*. 2003 Sep 1;2(3):265-85.
- [13] García-Quismondo M, Graciani C, Riscos-Núñez A. Membrane computing as a modelling tool: looking back and forward from Sevilla. In *Enjoying Natural Computing 2018* (pp. 114-129). Springer, Cham.
- [14] Macías - ramos LF, Song B, Valencia - Cabrera L, Pan L, Pérez - jiménez MJ. Membrane fission: A computational complexity perspective. *Complexity*. 2016 Jul;21(6):321-34.
- [15] Orellana-Martín D, Valencia-Cabrera L, Riscos-Núñez A, Pérez-Jiménez MJ. Minimal cooperation as a way to achieve the efficiency in cell-like membrane systems. *Journal of Membrane Computing*. 2019 Jun 1;1(2):85-92.
- [16] Aman B, Ciobanu G. Mobile membranes: Computability and complexity. In *International Colloquium on Theoretical Aspects of Computing 2013 Sep 4* (pp. 59-75). Springer, Berlin, Heidelberg.
- [17] Alexiou AT, Psiha MM, Rekkas JA, Vlamos PM. A stochastic approach of mitochondrial dynamics. *World AcadSciEng Technol*. 2011 Jul 29;55:77-80.
- [18] Aman B, Ciobanu G. Mobile Membranes. *IEEE Access*. 2020 Jul 24;8:147439-50.
- [19] Krishna SN, Păun G. P systems with mobile membranes. *Natural Computing*. 2005 Sep 1;4(3):255-74.
- [20] Macías-Ramos LF, Pérez-Jiménez MJ, Riscos-Núñez A, Valencia-Cabrera L. Membrane fission versus cell division: When membrane proliferation is not enough. *Theoretical Computer Science*. 2015 Dec 10; 608:57-65.
- [21] Alhazov, A., & Pan, L. Trading Polarizations for Labels in P Systems with Active Membranes, submitted, 2004, 7(1), 141:159.
- [22] Alhazov A, Pan L, Păun G. Trading polarizations for labels in P systems with active membranes. *Acta Informatica*. 2004 Dec 1;41(2-3):111-44.
- [23] Mishra P, Chan DC. Metabolic regulation of mitochondrial dynamics. *Journal of Cell Biology*. 2016 Feb 15;212(4):379-87.
- [24] Păun G. Computing with membranes. *Journal of Computer and System Sciences*. 2000 Aug 1;61(1):108-43.
- [25] Păun A. On P systems with active membranes. In *Unconventional Models of Computation, UMC'2K 2001* (pp. 187-201). Springer, London.
- [26] Păun G. Computing with membranes: Attacking NP-complete problems. In *Unconventional models of Computation, UMC'2K 2001* (pp. 94-115). Springer, London.
- [27] Martín-Vide C, Păun G, Pazos J, Rodríguez-Patón A. Tissue P systems. *Theoretical Computer Science*. 2003 Mar 8;296(2):295-326.
- [28] Păun G. Computing with membranes: Attacking NP-complete problems. In *Unconventional models of Computation, UMC'2K 2001* (pp. 94-115). Springer, London.
- [29] Margenstern M, Martín-Vide C, Păun G (2002) Computing with membranes: variants with an enhanced membrane handling. *DNA computing*. Springer, New York, pp 340-349
- [30] Wang T, Wang J, Ming J, Sun Z, Wei C, Lu C, Pérez-Jiménez MJ. Application of neural-like P systems with state values for power coordination of photovoltaic/battery microgrids. *IEEE Access*. 2018 Aug 13;6:46630-42.
- [31] Păun G, Pérez-Jiménez MJ et al (2012) Languages and P systems: recent developments. *ComputSci* 20(2):59
- [32] Barbuti R, Maggiolo-Schettini A, Milazzo P, Pardini G, Tesi L (2011) Spatial P systems. *Nat Comput* 10(1):3-16
- [33] Giannakis K, Andronikos T. Membrane automata for modeling biomolecular processes. *Natural Computing*. 2017 Mar 1;16(1):151-63.
- [34] Peng H, Wang J, Ming J, Shi P, Pérez-Jiménez MJ, Yu W, Tao C. Fault diagnosis of power systems using intuitionistic fuzzy spiking neural P systems. *IEEE Transactions on Smart Grid*. 2017 Feb 16;9(5):4777-84.
- [35] Zhao J, Wang N. A bio-inspired algorithm based on membrane computing and its application to gasoline blending scheduling. *Coputers & chemical engineering*. 2011 Feb 9;35(2):272-83.
- [36] Peng H, Wang J, Shi P, Riscos-Núñez A, Pérez-Jiménez MJ. An automatic clustering algorithm inspired by membrane computing. *Pattern Recognition Letters*. 2015 Dec 15;68:34-40.
- [37] Cooper J, Nicolescu R. The Hamiltonian cycle and travelling salesman problems in cP systems. *Fundamenta Informaticae*. 2019 Jan 1;164(2-3):157-80.
- [38] Zandron C, Ferretti C, Mauri G. Solving NP-Complete Problems Using P Systems. In *Unconventional Models of Computation, UMC'2K: Proceedings of the Second International Conference on Unconventional Models of Computation,(UMC'2K) 2012 Dec 6* (p. 289). Springer Science & Business Media.
- [39] Gutiérrez-Naranjo MA, Pérez-Jiménez MJ, Riscos-Núñez A, Romero-Campero FJ. On the power of dissolution in P systems with active membranes. In *International workshop on membrane computing 2005 Jun 18* (pp. 224-240). Springer, Berlin, Heidelberg.
- [40] Pan L, Ishdorj TO. P Systems with Active Membranes and Separation Rules. *J. UCS*. 2004 May 28;10(5):630-49.
- [41] Sosik P, Păun A, Rodríguez-Patón A. P systems with proteins on membranes characterize PSPACE. *Theoretical Computer Science*. 2013 Jun 3;488:78-95.
- [42] Song B, Pérez-Jiménez MJ, Pan L. An efficient time-free solution to QSAT problem using P systems with proteins on membranes. *Information and Computation*. 2017 Oct 1;256:287-99.
- [43] Aman B, Ciobanu G. Turing completeness using three mobile membranes. In *International Conference on Unconventional Computation 2009 Sep 7* (pp. 42-55). Springer, Berlin, Heidelberg.
- [44] Krishna SN. The power of mobility: Four membranes suffice. In *Conference on Computability in Europe 2005 Jun 8* (pp. 242-251). Springer, Berlin, Heidelberg.
- [45] Csuhaj-Varjú E, Vaszil G. On the power of P automata. In *International Conference on Unconventional Computing and Natural Computation 2013 Jul 1* (pp. 55-66). Springer, Berlin, Heidelberg.
- [46] Cardelli L, Paun G. An universality result for a (mem) brane calculus based on mate/drip operations. *International Journal of Foundations of Computer Science*. 2006 Feb;17(01):49-68.
- [47] Mishra P, Chan DC. Metabolic regulation of mitochondrial dynamics. *Journal of Cell Biology*. 2016 Feb 15;212(4):379-87.
- [48] Valiant LG, van Leeuwen J. Handbook of theoretical computer science. In *Algorithms and Complexity, chapter General Purpose Parallel Architectures 1990* (pp. 943-971). Elsevier Science.
- [49] Mauri G, Paun G, Pérez-Jiménez MJ, Rozenberg G, Salomaa A, editors. *Membrane Computing: 5th International Workshop, WMC 2004, Milan, Italy, June 14-16, 2004, Revised Selected and Invited Papers*. Springer Science & Business Media; 2005 Mar 7.
- [50] Gheorgue M, Paun G, Pérez Jiménez MD. Frontiers of membrane computing: Open problems and research topics. *Proceedings of the Tenth Brainstorming Week on Membrane Computing, 171-250*. Sevilla, ETS de Ingeniería Informática, 30 de Enero-3 de Febrero, 2012.
- [51] Song B, Pérez-Jiménez MJ, Pan L. Efficient solutions to hard computational problems by P systems with symport/antiport rules and membrane division. *BioSystems*. 2015 Apr 1;130:51-8.
- [52] Leporati A, Manzoni L, Mauri G, Porreca AE, Zandron C. Simulating elementary active membranes. In *International Conference on Membrane Computing 2014 Aug 20* (pp. 284-299). Springer, Cham.
- [53] Zandron C, Leporati A, Ferretti C, Mauri G, Pérez-Jiménez MJ. On the computational efficiency of polarizationless recognizer P systems with strong division and dissolution. *Fundamenta Informaticae*. 2008 Jan 1;87(1):79-91.
- [54] Song B, Song T, Pan L. Time-free solution to SAT problem by P systems with active membranes and standard cell division rules. *Natural Computing*. 2015 Dec;14(4):673-81.

# Skin Lesions Classification and Segmentation: A Review

Marzuraikah Mohd Stofa, Mohd Asyraf Zulkifley, Muhammad Ammirul Atiqi Mohd Zainuri  
Department of Electrical, Electronic and Systems Engineering, Universiti Kebangsaan Malaysia, Bangi, Malaysia

**Abstract**—An automated intelligent system based on imaging input for unbiased diagnosis of skin-related diseases is an essential screening tool nowadays. This is because visual and manual analysis of skin lesion conditions based on images is a time-consuming process that puts a significant workload on health practitioners. Various machine learning and deep learning techniques have been researched to reduce and alleviate the workloads. In several early studies, the standard machine learning techniques are the more popular approach, which is in contrast to the recent studies that rely more on the deep learning approach. Although the recent deep learning approach, mainly based on convolutional neural networks has shown impressive results, some challenges remain open due to the complexity of the skin lesions. This paper presents a wide range of analyses that cover classification and segmentation phases of skin lesion detection using deep learning techniques. The review starts with the classification techniques used for skin lesion detection, followed by a concise review on lesions segmentation, also using the deep learning techniques. Finally, this paper examined and analyzed the performances of state-of-the-art methods that have been evaluated on various skin lesion datasets. This paper has utilized performance measures based on accuracy, mean specificity, mean sensitivity, and area under the curve of 12 different Convolutional Neural Network based classification models.

**Keywords**—Lesion segmentation; lesion classification; machine learning; deep learning; skin lesions

## I. INTRODUCTION

Skin cancer is one of the most dangerous types of cancer that infected humans regularly. In the field of dermatology, there are two types of skin cancers, which are melanocytic and non-melanocytic. For example, melanoma is a type of melanocytic cancer, which is found to be a riskier version of cancer compared to the non-melanocytic type. Therefore, diagnosis of the correct type of cancer at an early stage is important to reduce the mortality risk [1], [2]. Besides that, there are certain parts of the body that have a higher probability of infection such as the chest, back, and legs. Then, this paper observed that most research in recent years has focused on establishing an automated intelligent system for the unbiased diagnosis of pigmented skin lesions. The general framework of the system involves pre-processing, feature extraction, segmentation, and classification phases, which are necessary steps in obtaining accurate localization of the skin lesion map. Masood et al. [3] and Adeyinka et al. [4] is also found that diagnosis of skin cancer at an early stage using computer vision provides a significant improvement when machine learning techniques are implemented. First, the diagnosis process begins by removing unnecessary structures or artifacts

on the skin lesion image that might interfere during the segmentation process, such as air bubbles, hair, blood vessels, and oily surfaces. In general, skin lesions come in various colors, shapes, and sizes that limit the standard machine learning ability to obtain high levels of accuracy. This process involves complex annotations during manual screening even for dermatologists. Therefore, Al-Masni et al. [5] presented that an automated computerized diagnostic system is an important tool in skin lesion analysis that will be able to assist and support dermatologists in making timely decisions. Abdani et al. [6] show that deep learning has demonstrated its effectiveness in various applications, particularly in computer vision-related systems that use convolutional neural networks (CNN) as the base framework, even for a compact version. For example, a previous study in [7] has shown that the popular method in deep learning is through CNN utilization, which can process common and highly variable tasks in handling delicate objects. Krizhevsky et al. [8] and Lecun et al. [9] prove that this sophisticated and optimized model has better ability than handcrafted features in extracting outstanding features from the entire images of skin lesions.

The development of computer-aided algorithms is essential to address the increasing problem of global skin cancer cases where it is able to handle large amounts of data in real time and automatically. It is important to review the performance of deep learning algorithms in the classification and segmentation of skin lesions due to recent advances in deep learning paradigms, and particularly in medical imaging it shows excellent performance. So, in this study, an extensive investigation of the various approaches for analyzing skin lesions was conducted. In addition, the classification techniques are reviewed and compared in Section II, which is the process of categorizing the classes of skin lesions and other types of surfaces. A comparison between all the segmentation techniques is presented in the following Section III. In addition, a comparative analysis using deep learning methods for classification and segmentation of skin lesions was performed in Section IV to show the strengths and weaknesses of each method, and subsequently the conclusion section.

## II. CLASSIFICATION

The skin cancer detection system is made more accessible by categorizing images of lesions. This classification process can assist dermatologists in detecting the possibility of early skin cancer through visual-based sensing. According to the standard medical practice, skin lesions are often classified as benign or malignant cancer. Thence, each of the lesion types can be further classified into seborrheic keratosis, solar lentigo, squamous cell carcinoma, nevi, actinic keratosis, basal cell

carcinoma, melanoma, and others. In this paper, both the traditional and recent state-of-the-art methods were reviewed. Table I summarizes the differences between various general deep classification networks.

TABLE I. COMPARISON BETWEEN GENERAL CNN ARCHITECTURES FOR SKIN LESION CLASSIFICATION TASK

Techniques	Description	Advantages	Disadvantages
AlexNet [10]	Includes three fully connected layers and five convolutional layers. This model used various sizes of filter.	GPU are used as an accelerator to handle the complex architecture.	The probability of generating artifacts from feature maps is high because the filter's size is quite large.
VGGNet [11]	Uses only 3x3 of convolutional filters, placed on top of each other to increase the network depth.	Encouraging performance that uses up to 19 layers with significant improvement over the previous arrangements.	It is challenging to train the model, especially for the cases without transfer learning.
GoogleNet [12]	An architecture that has 22 layers of deep network.	There is no uncontrolled increment in computing complexity when more units are added at each level.	Difficulty in customizing the parameters due to the use of heterogeneous topology.
ResNet [13]	Applies feedforward neural network layers with skip connection by performing identity mapping and added them to the stacked-layer output.	Increase the network's depth and easier to optimize, while reducing zero diminishing gradient issues, which indirectly improves the accuracy.	Information on the features map is complicated and may be degraded throughout the feed-forward procedures.
Xception [14]	An "extreme" version of the Inception module that replaces the module with depth-wise separable convolution	Easy to define and modify with high accuracy performance.	High computational cost due to multiple layers of CNN with 728 filters.
DenseNet [15]	Have a complex connection to achieve maximum information flows between forward and backward layers.	Training is relatively easy due to the enhanced flows of gradient and information across the network.	The number of parameters increases a lot between shallow and deep configurations because of more feature maps in each layer.
EfficientNet [16]	The architecture model consists of eight configurations from B0 to B7, with each subsequent model refers to a variant with more parameters and higher accuracy.	Reduce computation cost and can produce faster classification inference.	In order to catch fine-grained patterns on huge images, the network requires additional layers that increase the receptive field size and uses more channels.

A. Recent Works on Conventional Classification Method

At the beginning of the study on skin lesion classification, the traditional machine learning approach was commonly used, whereby region-based or threshold-based approaches are utilized to extract the features. Some of the most popular conventional approaches nowadays are support vector machine (SVM), k-nearest neighbor, artificial neural network (ANN), and naive Bayesian algorithm [17], [18]. Then, the deep learning-based method was started to be developed to overcome the limitations of previously mentioned conventional approaches. Han et al. [19] presented the conventional methods require significant effort from humans to design the feature extractors, still they do not produce accurate multi-class skin lesions detection.

B. Recent Works on Deep Learning Classification Method

The deep learning method based on the CNN classifier has exceeded the general human capability in performing object classification tasks, whereby historically, it begins to gain popularity in 2012 [20]. Fig. 1 shows the general CNN architecture with standard major components such as CNN layers, activation function, and the trainable hyperparameters. Several previous studies have implemented CNN that was introduced in [7] to produce dermatologist-equivalent skin cancer classifiers [21], [22]. Compared to the traditional methods, the CNN-based methods proved to be more effective. Many CNN architectures are available for skin lesion classification such as AlexNet [10], GoogleNet/InceptionNet [12], VGG Net [11], ResNet [13], XceptionNet [14], DenseNet [15] or EfficientNet [16]. All these methods are discussed as follow:

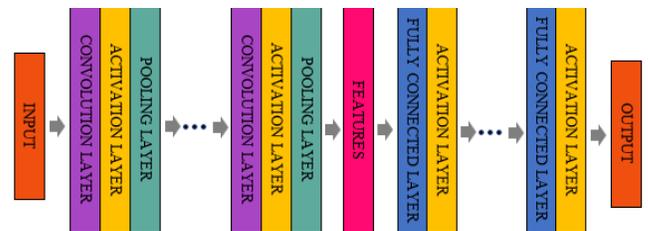


Fig. 1. General Architecture of CNN.

1) AlexNet: AlexNet is a system developed over 10 years ago [10]. It utilizes two operators, the convolutional network and the pooling layer, which will be the main building blocks of the network. The network starts with several layers of convolutional layers, followed by the fully connected layers, which are aligned through flatten operator. AlexNet has also been developed for implementing deep neural networks (DNNs) methodology in speech recognition and computer vision. Such as in 2019, the work in [23] has applied AlexNet to classify skin lesions using various configurations. The proposed method managed to overcome the overfitting problem by adjusting the weight values and enriching the data set with synthetic data generated from different rotation angles. The final classification layer is then replaced with the softmax layer to categorize more than two types of skin lesion categories. The experiment results have exceeded the initial performance expectations, whereby this model is still being

used as the benchmark in classifying the skin lesions. This general architecture of this network is illustrated in Fig. 2.

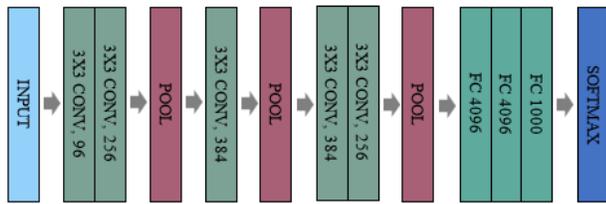


Fig. 2. Diagram of AlexNet Architecture.

2) *VGGNet*: In comparison to AlexNet, VGGNet is a deeper and more complicated network. This model has been further improved by lowering the number of parameters [11]. In fact, it has been used as the building block for many compact applications [24], [25]. This model has been tested in large deep CNN configurations that consist of many convolutional layers followed by pooling layers for huge image classification tasks. Besides that, the pre-trained VGG network is also commonly utilized in various transfer domain applications. However, this model uses a significant amount of processing resources, and hence makes the application of the VGG model a tiresome task. Sun et al. [26] have recommended the usage of VGGNet to diagnose 198 types of skin lesions which were trained until they reached an optimal set of hyperparameters. They have utilized the DermQuest data set, which included 6,584 clinical pictures, whereby they have managed to obtain 50.27% average accuracy. Fig. 3. shows the general VGG 16 architecture, which is one of the biggest VGG network variants.

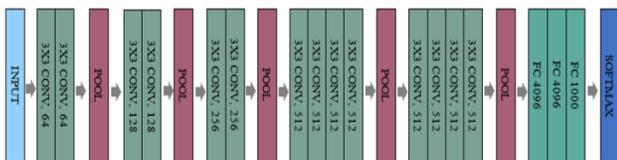


Fig. 3. Diagram of VGG 19 Architecture.

3) *GoogleNet*: GoogleNet is also popularly known as the InceptionNet [12]. It is composed of a 22-layer convolutional network structure. The primary goal of this design is to observe how the optimal local sparse structure can be handled and protected by the existing compact components. Most commonly, an Inception system is formed from modules that are stacked on top of one another. As Inception modules are stack on top of each other, their output correlation varies because deeper layers will capture better abstraction features, while the spatial concentration is expected to decrease accordingly. This reduction is done as such it will help the model to attain a faster training convergence. Thurnhofer-Hemsi et al. [27] have also used the CNN methodology to classify the skin lesion type based on the DermQuest database. The raw images were directly inserted into the CNN model to determine the presence of melanoma or not. They found out that GoogleNet and AlexNet produced the best results among the tested models. The authors have produced a highly accurate

system in terms of mean accuracy compared to the benchmarked models, even without utilizing any pre-processing step. The multiple inception modules are shown in Fig. 4.

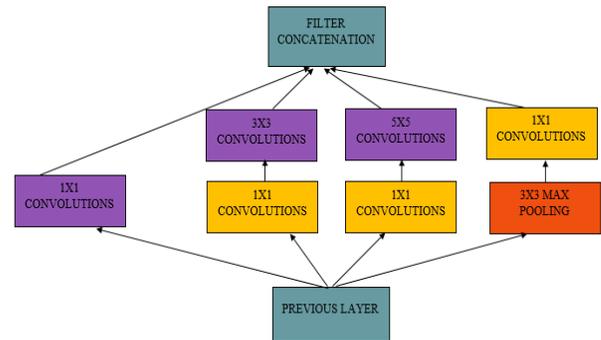


Fig. 4. Architecture of the GoogleNet Inception Module.

4) *ResNet*: As previously mentioned in [13], the residual modules in ResNet architecture can be used to train a very deep network effectively just by using the conventional stochastic gradient descent (SGD). He et al. [13] have shown that the residual networks with 152 layers can easily be trained and optimized to produce a model with good accuracy as its architecture becomes deeper. Moreover, they have also applied a feedforward neural network scheme with skip connection by performing identity mapping to combine the existing and skipped layers. This architecture is eight times deeper than VGGNet but it is still less complex and easier to train. Le et al. [28] have proposed a model that leverages the transfer learning method by using pre-trained models of ResNet 50, VGG 16, and MobileNet, coupled with weights and loss functions that focus on the classification process. Their results indicate that the ResNet 50 model produced the best performance with an average accuracy of 93% and total accuracy within the range [0.7, 0.94], which has surpassed the accuracy of dermatologists with an average accuracy of 84%.

5) *XceptionNet*: As an extension of the Inception design, Xception uses a stack of depth-separable convolution schemes to replace the Inception modules. In the newer versions of the Inception, some of the modules have replaced the different spatial dimensions ( $1 \times 1$ ,  $3 \times 3$ , and  $5 \times 5$ ) with a single dimension ( $3 \times 3$ ), followed by a pointwise convolution ( $1 \times 1$  convolution) to manage the computational complexity [14]. The feature extraction layer in the Xception architecture has a total of 36 convolutional layers with a large filter utilization of 728. Chaturvedi et al. [29] have suggested an automatic multiclass skin cancer disease classification system by conducting training procedures to obtain the optimal hyperparameter for five CNN models including Xception, ResNext 101, NasNetLarge, Inception V3, InceptionResNet V2, and the ensemble model. The best accuracy for the individual model was obtained by ResNext 101 and the best accuracy for the ensemble model was obtained by the combined network of InceptionResNet V2 and ResNetXt 101. However, the individual Xception model and the ensemble

model that contain Xception architecture also obtained good accuracy performances.

6) *DenseNet*: DenseNet is quite similar to ResNet from the architecture perspective, but the integration format of the two incoming networks is different, which leads to different network behaviors. Huang et al. [15] have developed an architecture with a simple connection pattern to ensure the maximal information flows between forward and backward layers to resolve the vanishing gradient problem. DenseNet accommodates the additional input from all previous layers by using cross-layer connectivity through the concatenation operator. Then, it transmits its feature maps to all subsequent layers, again via cross-layer connectivity. For image recognition, down-sampling layers divided the whole architecture into several densely connected blocks. Transition layers are also inserted between the convolution and pooling layers of various blocks. Hassan et al. [30] have implemented DenseNet-121 architecture to classify seven different types of skin lesions based on the HAM10000 dataset. Their model was trained by using supplemented augmentation data that managed to reach 92% of categorical accuracy and 97% of top2 accuracy which is much better than other models. The illustrated DenseNet architecture is shown in Fig. 5.

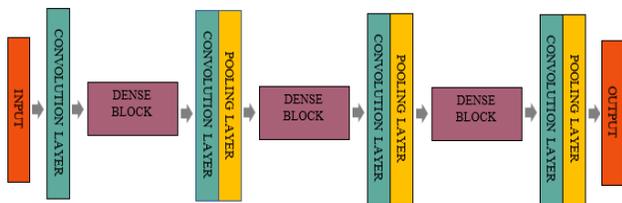


Fig. 5. Diagram of DenseNet Architecture.

7) *EfficientNet*: Recently, the EfficientNet model was introduced with a new up-and-down scaling strategy that scales uniformly the depth, width, and parameter resolution by using an effective compound coefficient [16]. One of the primary components of EfficientNet is MBConv or MobileNet, which follows an inverted bottleneck design. It is paired with an in-depth separable convolution by taking a shortcut between the bottlenecks, whereby it utilizes a considerably smaller number of channels. This model has achieved better classification accuracy compared to the existing models such as ResNet, DenseNet, Inception-V4, and NASNet when tested using a large ImageNet dataset. Gessert et al. [31] have implemented an ensemble of deep learning models to classify skin lesions using various EfficientNet architectures (B0-B6). They have boosted the training data by using meta information from ISIC 2019, whereby they have achieved the highest accuracy of 63.6% with AUC above 80% for the detection of skin lesions of eight different classes of skin.

### III. RECENT APPLICATION OF CNN MODELS FOR CLASSIFICATION TASKS

Many studies have indicated that CNN is a suitable method to be implemented for biomedical image applications, especially in the automated analysis of skin lesions. Esteva et

al. [7] have presented a method to classify malignant melanoma with significant accuracy by using a CNN architecture, which is through Google Inception V3 that has been pre-trained on 1.28 million images of general objects. Their automated system was then retrained with 129,450 clinical data of 2,032 different classes and managed to achieve 72.1% accuracy, whereas the two benchmark dermatologists only managed to obtain accuracy rates of 65.56% and 66%. Through the transfer learning scheme, the CNN classifier was able to achieve more or less a similar performance to those of 21 dermatologists in identifying malignant lesions, in which the CNN classifier produced an overall area under the curve (AUC) of >91%. Brinker et al. [32] then experimented on CNN deep learning architecture in categorizing skin lesions from 12,378 dermoscopic images, which were categorized into two classes of melanoma and atypical nevi. The findings were compared with the performances of dermatologists from various levels of competency and experience that also includes a few resident physicians from 12 German university hospitals. The CNN-based approach has managed to outperform the average accuracy of dermatologists.

Furthermore, Ratul et al. [33] have developed a computer-aided detection system for malignant skin lesions cases. Dilated convolution was used in four different architectures, namely InceptionV3, MobileNet, VGG16, and VGG19. The HAM10000 data set, which contains 10,015 dermoscopic images consisting of seven skin lesion classes were used to train, validate and test the algorithm with accuracy rates of 89.81%, 88.22%, 87.42%, and 85.02% for the previously mentioned models, respectively. Gessert et al. [34] researched further on the usage of patch-based techniques to extract fine-grain variations between different skin lesions using high image resolution input. Then, each image was divided into 5, 9, and 16 patches, which will be incorporated into a standard CNN architecture. Finally, three popular architectures were used to classify the skin lesions from high-resolution image patches, namely DenseNet, Inception V3, and SE-Resnext50.

Instead of using a fixed learning rate, Alqudah et al. [35] were integrated gradient descent with adaptive momentum learning rate and transfer learning approaches into two CNN architectures, which are AlexNet and GoogleNet for skin lesion classification tasks. Their method considered three types of skin lesions, which are benign, melanoma, and seborrheic keratosis, whereby the proposed classification approach was tested and evaluated using the International Skin Imaging Collaboration database. The system aimed to analyze input images to produce segmented and non-segmented skin lesions and reported accuracy rates of 92.2% and 89.8%, respectively. Contrary to the previous work, Akram et al. [36] developed a new framework for skin lesion classification that incorporates in-depth feature information to build the best discriminatory feature vectors while preserving the original feature space. To select discriminant features and reduce dimensionality, the authors have used the entropy-controlled neighborhood component analysis. The system employed several deep learning architectures, including Inception-V3, DenseNet 201, and Inception-ResNet-V2, as the classifiers. The proposed system was evaluated using different data sets, namely ISIC MSK, ISIC UDA, ISBI-2017, and PH2, with a common aim of

categorizing the skin lesions and obtained performance results of 98.8%, 99.2%, 97.1%, and 95.9%, respectively. The authors managed to cut off the features to less than 3% of the overall features, which resulted in improved classification accuracy by eliminating the redundancy and minimizing the computation time.

Researchers have also developed an integrated approach for skin lesion segmentation and multi-class lesion classification [37]. In this work, full-resolution convolutional network models have been applied for segmenting the lesion regions using popular CNN backbones of Inception, Densenet201, and ResNet-Inception to classify the segmented skin lesions. The Inception-ResNet model provided the most remarkable results out of the tested techniques. This model performed the best if it is trained with balanced data rather than imbalanced data. Using a similar approach, Purnama et al. [38] have tested two pre-trained CNN models, Inception V3 and MobileNet V1 for skin lesion classification. Then, they introduced an innovation through a web classifier. Their proposed method used a benchmark dataset of MNIST HAM 1000, where the results showed that Inception V3 had 72% accuracy, whereas MobileNet V1 only had 58% accuracy.

A unique multiple CNN models approach was proposed in [39] for solving challenging classification tasks due to the presence of artifacts, low-contrast images, and high intraclass differences in dermoscopic images. Multiple pre-trained CNN architectures were explored that include AlexNet, ResNet, GoogleNet, and VGG16 to speed up the training process using the dataset of ISIC 2016. This approach achieved an accuracy of 97.78% with an AUC of 0.98 for the training dataset and 85.22% with an AUC of 0.81 for the testing dataset. Instead of four models, Miglani and Bhatia [40] compared only two deep CNN models, ResNet-50 and EfficientNet-B0 for skin lesion classification purposes. The models were tested using the HAM10000 dataset, which resulted in the EfficientNet-B0 outperforming the ResNet-50 by achieving mean macro and micro AUC of 0.93 and 0.97, respectively. Their test has concluded that the recent CNN model is better in extracting richer, more complex, and fine-grain features of dermoscopic skin lesion images. Table II shows a comparison of the recent methods for skin lesion classification using the deep CNN methods.

TABLE II. COMPARISON OF RECENT CNN METHODS USED FOR SKIN LESION DETECTION

References	Datasets	Skin lesion classes	CNN architectures	Performance measures
[7]	ASIC, Edinburgh Dermofit Library, Stanford Hospital [7]	Benign and Malignant	Google Inception V3	Accuracy: 72.1%
[32]	HAM 10000 [41]	Melanoma and Nevi	ResNet50	Mean Specificity: 64.4% Mean Sensitivity: 89.4% ROC: 0.769
[33]	HAM 10000 [41]	Melanocytotic nevus, basal cell carcinoma, vascular lesions, dermatofibroma, benign keratosis, melanoma, and actinic keratosis	VGG16 VGG19 MobileNet InceptionV3	Accuracy; VGG16: 90.10% VGG19: 86.39% MobileNet: 89.48% InceptionV3: 90.95%
[34]	HAM 10000 [41]	Melanocytotic nevus, benign keratosis, vascular lesions, dermatofibroma, basal cell carcinoma, melanoma, and actinic keratosis	Inception V3 DenseNet121 SE-Resnext50	MC-Sensitivity; Inception V3: 64.0% DenseNet121: 67.8% SE-Resnext50: 66.9%
[35]	ISIC 2017 [42]	benign, melanoma, and seborrheic keratosis	AlexNet GoogleNet	Non-segmented accuracy; AlexNet: 92.2% GoogleNet: 92.2% Segmented accuracy AlexNet: 89.8% GoogleNet: 86.0%
[36]	PH2 [43] ISIC 2017 [42] ISIC-UDA, ISIC-MSK [44]	PH2: benign and melanoma ISBI 2017: melanoma, keratosis and benign ISIC-UDA, ISIC-MSK: benign and melanoma	Inception-V3 Inception-ResNet-V2 DenseNet-201	Accuracy; PH2: 98.80% ISBI-2017: 95.90% ISIC-UDA: 97.10% ISIC-MSK: 99.20%
[37]	ISIC 2016 [44] ISIC 2017 [42] HAM 10000 [41]	ISIC 2016: benign and melanoma ISIC 2017: benign, seborrheic keratosis, and melanoma HAM 10000: Melanocytotic nevus, basal cell carcinoma, vascular lesions, dermatofibroma, benign keratosis, melanoma, and actinic keratosis	DenseNet-201 ResNet-50 Inception-v3 Inception-ResNet-v2	ResNet-50 accuracy; ISIC 2016: 81.79% ISIC 2017: 81.57% ISIC 2017: 89.28%
[38]	MNIST HAM 10000 [41]	Melanocytotic nevus, basal cell carcinoma, vascular lesions, dermatofibroma, benign keratosis, melanoma, and actinic keratosis	MobileNet v1 Inception V3	Accuracy; Inception V3: 72% MobileNet v1: 58%
[39]	HAM 10000 [41]	Melanocytotic nevus, basal cell carcinoma, vascular lesions, dermatofibroma, benign keratosis, melanoma, and actinic keratosis	AlexNet VGG16 GoogleNet ResNet	AUC; Training: 0.99 Validation: 0.72
[40]	HAM 10000 [41]	Melanocytotic nevus, basal cell carcinoma, vascular lesions, dermatofibroma, benign keratosis, melanoma, and actinic keratosis	EfficientNet	Averaged AUC; macro: 0.93 micro: 0.97

#### IV. SEGMENTATION

Image segmentation is needed in a large-scale approach to diagnosing skin lesions automatically. It is an important step where the images will undergo pattern recognition or the utilization of a rule-based method to segment the region of interest (ROI). Al-Masni et al. [5] have defined ROI as the lesion areas that are separated from the non-lesion region. Generally, identifying the ROI requires a module to detect gaps in the images, before applying the similarity criteria to segment the lesions together [45]. The conventional approach involves handcrafted feature-based methods such as the edge [46], region [47], threshold [48], and intelligence-based methods [5]. The machine learning methods include both deep learning and conventional techniques, which will be discussed in the following section to examine and compare the segmentation performance. Table III shows the comparison between all segmentation techniques.

##### A. Recent Works on Skin Lesion Segmentation using Conventional Intelligence-Based Method

Conventional artificial intelligence allows rapid implementation of the skin lesion segmentation without much training requirement with a much lesser dataset compared to the deep learning approach. It can be easily implemented as such it allows a wider spread of the application to help with skin-related disease diagnosis. Researchers have analyzed the ability of artificial intelligence-based approaches by performing image analyses based on perception, reasoning, and learning using the existing medium-sized image datasets. The most recent popular artificial intelligence-based segmentation methods are ANN models [49], Fuzzy C-Means [52], and genetic algorithms [50], [51]. Artificial intelligence usually utilizing an analytical planning to make machine learn without program it especially using existing dataset while deep learning further with neural networks that imitate the neurons in human brain and enclose with multiple architecture layers. However, starting from 2015, the deep learning approach starts to be implemented due to the introduction U-Net, which changes the research direction in many bio-medical applications.

##### B. Recent Works on Deep Learning Approach to Skin Lesion Segmentation

The deep learning approach has been proven to be state-of-the-art in supervised image segmentation applications. Despite the heavy complexity of deep learning models, more information from the raw images can be learned optimally rather than being designed by a human designer. Researchers have utilized various deep learning models to segment skin lesions, including U-Net [64], fully CNN (FCNN) [65], deep fully convolutional residual network (FCRN), and SegNet [66].

1) *FCNN architecture*: FCNN is a segmentation module with deeper encoder parts compared to the decoder parts. This model has been used in [53] to segment the skin lesions automatically. Besides that, researchers have also developed multi-stage FCNN for skin lesion segmentation by using a parallel integration method. An evaluation of the suggested technique has been tested using the ISBI 2016 dataset, which has revealed a high segmentation performance with a dice coefficient score of 91.18% and an accuracy of 95.51%. Yuan

et al. [54] then presented a modified deep FCNN-based method for skin lesion segmentation, which was evaluated using two different databases; one is from the ISBI 2016 database and the other one is from the PH2 database. The modified method was found to outperform the previously mentioned techniques. Jafari et al. [55] then used a pre-processing approach to start the image analysis as such the pixels are smoothed so that the extracted edges will be larger with reduced noise artifacts such as hair. Then, each pixel of the pre-processed image is fed into the FCNN to obtain 98.5% accuracy and 95% sensitivity performance.

TABLE III. COMPARISON BETWEEN CONVENTIONAL METHODS AND INTELLIGENCE-BASED METHODS FOR SKIN LESION SEGMENTATION

Techniques	Description	Advantages	Disadvantages
Edge and region-based method [46], [47]	This method performs edge detection first, followed by detecting and linking the edge pixels to form connected contour. Then, region identification is done by comparing surrounding pixels that have comparable grey levels.	This method performs very well, whereby the algorithm rapidly converges when a massive number of dermoscopy images is used for training.	Requires extensive computational resources since this technique utilizes pixel level information with the presence of noises.
Threshold-based method [48]	The lesion will be removed from the background skin in the image using the thresholding approach, followed by analysis on blue channel image.	Easy to implement and extremely fast.	This method does not perform well since it is sensitive to noises.
Intelligence-based method: - ANN models [49] - Genetic Algorithms [50], [51] - Fuzzy C-Means (FCM) [52]	The system is based on artificial intelligence approach, which is the most popular approach in automated dermatology field. This approach can better inform the patients on the state of skin lesion by increasing the sensitivity and accuracy of skin lesion examination.	Less costly and fast computational time during inference stage.	Difficult to obtain prior information on the number of clusters due to skin lesions complexity.
Deep Learning: - Fully Convolutional Neural Network (FCN) [53]–[55] - U-Net [56]–[58] - Deep Residual Network [59]–[61] SegNet [62], [63]	Deep learning can learn optimal hierarchical features from the raw images directly rather than hand-crafted features by the network designer.	Perform end-to-end learning where raw data will be processed into network, whereby the network learns for optimal automation of the task.	Requires large memory storage and more expensive computation compared to other methods.

2) *U-Net architecture*: U-Net was inspired by the FCNN, which consisted of equal distribution of encoder and decoder paths, coupled with few feedforward layers. In addition, pooling layers are used to down-scale the encoder feature maps, while standard interpolation is used to up-scale the decoder parts. Moreover, in between the encoder and decoder paths, there are shortcut skip connections. U-Net has become a well-known architecture after it has achieved outstanding segmentation performances in various medical applications with limited training datasets. Many recent studies have also been conducted based on this architecture for skin lesion segmentation purposes. Skin lesion segmentation performance was improved by adding dilated convolution and batch normalization layers to the U-Net architecture as proposed in [56]. Moreover, Iranpoor et al. [57] have proven that the modified U-Net has significantly improved the architecture efficiency by utilizing a pre-trained ResNet model in the encoder path. According to [58], the SkinNet system is also based on a modified U-Net architecture but uses dilated convolution to improve the encoder branch. Fig. 6 shows the modified U-Net architecture for improved segmentation performance.

3) *Deep FCRN*: The deep residual network is a unique network invention that uses skip connections to jump over some convolutional layers to build a pyramid-like structure. Generally, it consists of multiple feedforward convolutional

layers. A fully convolutional residual network was developed in [59] to segment skin lesions in dermoscopic images. This method proposed a deep CNN model with an effective training process that can be used to evaluate complex medical images. Li and Shen [60] have used the fully convolutional residual network to develop the lesion index calculation unit in 2018 for skin lesions segmentation. Besides that, Nathan and Kansal [61] have suggested a base of U-Net architecture with deep residual units as the backbone of encoders and decoders. Each downsampling block consists of one convolutional layer and two deep residual units to improve skin lesion segmentation performance.

4) *SegNet architecture*: This architecture is based on a deep neural network with a straight flow of an encoder network followed by a corresponding decoder network, whereby the final layer is formed for pixel-wise classification tasks. The feature maps are produced by implementing convolution with a filter bank in each encoder network. Additionally, a recent study in [62] has proposed a modified SegNet for skin lesion segmentation. The authors have reduced the total learned parameter of the architecture by lowering the downsampling and upsampling layers of the original SegNet. Similarly, the work in [63] has utilized the SegNet architecture in skin lesion segmentation application and has been found to be accurate based on PH2 dataset testing.

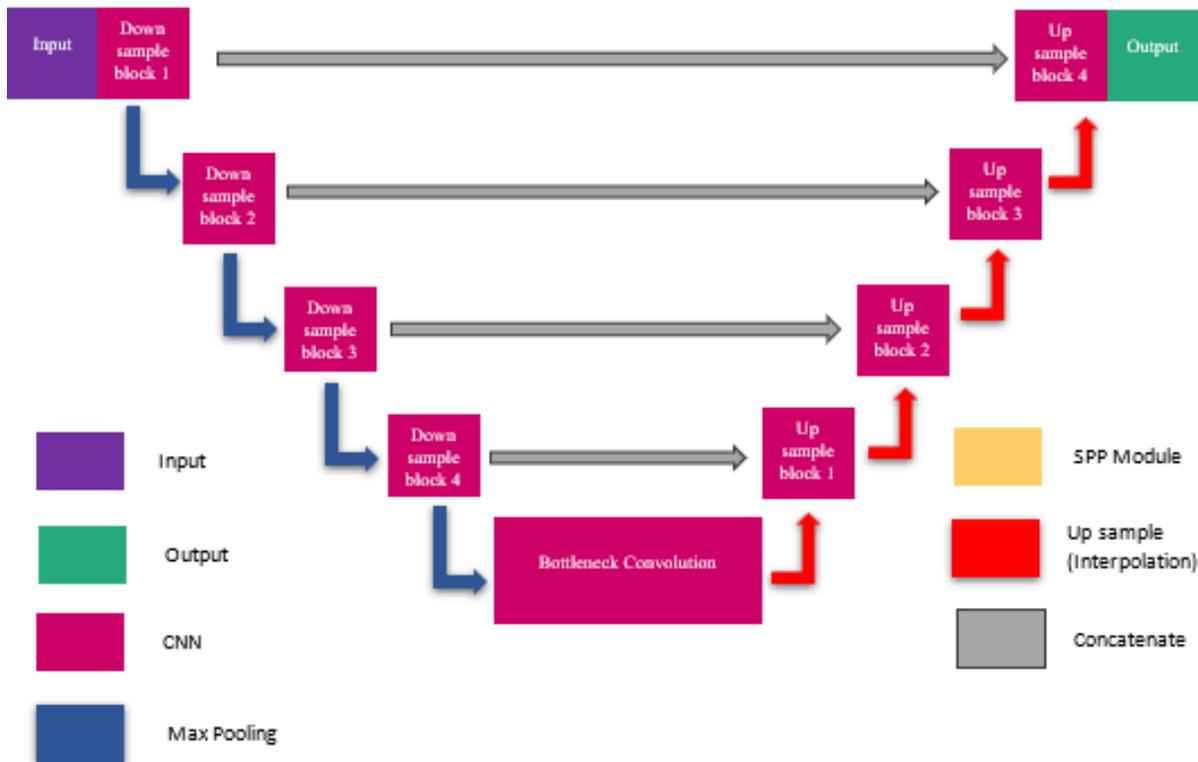


Fig. 6. Workflow Diagram of the U-Net Architecture.

## V. CONCLUSION

This paper presents a comparative study of state-of-the-art techniques, models, and methodologies for analyzing skin lesion images. This study has described the analysis process of skin lesions from segmentation to classification. Recently, researchers have paid more attention and effort into improving the accuracy of the diagnosis of skin lesions. However, some challenges remain difficult, especially in the interpretation of dermoscopic skin lesion images that contain noises such as bubbles, blood vessels, and hair. On the other hand, owing to the newest advancements in deep learning and its exceptional achievement in medical imaging, performance assessment of the deep learning approach for skin lesion segmentation and classification is worth to be reviewed. In this regard, state-of-the-art CNN models such as ResNet, Inception, Xception, DenseNet, and EfficientNet have generally shown excellent performances. However, these models require extensive computational resources with a long time to reach an optimal convergence state. This paper summarises the most important developments in this field and provides a complete discussion of the current approaches. Deep learning framework capabilities combined with pre and post-processing approaches are expected to improve future results and open the path for trustworthy screening and diagnostic systems.

Further research works should be tested using multiple open datasets to allow for better comparison. Besides that, more variations on the skin tone should be validated as most of the existing datasets are focusing on individuals with fair skin tones. Therefore, skin lesions with dark skin tone datasets also should be developed to produce a more robust testing platform that consists of all skin color types. A comprehensive analysis of various segmentation algorithms must be performed on the same dataset to achieve better accuracy, so that reliable results can be obtained. After that, a performance comparison of classification and segmentation models should also be tested on the same data set to produce a fair baseline model comparison.

## ACKNOWLEDGMENT

The authors would like to acknowledge funding from Universiti Kebangsaan Malaysia (Geran Universiti Penyelidikan: GUP-2019-008) and Ministry of Higher Education Malaysia (Fundamental Research Grant Scheme: FRGS/1/2019/ICT02/UKM/02/1).

## REFERENCES

- [1] S. R. Abdani, M. A. Zulkifley, and N. Hani Zulkifley, "A Lightweight Deep Learning Model for COVID-19 Detection," in 2020 IEEE Symposium on Industrial Electronics and Applications, ISIEA 2020, 2020, pp. 1–5.
- [2] N. A. Mohamed, M. A. Zulkifley, and A. Hussain, "On analyzing various density functions of local binary patterns for optic disc segmentation," in ISCAIE 2015 - 2015 IEEE Symposium on Computer Applications and Industrial Electronics, 2015, pp. 37–41.
- [3] A. Masood and A. A. Al-Jumaily, "Computer aided diagnostic support system for skin cancer: A review of techniques and algorithms," International Journal of Biomedical Imaging. 2013.
- [4] Adeyinka A.A., Viriri S. "Skin Lesion Images Segmentation: A Survey of the State-of-the-Art," In: Groza A., Prasath R. (eds) Mining Intelligence and Knowledge Exploration. MIKE 2018. Lecture Notes in Computer Science, vol 11308. Springer, Cham.
- [5] M. A. Al-masni, M. A. Al-antari, M. T. Choi, S. M. Han, and T. S. Kim, "Skin lesion segmentation in dermoscopy images via deep full resolution convolutional networks," vol. 162, pp. 221–231, 2018.
- [6] S. R. Abdani, M. A. Zulkifley, and A. Hussain, "Compact Convolutional Neural Networks for Pterygium Classification using Transfer Learning," in Proceedings of the 2019 IEEE International Conference on Signal and Image Processing Applications, ICSIPA 2019, 2019, pp. 140–143.
- [7] Esteva A, Kuprel B, Novoa RA, Ko J, Swetter SM, Blau HM, Thrun S, "Dermatologist-level classification of skin cancer with deep neural networks," Nature 542, pp. 115–118, 2017.
- [8] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," Commun. ACM, 2017.
- [9] Y. Lecun, Y. Bengio, and G. Hinton, "Deep learning," Nature. 2015.
- [10] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," 2012.
- [11] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2015.
- [12] Szegedy, C., Liu, W., Jia, Y., Sermanet, P., Reed, S.E., Anguelov, D., Erhan, D., Vanhoucke, V., & Rabinovich, A., "Going deeper with convolutions," in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2015, pp. 1–9.
- [13] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition, 2016, pp. 770–778.
- [14] F. Chollet, "Xception: Deep learning with depthwise separable convolutions," in Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, 2017, pp. 1800–1807.
- [15] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in Proceedings - 30th IEEE Conference on Computer Vision and Pattern Recognition, CVPR 2017, 2017, pp. 2261–2269.
- [16] M. Tan and Q. V. Le, "EfficientNet: Rethinking model scaling for convolutional neural networks," 2019.
- [17] U. Jamil and S. Khalid, "Comparative study of classification techniques used in skin lesion detection systems," in 17th IEEE International Multi Topic Conference: Collaborative and Sustainable Development of Technologies, IEEE INMIC 2014 - Proceedings, 2014, pp. 266–271.
- [18] M. Q. Khan, A. Hussain, S. U. Rehman, U. Khan, M. Maqsood, K. Mehmood, and M. A. Khan, "Classification of Melanoma and Nevus in Digital Images for Diagnosis of Skin Cancer," IEEE Access, vol. 7, pp. 90132–90144, 2019.
- [19] S. S. Han, W. Lim, M. S. Kim, I. Park, G. H. Park, and S. E. Chang, "Interpretation of the Outputs of a Deep Learning Model Trained with a Skin Cancer Dataset," The Journal of investigative dermatology, 138(10), pp. 2275–2277, 2018.
- [20] Russakovsky, O., Deng, J., Su, H., Krause, J., Satheesh, S., Ma, S., Huang, Z., Karpathy, A., Khosla, A., Bernstein, M., Berg, A. C., & Fei-Fei, L., "ImageNet Large Scale Visual Recognition Challenge," International Journal of Computer Vision, 2015, 115(3), pp. 211–252.
- [21] Brinker, T. J., Hekler, A., Enk, A. H., Klode, J., Hauschild, A., Berking, C., Schilling, B., Haferkamp, S., Schadendorf, D., Fröhling, S., Utikal, J. S., & von Kalle, C., "A convolutional neural network trained with dermoscopic images performed on par with 145 dermatologists in a clinical melanoma image classification task. European," Journal of Cancer (Oxford, England 1990), 111, pp. 148–154, 2019.
- [22] S. S. Han, M. S. Kim, W. Lim, G. H. Park, I. Park, and S. E. Chang, "Classification of the Clinical Images for Benign and Malignant Cutaneous Tumors Using a Deep Learning Algorithm," The Journal of investigative dermatology, 138(7), pp. 1529–1538, 2018.
- [23] K. M. Hosny, M. A. Kassem, and M. M. Foad, "Classification of skin lesions using transfer learning and augmentation with Alex-net," PLoS One, 2019.
- [24] M. A. Zulkifley and N. Trigoni, "Multiple-Model Fully Convolutional Neural Networks for Single Object Tracking on Thermal Infrared Video," IEEE Access, vol. 6, pp. 42790–42799, 2018.
- [25] M. A. Zulkifley, "Two streams multiple-model object tracker for thermal infrared video," IEEE Access, vol. 7, pp. 32383–32392, 2019.

- [26] X. Sun, J. Yang, M. Sun, and K. Wang, "A Benchmark for Automatic Visual Classification of Clinical Skin Disease Images," *Proc. ECCV*, pp. 206-222, 2016.
- [27] K. Thurnhofer-Hemsi and E. Domínguez, "Analyzing Digital Image by Deep Learning for Melanoma Diagnosis," In: *Proceedings of the 15th international work-conference on artificial neural networks (IWANN)*, pp. 270-279, 2019.
- [28] D. N. T. Le, H. X. Le, L. T. Ngo, and H. T. Ngo, "Transfer learning with class-weighted and focal loss function for automatic skin cancer classification," Sep. 2020.
- [29] S. S. Chaturvedi, J. v. Tembhumbe, and T. Diwan, "A multi-class skin Cancer classification using deep convolutional neural networks," *Multimedia Tools and Applications*, vol. 79, no. 39-40, Oct. 2020.
- [30] S. R. Hassan, S. Afroge, and M. Binte Mizan, "Skin Lesion Classification Using Densely Connected Convolutional Network," *IEEE Region 10 Symposium (TENSYP)*, pp. 750-753, 2020.
- [31] N. Gessert, M. Nielsen, M. Shaikh, R. Werner, and A. Schlaefler, "Skin lesion classification using ensembles of multi-resolution EfficientNets with meta data," *MethodsX*, vol. 7, 2020.
- [32] Brinker, T. J., Hekler, A., Enk, A. H., Klode, J., Hauschild, A., Berking, C., Schilling, B., Haferkamp, S., Schadendorf, D., Holland-Letz, T., Utikal, J. S., von Kalle, C., & Collaborators, "Deep learning outperformed 136 of 157 dermatologists in a head-to-head dermoscopic melanoma image classification task," *European journal of cancer (Oxford, England : 1990)*, 113, pp. 47-54, 2019.
- [33] M. Ratul, M. H. Mozaffari, W.-S. Lee, and E. Parimbelli, "Skin Lesions Classification Using Deep Learning Based on Dilated Convolution," *BioRxiv*, Jan. 2019, Art. no. 860700.
- [34] Gessert, N., Sentker, T., Madesta, F., Schmitz, R., Knip, H.C., Baltruschat, I.M., Werner, R., & Schlaefler, A., "Skin Lesion Classification Using CNNs With Patch-Based Attention and Diagnosis-Guided Loss Weighting," *IEEE Transactions on Biomedical Engineering*, 67, pp. 495-503, 2020.
- [35] A. M. Alqudah, H. Alquran, and I. A. Qasmieh, "Segmented and non-segmented skin lesions classification using transfer learning and adaptive moment learning rate technique using pretrained convolutional neural network," In *Journal of Biomimetics, Biomaterials and Biomedical Engineering 2019*; 42, pp. 67-78.
- [36] Akram, T., Lodhi, H.M.J., Naqvi, S.R. et al., "A multilevel features selection framework for skin lesion classification," *Human-centric Comput. Inf. Sci.*, vol. 10, pp. 1-26, 2020.
- [37] M. A. Al-masni, D. H. Kim, and T. S. Kim, "Multiple skin lesions diagnostics via integrated deep convolutional networks for segmentation and classification," *Comput. Methods Programs Biomed.*, vol. 190, 2020.
- [38] I. K. E. Purnama et al., "Disease Classification based on Dermoscopic Skin Images Using Convolutional Neural Network in Tele dermatology System," *International Conference on Computer Engineering, Network, and Intelligent Multimedia (CENIM)*, 2019, pp. 1-5.
- [39] Y. Guo, A. S. Ashour, L. Si, and D. P. Mandalaywala, "Multiple Convolutional Neural Network for Skin Dermoscopic Image Classification," in *2018 IEEE International Symposium on Signal Processing and Information Technology, ISSPIT 2018*, 2019, pp. 365-369.
- [40] V. Miglani and M. Bhatia, "Skin Lesion Classification: A Transfer Learning Approach Using EfficientNets," in *Advances in Intelligent Systems and Computing*, 2021, pp. 315-324.
- [41] N. Codella et al., "Skin lesion analysis toward melanoma detection 2018: A challenge hosted by the international skin imaging collaboration (ISIC)," *arXiv*. 2019.
- [42] N. C. F. Codella et al., "Skin lesion analysis toward melanoma detection: A challenge at the 2017 International symposium on biomedical imaging (ISBI), hosted by the international skin imaging collaboration (ISIC)," in *Proceedings - International Symposium on Biomedical Imaging*, 2018, pp. 168-172.
- [43] T. Mendonca, P. M. Ferreira, J. S. Marques, A. R. S. Marcal, and J. Rozeira, "PH2 - A dermoscopic image database for research and benchmarking," in *Proceedings of the Annual International Conference of the IEEE Engineering in Medicine and Biology Society, EMBS*, 2013, pp. 5437-5440.
- [44] Gutman, David; Codella, Noel C. F.; Celebi, Emre; Helba, Brian; Marchetti, Michael; Mishra, Nabin; Halpern, Allan., "Skin Lesion Analysis toward Melanoma Detection: A Challenge at the International Symposium on Biomedical Imaging (ISBI) 2016, hosted by the International Skin Imaging Collaboration (ISIC)," pp. 3-7, 2016.
- [45] M. Filho, Z. Ma, and J. M. R. S. Tavares, "A Review of the Quantification and Classification of Pigmented Skin Lesions: From Dedicated to Hand-Held Devices," *Journal of Medical Systems*. 2015.
- [46] J. H. Jaseema Yasmin, M. Mohamed Sathik, and S. Zulaiyka Beevi, "Robust segmentation algorithm using LOG edge detector for effective border detection of noisy skin lesions," in *2011 International Conference on Computer, Communication and Electrical Technology, ICCCT 2011*, 2011, pp. 60-65.
- [47] H. Zhou, G. Schaefer, M. E. Celebi, F. Lin, and T. Liu, "Gradient vector flow with mean shift for skin lesion segmentation," *Comput. Med. Imaging Graph.*, vol. 35, no. 2, pp. 121-127, 2011.
- [48] M. Emre Celebi, Q. Wen, S. Hwang, H. Iyatomi, and G. Schaefer, "Lesion Border Detection in Dermoscopy Images Using Ensembles of Thresholding Methods," *Ski. Res. Technol.*, vol. 19, 2013.
- [49] Hogarty, D. T., Su, J. C., Phan, K., Attia, M., Hossny, M., Nahavandi, S., Lenane, P., Moloney, F. J., & Yazdabadi, A., "Artificial Intelligence in Dermatology—Where We Are and the Way to the Future: A Review," *American journal of clinical dermatology*, 21(1), pp. 41-47, 2020.
- [50] R. B. Aswin, J. A. Jaleel, and S. Salim, "Hybrid genetic algorithm - Artificial neural network classifier for skin cancer detection," in *2014 International Conference on Control, Instrumentation, Communication and Computational Technologies, ICCICT 2014*, 2014, pp. 1304-1309.
- [51] F. Xie and A. C. Bovik, "Automatic segmentation of dermoscopy images using self-generating neural networks seeded by genetic algorithm," *Pattern Recognit.*, vol. 46, no. 3, pp. 1012-1019.
- [52] A. A. I. Mohamed, M. M. Ali, K. Nusrat, J. Rahebi, A. Sayiner, and F. Kandemirli, "Melanoma Skin Cancer Segmentation with Image Region Growing Based on Fuzzy Clustering Mean," *Int. J. Eng. Innov. Res.*, vol. 6, no. 2, pp. 91-95, 2017.
- [53] L. Bi, J. Kim, E. Ahn, A. Kumar, M. Fulham, and D. Feng, "Dermoscopic Image Segmentation via Multistage Fully Convolutional Networks," *IEEE Trans. Biomed. Eng.*, vol. 64, no. 9, pp. 2065-2074, 2017.
- [54] Y. Yuan, M. Chao, and Y. C. Lo, "Automatic Skin Lesion Segmentation Using Deep Fully Convolutional Networks with Jaccard Distance," in *IEEE Transactions on Medical Imaging*, vol. 36, no. 9, pp. 1876-1886, Sept. 2017.
- [55] Jafari, M., Karimi, N., Nasr-Esfahani, E., Samavi, S., Sorousmehr, S.M., Ward, K., & Najarian, K., "Skin lesion segmentation in clinical images using deep learning," *23rd International Conference on Pattern Recognition (ICPR)*, pp. 337-342, 2016.
- [56] L. Liu, L. Mou, X. X. Zhu, and M. Mandal, "Skin Lesion Segmentation Based on Improved U-net," in *2019 IEEE Canadian Conference of Electrical and Computer Engineering, CCECE 2019*, 2019, pp. 1-4.
- [57] R. Iranpoor, A. S. Mahboob, S. Shahbandegan, and N. Baniasadi, "Skin lesion segmentation using convolutional neural networks with improved U-Net architecture," in *6th Iranian Conference on Signal Processing and Intelligent Systems, ICSPIS 2020*, 2020, pp. 1-5.
- [58] S. Vesal, N. Ravikumar, and A. Maier, "SkinNet: A deep learning framework for skin lesion segmentation," *arXiv*. 2018.
- [59] L. Yu, H. Chen, Q. Dou, J. Qin, and P. A. Heng, "Automated Melanoma Recognition in Dermoscopy Images via Very Deep Residual Networks," in *IEEE Transactions on Medical Imaging*, vol. 36, no. 4, pp. 994-1004, April 2017.
- [60] Y. Li and L. Shen, "Skin lesion analysis towards melanoma detection using deep learning network," *Sensors (Switzerland)*, vol. 18, 2018.
- [61] S. Nathan and P. Kansal, "Lesion Net-Skin Lesion Segmentation Using Coordinate Convolution and Deep Residual Units," pp. 1-8, 2012.
- [62] Q. C. Ninh, T. T. Tran, T. T. Tran, T. Anh Xuan Tran, and V. T. Pham, "Skin lesion segmentation based on modification of SegNet neural

- networks,” in Proceedings - 2019 6th NAFOSTED Conference on Information and Computer Science, NICS 2019, 2019, pp. 575–578.
- [63] P. Brahmhatt and S. N. Rajan, “Skin Lesion Segmentation using SegNet with Binary Cross-Entropy | Papers with Code,” International Conference on Artificial Intelligence and Speech Technology, 2019.
- [64] O. Ronneberger, P. Fischer, and T. Brox, “U-net: Convolutional networks for biomedical image segmentation,” In: Navab N., Hornegger J., Wells W., Frangi A. (eds) Medical Image Computing and Computer-Assisted Intervention – MICCAI 2015. MICCAI 2015. Lecture Notes in Computer Science, vol 9351. Springer, Cham.
- [65] J. Long, E. Shelhamer and T. Darrell, "Fully convolutional networks for semantic segmentation," in 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 2015 pp. 3431-3440.
- [66] V. Badrinarayanan, A. Kendall, and R. Cipolla, “SegNet: A Deep Convolutional Encoder-Decoder Architecture for Image Segmentation,” in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 39, no. 12, pp. 2481-2495, 1 Dec. 2017.

# The Development of Borneo Wildlife Game Platform

Ramadiani Ramadiani<sup>1</sup>, Erdinal Respatti<sup>2</sup>, Gubta Mahendra Putra<sup>3</sup>, Muhammad Labib Jundillah<sup>4</sup>  
Tamrin Rahman<sup>5</sup>, Muhammad Dahlan Balfas<sup>6</sup>, Arda Yuniarta<sup>7\*</sup>, Hasan Jamal Alyamani<sup>8</sup>

Department of Informatics, Faculty of Engineering, Mulawarman University, Samarinda, Indonesia<sup>1, 2, 3, 4, 5, 6</sup>

Faculty of Computing and Information Technology Rabigh, King Abdulaziz University, Jeddah, Kingdom of Saudi Arabia<sup>7, 8</sup>

**Abstract**—Games are a unique, interesting, and fun entertainment medium. Games can contain education, introduction to certain flora and fauna, work and daily life, intelligence and dexterity. The game built in this study aims to introduce the flora and fauna found in the forests of East Borneo (Kalimantan), Indonesia as the object of a platform game. Games are built using the Game Development Life Cycle method in order to make good and organized games. The GDLC method contain 6 stages, first is the initiation for the initial idea, second is to preproduction for the asset creation, third stage is production for the system creation, fourth is the testing for the trial, fifth is the beta for the external trial, and the sixth stage is to release for publication. The results of the study resulted in the Borneo Wildlife game platform. This game introduces the unique flora and fauna in East Borneo, Indonesia, such as Black Orchids, Ironwood trees, Proboscis monkeys, Mahakam dolphins and Hornbills, as well as how to protect and preserve their nature. The game received 46 downloads from March 1, 2021 to May 24, 2021.

**Keywords**—Game development; Kalimantan; Borneo; wildlife game

## I. INTRODUCTION

The island of Borneo (Kalimantan) is one of the five largest islands in Indonesia, in addition to the island of Sumatra, the island of Sulawesi, the island of Java and the island of Papua. The island of Kalimantan or internationally known as Borneo, is the third largest island in the world, with an area of 748,168 km<sup>2</sup>. The island of Borneo is surrounded by the South China Sea to the west and north-west, the Sulu Sea to the north-east, the Sulawesi Sea and Makassar Strait to the east and the Java Sea and the Karimata Strait to the south. On the island of Borneo there are 3 countries; Indonesia (73%), Malaysia (26%) and Brunei Darussalam (1%). The Indonesian provinces of North Kalimantan, South Kalimantan, East Kalimantan, West Kalimantan, and Central Kalimantan make up the southeastern part of the island [1-4].

The island of Borneo is dominated by tropical rain forests. In fact, in the midst of rampant deforestation, as much as 50% of the Kalimantan area is still a tropical rain forest area. Local problems that exist on the island of Kalimantan are illegal logging, forest fires and poaching of protected animals [3-4]. So in the design of this game, besides aiming to introduce flora and fauna, it also teaches the community how to protect the forest and protect the wildlife in it from damage and poachers. This is the map of Kalimantan shown in Fig. 1.

In this study, Game application was chosen to introduce the natural wealth on the island of Borneo. The game application was chosen because it is interesting, many users from the

younger generation like it, and it is a fun learning media to introduce the unique flora and fauna on the island of Borneo, for example hornbills, Mahakam dolphins, black orchid flowers, Ulin trees, orangutans and long nosed monkeys or proboscis monkeys [3-8]. All the uniqueness of the flora and fauna can be used as the object of the story, can be introduced to the world and can make local games more interesting. In the Fig. 2 we can see Hornbills, Proboscis monkeys, Black Orchid flowers, Ulin trees, and Mahakam dolphins as Gallery Item.



Fig. 1. The Map of Kalimantan (Borneo) [2].



Fig. 2. Hornbills, Proboscis Monkeys, Black Orchid, Ulin Trees, and Mahakam Dolphins.

The purpose of this research is to produce a game with the platform "Borneo Wildlife" with the theme of flora and fauna of Borneo and the application of the Game Development Life Cycle method (GDLC) method. This method is used to develop games with a standard flow of game development in general, starting from the planning process to the release process to

\*Corresponding Author

make it easier to produce or develop a game [9-12]. The details methodology steps to develop this game presented in Section II, which has 6 stages, namely initiation for the initial idea stage, preproduction for the asset creation, production for the system development, testing for the internal tester, beta for the external tester, and release for the game publication [9-12]. Section III focuses on result and discussion for this research. Furthermore, the game application testing explained in details in Section IV. The last Section is Section V is for conclusion and future works of this study.

## II. RESEARCH METHODOLOGY FOR GAME DEVELOPMENT

The method used in this study is the Game Development Life Cycle method which has 6 stages, namely 1) initiation for the initial idea stage, 2) preproduction for the asset creation stage, 3) production for the manufacturing stage system, 4) testing for the trial phase, 4) beta for the external trial phase, and 5) release for the publication phase [10-15]. We can see the stages of game development as shown in Fig. 3.

### A. Study of Literature

This stage searches and reads previous research literature related to develop the game, such as reading information about the flora and fauna typical of Kalimantan, system development methods, game engines used, and information about game platforms, stages of development and system testing method.

There was many research on the game development especially about the methodology for the game development [15-25]. From various existing research, we study, compare and try to analyze the suitable method to develop the game application for this work. The result from the literature review process, we found important stages to develop a game application and we use 6 general stages of the game development that already explained in the beginning of Section II.

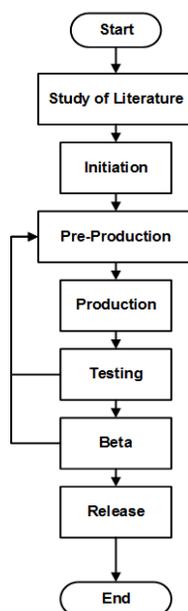


Fig. 3. The Stages of Game Development.

### B. Initiation

In this research, a Game with the Platform genre is built where players pass obstacles and defeat existing poachers. The background of this game is to introduce the flora and fauna of Kalimantan Indonesia. The concept of this game is that the player will control a character where to move to the next level the player must find a way and defeat the existing poachers. For age restrictions, this game can be played at all ages. The game will have 6 levels, where there are 2 different levels, namely a special bonus level, and a special level against the last poachers.

This game is built using the Unity game engine with the target device being an Android smartphone device. Some of the features in this game are:

- 1) Single Player Games.
- 2) Game can save player progress
- 3) Game has touch control.
- 4) The game has a gallery feature where there is info on the flora and fauna of Indonesian Borneo.
- 5) Players can adjust the sound volume in the game.

### C. Pre-Production

At this stage, the initial game design stage will be carried out, such as creating stories, game rules, determining the software to be used, creating and finding assets, making level designs, game displays, in-game items, and in-game buttons [26-28].

- 1) The draft Story of Game Borneo WildLife is as follows:

The main character is a forest ranger named Agus, ordered by his superior named "Mr. Fery" to solve the problem of existing illegal loggers. Agus was then given 3 main orders by Mr. Fery, namely, destroy the wood machine, destroy the bulldozer, and defeat the leader of the illegal loggers. After that, Agus began to do his first task, namely destroying wood machines, while on his way Agus saw animals such as hornbills and dolphins. Then Agus saw a woodworking machine and smashed it. After destroying the woodworking machine, Agus continued his task of finding bulldozers and destroying them. Then Agus found the Bulldozer engine and then destroyed it. In the end, Agus' task reached the last one, which was to defeat the leader of the loggers, then Agus met the leader of the illegal loggers named Jono, and Agus defeated him. Finally, the forest was spared from the threat of illegal loggers and finished.

- 2) Game rules:

- a) If the player's HP runs out then the game ends.
- b) If the player falls into the water (not included in the bonus level) then the game is over.
- c) The player can go to the next level when the player defeats the boss or reaches the level finish point.
- d) Players will get 1 medkit to replenish HP when players collect 10 coins.

3) Software to be used:

- a) The Game Engine to be used is Unity 2020.01.b8.
- b) Software that will be used as asset creation is Aseprite and PS.

4) Image assets:

a) TileSet

This asset is an asset that will be used for making levels in this game shown in Fig. 4.

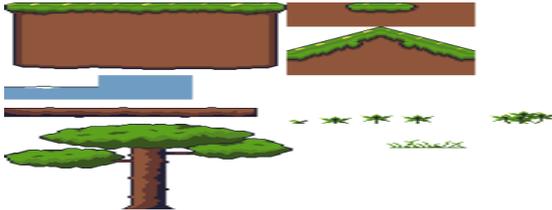


Fig. 4. TileSet.

b) Control User Interface (UI)

This asset is the asset that will be used for the creation of the player UI control buttons shown in Fig. 5.



Fig. 5. UI Control.

c) Status UI

This asset is an asset that will be used for making UI status of players and enemies in this game such as UI health of players and bosses shown in Fig. 6 and shown in Fig. 7.



Fig. 6. Icon Medkit, Health Effects and Player HealthBar.



Fig. 7. Boss HealthBar.

d) Menu UI

This asset is an asset that will be used for the creation of the main menu UI in this game shown in Fig. 8.



Fig. 8. UI Menu.

e) Gallery Icon UI

This asset is an asset that will be used for making the Gallery Menu in this game shown in Fig. 9.



Fig. 9. Icon Gallery Item.

f) Title UI

This asset is an asset that will be used for making the title and menu background in this game. The image of the dolphin used for the gallery description shown in Fig. 10 and shown in Fig. 11.



Fig. 10. Background Menu.



Fig. 11. Game Icon and Game Logo.

g) Animation Spritesheet

This asset is an asset that will be used to create animated characters, enemies, and entities in this game shown in Fig. 12 to 19.



Fig. 12. Player Spritesheet Animation.

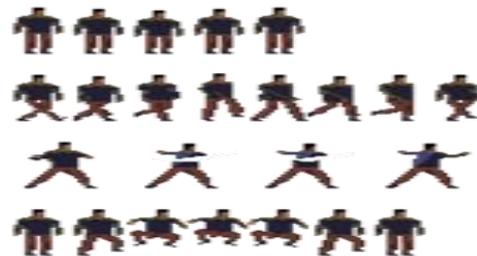


Fig. 13. Enemy Spritesheet Animation.

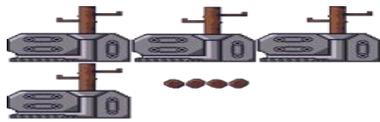


Fig. 14. Lumbermachine Spritesheet Animation.



Fig. 15. Bulldozer Spritesheet Animation.



Fig. 16. Proboscis Monkey Spritesheet Animation.



Fig. 17. Pesut Spritesheet Animation.



Fig. 18. Spritesheet Animation.



Fig. 19. Coin Spritesheet Animation.

5) Audio assets are obtained from:

- a) Mixkit <https://mixkit.co/free-sound-effects/>
- b) RPG music pack <https://svl.itch.io/rpg-music-pack-svl>

6) *Display game design:* The main menu will display several options such as play to play the game from the beginning shown in Fig. 20, continue to continue the progress of the game, gallery to display the gallery menu shown in Fig. 21, settings to display the configuration menu, and exit to close the game application.



Fig. 20. Main Menu.



Fig. 21. Gallery Menu.



Fig. 22. Gallery Description.

In the gallery menu, players can see information on the flora and fauna in this game, such as descriptions and original pictures of the flora and fauna shown in Fig. 22.



Fig. 23. Settings Menu.

In the settings menu, players can adjust the volume and sound in the game shown in Fig. 23.

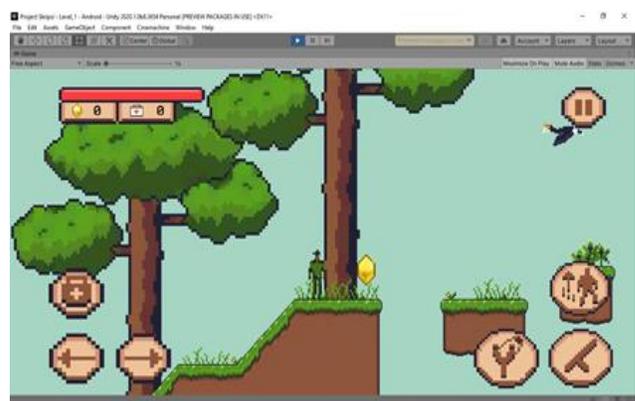


Fig. 24. The Gameplay Menu.

The gameplay view of the game shown in Fig. 24 includes several UIs such as player HP information, coins and medkits, and several UI control Mobile players such as left and right motion buttons, jump buttons, slingshot buttons, medkit buttons, pause buttons, and stick buttons to hit shown in Fig. 25.



Fig. 25. Pause Menu Display.

Pause display when the player presses the pause button.



Fig. 26. Gameover Menu.

Gameover display when the player's HP hits 0 or when the player falls into the water shown in Fig. 26.

7) Items inside the game shown in Table I.

TABLE I. ITEMS IN THE GAME

Name	Symbol	Function
Coin		If the player collects 10 coins, then the player will be given 1 medkit.
Medkit		Medkits can be used to restore blood to the player character.
Movement		To move the character right or left
Pause		To pause the game
Attack		Command the character to attack using the stick
Jump		Character command to jump
Ranged Attack		Command the character to attack using the catapult
Attack		Command the character to attack using the stick

#### D. Production

At this stage, the author begins to build a game system, such as creating a game plot, creating level designs, and creating a gameplay system shown in Fig. 27.

1) *Game system flowchart*: The game will display the main menu when it is first opened, there are several options on the menu such as play to start the game from the beginning, continue to continue the game based on player save data, gallery to display information on flora and fauna in the game, settings to display the settings menu games such as game volume settings, and exit to close game applications shown in Fig. 28.

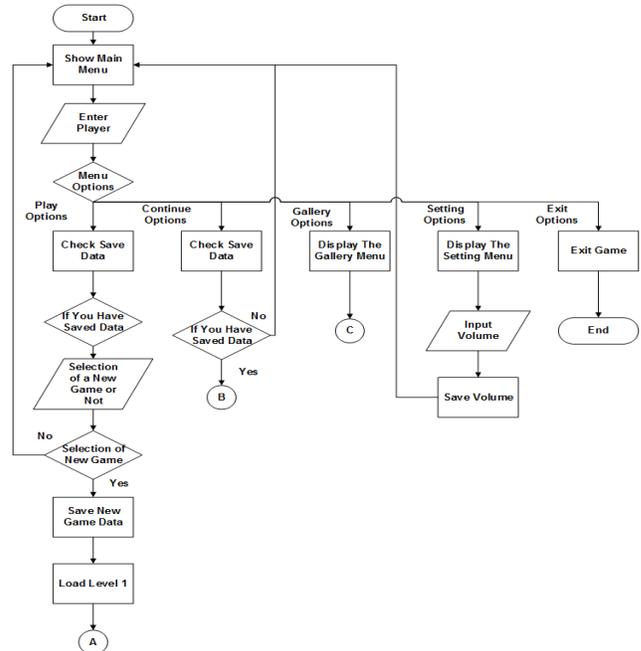


Fig. 27. Flowchart of the Game Menu.

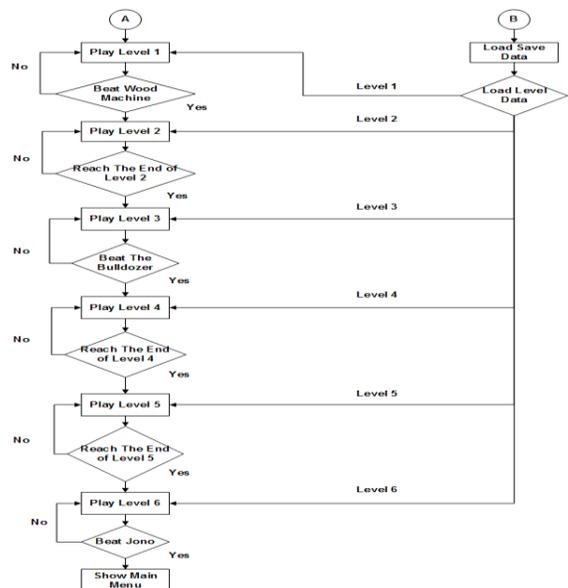


Fig. 28. Flowchart of Gameplay Flow when Conditions Win

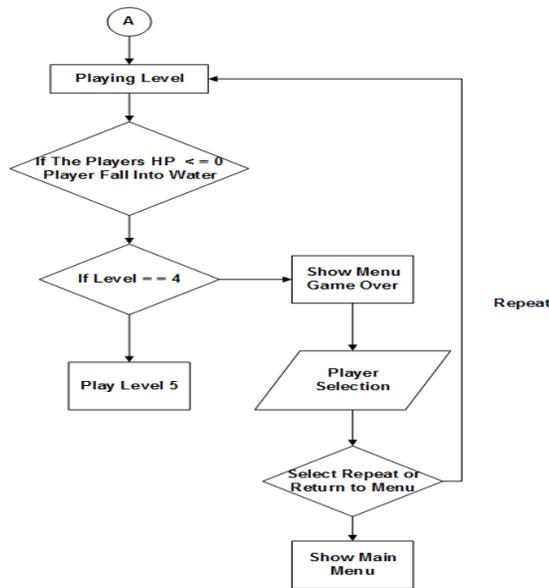


Fig. 29. Flowchart of Gameplay when Losing Conditions.

When loading a level, the game will check the existing save data and load the level based on the existing save data, players can complete the level by defeating the boss or reaching the end point of the level. By the time the player has completed level 6 then the game will be over and over shown in Fig. 29.

When the player's HP reaches 0 or falls into the water, the game will display a game over display with two options, namely to repeat or return to the initial menu, except for level 4 conditions where if the player falls into the water or HP reaches 0 then the player can continue to level next shown in Fig. 30.

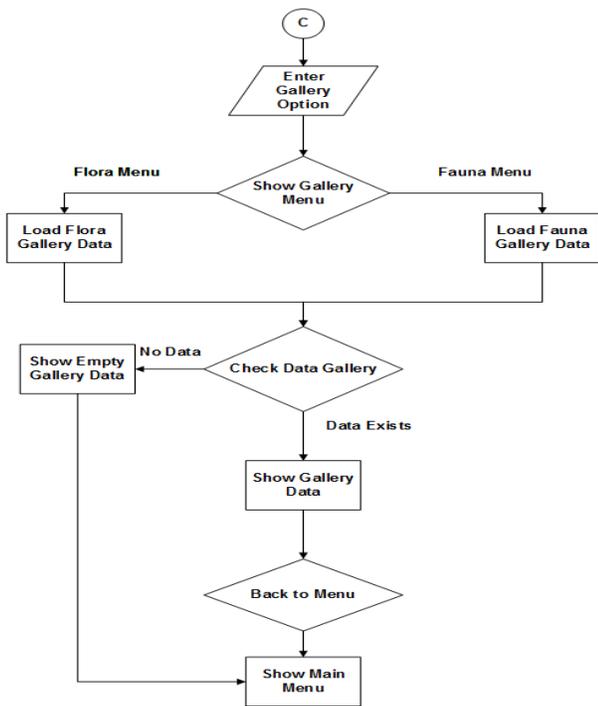


Fig. 30. Flowchart Gallery Menu.

### E. The Testing Stage

At this stage a trial is carried out from internal users who will test the game using the provided instruments, assessing the game's function and game balance. The results of these trials are bug reporting, change requests, and video game development decisions. The details explanation about the testing process will explain on the part IV Application Testing.

### F. Beta Stage

The beta stage requires external testers as game users and assesses the success rate of games that have been built before being released to the public. They tested whether changes to the features or gameplay were needed, whether there were still weaknesses in each level of the game. If there are still weaknesses, the GDLC cycle can be repeated. The details explanation about the Beta version will explain on the part IV Application Testing.

### G. Release Stage

This stage is the completion of the video game that has been built and is ready to be released. The details explanation about the release version will explain on the part IV Application Testing.

## III. RESULT AND DISCUSSION

When opening the gallery menu, the game will load the flora and fauna gallery save data that has been opened by the player's progress and display it.

1) *Design level:* Design Level 1 shown in Fig. 31 which is the first level, at this level there are new flora, namely ironwood trees and black orchids, there is a new fauna namely hornbills, at this level there are also 32 coins, 1 moving platform, 7 enemies, 1 boss which is a machine wood, and 5 dialogues which include 1 dialogue at the beginning of the conversation game between Agus and Pak Fery, 1 dialogue when seeing a hornbill for the first time and 3 dialogues for how to play this game.

Level 2 designs, at this level there are 39 coins, 4 moving platforms, 11 enemies, and 2 dialogues including 1 level 2 opening dialogue and 1 dialogue when level 2 is finished.

Level 3 design, at this level there is a new fauna, namely the Mahakam dolphin, at this level there are also 28 coins, 8 moving platforms, 12 enemies, 6 entities of which there are 4 dolphins and 2 hornbills, 1 boss, namely a bulldozer, and 2 dialogues including 1 dialogue when you see the Mahakam dolphin, and 1 dialogue when you meet the bulldozer boss.

Level 4 designs, this level is a bonus level where there are only 24 coins and 28 platforms that can fall. At this level there are no conditions that make the game over.



Fig. 31. Design Level 1.

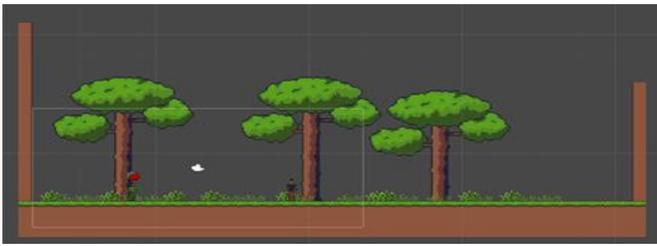


Fig. 32. Design View Level 6.

Design Level 5, at this level there is a new fauna namely Proboscis monkeys, at this level there are also 27 coins, 36 enemies, 6 entities namely proboscis monkeys, and 3 dialogues including 1 dialogue when entering this level, 1 dialogue when viewing proboscis monkeys and 1 dialogue when this level is finished.

Design Level 6 shown in Fig. 32, which is the last level in this game, this level is specifically only against the last boss, namely Jono, the leader of the illegal loggers. At this level there are also 2 dialogues, namely when entering this level and at the time after defeating Jono.

2) *Game system creation*: The basic character behavior that can be done by players, namely hitting, jumping, using a slingshot, moving right and left, using a slingshot, reducing blood, saving character data is made in 3 scripts, namely Player Behaviour, Player Projectile Behaviour, and Player Scriptable shown in Fig. 33 and Fig. 34.



Fig. 33. Player Movement.



Fig. 34. Player Jump.



Fig. 35. Dialog System.



Fig. 36. Behavior of the Enemy Hitting.

In this game the story will be used in the dialog system shown in Fig. 35, while the dialogue system in this game has several parts, namely the speaker avatar, dialogue text, speaker name, dialogue control and dialogue trigger. This dialogue system is made using 3 scripts, namely Scriptable Dialog, Dialog Manager, and Trigger Dialog.

This game has enemies that can attack the player and can walk up to the player, for an enemy system like this is made using 4 scripts, namely EnemyAttribute, EnemyBehaviour, EnemyMovement\_1, PreventObjectOnPosition shown in Fig. 36.

The bosses in this game have their own uniqueness and behavior, where bosses such as wood machines cannot move but can remove wood, bulldozer bosses that can move quickly to the right and left, and the last boss Jono who can call for reinforcements. For making the boss, it is necessary to use enemy scripts and 5 additional scripts, namely 2 scripts for the wood machine boss, 2 scripts for the bulldozer boss, and 1 script for the last boss Jono shown in Fig. 37 and Fig. 38.



Fig. 37. Wood Machine Boss.



Fig. 38. Bulldozer Boss.



Fig. 39. Platform System.



Fig. 40. Dolphin.

The platform system shown in Fig. 39, can move as a player challenge which is made using 2 scripts, namely FallPlatform, and PlatformScript. For the next level system, game over, pause, save data, audio sound effect settings, gallery and UI related, 11 scripts are needed, namely, 3 scripts for UI which include GalleryMenu, HealthUiScript, UIControl, and 8 scripts for game manager including AddToGallery, AudioAmbienceSettings, AudioSettingsUI, GalleryScriptable, GameManager, SaveManager, SceneManagement, and SoundManager.

For AI entities, hornbills and dolphins need 2 scripts, respectively, namely hornbill behavior and dolphin behavior shown in Fig. 40.

#### IV. APPLICATION TESTING

##### A. Blackbox Testing

The game will be tested by the developer using the Blackbox testing method to see if the various scenarios and functions in the game are running properly. Testing is carried out using the blackbox testing method that focuses on the user's perspective and divided into testing Blackbox UI main menu (Table II), testing Blackbox UI gameplay (Table III), testing Blackbox gameplay scenario (Table IV), and testing for the device (Table V) [26-30].

TABLE II. TESTING BLACKBOX UI MAIN MENU

Scenarios	Success Indicator	Status
Play button on menu (When no save data)	level 1	Success
Play button on menu (When have save data)	Displays the display to create a new save data or not	Success
Continue button on menu (When having save data)	Loading game level according to save data Success	Success
Continue button on menu (When having save data)	level 1	Success
Gallery button on the menu	Displays a display to view fauna and flora gallery data from save data	Success
The flora button in the gallery	Displays a list of flora gallery items	Success
Fauna button in gallery	Displays a list of fauna gallery items	Success
Items in the gallery	Displays a description of the clicked gallery item	Success
Settings button on the menu	Displays the settings	Success
Volume slider in settings menu	Change game sound volume	Success
Toggle enable sound in settings menu	Turn game sound on or off	Success
Exit button on the menu	Exit the game application	Success

TABLE III. TESTING BLACKBOX UI GAMEPLAY

Scenarios	Success Indicator	Status
Move button to the right	Character goes to the right	Success
Move button to the left	Character goes to the left	Success
Jump button	Character jump	Success
Stick button	Character hit	Success
Slingshot button	Character attacks with slingshot	Success
medkit button (when having a medkit)	Replenish the character's HP	Success
Pause button	Pauses game	Success
Continue button on pause	Continue and stop pause in game	Success
Menu button on pause	Return to main menu	Success
Retry button on game over	Repeating the game at that level	Success
Menu button on game over	Return to main menu	Success

TABLE IV. TESTING BLACKBOX GAMEPLAY SCENARIOS

Scenarios	Success Indicator	Status
Fall into the water (except level 4)	Display game over	Success
Player's HP 0	Displays game over	Success
The player hits the enemy or the enemy's catapult.	The enemy takes damage	Success
Enemy hits player	Player takes damage	Success
Players take coins	Player coins increase	Success
Players take coins to 10	Players get medkits and coins return to 0	Success
Level completed	Checkpoint move to next level and save data	Success
Game over (level 6 completed)	Checkpoint move to level 1 and save data	Success
Player reaches the end of the level (level 2 and 5)	Displays the completed level display	Success
The player defeats the existing boss (level 1, level 3, and level 6)	Displays the completed level	Success
Dialog display appears	Character stops	Success
Screen is touched when dialog appears	Displays next dialog	Success
Touch screen when dialog ends	UI will disappear	Success

TABLE V. TESTING THE DEVICES USED BY THE GAME

Device	Specification	Status
Xiaomi redmi note 7	Android 10, Ram 4GB, Resolusi 1080x2340	Runs smoothly
Advan i5c plus	Android 7.0, Ram 2GB, Resolusi 1280x720	Runs smoothly
Nokia 5	Android 7.1, Ram 3GB, Resolusi 1280x720	Runs smoothly

##### B. BetaTesting

The game will be shared to itch.io using a link and with open beta conditions so that the beta version can be played and tested directly by players, in order to get input or bug reports that the developer did not find. The beta lasts for 2 months from March 11<sup>th</sup>, 2021 to May 20<sup>th</sup>, 2021. The target game tester is university friends or gamers from outside to get better

input. The minimum number of players is 10. The players will fill out a form, which contains suggestions and input that has been provided in the game description, through the 8 question tables that have been provided. Here are the results of the beta input from some players:

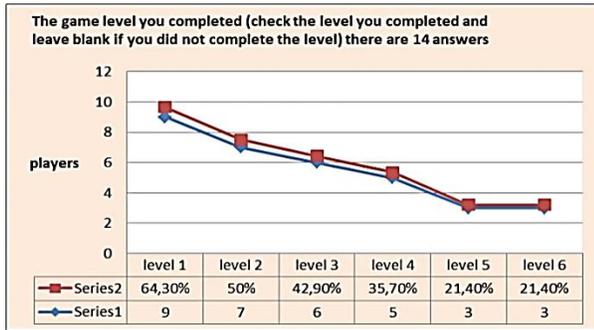


Fig. 41. The Results of the Level Input that have been Completed by the Tester.

Based on Fig. 41, it can be concluded that there are 5 testers who cannot even pass the first level and there are 3 testers who can finish this game.

TABLE VI. UI EXPERIENCE TESTER INPUT RESULTS

UI Experience	Number of Respondents
Great	8 people
Average	6 people
Bad	0
Terrible	0

Based on Fig. 41 and Table VI, it can be concluded that more than 50% of the testers were very satisfied with the UI display in the game.

TABLE VII. RESULTS OF INPUT CONTROL AND UI TESTER

No.	Feedback control and UI Tester
1.	Great, easy to understand, the function of each icon is clear.
2.	For people who have never played the game, it's fun and easy to use
3.	Sometimes it's a bit hard to control the character, UI is standard like other game
4.	Good
5.	Average, not good not so bad
6.	It's good because it works as it should
7.	There is a lack of control, namely when jumping, you can't shoot with a slingshot at the same time. It has a retro atmosphere. And the lack of in-game map instructions is still not available.
8.	the control feels great and the UI fits perfectly for mobile devices
9.	Safe and comfortable, fits well on the thumb.
10.	Reasonable
11.	The UI appearance is good, for control there are still touches that need to be improved again.
12.	Already good
13.	I like the UI design, it looks fresh and the colors chosen are good and match the theme (especially the trees and proboscis monkeys), but for some dialogs there are typos! The controls were a little less smooth as expected and therefore it was a bit difficult for me to complete the levels (especially at level 3, when I first encountered the Mahakam dolphin) and hopefully in the future I can punch or shoot enemies while walking! Because it's so hard to have to stop walking before you can hit! But overall it's a great UI and I love it! (P.S. hopefully in the future I can see my favorite animal (aka Crocodile) on there)
14.	UI controls can be replaced with analog or can choose between analog and buttons

Based on Table VII, it can be concluded that the tester likes the existing controls and UI and can be developed even better.

TABLE VIII. INPUT RESULTS ABOUT ENEMY AI BY TESTER

Enemy AI Experience	Number of Respondents
Great	8 people
Average	6 people
Bad	0
Terrible	0

Based on Table VIII, it can be concluded that the tester is quite satisfied with the existing enemy AI

TABLE IX. RESULTS OF INPUT CONTROL AND UI TESTER

No.	Feedback enemy AI Tester
1.	The enemy continues to follow the player even if he is not looking at the player (on the platform above or below the player)
2.	Pretty fun
3.	As expected, not too hard and not too easy
4.	Good
5.	Need more alive
6.	Here we cannot walk through the water but must be jumped and the enemy can be Diageo and stop when the enemy is too far from us
7.	The enemy is quite aggressive, the damage is also very strong.
8.	The AI for the enemy is great! but the difficulty for the bosses is too hard for the people who play it at first
9.	safe
10.	Can you give some coin after we killed the enemy?
11.	For the AI aspect, it's pretty good
12.	Already good
13.	I think the enemy is not bad (not easy and not too difficult), but for the boss level, it's really difficult and I think there's a bug when we accidentally jump over and get stuck with the boss, we can't help but quit the game and start over.
14.	But overall I enjoy preventing the enemy from destroying the forest to save our Kalimantan!
15.	Ordinary

Based on Table IX above, it can be concluded that the tester has various inputs about the AI in this game and the playing experience is quite different.

TABLE X. GALLERY MENU INPUT RESULTS BY TESTER

Knowing There's Gallery Menu	Number of Respondents
Yes	12 people
No	2 people

TABLE XI. GALLERY MENU INPUT RESULTS BY TESTER

No.	Gallery Information Tester Feedback
1.	Information for flora and fauna is quite complete and interesting.
2.	Very helpful
3.	Quite informative
4.	Good
5.	The gallery menu is quite interesting because we can see a pixelate version of the flora and fauna in Kalimantan and not only that, when the flora and fauna image is clicked it will display more info about the flora and fauna.
6.	it is informative, it has great description and picture to describe the flora and fauna in Kalimantan
7.	the information is complete enough
8.	In my opinion it is very informative but the number of flora and fauna is still small but it doesn't matter.
9.	I like it the design is great and hopefully in the future add more flora and fauna!
10.	The information provided is quite informative and accurate.

Based on Table X above, it can be concluded that more than 80% of testers know that this game has a gallery function to introduce flora and fauna on the Borneo Island.

Based on Table XI above, it can be concluded that the testers already liked the information about flora and fauna displayed on the gallery menu in the game.

TABLE XII. RESULTS OF INPUT, SUGGESTIONS, BUG REPORTS

No.	Tester suggestion, feedback, and bug report
1.	Sometimes when I'm on top of the enemy, the right and left directional buttons don't work, so I have to reset the level.
2.	Need a final look where animals are not scared, get stuck again while finishing the game
3.	Maybe a more minimized dialogue
4.	Sometimes I got stuck when jumping on enemy Other than that maybe you can add achievement system or time attack stage, and English version? Nice game
5.	Very good improve
6.	Bug when player jump above the enemy,
7.	I need a skip tutorial button
8.	A checkpoint needs to be made, so it's not too far to repeat it. Same controls shooting catapults while jumping are made.
9.	It is great! Only minor bug! other than that maybe the font in game seemed too "office" style, try to use more pixelated font for dialog.
10.	When stepping on the enemy (which is normal), there it stuck.
11.	Upgrade control. Get more coins by killing the enemies. Change agus's shirt colour. Tap twice for higher jumping. More damage weapon.
12.	Controls & bugs overhead
13.	I found a bug where people can get stuck and can be crushed if hit by wood that rotates up and down.
14.	add crocodile, thanks
15.	Bug: there is a bug when jumping and landing on the enemy's head Suggestion: -Information in the gallery can be added with information about why the animal/fauna is threatened with extinction, or the bad impact caused if the animal/fauna is threatened or extinct. -Level 4 gameplay is too repetitive, too many NPC Enemy which makes insufficient blood supply. -variation of animals/fauna can be added again

Based on Table XII above, it can be concluded that most of the testers had problems when players were at the head of the enemy causing bugs, this can be fixed in the next iteration of the GDLC cycle before it is released.

### C. Gameplay System Revision

Based on the bug report given by the tester, it was more inclined towards a problem where when the player was above the enemy's head causing a problem, then a fix was made for this problem in the game system changes and there was an iteration of the GDLC method, the developer then fixed this problem by making the player move. Penetrate past the enemy so that the previous problem will not occur again with duration of 5 days from May 20<sup>th</sup>, 2021 to May 24<sup>th</sup>, 2021.

### D. Release

After going through the cycle of making, repairing, and following input from several testers. Finally, the game enters the final stage, which is a release that is ready to be released on Itch.io by changing its status from in development to release on May 24<sup>th</sup>, 2021; the download link for this game will be shared to several social media such as Facebook and Instagram. The game received 46 downloads from March 1<sup>st</sup>, 2021 to May 24<sup>th</sup>, 2021 shown in Fig. 42.

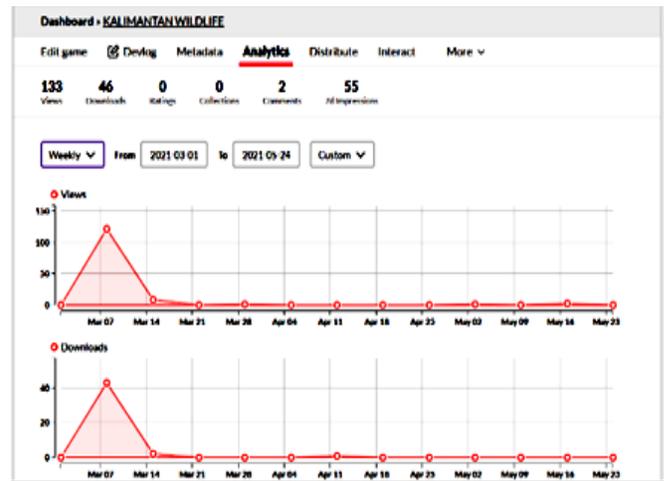


Fig. 42. Borneo Wildlife Download Statistics.

The rating of this game refers to the ESRB at the following link <https://www.esrb.org/ratings-guide/>, namely with a rating of all ages, because it does not contain abusive language and violence.



Fig. 43. Rating Images for All Ages.

## V. CONCLUSION

Based on the results of research that has been carried out in the design and development of the game "Kalimantan Wild Life", the author draws several conclusions, namely the research produces a game platform "Borneo Wildlife" with the theme of flora and fauna on Borneo Island, Indonesia, the design and manufacture of the game "Borneo wildlife" has passed the stages of the GDLC method with the longest phase being the Beta test for 2 months, and the shortest phase being the release for 1 day. In the development of the game "Borneo Wildlife" a revision was made to provide a better playing experience from the considerations and inputs of the existing testers. The future work from this study is to analyze the impact of this educational game because of the main expectation of this game is to introduce the flora and fauna in the Borneo island to the world and give positive impact to the young generation.

### REFERENCES

- [1] I. Graham, "Nineteenth-Century Borneo: A Study in Diplomatic Rivalry", Brill, Vol. 15, 1955.
- [2] C. Helliwell, "The Japanese Malay Ethnic Categorisation in Southwest Borneo," *Bijdragen Tot De Taal- Land- En Volkenkunde*, vol. 170, no. 2-3, pp. 191-214, 2014.
- [3] H. R. Davis, A. M. Bauer, T. R. Jackman, I. Nashriq, and I. Das, "Uncovering karst endemism within Borneo: two new *Cyrtodactylus* species from Sarawak, Malaysia," *Zootaxa*, vol. 4614, no. 2, pp. 331-352, Jun, 2019.
- [4] R. Butler, "Indonesia: As forests die, expect hotter days, longer droughts", *Straits Times*. Sept 30<sup>th</sup>, 2019.

- [5] M. J. Abdullah, "Species conservation priorities in the tropical forest of Southeast Asia", Proceedings of a Symposium held at the 58<sup>th</sup> Meeting of the IUCN Species Survival Commission (SSC) Oct, 4<sup>th</sup>, 1982.
- [6] D. Krebs, and I. Susanti, "Pesut Mahakam abundance & threat monitoring survey," Yayasan konservasi Rare Aquatic Species of Indonesia (RASI). Nov, 2010.
- [7] K. MacKinnon, G. Hatta, A. Mangalik, H. Halim, "The Ecology of Kalimantan, Indonesian Borneo," Oxford University Press. 1997.
- [8] J. Mellawati, F. Yarianto, and T Laddade, "Identification of flora and fauna biodiversity at Berau, East Kalimantan in NPP pre site survey," Jurnal Pengembangan Energi Nuklir. 12(2), 66-74, 2010.
- [9] C. A. McAlpine, A. Johnson, A. Salazar, J. Syktus, K. Wilson, E. Meijaard, L. Seabrook, P. Dargusch, H. Nordin, and D. Sheil, "Forest loss and Borneo's climate," Environmental Research Letters, vol. 13, no. 4, pp. 044009, 2018/03/23, 2018.
- [10] R. Ramadan and Y. Widyani, "Game development life cycle guidelines," International Conference on Advanced Computer Science and Information Systems (ICACSIS), pp. 95-100, 2013. doi: 10.1109/ICACSIS.2013.6761558.
- [11] L. Husniah, B. F. Pratama, and H. Wibowo, "Gamification And GDLC (Game Development Life Cycle) Application For Designing The Sumbawa Folklore Game "The Legend Of Tanjung Menangis (Crying Cape)""", KINETIK, vol. 3, no. 4, pp. 351-358, Oct. 2018.
- [12] S. Aslan, and O. Balci, "GAMED: digital educational game development methodology," SIMULATION, vol. 91, no. 4, pp. 307-319, 2015.
- [13] S. Aleem, L. F. Capretz, and F. Ahmed, "Game development software engineering process life cycle: a systematic review," Journal of Software Engineering Research and Development, vol. 4, no. 1, pp. 6, 2016/11/09, 2016.
- [14] T. McKenzie, M. M. Trujillo, and S. Hoermann, "Software Engineering Practices and Methods in the Game Development Industry," in Extended Abstracts of the Annual Symposium on Computer-Human Interaction in Play Companion Extended Abstracts, Barcelona, Spain, 2019, pp. 181–193.
- [15] K. Subhash Babu and R. Maruthi. Lifecycle for Game Development to Ensure Enhanced Productivity. International Journal of Innovative Research in Computer and Communication Engineering Vol. 1, Issue 8, pp. 1490-1503, Oct 2013.
- [16] I. van de Weerd, S. de Weerd, and S. Brinkkemper, "Developing a Reference Method for Game Production by Method Comparison," Situational Method Engineering: Fundamentals and Experiences. pp. 313-327.
- [17] D. Meng, B. Jianbo, Q. Yizhong, F. Yao and L. Shuqin, "Design of Amazon Chess Game System Based on Reinforcement Learning," Chinese Control and Decision Conference (CCDC), 2019, pp. 6337-6342, 2019. doi: 10.1109/CCDC.2019.8832999.
- [18] A. Aktaş, and E. Orçun, "A survey of computer game development," The Journal of Defense Modeling and Simulation, vol. 13, no. 2, pp. 239-251, 2016.
- [19] G. McAllister, and G. White, "Video Game Development and User Experience". In: Bernhaupt R. (eds) Game User Experience Evaluation. Human-Computer Interaction Series. Springer, Cham. Springer International Publishing Switzerland 2015. [https://doi.org/10.1007/978-3-319-15985-0\\_2](https://doi.org/10.1007/978-3-319-15985-0_2)
- [20] A. Setiawan, "Game Development Life Cycle", 2016, Accessed January 3, 2021, from <https://arifsetiawan.com/2016/01/game-development-life-cycle>.
- [21] A. Thompson, "The Importance of Video Game Narrative". 2021. Accessed from <https://sbanimation.com/the-importance-of-video-game-narrative/>.
- [22] D. Tyler, "What Makes A Game Great? We Look At Some of the Greatest Games To Find Out", 2018. Accessed January 3, 2021, from <https://www.gamedesigning.org/gaming/great-games/>.
- [23] T. Minkinen, "Basics of Platform Games (Kajaani University Of Applied Sciences, Finland)", 2016. <https://tekno.kompas.com/read/2013/04/30/14353642/Mengemas.Informasi.dalam.Game?page=all>.
- [24] L. S. Mongi, A. S. M. Lumenta, and A. M. Sambul, "Rancang Bangun Game Adventure of Unsrat Menggunakan Game Engine Unity". Jurnal Teknik Informatika, vol. 13, no.1, 2018. <https://doi.org/10.35793/jti.13.1.2018.20191>.
- [25] A. Rafiqin, and D. Saputra, "Pembuatan Aplikasi Game Kuis "Pontianak Punye" Berbasis Android", Jurnal Khatulistiwa Informatika, V(2), 71–84, 2017.
- [26] R. Ramadiani, A. Azainil, A. N. Hidayanto, D. M. Khairina, and M. L. Jundillah, "Teacher and student readiness using E-learning and M-learning," 2020, vol. 9, no. 3, pp. 7, 2020-06-01, 2020.
- [27] S. Sari, R. Anjani, I. Farida, and M. A. Ramdhani, "Using Android-Based Educational Game for Learning Colloid Material," Journal of Physics: Conference Series, vol. 895, pp. 012012, 2017/09, 2017.
- [28] N. Kidi, B. Kanigoro, A. G. Salman, Y. L. Prasetio, I. Lokaadinugroho, and A. A. Sukmandhani, "Android Based Indonesian Information Culture Education Game," Procedia Computer Science, vol. 116, pp. 99-106, 2017/01/01/, 2017.
- [29] Ramadiani, Azainil, U. Haryaka, F. Agus, and A. H. Kridalaksana, "User Satisfaction Model for e-Learning Using Smartphone," Procedia Computer Science, vol. 116, pp. 373-380, 2017/01/01/, 2017.
- [30] R. Ramadiani, A. Azainil, D. M. Khairina, and M. L. Jundillah, "Factors Affecting the Failure and Success of Online Learning in Samarinda", Educational Administration Research and Review Journal, Vol 5, No 1. 2021.

# Design of a Novel Architecture for Cost-Effective Cloud-based Content Delivery Network

Suman Jayakumar<sup>1</sup>, Prakash .S<sup>2</sup>, C.B Akki<sup>3</sup>

Research Scholar, Department of CSE, VTU, Belgaum, India<sup>1</sup>

Professor and Executive Director, University Institute of Engineering, Chandigarh University<sup>2</sup>

Professor and Registrar, Department of Computer Science and Engineering<sup>3</sup>

Indian Institute of Information Technology (IIIT) Dharwad, Dharwad, India<sup>3</sup>

**Abstract**—Content Delivery Network (CDN) offers faster transmission of massive content from content providers to users using servers that are distributed geographically to offer seamless relay of service. However, conventional CDN is not capable of catering to the larger scope of demand for data delivery, and hence cloud-based CDN evolves as a solution. In a real-world scenario, each requested content has different popularity for different users. The problem arises with deciding which content objects should be placed in each content server to minimize delivery delays and storage costs. A review of existing approaches in cloud-based CDN shows that yet the problem associated with content placement is not solved. In this regard, a precise strategy is required to select the contents objects to be placed in a content server to achieve higher efficiency without affecting the CCDN performance. Therefore, the proposed system introduces a novel architecture that addresses this practical problem of content placement. The study considers placement problem as optimization problem with the ultimate purpose of maximizing the user content requests served and reducing the overall cost associated with content and data delivery. With an inclusion of a bucket-based concept for cache proxy and content provider, a novel topology is constructed where an optimal algorithm for placement of content is implemented using matrix operation of row reduction and column reduction. Simulation outcome shows that the proposed system excels better performance in contrast to the existing content placement strategy for cloud-based CDN.

**Keywords**—Content delivery network; content placement; cloud; optimization; data delivery; cost

## I. INTRODUCTION

In the area of Content Delivery Network (CDN), the prime target is to offer a seamless relay of data and services associated with the delivery of contents by the content provider to a destined user [1]. There is various research being carried out towards this purpose while it was seen that it is challenging to offer this service of content delivery to large scale deployment regions by the conventional CDN [2]. Apart from constructing an appropriate CDN system and carrying out explicit maintenance of the distributed storage, followed by the delivery of appropriate content is heavily expensive from content providers' perspective. There is always a dependency of appropriate resources to perform maintenance of such servers [3]. To sort out this problem, the content providers are now seeking an alternative option of hosting the CDN over the cloud environment with much cost-effective solution [4]. Adopting the cloud environment is feasible to offer on-demand

delivery of an appropriate content in much reduced time and at a cheaper cost [5]. At present, data are evolving exponentially with respect to size and complexity, while processing such data is now feasible in cloud computing owing to its capability to offer distributed storage and analytical options more effectively [6]. Existing trends of research also showcase that cloud-based CDN has become a pivotal topic when it comes to content delivery [7]. It is also noticed that the majority of the research work is focused on performing optimization approaches towards solving the problems associated with effective placement of contents in the presence of low usage of resources [8]. Basically, the term resource in this domain of discussion pertains to the quantity of storage that is demanded to be used by the content providers for the Cloud. Out of this, the essential problem is to find out the mechanism of positioning the informative contents over the incorrect server location [9]. The idea is to accomplish the optimal cost of the content delivery system as well as to ensure the minimal consumption of cumulative cloud storage [10]. Irrespective of the availability of various forms of literature towards improving this issue, it is found that the majority of the existing approaches emphasize a specific set of problems with narrowed usage of parameters [11]. However, problems associated with optimizing the storage as the resource are not much addressed in the existing solution. Existing approaches also don't offer a discussion of the inclusion of any user or computing devices and its related connection with the cloud terminals. Therefore, there is a need to carry out an investigation in order to offer a cost-effective solution in terms of modelling content placement approach with a target to offer a higher degree of performance of content delivery in cloud-based CDN. It is also necessary to ensure that the modelling is carried out considering practical constraints that are normally connected to the incoming and outgoing stream of data. Therefore, this paper presents a novel architecture in the form of a framework that is meant for cloud-based CDN with a single target of achieving optimal cost of allocation of resources. The core goal of this study is to ensure optimal performance achievement. The significant contribution of this paper is highlighted as follows:

- A bucket concept is considered which have a caching proxy and content server, with specific storage capacity.
- A novel topology construction is performed using graph theory for the bucket placement that keeps the content server close to the users for faster content access and

cost-effective task allocation under peak traffic conditions. This not only reduces request latency, but also balances the load between content servers.

- The study utilizes node centrality and computes sparsity towards analyzing higher probability of the request and determining efficient localization of content servers hosted overcloud.
- Content placement is considered as optimal assignment problem, which is solved using an explicit function constructed based on the matrix operation with minimum cost.

The organization of the proposed manuscript is as follows: Section II discusses the explicit problem, and their corresponding solution evolved in present times. Briefing of identified issues in existing solutions towards content placement is carried out in Section III. The highlights of the proposed architecture are carried out in Section IV, followed by an elaborated discussion of adopted research methodology in Section V. Discussion of obtained simulation outcome is done in Section VI, while a conclusive summary of paper with respect to its contribution is carried out in Section VII.

## II. RELATED WORK

At present, there have been various works being carried out towards the content-delivery network. Existing approaches have addressed various forms of problems associated with the content delivery network. The most recent work of Qazi et al. [12] has addressed the problem associated with unnecessary caching, leading to cost maximization of various network resources in a content centric network. The work has introduced an optimization concept that minimizes network resources targeting to control the latency and channel capacity. Problems associated with excessive channel capacity usage are also one topic of investigation in existing schemes, which affects the content delivery process over cloud-hosted applications. Research in this direction has been carried out by Khabbiza et al. [13], where the case study of multimedia streaming has been considered. According to this solution, the traffic is directed towards the adjacent node instead of the central server, thereby controlling the servers' load.

The advanced variant of cloud usage, i.e., fog computing, was also used to enhance the content delivery network's operation. The problem associated with cost connected with the content server's placement has been discussed by Liu et al. [14]. According to the author, the existing scheme is not capable of better decision-making considering global dynamics. The authors have used the Q-learning approach to facilitate a significant decision for routing operation over a tree structure. The model performs a selection of paths based on the low cost associated with it for effective content delivery. However, this approach can still not offer much information about the topology, which will affect any form of the pricing scheme.

Moreover, such an approach is not suitable for small-scale content providers. This absence of topological information is discussed by Duan et al. [15] has used a software-defined network where the infrastructure provider hosts the cache

servers. This strategy maintains a balance between the content provider and infrastructure provider.

Further work towards content placement is carried out by Qu et al. [16], where problems associated with backhaul congestion are addressed. The study presented the solution to reduce the delay attribute associated with content delivery where mixed-integer linear programming has been used. Apart from content placement, existing studies were also carried out towards virtual network function, a part of the content delivery system. This completely depends upon the resource availability and its quantity. As per the discussion stated by Benkacem et al. [17], this problem is reported to be solved using their mathematical approach for cost minimization and upgrading quality of experience. The work carried out by Alghamdi et al. [18] has addressed the problem associated with the availability of content by using an improved version of the optimized link-state routing protocol. The study has a joint implementation of caching based on popularity and routing scheme over a cloud-based content delivery network. Similar problems of dedicated transmission of contents have been addressed by Asheralieva and Niyato [19] using game theory to model stochastic network control. The study has also used the Lyapunov optimization approach that emphasizes mobile nodes' activity connected with the operator. Another study carried out by Bosunia, and Jeong [20] addresses the challenges associated with the growing mobile internet market that affects seamless content delivery. The study has presented the usage of content-centric networking to carry out content delivery in the presence of a converged network. A case study of heterogeneous networks with radio access over Cloud is also seen in the literature concerning content delivery network investigation. The importance of using both qualities of wireless channels and their respective connection with the mobile station plays a significant role in improving the content delivery network's performance. The work carried out by Liu et al. [21] has addressed the problem associated with increasing the system's utilization using the belief propagation method. The study also presents a solution towards interference among the cells to resist the mobile station's overload at the remote radio unit. However, the adoption of a radio access network offers a significant issue over the delivery and caching of the contents and the capacity of processing. This problem has been considered in the work of Wang et al. [22], where a zone-based approach has been used for content caching cooperatively. The study has used a heuristic-based cooperation policy to better availability, and the transmission of more massive content is possible.

The existing content delivery network uses cloud radio access to support transmission in a faster network like 5G. However, the conventional caching principle offers degradation in network traffic. This problem is solved in a unique study carried out by Lau et al. [23] that has used content distribution based on humans' mobility patterns—the study aimed for the spatial allocation of radio resources and targets for resource efficiency. The resource provision methods always challenge balancing the war between the under and over-provisioning to handle the trade-off between an uncertain pattern of the user demand and their level of experiences as feedback. The authors, Haghghi et al., 2018, have designed an

optimization model for the resource assignment using Markov principles suitable for the C-CDN[24][25]. The problems associated with responsive factor in content-centric delivery are addressed in the work of Sinky et al. [26], which discusses the importance of using multiple cloudlets with contents and caching policies in a heterogeneous network.

Apart from the content mentioned above, placement approaches and existing schemes have reported various alternative schemes for content placement viz. Approaches for web content delivery for internet architecture of future (Siracusano et al. [27]), caching using the push-based strategy (Fan et al. [28]), hierarchical modelling (Papagianni et al. [29]), preemptive hierarchical approach (Salahuddin et al. [30]), bee-colony optimization algorithm (Ghalehtaki et al. [31]), cache placement approach (Ha and Kim [32]), and network-slicing (Retal et al. [33]). The next section discusses the problems associated with the existing content placement approaches, followed by a proposed solution to thwart this problem.

### III. PROBLEM STATEMENT

After reviewing the existing approaches, the following are the issues explored:

- Less emphasis on Quality of Experience (QoE): Existing studies have implemented a sophisticated mechanism of different types to address the content placement problem. However, these mechanisms do not consider the user's computing and communication device to exercise delivery services. Existing approaches do not offer much scalability concerning QoE regarding peak traffic conditions in both access and core networks.
- Impediment towards heavy file delivery: It is well known that CDN is mainly meant to handle more massive data delivery. However, theories in the paper differ from real-time demands owing to a lack of benchmarking approach. To deal with communication channels with inferior Quality of Service, the transmission rate is reduced to work at a specific limit. However, such approaches are not applicable when it comes to stream real-time multimedia content. Another practical problem is that users are usually considered connected with only one technology of access and hence, the issues shoot up.
- Scheduling of Resources: A specific amount of resources are required to carry out the problem of content placement. Management of resources can be optimized by using resource allocation for controlling cost factors. However, this is not a simplified form of the task as it demands precise information on the topology of the nodes and information by the content providers. Unfortunately, it is not there in the existing system and without which it cannot be deployed over a much complex environment of Cloud.
- Caching Related Issues: While transmitting more massive files or streaming content over the internet, it is essential to reduce the latency/delay. It is also known

that the conventional content delivery network offers varied caching algorithms; however, it is not much considered that this algorithm must be run over edges of the delivery network. This increases the complexity of multi-fold when it comes to cloud computing-based content delivery network. As the scale of deploying content servers extends exponentially when hosted over Cloud, developing an algorithm for caching management over edges is highly a complicated task.

- Ambiguity in cost modelling: There have been various models in existing approaches where cost-related modelling has been carried out. However, considered parameters in cost modelling and its relationship with the content placement problem have not yet been built. At present, the term cost is associated with the financial terms connected with the deployment of services. For effective cost modelling, it is necessary to consider all latent parameters that are the indicators of resource allocation and maintain a good streamline with user and content provider. Such consideration is missing in existing approaches.

All the problems mentioned above are addressed in the proposed system discussed in the next section.

### IV. PROPOSED SYSTEM

The proposed study's primary goal is to develop an analytical framework that could carry out a content placement in a cloud-based content delivery network. The secondary goal is to develop a cost-effective allocation of tasks from the user to the content servers over peak traffic conditions.

Fig. 1 highlights the proposed system's architecture, which shows that the model initiates by taking an input of several requests, bucket formation, and area of deployment. Each bucket is considered to possess a caching proxy and content server with an explicit storage capacity allocated for both of them. The proposed study uses graph modelling for constructing the topology by applying a directional graph where each vertex corresponds to a bucket. Geographical modelling is further carried out considering the domain-based CDN nodes where an orthogonal and symmetric directionality of the node placement is carried out. This directionality attribute plays a vital role in searching for optimal content placement over the buckets. The next step is to construct a proximity priority module where the node centrality is incorporated to understand the node's significance, considering the probability of the request. The traffic stream is judged based on the weight factor associated with the structure of in-degree and out degree nodes. The sparsity computation is carried out to find the best links out of many that lead to the efficient location of content servers hosted over cloud. After this process is carried out, the proximity priority model is executed further, followed by matrix-based operation development to carry out optimal placement using a function for performing allocation and cost estimation. This is based on the allocation of tasks to find an efficient node for content placement in cloud-based CDN. This process's outcome leads to the allocation of the task and the estimated cost of the evaluation. The next section discusses the adopted methodology.

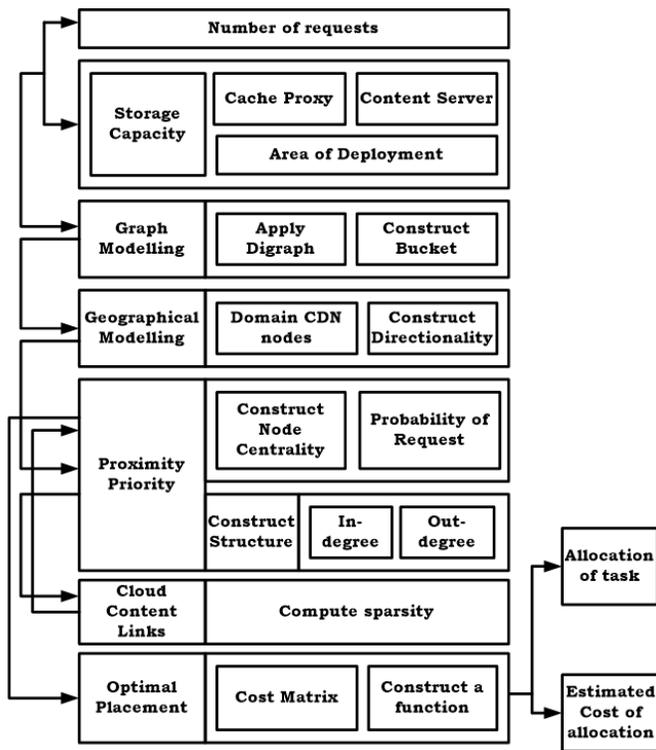


Fig. 1. Architecture of Proposed System.

V. RESEARCH METHODOLOGY

The proposed research work's prime objective is to ensure that end user is facilitated with a higher degree of service quality using the cloud-based content delivery network's proposed model. The proposed system's solution is based on the appropriate placement of the distributed cloud environment's contents. The idea of the proposed logic is that if the content placement is done accurately in a shared manner, it is feasible to minimize the cost of content maintenance over a server. The proposed system applies a novel optimization approach that can facilitate a better form of content server update and dynamic updating of contents replication. Hence, an analytical research methodology is constructed for this purpose, which can finally ensure a better form of content delivery with a controlled reduction in latency in the content transmission process. This section offers details about the comprehensive process that is adopted for appropriate, cost-effective content placement.

A. Topology for Content Placement

According to the novel concept of content placement, the prime logic is to ensure a better symmetry in the node's geographical distribution. In existing times, the content placement is carried out based on the location of users, which is highly a dynamic event. Hence, toggling the location of contents based on user location (mobility) will demand more cost consumption owing to the non-symmetrical locus of the content server. Hence, better symmetric localization of content servers will lead to better delivery performance and better service availability. Therefore, the proposed topology considers the asymmetric distribution of buckets B, as shown in Fig. 2. Buckets are the nodes, which bear all the information

and are directly synched with the cache proxy and content server. The topology also considers a centralized server CN which is equidistant from all the buckets.

The study considers a test region R, which is further classified into *i* number of regions where the placement of the buckets is carried out. It can be empirically expressed as,

$$R_i = \{R_1, R_2, \dots, R_i\}$$

Each region is assumed to consist of buckets B, which will mean that  $B = B_1, B_2, \dots, B_N$ , where  $N=i$ . It is considered that each bucket B has cache proxy C1 and content server C2, which will mean that,

$$B_N = \{(C_{1N})_{ij} | (C_{2N})_{ik}\}$$

In the above expression, *N* represents the total number of buckets, *i* represents several regions, and *j* represents the maximum number of the proxy server while *k* represents the content server's highest capacity. The proposed concept of placement of content on multi-cloud architecture takes 'N' buckets (B) in geographically distributed Data Center (shown as CN in Fig. 1) acts both as Cache-Proxy as well as Content Server. Both of them are interconnected bi-directionally to each other under with a weight (w). The weight (w) is considered a set of the properties {caching, cost, latency, dynamicity/ambiguity, and interoperability}. The context of the  $N=4$  as  $\{B_1, B_2, B_3, B_4\}$  with the connectivity possibility of pair of  $:\{[(B_1-B_2), (B_1-B_3), (B_1-B_4)], [(B_2-B_4), (B_2-B_1)], [(B_3-B_2)], [(B_4-B_3), (B_4-B_1), (B_4-B_2)]\}$  as shown in the Fig. 2.

The respective weight for different capacities of the connection network,  $W = [B_1/3' B_1/3' B_1/3' B_2/2' B_2/2' B_3' B_4/3' B_4/3' B_4/3']$ . The proposed system performs modeling using graphical constructs, i.e.,  $G(V, E)$ , where the vertices 'V' represents the bucket  $B \rightarrow C1/C2$  and the edges 'E' represents connecting links among the respective nodes, is represented in Fig. 3. These associating weights mechanism assists in the proper identification of appropriate links connecting to various buckets that have reduced cost factors involved.

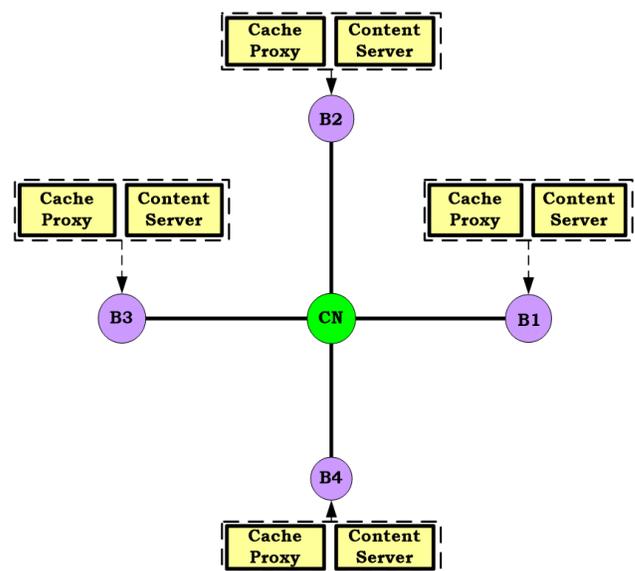


Fig. 2. Proposed Topology of Content Placement.

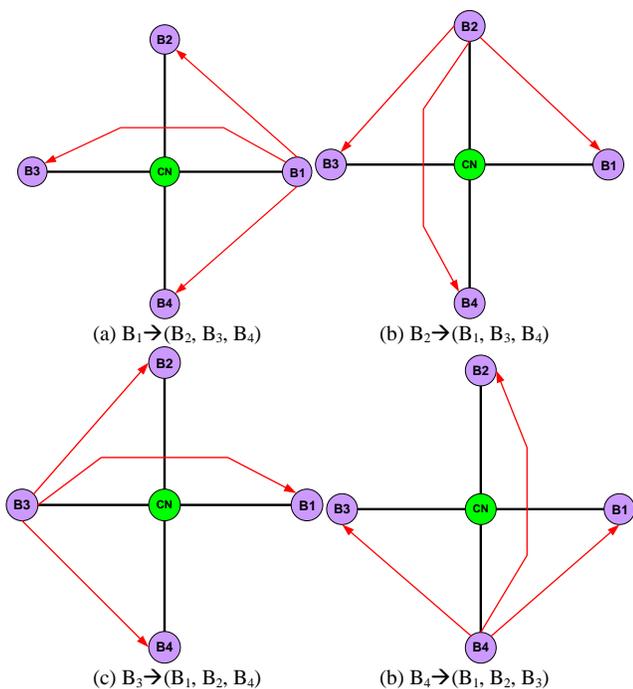


Fig. 3. Connectivity among the Buckets.

All these forms the shape of the matrix, and the entries of the adjacency matrix take either the complete or a sparse of the numeric data with the input elements of the connections of the network as edges among the nodes as a non-zero element. The value represents the weight of the edge connection and if it is a logical adjacency that results in an unweighted graph. If there are non-zero values in the diagonal representing a self-loop, the nodes are connected to themselves with an edge.

The standard topology consists of bucket placement in 4 different directions, which are the right angles. However, for better connectivity, more symmetrical placement is required for effective data transmission. The content bucket modeling for the consistency in the geographical distribution to achieve balanced latency is modeled as locational mapping with the placement of the proxy/content buckets in the location of the  $L = \{\text{North (N), South (S), East (E), West (W), North-East (NE), North-West (NW), South-East (SE), South-West (SW)}\}$  as shown the Fig. 4.

Fig. 5 highlights the 8 nodes placement of the bucket in a highly symmetric fashion. One of the advantages of this topology is that it offers complete supportability of sharing content in any of the buckets during the dynamic traffic scenario. Hence, the proposed topology is supportive of users with dynamic mobility. One case study of the data center CN's connectivity with all the 8 respective bucket positions is shown in Fig. 6. A graphical direction is given from the data center to the respective buckets.

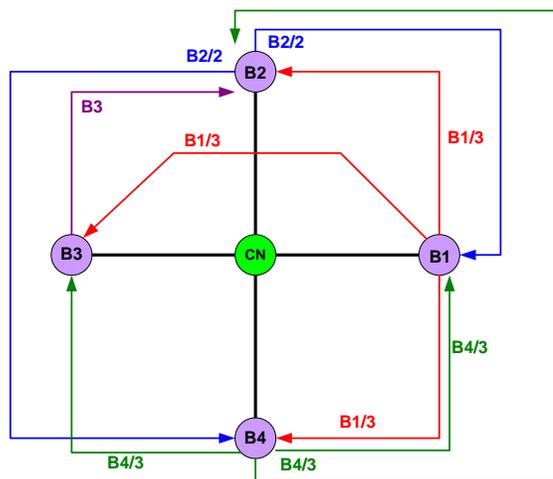


Fig. 4. Constructed Graph with Weights.

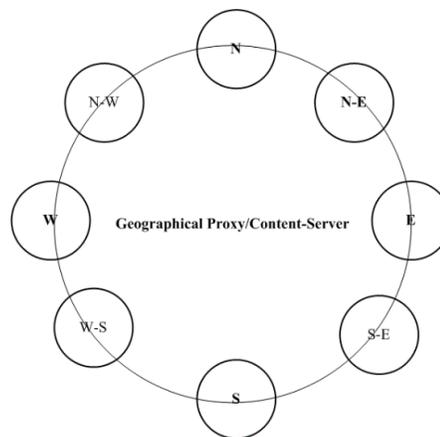


Fig. 5. Geographical Distribution of Cache/Content Server.

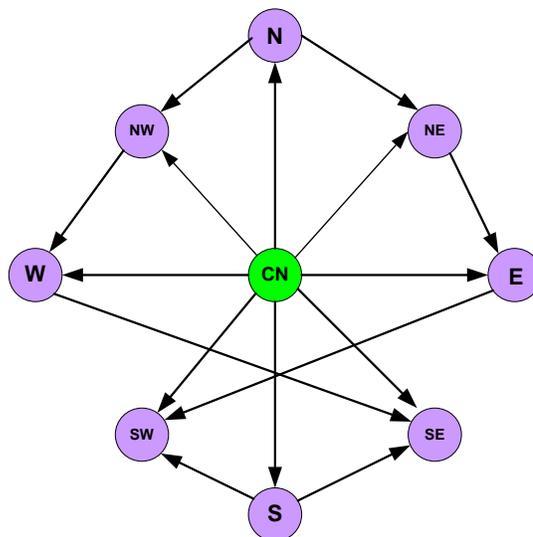


Fig. 6. Directed Graph for Optimal Connectivity.

The information associated with the degrees is captured from each node, assuming that the datacenter hosts a node with a domain `http://cdnserviceprovider.com/Central`. Therefore, the extracted features will be:

- CN: node `http://cdnserviceprovider.com/Central`
  - In-degree: 0, Out-degree: 8
- NW: node `http://cdnserviceprovider.com/NW`
  - In-degree: 2, Out-degree: 1
- NE: node `http://cdnserviceprovider.com/NE`
  - In-degree: 2, Out-degree: 1
- SE: node `http://cdnserviceprovider.com/SE`
  - In-degree: 3, Out-degree: 0
- SW: node `http://cdnserviceprovider.com/SW`
  - In-degree: 3, Out-degree: 0
- W: node `http://cdnserviceprovider.com/West`
  - In-degree: 2, Out-degree: 1
- N: node `http://cdnserviceprovider.com/North`
  - In-degree: 1, Out-degree: 2
- S: node `http://cdnserviceprovider.com/S`
  - In-degree: 1, Out-degree: 2
- E: node `http://cdnserviceprovider.com/East`
  - In-degree: 2, Out-degree: 1

All the above features are used for computing the cost factor involved in the proposed cloud-based content delivery network. The proposed system enables the connectivity with the cache proxy with the nearest bucket available in the topology. Apart from this, all the buckets are connected and synced with each other, as shown in Fig. 5. This interconnection of the graph edges facilitates the proposed cloud-based content delivery network to carry out the delivery of the contents in a dynamic pattern. The study also considers that datacenter CN consists of all the source content, and it is also directly linked with all the buckets in the proposed cloud-based content delivery network. In the conventional data delivery mechanism, the user-based contents required to be shared with users are duplicated over various variants of the cache proxies. However, this mechanism calls for a significant imbalance between content servers and the data transmission cost as there are a maximized number of increasing replicated files. The novelty of the proposed system is that it can eliminate the duplicated file from cache proxies and save them over different buckets in their respective buckets, unlike existing approaches. This mechanism can significantly minimize the quantity of the replicated file and potentially control the cost of content server placement. The algorithm developed for optimal cost computation is as follows:

---

#### Algorithm for Optimal Cost Computation

---

**Input:**  $s, t, B, N, D$

**Output:**  $c$

**Start**

1. Define  $s, t (B_N), D$
2. Apply graph,  $G(s, t)^D$
3.  $pr \rightarrow f_1(G)$
4. struct  $G=[pr, id, od]$
5. Apply  $f_2(G)$
6. obtain  $G_{sub}(G, sig_{p>p})$
7.  $c \rightarrow$  Apply  $f_3(pr)$

**End**

---

The above algorithm is responsible for computing the optimal cost in the proposed cloud-based content delivery network, which takes the input of  $s$  (source),  $t$  (destination),  $B$  (bucket),  $N$  (number of buckets), and  $D$  (domain hosted) that after processing yields an outcome of  $c$  (cost). The proposed algorithm's initial step is defining the particular  $N$  number of buckets concerning source and destination (Line-1). A digraph structure  $G$  is used for this purpose in order to give a shape of connected buckets in topology (Line-2). The next part of the implementation is about computing the centrality of graph  $G$  (Line-3). It is computed by dividing each bucket's value by one a smaller number of nodes that essentially represents the number of edges connected to the buckets. This operation results in a priority factor  $pr$  (Line-3). Once the priority factor is computed, the proposed system constructs a graphical structure  $G$ , which consists of priority factor  $pr$ , in-degree  $id$ , and outdegree  $od$  (Line-4). Finally, the proposed system constructs a sparsity pattern for the given buckets as variable test cases of different placement of the buckets. This is carried out to testify the sustainability of the algorithm towards lower latency over the various position of the bucket in a defined area. This operation is further followed by applying a digraph structure over  $G$  (Line-5). Finally, the sub-graph  $G_{sub}$  is obtained, and only those buckets are selected, whose priority factor is found to be statistically significant ( $>0.005$ ) (Line-6). Finally, the algorithm constructs an explicit function  $f_3(x)$ , which is responsible for obtaining the optimal cost of the content delivery placement. This mechanism is carried out using matrix-based operation where the buckets and their region-specific information are considered priority factor  $pr$ . The formation of this function is carried out in the following manner:

**Problem Formulation:** A case study using matrix-based operation is considered to understand the proposed study's problem formulation. As the proposed system uses information associated with buckets and priority factors associated with the content placement, it is easier to represent this fact using a matrix. The proposed system constructs a squared matrix of  $n \times n$ , which exhibits the associated cost for all  $n$  buckets to obtain buckets' optimal placement concerning the data center. The complete goal is to reduce the overall cost. As one bucket can be utilized for carrying out one set of job processing and all jobs should be allocated uniquely to each bucket in its respective position. Therefore, this allocation will formulate an independent set of matrix  $M$  as below:

$$M(i,j) = \begin{matrix} & \begin{matrix} a & b & c & d \end{matrix} \\ \begin{matrix} p \\ q \\ r \\ s \end{matrix} & \begin{bmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 6 & 8 \\ 3 & 6 & 9 & 12 \\ 4 & 8 & 12 & 16 \end{bmatrix} \end{matrix}$$

In such a situation, a random allocation is used where the bucket  $p$  is allocated job  $b$ , bucket  $q$  is allocated job  $d$ , and it goes on following such a pattern. The cost factor involved in such a case of job allocation will be 23, while the problem will be to search for allocating much minimal cost value. The constraint will be to perform all the individual allocation has to be relatively discrete and different overall the given rows and columns in matrix  $M$ . In order to find a solution to this problem, a brute-force approach can be used that can lead to a yield of a different independent set of  $M$  matrix. It should result in overall cost for all the content placements and explore the smaller set. However, it has to be noted that the complete computational complexity factor is associated with the size of the squared matrix and its associated allocation of buckets. It will mean that  $n$  choices will be the primary allocation while  $(n-1)$  will be the second allocation that finally leads to factorial  $n$  feasible sets of allocation. Hence, a significant complexity associated with computational run time is associated with this process. While selecting the assignment, the respective rows and columns must be eliminated; therefore, a problem will be to find the optimality of this reduction process. This leads to higher computational complexity. In this regard, the study presents optimal strategy based on cost matrix formulation as shown in Fig. 7.

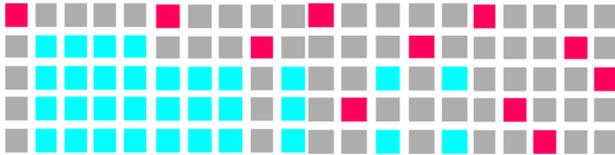


Fig. 7. Visual Representation of Cost Matrix.

Solution: The solution to this problem is carried out by constructing a function  $f_3(x)$ . The matrix operation carried out in this function is showcased in Fig. 8. There are six steps of operation that are carried out to solve this problem viz. i) a non-squared matrix of  $n \times m$  is constructed where the elements depict cost factor associated with the allocation of one of  $n$  bucket to one unique  $m$  job. The matrix  $M$  is rotated in such a way that there is always a minimum number of rows and columns and considers  $k \rightarrow \text{argmin}(n, m)$ . ii) the next step is to search for the minimal element over all the rows in the  $M$  matrix and subtract it from all the elements present in the row, iii) the consecutive step is to look for the presence of zero in the outcome matrix. The absence of any zero in the row and the column calls for flagging that zero. It is iterated for all the matrix elements. iv) all the zero elements that are starred are covered concerning the column of its position. If  $K$  number of columns is covered, then the flagged zeros represent a cumulative set of non-repeating allocation. In such a case, the operation is completed, or else the next step is processed. v) All the zero elements that have not been covered up are identified and then are primed. In case of such primed zero, absence of any flagged zero over the row, the function performs next step, or else this particular row elements are covered, and all the columns consisting of flagged zero are uncovered. This process is repeated until and unless all the zero elements are covered. The minimal value of the uncovered element is saved, vi) a series of alternating flagged zero elements and primed zero elements is constructed, vii) the value of the result obtained in step 5 is added to all the elements over rows with covered elements, followed by subtracting it from all the values of a column that are uncovered. Without performing any alteration over covered lines, primes, and flags, the process returns to the 5th step. viii) The final step indicates the pairs of values to be allocated, considering the flagged zero elements' position over the  $M$  cost matrix. Therefore, if  $M(i,j)$  is flagged zero, then the values connected with this  $i$ th row are allocated to the  $j$ th column values.

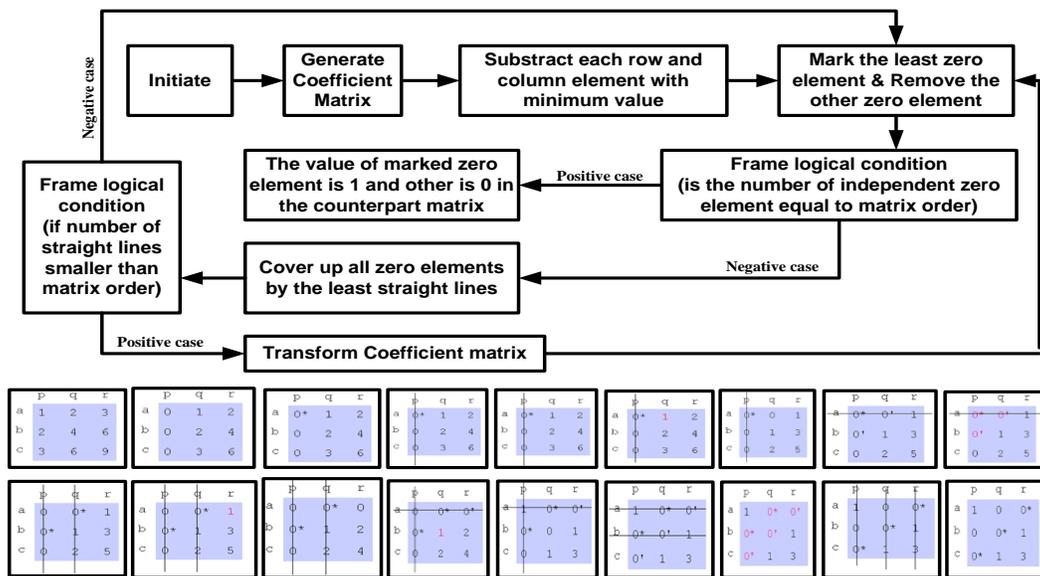


Fig. 8. Matrix Operation Carried Out in Function  $f_3(x)$ .

The function  $f_3(x)$  outcome is an optimal allocation with highly reduced cost based on the input argument cost matrix. The complete operation of  $f_3(x)$  is discussed concerning the proposed cloud-based CDN as follows:

Consider that there is  $\Phi$  number of jobs required to be accomplished based on the query generated by the  $\alpha$  number of computing devices of the user. Assuming that  $\Phi \leq \alpha$ , there is a possibility that any computing devices can be allocated in order to accomplish this task over a cloud environment, where each device incurs a cost in the form of resources as well as time to accomplish the task. Hence, the proposed cloud-based CDN system's objective function will be to carry out the complete task without the inclusion of maximized cost while performing a selection of the best resources and computing device for this purpose. Therefore, the objective function developed for this purpose is:

$$arg_{min} \sum_{i=1}^{\Phi} \sum_{j=1}^{\alpha} m_{ij} \cdot \beta_{ij} \mid \sum_{i=1}^{\Phi} \beta_{ij} = 1$$

$$0 \leq \sum_{j=1}^{\alpha} \beta_{ij} \leq 1, \beta_{ij} \in [0,1] \quad (1)$$

The expression (1) represents a cost matrix  $m_{ij}$  that essentially depicts the cost incurred by a computing device of user  $i$  to carry out the  $j^{\text{th}}$  task. The variable  $\beta$  represents a binary matrix whose value is considered 1 if a specific  $i^{\text{th}}$  computing device of the user is allocated a specific task of  $j$  or else it takes 0. The proposed algorithm of allocating the task offers by considering a bipartite graphical structure  $G=(V, E)$  where the vertices  $V$  is a union of all source node  $s$  and destination node  $d$ . All the vertex of the bipartite graph is labeled  $\gamma$ , and the condition for labeling is that all the labels are anticipated to map with the matching constraint in the distributed cloud environment. The system considers the possible labelling as a function that satisfies a criterion of  $\gamma(x)+\gamma(y) \geq \lambda(x,y)$ , where the variable  $\lambda$  represents the weight factor. The study considers that a vertex  $\alpha$  is only tagged as matching if this vertex is a part of the main vertex  $\alpha_m$ . The subgraph of  $G$  is represented by  $G_\lambda$  that consists of information about the edges. The study considers this subgraph  $G_\lambda$  to be a spanning tree of main graph bipartite  $G$ . Further; it amalgamates the complete available vertices from the main graph  $G$ . The feasibility of the allocation is ensured in this process by ensuring the inclusion of only those communication links (edges) from the core bipartite matched graph. Considering that  $\alpha'$  to be precisely matching with the spanning subgraph  $G_\lambda$  then  $\alpha'$  is considered to match with core graph  $G$  with the highest weight exhibiting the better allocation process and minimal cost. The implementation intends to exhibit that  $\alpha'$  is the only perfectly matching matrix where the weight computation for allocation is carried out as follows:

$$\lambda(\alpha) = \sum_{x,y \in \alpha} \lambda(x,y) \leq \sum_{x,y \in \alpha} \{g[\gamma(x,y)]\}$$

$$= \sum_x \gamma(x) + \sum_y \gamma(y) = \sum_{x,y \in \alpha} \{g[\gamma(x,y)]\}$$

$$= \sum_{x,y \in \alpha} \{\lambda(x,y)\}$$

$$= \lambda[\alpha'] \quad (2)$$

In the above mathematical expression (2), the variable  $g$  represents the summation operator while  $\alpha'$  signifies the highest form of matching for cost-effective allocation in cloud-based CDN, and thereby a global optimization is ensured. It should be noted that the complete process of cost-effective allocation in cloud-based CDN is applied over a dense matrix, which signifies that the proposed system is capable of withstanding peak traffic conditions. The study finds that such operation is capable of transforming the row and column by harnessing the potential advantage of the proposed data structure that is crossed linked. This structure is utilized to reposit the data while the links are manipulated to forward the data from the server to the users. There is another reason for the efficiency of allocation in the proposed cloud-based CDN. The proposed system uses the function  $f_3(x)$ , where the difference between the weight is reformulated in the form of a structure matrix. The structured matrix is then subjected to classification concerning its complete columnar elements into a specific number of blocks uniformly. A similar operation of classification is also carried out for row-wise elements. All the sub-problems are now solved in parallel fashion in the proposed system, ensuring the capability to perform job query processing from an incoming stream of traffic. All the tasks that are found to be unique are then checked. This ensures that if the same task resides within multiple computing devices of a user, then only the task with higher profit is only accepted and considered for allocation. With sparsity property aid, the proposed system offers better efficiency of allocation of job cost-effectively irrespective of the choice of operation either in a row or in column-wise. Therefore, the proposed system performs content in cloud-based CDN by formulating a novel topology using a bipartite graph. The solution offered by the.

## VI. RESULT ANALYSIS

The proposed system's implementation is carried out in an analytical fashion, where MATLAB was used for scripting. The analysis is carried out considering the graphical structures where cost and latency play a significant contributory role. Table I highlights the cost associated with each bucket in different position of North (N), East (E), West (W), South (S), North East (NE), North West (NW), South East (SE), South West (SW), and central node of the data center (CN). A bipartite graph is initially constructed for topology creation. The study assumes the simulation parameters as 25 cache proxy with 3000 MB of maximum capacity for each, 10 content servers with 5000 MB of maximum capacity for each, 9 areas of deployment of buckets. Table I shows the position of the buckets vertical wise while its respective cost is highlighted horizontally. The study's complete implementation has been carried out considering 9 buckets that have possession of both cache proxy and content server. The selection of the simulation parameters is highly flexible, and it is considered in such a way that there is an assignment of reduced capacity for the proxy server in contrast to the content server in the bucket. This is carried out in order to map with the practical environment of cloud-based CDN. Table I highlights the instance of the cost matrix for all location = { P/C-S-N (1), P/C-S-S (2), P/C-S-E (3), P/C-S-W (4), P/C-S-NE (5), P/C-S-NW (6), P/C-S-SE (7), P/C-S-SW(8), P/C-S-CN(9)}. Here, the variable P is an optimal position, and {S, N, W, E} represents 4 orthogonal directions

of south, north, west, and east for the considered topology. The variable Ct represents the cost of all 9 locations. The table highlights the nodes (buckets) under the different possible conditions of 4 orthogonal directions. Table II highlights the accomplished cost associated with all the nodes in 9 different positions in multiple nodes' directions. Table III represents the elements allocated in binary matrix  $\beta$  where the numerical

value of 0 will represent zero task allocation, while 1 will represent the allocated task from the user device to the bucket. Table IV highlights the estimated cost for all the nodes in 9 different positions. The estimation of cost is carried out by the proposed algorithm explicitly by applying the function for optimal placement  $f_3(x)$ .

TABLE I. COST AS LATENCY ALGORITHM

	Ct-1	Ct-2	Ct-3	Ct-4	Ct-5	Ct-6	Ct-7	Ct-8	Ct-9
P/C-S-N (1)	Co-1	Co-2	Co-3	Co-4	Co-5	Co-6	Co-7	Co-8	Co-9
P/C-S-S (2)	Co-10	Co-11	Co-12	Co-13	Co-14	Co-15	Co-16	Co-17	Co-18
P/C-S-E (3)	Co-19	Co-20	Co-21	Co-22	Co-23	Co-24	Co-25	Co-26	Co-27
P/C-S-W (4)	Co-28	Co-29	Co-30	Co-31	Co-32	Co-33	Co-34	Co-35	Co-36
P/C-S-NE (5)	Co-37	Co-38	Co-39	Co-40	Co-41	Co-42	Co-43	Co-44	Co-45
P/C-S-NW (6)	Co-46	Co-47	Co-48	Co-49	Co-50	Co-51	Co-52	Co-53	Co-54
P/C-S-SE (7)	Co-55	Co-56	Co-57	Co-58	Co-59	Co-60	Co-61	Co-62	Co-63
P/C-S-SW(8)	Co-64	Co-65	Co-66	Co-67	Co-68	Co-69	Co-70	Co-71	Co-72
P/C-S-CN(9)	Co-73	Co-74	Co-75	Co-76	Co-77	Co-78	Co-79	Co-80	Co-81

TABLE II. ACCOMPLISHED COST

Position	Ct-1	Ct-2	Ct-3	Ct-4	Ct-5	Ct-6	Ct-7	Ct-8	Ct-9
P/C-S-N (1)	70	72	27	64	22	92	4	24	55
P/C-S-S (2)	64	97	15	96	67	0	18	92	43
P/C-S-E (3)	3	53	28	24	84	46	72	27	64
P/C-S-W (4)	7	33	44	68	34	42	47	77	65
P/C-S-NE (5)	32	11	53	29	78	46	15	19	68
P/C-S-NW (6)	53	61	46	67	68	77	34	29	64
P/C-S-SE (7)	65	78	88	70	1	32	61	9	95
P/C-S-SW(8)	41	42	52	7	60	78	19	58	21
P/C-S-CN(9)	82	9	94	25	39	47	74	68	71

TABLE III. ELEMENTS OF BINARY MATRIX

Position	Ct-1	Ct-2	Ct-3	Ct-4	Ct-5	Ct-6	Ct-7	Ct-8	Ct-9
P/C-S-N (1)	0	0	0	0	0	0	1	0	0
P/C-S-S (2)	0	0	0	0	0	1	0	0	0
P/C-S-E (3)	0	0	1	0	0	0	0	0	0
P/C-S-W (4)	1	0	0	0	0	0	0	0	0
P/C-S-NE (5)	0	1	0	0	0	0	0	0	0
P/C-S-NW (6)	0	0	0	0	0	0	0	1	0
P/C-S-SE (7)	0	0	0	0	1	0	0	0	0
P/C-S-SW(8)	0	0	0	0	0	0	0	0	1
P/C-S-CN(9)	0	0	0	1	0	0	0	0	0

TABLE IV. ESTIMATED COST

Position	Bucket No	Cost
P/C-S-N (1)	Ct-7	4
P/C-S-S (2)	Ct-6	0
P/C-S-E (3)	Ct-3	28
P/C-S-W (4)	Ct-1	7
P/C-S-NE (5)	Ct-2	11
P/C-S-NW (6)	Ct-8	29
P/C-S-SE (7)	Ct-5	1
P/C-S-SW (8)	Ct-9	21
P/C-S-CN (9)	Ct-4	25

At present, the content placement approaches are mainly of two types, i.e., deterministic and randomized. The deterministic approach selects a static topology and does not offer any changes in the user's due course of query processing. The randomized process involves selecting randomized buckets in due course of task processing query from the user. However, the proposed system is optimal in its approach as it can offer a dynamic update and dynamic change of topology by adapting the new cost associated with the link leading to the content matrix. All the calculations are carried out in a similar environment concerning increasing simulation rounds. Each simulation rounds are incorporated with random allocation of the task from the user towards the edge's bucket. The idea is to assess the performance of the proposed content placement approach concerning multiple performance parameters, e.g., Algorithm processing time, latency, cost of allocation, and the probability of resource allocation.

Fig. 9 shows that the proposed system offers a 20% improvement in faster processing than the existing one. The prime reason behind this is the faster update exchange within the topology, where it consumes less time to find the efficient bucket for content placement than the existing approach.

Fig. 10 highlights that the proposed system offers a significantly higher reduction in latency, approximately 60% compared to the existing system. A closer look at the graphical outcome shows no significant difference in randomized and deterministic approach much. The reason behind it is that, in the existing approach, the problem is solved from local problem space, which consumes more time and hence is not scalable for more massive and dense traffic conditions.

However, the proposed system focuses on the global problem space by constructing a crosslinked data structure with different buckers. This makes the process of algorithm execution faster and ensures that incoming queued jobs are faster processed. Each cost matrix keeps track of indegree and outdegree, which are always balanced if there is more indegree than outdegree, causing better control of latency performance.

Fig. 11 highlights that the proposed system's cost performance is approximately 40% better than the existing approach. The deterministic approach performs calculation of the efficient algorithms in advance and then fixed its topology to perform query processing towards buckets. This allocation's static nature often contradicts the allocated weight of the links with the incoming traffic, which causes an increased cost of allocation.

On the other hand, a randomized approach exhibits better performance in the prior set of simulation rounds; however, this approach requires additional effort to explore a greater number of network indicators for efficient content placement with increasing rounds. So, it is only slightly better than the deterministic approach. The proposed approach offers a better cost reduction capability as it can carry out all task processing and allocation using a parallel approach and hence same data structure is reused for parallel allocation of job over the buckets. This drastically reduces the cost associated with allocation in order to find a better content placement.

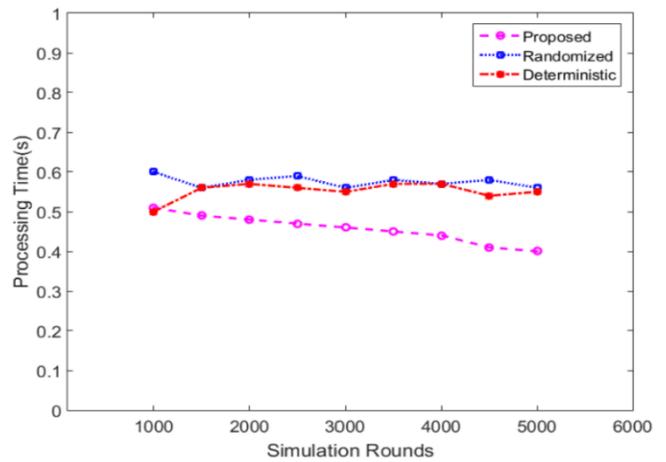


Fig. 9. Comparative Analysis of Processing Time.

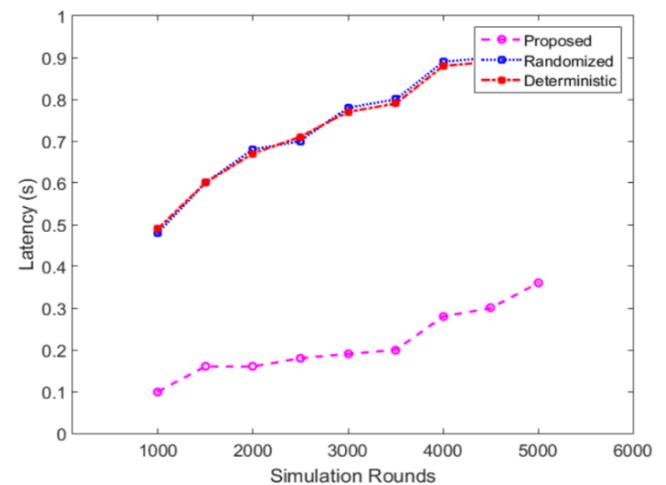


Fig. 10. Comparative Analysis of Latency.

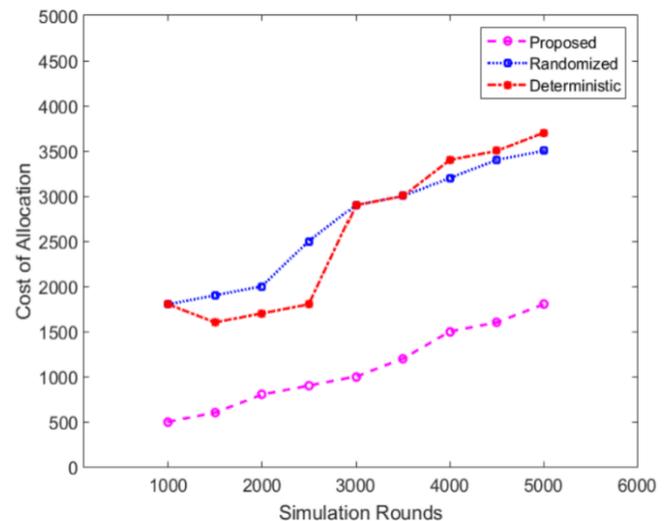


Fig. 11. Comparative Analysis of Cost.

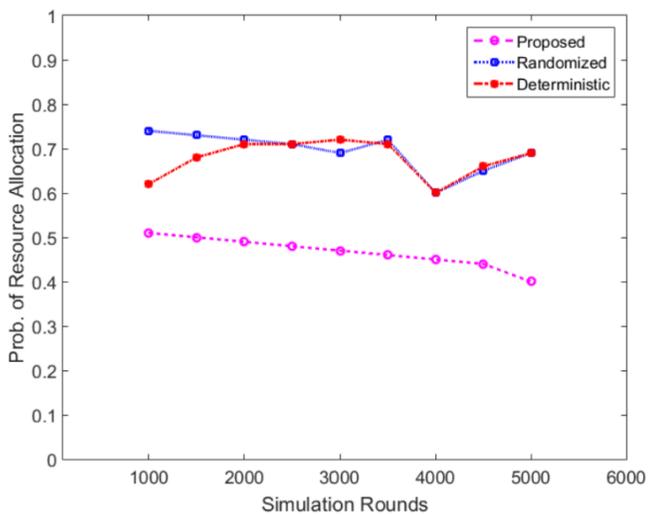


Fig. 12. Comparative Analysis of Allocation.

Fig. 12 highlights that the probability of resource allocation of the proposed system is approximately 35% better than the existing approach for a similar cause. Hence, based on this outcome, it can be said that the proposed system is capable of offering cost-effective content placement with reduced computational complexity and at par with meeting the demands of practical networks over a cloud environment.

### VII. CONCLUSION

This paper has presented a novel framework where a unique architecture towards cost modelling is carried out for content placement. The overall contribution of this paper is as follows: i) the paper introduces a novel way of using cost matrix using crosslinking data structure which can minimize the dependencies of replica in order to optimize the cost of content delivery, ii) the study achieves faster processing time over a stream of continuous data (or request) from the user making it suitable for practical world application over Cloud-based CDN, iii) the applicability of proposed system will have a higher score of quality of experience as well as the quality of service due to the following reason: it offers reduced dependency of resources thereby making it resource optimized approach, it uses data sparsity and offers reduced allocation cost capable of processing multiple jobs at one instance. This makes the system support both parallel processing over a distributed storage environment over Cloud. The key novelty is that the scheme presented in this paper, jointly addresses multiple issues such as content server placement and optimal content placement on the content server to support maximum content request and content delivery with less delay and higher throughput. The proposed system can be viewed as a support system in CCDN to enhance the user experience. Our future work will be towards further optimizing the performance.

### REFERENCES

[1] B.Zolfaghari,G. Srivastava, S. Roy, H. R Nemati, "Content Delivery Networks: State of the Art, Trends, and Future Roadmap", ACM Computing SurveysVol. 53, No. 2Content Delivery Networks: State of the Art, Trends, and Future Roadmap, 2019.  
[2] Salahuddin, M. A., Sahoo, J., Gliitho, R., Elbiaze, H., &Ajib, W. (2017). A Survey on Content PlacementAlgorithms for Cloud-based Content

Delivery Networks. IEEE Access: Practical Innovations, Open Solutions, 6, 91–114. doi:10.1109/ACCESS.2017.2754419.  
[3] Silva, Fabrício A., Azzedine Boukerche, Thais RM Braga Silva, Linnyer B. Ruiz, Eduardo Cerqueira, and Antonio AF Loureiro. "Vehicular networks: A new challenge for content-delivery-based applications." ACM Computing Surveys (CSUR) 49, no. 1 (2016): 1-29.  
[4] Yubao Zhang, Hao, Shuai, , Haining Wang, and Angelos Stavrou. "End-users get maneuvered: Empirical analysis of redirection hijacking in content delivery networks." In 27th {USENIX} Security Symposium ({USENIX} Security 18), pp. 1129-1145. 2018.  
[5] S. Qabil, U. Waheed, S. M. Awan, Y. Mansoor and M. A. Khan, "A Survey on Emerging Integration of Cloud Computing and Internet of Things," 2019 International Conference on Information Science and Communication Technology (ICISCT), Karachi, Pakistan, 2019, pp. 1-7, doi: 10.1109/CISCT.2019.8777438.  
[6] Banu, S. Sajitha, and S. R. Balasundaram. "Cost effective approaches for content placement in cloud CDN using dynamic content delivery model." International Journal of Cloud Applications and Computing (IJCAC) 8, no. 3 (2018): 78-117.  
[7] Gkatzikis, Lazaros, Vasilis Sourlas, Carlo Fischione, Iordanis Koutsopoulos, and György Dán. "Clustered content replication for hierarchical content delivery networks." In 2015 IEEE International Conference on Communications (ICC), pp. 5872-5877. IEEE, 2015.  
[8] R. W. L. Coutinho, A. Boukerche and A. A. F. Loureiro, "Design Guidelines for Information-Centric Connected and Autonomous Vehicles," in IEEE Communications Magazine, vol. 56, no. 10, pp. 85-91, OCTOBER 2018, doi: 10.1109/MCOM.2018.1800134.  
[9] Gupta, R. K., Hada, R., & Sudhir, S. (2017). 2-Tiered Cloud based Content Delivery Network Architecture: An Efficient Load Balancing Approach for Video Streaming. IEEE International Conference on Signal Processing and Communication. doi:10.1109/CSPC.2017.8305885  
[10] P. Osypanka and P. Nawrocki, "Resource Usage Cost Optimization in Cloud Computing Using Machine Learning," in IEEE Transactions on Cloud Computing, doi: 10.1109/TCC.2020.3015769.  
[11] Aral, Atakan&Ovatman, Tolga. (2018). A Decentralized Replica Placement Algorithm for Edge Computing. IEEE Transactions on Network and Service Management. 1-1. 10.1109/TNSM.2017.2788945.  
[12] Qazi, Faiza, Osman Khalid, Rao Naveed Bin Rais, and Imran Ali Khan. "Optimal content caching in content-centric networks." Wireless Communications and Mobile Computing 2019 (2019).  
[13] Khabbiza, El Hassane, Rachid El Alami, and Hassan Qjidaa. "Peer-Assisted Content Delivery to Reduce the Bandwidth of TSTV Service in IPTV System." International Journal of Digital Multimedia Broadcasting 2019 (2019).  
[14] Liu, Yujie, Dianjie Lu, Guijuan Zhang, Jie Tian, and Weizhi Xu. "Q-learning based content placement method for dynamic cloud content delivery networks." IEEE Access 7 (2019): 66384-66394.  
[15] Duan, Jie, Yuan Xing, Ruilin Tian, Guofeng Zhao, Shuai Zeng, Yuanni Liu, and Chuan Xu. "SCDN: A novel software-driven CDN for better content pricing and caching." IEEE Communications Letters 22, no. 4 (2018): 704-707.  
[16] Qu, Hua, Gongye Ren, Jihong Zhao, Zhenjie Tan, and Shuyuan Zhao. "Joint Optimization of Content Placement and User Association in Cache-Enabled Heterogeneous Cellular Networks Based on Flow-Level Models." Wireless Communications and Mobile Computing 2018 (2018).  
[17] Benkacem, Ilias, Tarik Taleb, Miloud Bagaa, and Hannu Flinck. "Optimal VNFs placement in CDN slicing over multi-cloud environment." IEEE Journal on Selected Areas in Communications 36, no. 3 (2018): 616-627.  
[18] Alghamdi, Fatimah, Saoucene Mahfoudh, and Ahmed Barnawi. "A novel fog computing based architecture to improve the performance in content delivery networks." Wireless Communications and Mobile Computing 2019 (2019).  
[19] Asheralieva, Alia, and Dusit Niyato. "Game theory and Lyapunov optimization for cloud-based content delivery networks with device-to-device and UAV-enabled caching." IEEE Transactions on Vehicular Technology 68, no. 10 (2019): 10094-10110.

- [20] Bosunia, Mahfuzur Rahman, and Seong-Ho Jeong. "Efficient Content Delivery for Mobile Communications in Converged Networks." *Wireless Communications and Mobile Computing* 2019 (2019).
- [21] Liu, Ling, Yiqing Zhou, Jinhong Yuan, Weihua Zhuang, and Ying Wang. "Economically optimal MS association for multimedia content delivery in cache-enabled heterogeneous cloud radio access networks." *IEEE Journal on Selected Areas in Communications* 37, no. 7 (2019): 1584-1593.
- [22] Wang, Ning, Gangxiang Shen, Sanjay Kumar Bose, and Weidong Shao. "Zone-based cooperative content caching and delivery for radio access network with mobile edge computing." *IEEE Access* 7 (2018): 4031-4044.
- [23] Lau, Chun Pong, Abdulrahman Alabbasi, and Basem Shihada. "An efficient content delivery system for 5G CRAN employing realistic human mobility." *IEEE Transactions on Mobile Computing* 18, no. 4 (2018): 742-756.
- [24] Haghghi, Ali A., Shahram Shah Heydari, and Shahram Shahbazpanahi. "Dynamic QoS-aware resource assignment in cloud-based content-delivery networks." *IEEE Access* 6 (2017): 2298-2309.
- [25] Haghghi, Ali A., Shahram Shahbazpanahi, and Shahram Shah Heydari. "Stochastic QoE-aware optimization in cloud-based content delivery networks." *IEEE Access* 6 (2018): 32662-32672.
- [26] Sinky, Hassan, Bassem Khalfi, Bechir Hamdaoui, and Ammar Rayes. "Responsive content-centric delivery in large urban communication networks: A LinkNYC use-case." *IEEE Transactions on Wireless Communications* 17, no. 3 (2017): 1688-1699.
- [27] Siracusano, Giuseppe, Roberto Bifulco, Martino Trevisan, Tobias Jacobs, Simon Kuenzer, Stefano Salsano, Nicola Blefari-Melazzi, and Felipe Huici. "Re-designing dynamic content delivery in the light of a virtualized infrastructure." *IEEE Journal on Selected Areas in Communications* 35, no. 11 (2017): 2574-2585.
- [28] Fan, Qilin, Hao Yin, Zexun Jiang, Haojun Huang, Yan Luo, and Xu Zhang. "Adaptive Content Management for UGC Video Delivery in Mobile Internet Era." *Mobile Information Systems* 2016 (2016).
- [29] Papagianni, Chrysa, Aris Leivadeas, and Symeon Papavassiliou. "A cloud-oriented content delivery network paradigm: Modeling and assessment." *IEEE Transactions on Dependable and Secure Computing* 10, no. 5 (2013): 287-300.
- [30] Salahuddin, Mohammad A., Amina Mseddi, Halima Elbiaze, and Roch H. Glitho. "Popularity and Correlation-aware Content Placement for Hierarchical Surrogates in Cloud-based CDNs." In *GLOBECOM 2017-2017 IEEE Global Communications Conference*, pp. 1-6. IEEE, 2017.
- [31] Ghalehtaki, Raziheh Abbasi, Somayeh Kianpisheh, and Roch Glitho. "A Bee Colony-based Algorithm for Micro-cache Placement Close to End Users in Fog-based Content Delivery Networks." In *2019 16th IEEE Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1-4. IEEE, 2019.
- [32] Ha, Minkeun, and Daeyoung Kim. "On-demand cache placement protocol for content delivery sensor networks." In *2017 international conference on computing, networking and communications (ICNC)*, pp. 207-216. IEEE, 2017.
- [33] Retal, Sara, Miloud Bagaa, Tarik Taleb, and Hannu Flinck. "Content delivery network slicing: QoE and cost awareness." In *2017 IEEE International Conference on Communications (ICC)*, pp. 1-6. IEEE, 2017.

# Intelligent Locking System using Deep Learning for Autonomous Vehicle in Internet of Things

S. Zaleha. H<sup>1</sup>, Nora Ithnin<sup>2</sup>, Nur Haliza Abdul Wahab<sup>3</sup>

School of Computing, Faculty of Engineering  
Universiti Teknologi Malaysia  
Johor, Malaysia

Noorhazirah Sunar<sup>4</sup>

School of Electrical, Faculty of Engineering  
Universiti Teknologi Malaysia  
Johor, Malaysia

**Abstract**—Now-a-days, we are using modern locking system application to lock and unlock our vehicle. The most common method is by using key to unlock our car from outside, pressing unlock button inside our car to unlock the door and many vehicles are using keyless entry remote control for unlocking their vehicle. However, all of this locking system is not user friendly in impaired situation for example when the user hand is full, lost the key, did not bring the key or even conveniently suited for special case like disable driver. Hence, we are proposing a new way to unlock the vehicle by using face recognition. Face recognition is the one of the key components for future intelligent vehicle application in the Autonomous Vehicle (AV) and is very crucial for next generation of AV to promote user convenience. This paper proposes a locking system for AV by using face deep learning approach that adapt face recognition technique. This paper aims to design and implement face recognition procedural steps using image dataset that consist of training, validation and test dataset folder. The methodology used in this paper is Convolution Neural Network (CNN) and we were program it by using Python and Google Colab. We create two different folders to test either the methodology capable to recognize difference faces. Finally, after dataset training a testing was conducted and the works shows that the data trained was successful implemented. The models predict an accurate output result and give significant performance. The data set consist of every face angle from the front, right (30-45 degrees) and left (30-45 degrees).

**Keywords**—Face recognition; deep learning; internet of things; convolution neural networks

## I. INTRODUCTION

The Internet of Things (IoT) was first invented in 1999 by Kevin Ashton. The introduction of the term is mainly to promote Radio-Frequency Identification (RFID) technology until later in 2011, the IoT term started to spread widely. This IoT is rapidly expanding with the aim of developing a global infrastructure by embedded sensors and actuators in physical objects that connect to the Internet [1, 2]. IoT devices were supplied with unique identifiers and known as Smart Devices. The Smart Device can be in a range from ordinary household objects to sophisticated industrial tools [1] to enable the communication with the IoT platform.

Sensors, gateways or connection, cloud, analytics, and user interface are the five (5) essential components of IoT systems. Sensors and devices are the rudimentary components of an IoT system. Every hardware device, including embedded cell phones, household appliances, hardware devices, and nearly

everything else encountered in daily life, contains sensors. Sensors or devices in an IoT system collect and send data [3] from the surrounding environment on the state of the device's operation. As a data transmission channel, a gateway or link is necessary. The gateway's job is to make communication and data sharing between devices easier.

As a connectivity of physical objects, IoT works as a bridge to all devices by transferring their data using a common language to connect with various sensors or devices. Basically, sensors acting as the data's supplier to the IoT platform and the data are gained from multiple sources. Moreover, the raw data needs to be analyzed [3] before useful information can be extracted. In the end, the data, automate processes and the efficiency can be enhanced and improved further by integrating it with other devices.

Furthermore, the IoT platform such as storage, actuation, sensing, enhanced services, and communication technologies are very important to gather and analyses data [4] from smart infrastructure. On the other hand, the IoT is changing our way of life and transforming how we interact with technology[4], and it is driving the world to become a better place.

Human lifestyle has been impacted in certain ways [4] by how people react to the way humans behave with all gadgets (things) in synchronize with the increasing IoT revolution. This revolution, as described in [5] provided and guaranteed the capacity to have seamless interaction when transmitting and sharing data across a network without needing any human-to-computer communication.

The cloud, which functioned as a platform for collecting, storing, managing, and analyzing real-time data, was a major component of IoT. Analytics will play a role in transforming analogue data from billions of devices into meaningful information that can subsequently be utilized for thorough analysis once the cloud handles the data. Data from devices and sensors is converted into a format that is simple to read and process.

Artificial intelligence (AI) is becoming more prevalent in IoT applications and deployments [6]. John McCarthy was the first to present AI in 1956, and he felt that AI included developing a machine that could really mimic human intellect [6, 7]. Simply put, AI was designed in a way that a machine can simply replicate it and do the tasks from easiest to the hardest.

The idea of AI is to replicate human cognitive processes. The developer and researcher's expectation towards AI is up until imitating humans in simulating processes including perception, reasoning and learning [6]. In a number of situations, AI systems outperform humans by a large margin [8]. It demonstrated that AI can defeat numerous computer games, including a world champion chess program and the top professional poker players in the world [9].

There are two types of AI which are weak and strong [10]. Every system that always does a single task is known as weak AI, while the strong AI always refers to a sophisticated and difficult system. The example for the weak AI is like video games and personal assistants and the famous personal assistants in this world is like Apple's Siri [11].

Other than that, computer games also are one of the examples of weak AI. On the other hand, there are many examples of strong AI nowadays such as operating rooms in hospitals and self-driving automobiles. These technologies are capable of solving problems without human intervention [12] because they have been trained before to deal with the circumstances.

Previous AI standards are becoming obsolete as technology develops [12, 13]. Nowadays, machines that calculate fundamental operation or read text by applying optical character recognition are formerly regarded to contain AI because these operations are now inspected standard computer functions. AI is continuously being enhanced [13] to benefit a wide range of businesses.

Mathematics, psychology, linguistics, and computer science are examples of multidisciplinary methods that are always used to wire machines [14]. We can even lock and unlock Autonomous Vehicles (AV) with our own face utilizing a deep learning approach using facial recognition, thanks to the advancement of AI models [15] that connect with IoT.

Furthermore, the AV idea is now at the forefront of the automotive industry's future security [16]. With the progress of technology, AV have the potential to reduce accidents, increase accessibility to transportation, especially for elderly persons, provide stress-free parking, and provide high-end security, among other benefits [16, 17]. However, technological advancements might sometimes have downsides for AV users. Sensors, for example, may malfunction, attracting a hacker to steal personal data from an AV user [17]. In Section 2, we'll go into AV in further detail.

Fig. 1 shows a process on how the data gathered from AV devices or sensors and then the data go through an analysis process before being transferred to the cloud. Basically, the data is gathered in edge computing after receiving from the AV. This data needs to be gone through pre-processing and decision-making in the edge node. Thenceforth, the data will be transferred to the cloud by the edge node after analyses locally by the IoT sensor[18]. The aim of this process is for less time-sensitive decision-making and for offline global processing.

Based on the diagram shown above, the road accident can be prevented by using obstacle recognition as shown in the diagram above. These time-sensitive choices are capable of

avoiding crashes in a shorter amount of time as illustrated in the edge node above [18]. To improve a driving experience, the cloud provides a platform for the data to analyses about the traffic, roads and also the driving habits.

The edge node as illustrated above shows that the AI models will be actively changed in terms of consumer needs, regulations, policies and appropriate laws. Moreover, in this node the amount of data sent by the IoT is bigger than the generated data in AVs because the data needs to be pre-processed, filtered and cleaned before proceeding to the cloud and by using this method the amount of cost and bandwidth can be reduced.

When it comes to the locking security in AV, normally the most common method is by using key to unlock our car from outside, pressing unlock button inside our car to unlock the door and many vehicles are using keyless entry remote control for unlocking their vehicle. However, all of this locking system is not user friendly in impaired situation for example when the user hand is full, lost the key, did not bring the key or even conveniently suited for special case like disable driver. Hence, we are proposing a new way to unlock the vehicle by using face recognition. Face recognition is the one of the key components for future intelligent vehicle application in the Autonomous Vehicle (AV) and is very crucial for next generation of AV to promote user convenience. This paper proposes a locking system for AV by using face deep learning approach that adapt face recognition technique.

In the remainder of this paper, Section II contains a brief history of AV including the superiority of AV, challenges of AV and the solution of the challenges; Section III discuss the component of machine learning and in that section, we have discussed of 10 sub-component of machine learning; Section IV discuss the methodology that have been used in this research paper including the way we collect the data to the way we implement the research; Section V conclude the result and discussion in this paper ; Section VI is our conclusion part for this research; Section VII discuss the future work for this research paper and lastly Section VIII dedicated the acknowledgement for this paper.

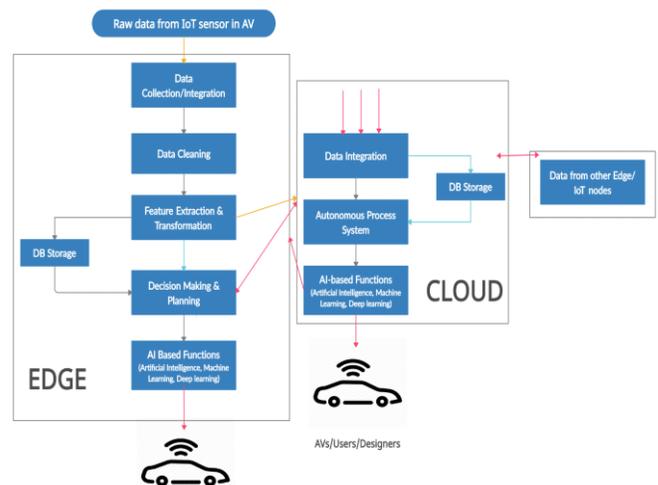


Fig. 1. The Basic Architecture for Artificial Intelligence and Internet of Things for Autonomous Vehicles.

## II. AUTONOMOUS VEHICLE

Autonomous Vehicle (AV) is one example of smart infrastructure [19]. A study from [16] had mentioned that AV was introduced in the 1980s and the research about AV was funded by Defense Advanced Research Projects Agency (DARPA) [16]. Thanks to AV because with the innovation of transport systems, combination of sensors and software to control, not only can reduce time, money and environmental impact yet can improve safety, increasing capacity, and minimizing traffic congestion [20].

Through the advancement of technologies in these modern days, the AV also known as driverless vehicles evolved by the ability to sense its surroundings, perform significance function, and operate by itself without interference by humans. An automation level generally divided into six levels which are from level 0 to level 5 and each level represents the operation control capabilities whichever the level 0 has the least automation control while the level 5 has the most control capabilities. The lowest level known as level 0 basically can't control all the operation and the whole process of driving needs to be done by humans [16]. On the other hand, the control process at the level 1 had been improved in terms of steering and braking control of the vehicle with the support of Advanced Driver Assistance System (ADAS).

As the level of automation increases, the vehicle becomes more advanced. As stated in [16], the level 2 automatics are capable of controlling the steering and braking by using the ADAS system. However, the drivers need to be focused and paying attention to the environment along the journey. At level 3 it becomes more advanced where the driver gives full control to the vehicle through Advanced Driving System (ADS). This system is capable of controlling all parts of the driving task with a few conditions. However, the human driver was allowed to control the vehicle when requested by ADS. In addition to that, the human driver executes the necessary tasks in the remaining conditions.

The ADS plays an important role in AV's system where at level 4 the system is capable to control and perform all tasks without any human intervention including supervision from the human. The last and the most advanced AV is at level 5, where in this level the AV is not only capable to perform all the driving tasks but also is capable to communicate with other devices [16] including traffic lights, signage and the environment of the roads and to perform this function this level requires 5G application.

Together with that, vehicle speed is also one of the important elements to the AV. To ensure the speed of AV kept at a safe distance, the Adaptive Cruise Control (ACC) is used. This system uses sensors to get the distance information and undertake the vehicle to perform tasks when the sensors send the signal to the vehicle such as perform brake when senses and predict any imminent and any vehicle ahead. These sensors give the information to the actuators in the vehicle and then proceed the control action activity in the vehicle such as braking, acceleration and steering [16]. Furthermore, the high level of AV is adept to control the automated speed in order to respond to the signals that come from the traffic lights and non-vehicular activities.

### A. Superiority of AV

Statistic states that usually vehicle crashes happen because of human error and it is proven when 90% of fatal vehicle accidents are due to human failure [21] hence, the AV's technologies got the potential to reduce the death statistics because of human error. Thus, driverless cars are a future technology that is needed by humans to scale down the deaths and injuries from car collisions. The reason for crashes comes from the driver's focus interruption [21]. On the other hand, there is a website called the house energy and commerce committee that claims that traffic deaths can be reduced up to 90% and can save up to 30,000 people yearly by using driverless vehicles or known as self-driving cars. Apart from that, there is a report from American Society of Civil Engineers (ASCE) that states that Americans can't avoid wasting their time in traffic every day [22] and surprisingly they used 6.9 billion hours for that purpose.

Furthermore, AV brings a lot of benefits to people, especially to senior citizens and for the disabilities drivers to handle vehicles safely. Other than reducing the numbers of accidents, the idea of AV is to help people in these groups to drive effortlessly. AV caters and provides more people to drive independently without worries about the safety issues [23]. Moreover, a study by [24] states that by accommodating AV technologies, will make life much easier and effortless to go to work, attend meetings with clients including going to the doctor especially for senior citizens and disability people.

Other than that, according to [23] Many benefits will be gained from the AV in terms of travel time, commuting and congestion time and also cut down the fuel consumption which is a good barrier to the citizen especially to the citizen who live in the city or town and crowded place and road. The country can save up to a trillion dollars when using AV and also can reduce manpower and law enforcers and save more money [25] to the country.

Safety and security issues are an important part of everyday life and are needed in many areas included in modern transportation. Moreover, these days AV concept is leading the future security of the vehicle industry [20]. AV has Light Detection and Ranging (LiDAR) sensor [16, 26, 27] It is capable of avoiding obstacles in an unknown environment and being able to classify dynamic objects in urban roads into cars, pedestrians, bicyclists and background [22]. LiDAR divides into two types which are non-scanning and also scanning LiDAR. In addition, scanning LiDAR comes with different features, other than single scanning, there is also one type called multi-line scanning LiDAR. In addition, LiDAR also has a non-scanning LiDAR type [23] that uses 3D-flash LiDAR.

The next feature in AV is Radio Detection and Ranging (Radar) [16, 26, 27]. Radars have proven effective for appearance on AV in the existence of fog and dust [25]. Besides that, radar is also designed to aid Off-road Light Autonomous Vehicle (OLAV) platforms in classification, map-reading, and detection [27]. Furthermore, Lidar and cameras are indeed very popular sensors, but radar gains much more advantage when compared to radar in terms of speed measurement capability and cost and target range [27]. AV also has an image sensor feature like rear-view cameras [27].

Rear-view cameras are used to detect obstacles behind the vehicle with aid of a fisheye lens [28]. The most important feature to AV is the locking system [29] when it comes to security factor.

Generally, a key of a vehicle is the most important thing to the vehicle to start the engine including to unlock the steering [26] such as by using pin tumblers lock, and then the lock changed to transponder key lock and after that an AV locking system became more advanced which can lock and unlock the vehicle by using Passive Keyless Entry and Start (PKES) system [29]. The PKES system is widely used in modern vehicles, the user can lock and unlock the vehicle whenever they are near to the vehicle without needing to take out the key from their pocket [29]. This system is very convenient to many users and makes life easier. Now, many manufacturers want to move to another level of vehicle locking security system by face recognition [30]. This paper invented the novel prototype of a safety system in AV, especially the locking system by using Keras, TensorFlow and Deep Learning (DL).

### B. Challenges of AV

The research done by [12] claims that though AV has been successfully programmed, an unpredicted flaw still may come after. On the other hand, the crazy advancement of technologies makes the older version equipment faced with the faulty code issues. With the many advanced technologies in the AV doesn't mean the vehicle can't be hacked by hackers. Hackers can hack AV systems easily because the system still has many vulnerabilities [16] as this is new to the world and the hackers definitely will steal the personal data through the AV.

The next drawback of AV is dysfunctional sensors [31]. Sensor failures often happened in AV [31], as an example the locking system. The locking system is a very crucial part in automated vehicles safety [32]. The AV user is very concerned about the locking system. AV provides the modern locking system to the user by maximizing the security and safety to the vehicle. Safety and vehicles cannot be apart. Safety is a very important element for the vehicle [16]. Basically, the common safety element in vehicles is like the lighting will turn on when the doors are unlocked, and the AV gives notification to the drivers by integrated control of the lighting.

However, AV locking systems also will have problems in the modern lifestyle, when the user's hand is full, lost the key, did not bring the key, the key can be duplicated by others or even conveniently suited for a special case like disable driver [33]. All of those factors demand a new locking system for AV users.

### C. Solution

As explained in the previous section, AI has been widely used in this world. Basically, AI is a technique that enables a machine to mimic human behavior. As example, an ability to sense, reason, engage and learn. AI operates autonomously and uses a variety of methods through data learning processes by machines [7]. By the recent advances in AI, many impacted areas have been affected by using AI techniques, as example voice recognition, Natural Language Processing (NLP),

computer vision algorithm, robotic and motion, planning and optimization, and knowledge capture [34, 35].

When we go deep in AI, we will find that AI is supported by an algorithm model known as Machine Learning (ML) and inside the ML there is another algorithm model called Deep Learning (DL) [36], [37]. Fig. 2 shows AI and the subfield.

ML is used to manage from the raw data, when ML gets the data, they need to be trained and this technique can be achieved by using specific algorithms. Basically, AI has a lot of methods that make machines operate autonomously through provided data [7], [37].

ML is created to be an independent computer program by learning itself from the data and ML algorithms is divided in a few categories [37], known as reinforcement, supervised, unsupervised and semi-supervised learning. This type of learning is illustrated in Fig. 3 below. Nowadays AI innovation is leads by ML techniques and nominal by Deep Neural Networks (DNN) [32, 33, 34, 37, 38] and this model widely used as black boxes.

Currently Deep Learning (DL) is a very popular algorithm and has been widely used by researchers and developers in various fields. The idea of DL is to imitate human brain function into machines. The most popular algorithms in DL are; a) Long Short-Term Memory Networks (LSTM), b) Convolutional Neural Network (CNN), c) Deep Belief Networks (DBN), d) Recurrent Neural Networks (RNN), e) Deep Boltzmann Machine (DBM) and f) Stacked Auto-Encoders. Moreover, the DL is focusing on the more complex and larger dataset [7, 11, 38] such as video, audio, text and image.

As mentioned above, the human brain acts as a major part for the evolution of DL. The design structure and frameworks of DL exactly look alike and function well as the human brain which is capable of differentiating patterns and can classify diverse types of data [38]. The evolution of DL makes the CNN become popular methods used in this field including Face Recognition (FR) technology based on CNN[39, 40]. FR is widely used nowadays in so many fields including to unlock mobile devices and the FR process includes the recognition task, feature extraction, alignment and detection [11]. On the other hand, the DL methods are able to support a huge dataset of faces and learn rich and compact representations of faces.

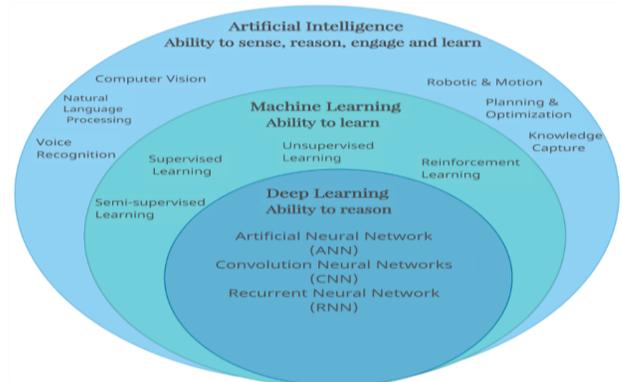


Fig. 2. Artificial Intelligent (AI) and the Subfield.

During 2012, a competition called ImageNet Large Scale Visual Recognition contesting became popular because of the CNN research that was initiated by Alex Krizhevsky [41]. After that competition the name of Alex became more popular. By using multiple processing layers and levels of features extraction, DL is capable of learning delegation of data [42]. On the other hand, fully connected layers, normalization layers, convolutional layers and pooling layers are a few examples of the layers that are hidden [38].in the CNN algorithm.

With DL, we can produce a new locking system for AV by using FR technique [43].The AI Researchers begin to use DL as a tool for training the face expression [44]. DL is knowingly an authoritative tool in the automation industry, and FR is part of the applications. FR is widely used in the military, finance industry, daily life and public security [45, 46], and FR is divided into two classes which are one to many augmentations and many to one normalization [46]. We will explain in detail about FR in Section 3 below. This method can solve the locking system problem. With the advancement of AI, the locking problem that was discussed in the previous section can be solved.

A survey done by [47] finds that FR technique will become a useful technique for AV users in terms of security, especially for locking systems. This technique requires a dataset to train before you can prove this technique meets the expected result. Moreover, with the help of IoT, the user will get notified [48] about the system failure.

In traditional methods, the system recognizes the human face by layers, which is one or two layers such as responses of filtering. With the emergence of DL, the landscape and framework of FR technique has been changed [49]and reshaped in all algorithm designs, evolution protocols, application scenarios including the dataset training.

FR needs three modules to run the system, the first one is a face detector. This module is needed to contain faces in images or videos. After that the next module is the face landmark detector and lastly is the FR module. This module is an anti-spoofing face [50]. There are two categories of FR [51], the first one is face verification and the other one is face identification.

In this study we are using ground truth research by using convolutional neural networks (CNN). This method is used for unlocking an AV by using our face. This model needs to be trained and validated in their own respective data. We will elaborate more in section 3 below about the methodology.

### III. MACHINE LEARNING

The advancement of ML was proven with minimal human interference and these methods are capable of analyzing the data before building an analytic model. Other than that, ML is intelligent in digesting information from raw data, analyzing the form of data and finding the decisions with least human supervision [52, 53]. Hence this new model of ML is definitely different from the traditional ML [54] which current ML was designed to learn from pattern recognition and can learn without being programmed to specific tasks but learn from data.

To be an independent model, ML’s interactive aspect is very crucial because ML works with the new data. The more ML learns about the data, the more ML will become smarter without any assistance from humans [55] and ML can produce reliable results and repeatable decisions.

Normally, to understand the data without human intervention, we need four kinds of algorithms that rely under ML, which are; a) semi-supervised learning, b) reinforcement, c) supervised, and d) unsupervised learning [36] Fig. 3 shows the ML types and the categories model in ML.

#### A. Supervised Learning

Supervised learning under the ML has been divided into two outcomes which are regression and classification. The regression outcome intention is to forecast based on the training sample set given, such as house pricing, weather forecast and market forecasting. Whereas the classification outcome’s goal is to identify pattern [36] such as identify fraud detection, image classification and diagnostics.

In supervised learning, there are three models [36], the first one is Classic Neural Networks or known as multilayer perceptron (MLP), the second one is Convolutional Neural Networks popular as CNN and the last model is Recurrent Neural Networks known as RNN.

Fig. 4 generally shows a normal workflow for classification in supervised learning algorithms. Above all, three steps are needed to classify data before generating the expectation output. The first step is to clean the raw data through the extraction process before gaining the quality or useful data. Secondly, the useful data including the labels are sent to the training stage by ML algorithm to analyze an excellent model.

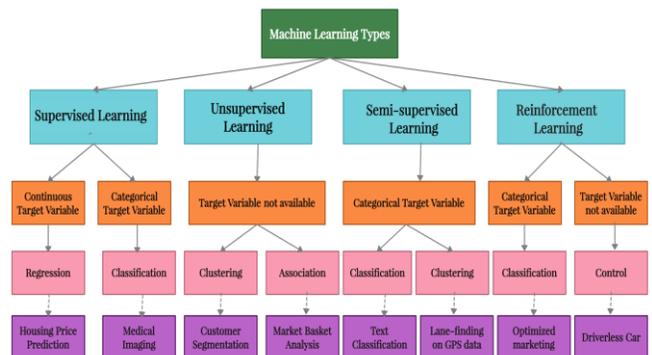


Fig. 3. Categories of Models in Machine Learning [49].

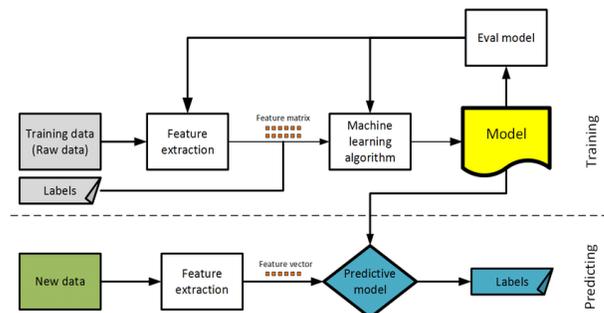


Fig. 4. A Flowchart of a Supervised Machine Learning Model [56].

To improve the accuracy of the model, the model needs adjustment from the evaluation step, because this step is capable of giving a point of view about the feature's extraction and learning stage. Before achieving the desired accuracy stage, the data needs to go through the training process [56] all over and over again. Once it done, the new data can be predicting easily.

### B. Multilayer Perceptron (MLP)

A simple algorithm that calculates the binary classification is called perceptron. Many real case's classified in this algorithm and this algorithm categorizes the input based on their own categories as an example cat or not cat and not fraud and fraud. While the MLP is composed of more than one perceptron [57].

A MLP involves a few layers and the layers have different types of uses. The common layers are known as output, hidden and input layers. Input layer task is to gain signal. Whereas core layer for MLP is the hidden layer, because this layer is the computational engine for MLP and lastly is the layer that functioning to predict the input and this layer known as output layer [58] Supervised learning technique is used in MLP for training purposes for every node and the technique called as back propagation and every node in this layer uses nonlinear activation function except the input node. The design of this layer is illustrated in Fig. 5.

To minimize the error the MLP's training does the altering parameters such as weights and biases. Then the MLP learns from the model's correlation between input and the output. Hence, not extraordinary when the MLP is capable of estimating the XOR operator and other nonlinear functions very well [58]. So, all of these are the advantages of MLP.

However, the parameters that are set by the MLP will become inefficient whenever the numbers of parameters become so high and it will cause redundancy in high dimensions. Moreover, it will disregard spatial information and make the flatter vectors as inputs [58].

### C. CNN

As discussed in the previous section, CNN play a paramount role in identifying and classifying images. Many researchers use CNN because of the magnificence of this algorithm in classifying images such as identifying objects, individuals, tumors, street signs, faces and many other data that are related to visuals. And these algorithms can perform the classification of images including photo search [34, 58].

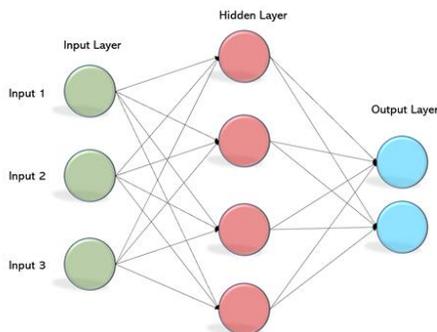


Fig. 5. Multilayer Perceptron Model[49].

CNN came within three layers. And all the layers are very famous among the researchers and developers known as convolutional, fully-connected and pooling layers. The function of the first layer, which is convolutional layers, is to obtain many attributes and diversity of features that are gained from the input images. These input images are then filtered to a specific size by the mathematical operation. This layer is then followed by the other layer [34, 58] known as the pooling layer. Decreasing connections between layers capable to reduce the computational cost by decrease the convolved feature's size.

In the end, the last layer is called a full connection layer. This layer is located before the output layer and makes another layer in CNN architecture. This layer comes along with weights and biases and the neuron elements. All of these elements are used to connect with different layers [34]. Fig. 6 shows CNN architecture where that architecture consists of an output layer, an input layer, a full connection layer, 2 max-pooling layers and 2 convolutional layers.

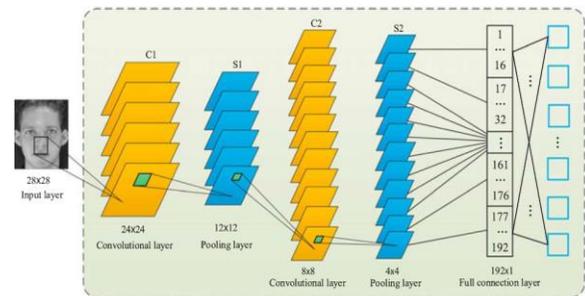


Fig. 6. An Example of a CNN Model for Face Recognition.

All algorithms in ML have their own advantages. For CNN, the advantages for this algorithm are advances in Computer Vision (CV). CV algorithm diversity used in technologies nowadays including treatments for the visually impaired, security, drones, medical diagnoses and driverless vehicle [59]. Other than that, CNN is widely used in business-oriented tasks[58] such as making natural-language processing available on analogy and manuscript documents, whereby the images are symbols to be transcribed and to digitize text known as Optical Character Recognition (OCR).

However, the CNN are naturally slower because of the operation, like maxpool and in addition the training process will become slower when the CNNs have several layers because the computer doesn't consist of a good GPU. Other than that, based on [59] the author stated that to process and train the neural network CNN require a large Dataset.

### D. Recurrent Neural Network (RNN)

Artificial Neural Network (ANN) alongside internal loops is called RNN [60] and this is a powerful technique. The interesting part about RNN is this technique is being used every day such as image recognition that capable to tell the picture's content, speech recognition, language translation, stock prediction and also driverless vehicle RNN indeed a powerful algorithm for prediction purposes because this algorithm can divide text and words into sequences, especially on sequence data modelling and the sequence data appear in

many patterns like text and audio. RNN predicts the data by having a concept of sequential memory. For example, as a human we can easily mention the alphabet in sequence because we already memorized it. However, when we want to mention the alphabet backwards it's pretty hard for us because we have not memorized it. A human brain capable to recognize sequence of patterns [60] by using sequential memory mechanism.

RNN replicates the concept of sequential memory of the human brain by using 3 layers called as an output, hidden and an input layer. In RNN exists a looping mechanism that can pass the previous information forward. This looping performs as an expressway to flow information from one step to another [60]. The previous input information is kept in the hidden state. As an example, by using RNN we can build a chat box and the chat box capable to classify intentions from the user inputted text [60].

As mentioned in the previous sentence, the hidden layer representation of previous input and it will be modified. This modified hidden state contain data from all the earlier steps and continue to loop until no more words and then gives to the output to feed the board layer and it gives the forecast. Forward pass control flow of a RNN can be done by for loop [61].

The RNN architecture workflow quite simple to understand by many. Example of RNN such as previous information is taken by present cell before come out the output. Meanwhile, by referring the Fig. 7, it represents the processed word,  $t$  also will be the input after the word was processed. All the text available to process when the sequence dimensions are reduced to a certain value. The sequence needs to meet the size requirement, otherwise the sequences will be filled until the specified value. However, the excess will be barred if the sequence size is more than the specified value [62].

Training in neural network consists of three crucial steps. The first step is to make a prediction by forward pass, then by using loss function the networks can differentiate the output prediction to the ground truth. On the other hand, when the loss function gives an error value as their outputs, it means the network is performing badly. Finally, this network calculates the gradients for every node to do back propagation by using the error value [61]. In this case, gradients referred to a value that mainly used for allowing the network to learn by adjusting the network's internal weight and if more the gradient, hence the more the adjustment.

However, a short-term memory is inside the hidden state. This is common memory to other neural network architectures and exist because of the infamous problem which known as vanishing gradient. This problem appears on a one reason, which is the information that have been kept in the previous step have error[61], and basically during training and optimize neural network processes, this problem is normal nature to back propagation algorithms.

The computation of RNN model is slow, this drawback led to difficulty to train the data when the researchers using the activation functions because it will make a very exhausting process which makes the long sequences process [63]. Hence, the exploding or gradient vanishing will happen.

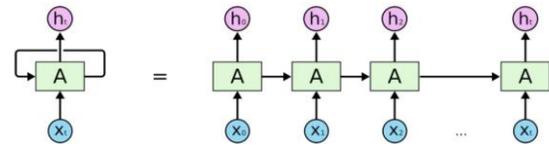


Fig. 7. An Example of RNNs Model.

### E. Unsupervised Learning

Supervised Learning is different from unsupervised learning in so many ways. This algorithm trains the samples without training the labels. The unsupervised learning is divided into two outcomes which are clustering and dimensionality reduction. Clustering outcome formulated using the algorithm to find consistent patterns become apparent, the similar data points can be clustered together, and different data points will be in different clusters in the data such as recommender system, targeting marketing and customer segmentation. While dimensional reduction outcomes are like finding suitable structure and pattern in the data [58, 61] such as big data visualization, structure discovery and feature elicitation.

The unsupervised Models also consist of three different models [58]. The first one is a self-organizing map or known as Self-Organizing Map (SOM), secondly is the Boltzmann Machines model and lastly is AutoEncoders model.

### F. SOM

A neural network based on dimensionality reduction algorithm is called as SOM commonly utilize two-dimensional discretized pattern to perform a high-dimensional dataset [58]. Dimensionality decreases will occur whenever to retaining the data's topology in the primary feature space.

The input space of the training samples will produce a low dimensional discrete on this type of neural network, called as map [34]. In addition, this technique capable to do reduction of the dimensionality.

The similarities in the data could be observed easily by using the dimensionality reduction and grid clustering, that makes this type of neural network is easily to understood and clearly explained [64]. However, cluster inputs need sufficient neuron weights. If the weights not sufficient the map will produce inaccurate results. The SOM model is illustrated in the Fig. 8.

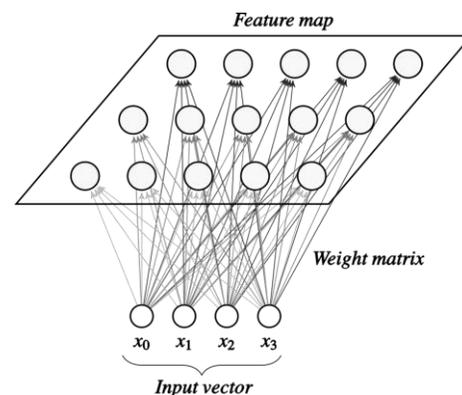
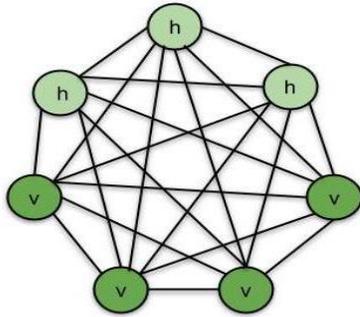


Fig. 8. SOM Model [53].

### G. Boltzmann Machines Model

Unlike others neural network, Boltzmann model only have two kind of nodes called as visible and hidden nodes without an output node [63]. This situation makes this model known as non-deterministic features.

Two computational error can be fix by using this model. As example, optimization problem and search problem may happen and by fixing the weights on the connections the problem will solves and this method also is a cost function [63]. That is illustrated in the Fig. 9.



v - visible nodes, h - hidden nodes

Fig. 9. Boltzmann Machines Model [51].

The main disadvantage is that Boltzmann learning is significantly slower than backpropagation [63]. However, this model also has numerous problems in the use of algorithms. The example of the problems encountered are such as weight adjustment, the time needed to collect statistics in order to calculate probabilities, the times weights change at a time, the difficulties of adjust the temperature during simulated annealing and the difficulties to decide when the network has reached the equilibrium temperature [63].

### H. AutoEncoders Model

To learn an encoding data set, autoencoder model need to use training technique in unsupervised way. In order to learn an encoding data set focusing on dimensionality reduction, autoencoder need to training the network to overpass the signal noise [65].

Learning to encode a data set is the main focus for an autoencoder. Generally, autoencoder will reduce the dimensionality to neglect the noise's signal by network's training. In addition, autoencoders will provide a model to user by referring the data rather than predefined filters [65].

In general, the autoencoders provide the users a filter that may fit the user's data better [65]. However, Generative Adversarial Networks is much more efficient than autoencoders in term of recreate an image. In addition, images will start blurry whenever the complexity of the images increase [65]. That is illustrated in the Fig. 10.

### I. Semi-Supervised Learning

Semi-supervised learning falls in the middle of unsupervised and supervised learning. In reality, hiring an expertise worker needs a lot of money because we need to pay their skilled, because of that the cost of label is high [66].

Hence, semi-supervised algorithm became the best methods for the building the model especially for the less labels data. To put it clear, this data brings crucial information about the group parameters even from the unknown group of unlabeled data.

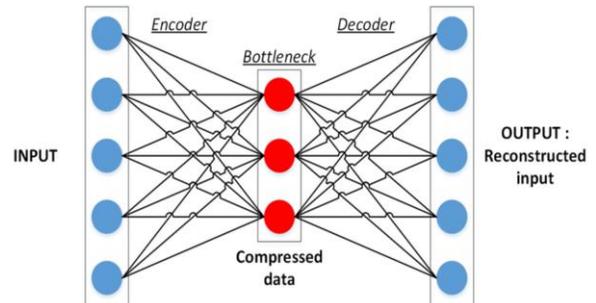


Fig. 10. Autoencoder's Model.

### J. Reinforcement Learning

Machine Learning that has a representative like robots that know how to behave in an environment by evaluate the results is called as Reinforcement Learning. In addition, the robot will get a reward through the points given to them based on their performance on gives correct response in every situation. This point will boost up the robot's confident to take more actions. This process is like Markov Decision Process also known as (MDP). On the other hand, data classification in reinforcement learning is useless [67] because the robot learns from trial and error and support by the concept reward and punishment by MDP.

## IV. METHODOLOGY

Based on those algorithms mentioned in the above sections, we chose the CNN algorithm. A study by found that the trendiest technique of neural network for working with image data is CNN. Other than that, CNN are very good in extract image features that makes this neural network became famous and our research paper is based on image data, so CNN is the best algorithm to build our model. On top of that as our research paper used image and pattern recognition, hence CNN is the best choice for our research as this network can solve our problems with using their technique whereas other neural network doesn't have this technique.

The interesting part in this paper is about our methodology stages. Firstly, pre-processing step is being used to haul the images of test data before predicting the classes for these images utilize the trained model. There are seven sequences to construct this model. Firstly, we need to set up Google colab, secondly, we need to import libraries, thirdly we need to load and pre-process data. This step took around three minutes, and then we needed to create a validation set. The next step is defining the model structure, this step took around one minute. Then we need to train the model. This step took around five minutes and the last step was to make a prediction and this step took around one minute. After that we may predict the pattern of the model and analyze its performance using `model.predict()`.

In this study, we are using our own dataset to present the training set. To set up the structure of our image data, we prepared two folders for our data set, the first one is set A

which is named as known folder and the other one is set B which is named as unknown folder. Firstly, we create three folders in each set, the first folder is the train folder, the second folder is the test folder, and the last folder is the validation folder. These sets contain the images of all the test images but no labels. The reason is because the images set will be trained on our model and the testing set images will predict the data by label it.

After that we split the model building's process into four stages. The first one is loading and pre-processing data which takes 30% of all time, the second one is defining model architecture which takes 10% of all time. The third stage is training the model. This model took half of all time for this process. The last stage is estimation of performance. This stage took 10% of the time.

Validation set should be constructed before disclosing to the test set, these methods used to perform the unseen data. Train and validate the data should be done on their own data respectively by subdivide those data set. All the parameters applied in Table I. The model trained a few times using the list of parameters in the table and the results are shared in the next section of this paper.

#### A. Stage 1: Loading and Pre-processing Data

To begin with, we need a dataset to train on. Data is a new gold. ML and DL are not magic, they need data to train. As mentioned above, the first section is loading and pre-processing data. This is a very important step in any research. With having a good number in training set means it determine the better performance of the model and the architecture of the model determine the pattern of data in order to create the validation set.

In this study we are using our own dataset. As shown in Table II, our data consists of 255 images and the images represent two different datasets which are known face and unknown face folder. This process just needs a very little Pre-processing process because by considering the small size of the images, hence the dataset is very easy to upload. Firstly, we need to import the necessary libraries. We are using a matplotlib array and diverse modules correlate with TensorFlow and Keras.

TABLE I. THE PARAMETER USED DURING MODEL TRAINING

PARAMETERS	VALUES
Optimiser	Adaptive Moment Estimation (adam)
Learning Rate	0.0005
Batch Size	1, 20
Epochs	10, 20, 30, 40, 50, 60, 70, 80

TABLE II. THE SUMMARY OF THE IMAGES USED TO FEED THE MODEL

Input Image Size	378 x 378 pixels
Original Image Quantity	255 pieces belong to 2 classes
Training Images Quantity	72.5% of 255 images belong to 2 classes
Validation Images Quantity	69% of 255 images belong to 2 classes

In this research paper, the data images are shrunk to one similar size of training data images: 150 x 150 pixels during training.

Then we need to prepare the data. In this section we need to load and import our data In this section we can determine the data that we want to load by using load\_img() function. However, negative  $\text{impact}$  will happen if the amount is huge. On top of that, we set our data image to 150 wide and 150 heights. In this stage we need to normalize our input data.

Our research uses image as our input value. Its value is between 0 and 255. On the other hand, we need to normalize the data by divide the image value with 255. To predict the number of neurons that we need to compress in the last layer, firstly we need to declare the data type as an integer in the dataset and fix the number of classes. In our case, we utilize ImageDataGenerator (rescale = 1. /255) command because its currently an integers value.

#### B. Stage 2: Defining the Model's Architecture

Model architecture is very crucial step to define. CNN model was designed in this stage and estimate the number of convolutional layers and hidden layers that we need. After that we need to define the format that we will use for the model. We are choosing Keras because Keras has few different formats to create the models. In Keras sequential format is very popular because of those factors we import it from Keras.

A convolutional layer was used in our first model and this layer also will run in input nodes specifying the number of filters is very important to implement in Keras, the size of filters that we want, In our case we are using 64 filters of dimension 3 x 3, the input shape and the activation and padding that we need. So, the activation that we use is ReLU since it is the common activation in DL; however we can string the activation and pooling together.

Dropout layer were created to prevent overfitting. To do this, we need to eliminate some of the connections between the layers. We are using string dropout (0.5), so we can drop 50% of the existing connection. After that we are doing batch normalization where the input heads to the layer after and make sure that the network continuously provides activations with the similar circulation needed.

Then, to learn more complex presentation of network we need to increase the filter's size, hence another convolution layer will appear. Adding a convolution layer means the filter's numbers is increased too, hence, more complex images will be learnt. We also used a pooling layer. In the pooling layer, as discussed in the previous section this layer makes the image classifier more robust so it can learn relevant patterns. However, pooling layers discards some data, so we don't use many of those layers. Because of our data already in small size, we just twice the pool. After that we did over these layers to give our network look more representation. Then we used fully connected layers and sigmoid activation algorithms.

#### C. Stage 3: Training of the Model

After defining this architecture's model, then we do the training of the model stage. In this stage we need to compile it and need to detail up the epoch's number that we prefer to train

and the optimizer that we need to use. In order to reach the fewest point of loss, we need to use the right optimizer to tune the weights for the network and that why we choose Adam optimizer algorithm as it provides good output on most problem situations. In this stage we need to combine with our chosen model's parameter and also determine the metric to be implemented. We are using Adam optimizer as the optimizing function and binary\_crossentropy as the loss function while training the data.

Then, the model's summary can be print out to analyses the pattern. There is a lot of info inside the summary such as type of layer, the output shape and the parameter. To train the model we need to use the fit() functions on the model and pass in the chosen parameters. We will have the validation set which is different from the testing set. In this stage, we just want to make sure the test data is set aside but not to be trained.

For training models, we require two important data sets. The first one is the true labels and training images, and the other one is the validation images and true labels. The true labels in validation images are needed not for the training phase, but to validate the model.

D. Stage 4: Estimating the Model's Performance

Lastly is the estimating the model's performance stage. In this stage we can see the accuracy result, loss result, plot loss and plot accuracy for each validation and training epoch. Finally, we can test the model on the random train image for both sets; the flow of train image in our work is shown in the Fig. 11.

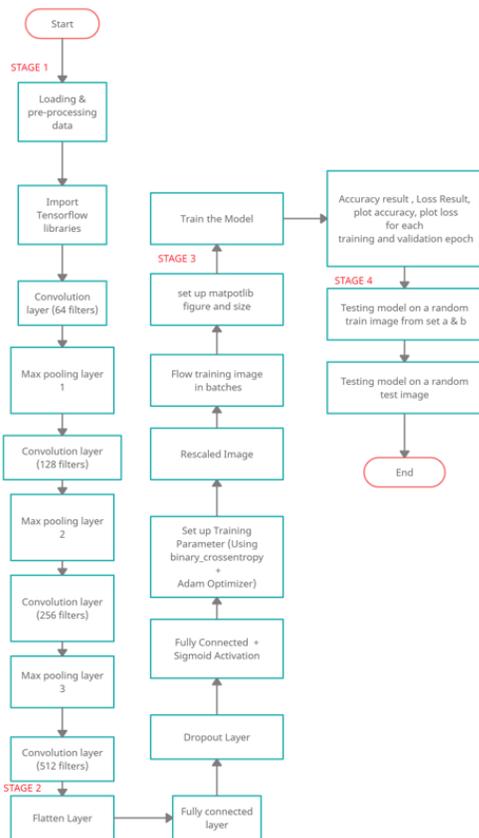


Fig. 11. The Flow of the Proposed Work.

To excellency support of the proposed approach, we compared the results of our approach with some other methods of face recognition in the literature based on existing methods including ANN, support vector machine (SVM) and Principal component analysis (PCA).

V. RESULT AND DISCUSSION

Few parameters are being adjusted on the validation and training process. The training was done repeatedly in eighty sets, and the Table III shown the experiment output. We also show our training and validation result in graph foam. The graph shows in Fig. 12 and 13.

TABLE III. THE PARAMETERS USED DURING MODEL TRAINING AND RESULTS, RESPECTIVELY

Step	Loss	Epoch	Learning Rate	Test Accuracy
355ms/step	0.5043	1	0.001	0.8889
350ms/step	0.0820	2	0.001	1.0000
340ms/step	0.0092	3	0.001	1.0000
346ms/step	0.5049	4	0.001	0.8750
349ms/step	0.0360	5	0.001	1.0000
362ms/step	0.5936	6	0.001	0.8889
363ms/step	0.0458	7	0.001	1.0000
347ms/step	0.2920	8	0.001	0.8889
361ms/step	0.1855	9	0.001	0.8889
350ms/step	0.0236	10	0.001	1.0000

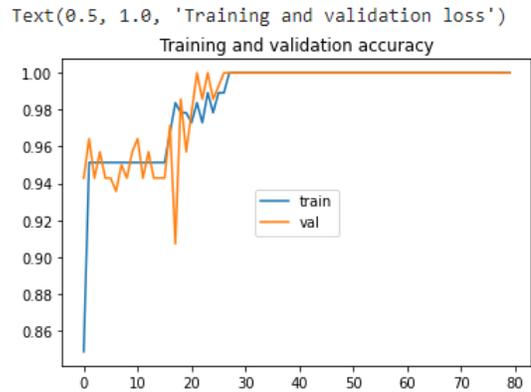


Fig. 12. Training and Validation Accuracy Graph.



Fig. 13. Training and Validation Loss Graph.

Fig. 12 shows the training and validation accuracy graph for our research. The meaning of accuracy here is the number of correct predictions. The training accuracy is actually the accuracy that we get when we use the model on the training data; on the other hand, the validation accuracy is the accuracy on the validation data. As we can see in our graph below the training accuracy in our research achieves the 100-percentage accuracy before the 30 epochs.

Fig. 13 shows a training and validation loss graph for our research. As we can see the graph shows training which is the blue line against validation loss which is the orange line. Training loss means that is the error on the training set of data, while validation loss means that the trained data got error after running the validation, so when the epochs increase the both training and validation error drop. Our graph shows that the training error continues to drop, it also shows that the training error totally drops before the 30 epochs that means the network learns the data better and better.

Fig. 14 shows the testing model on a random train image from set A in our research. The figure shows the target size of the random image as shown in the figure.

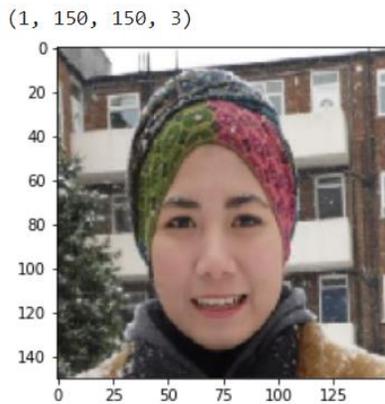


Fig. 14. Testing Model on a Random Train Image from Set A.

Fig. 15 shows the testing model on a random train image from set B in our research. The figure shows the target size of the random image as shown in the figure.

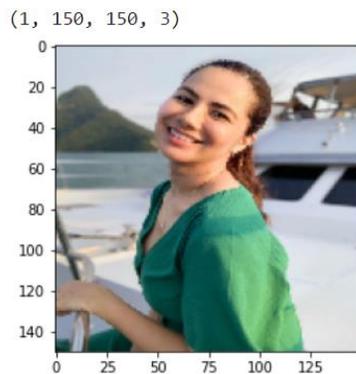


Fig. 15. Testing Model on a Random Train Image from Set B.

Table III shows the parameters used during model training. In our research, we are using six parameters which are epoch, step per epoch which is calculated in second, loss, accuracy,

validation loss and validation accuracy. Epoch means the integer of the total number of repetitions on the data. In this research, we are using 80 epochs. While the step per epoch means the total number of steps that get from the generator before declaring one epoch finished and starting the next epoch. In our research the first step took around 53 seconds to finish before starting to the second epoch. For the epoch number 2 until 80 the range step per epoch took about 35 and 36 seconds for each step. The next parameter is loss that represents how much worst the model's prediction on one example.

Normally, the loss value will be reduced after each model training repetition. The model prediction is considered perfect if the loss is zero and vice versa. As we can see in the table IV below our loss value keeps reducing for every epoch, it means that our model prediction is perfect. The next parameter is accuracy; the accuracy of a model is defined as a percentage of correct predictions for the test data. In our research, the accuracy of the model increases in every epoch and achieves 100 percent accuracy before the epoch of 30. Next is the validation loss parameter, the validation loss means that the trained network has error after the data set have been run through the validation set, as we can see in table IV the validation loss of our research reduces in every epoch. That means the error is reduced in every epoch. The last parameter is validation accuracy parameter; validation accuracy is the accuracy on the validation data. As we can see in our table below the validation accuracy in our research achieves the 100-percentage accuracy before the 30 epochs.

TABLE IV. THE PARAMETERS USED DURING MODEL TRAINING AND RESULTS, RESPECTIVELY

Epoch	Step per epoch (second)	loss	accuracy	Validation Loss	Validation Accuracy
1	53s	0.4079	0.8486	0.2428	0.9429
5	36s	0.2305	0.9514	0.2325	0.9429
10	35s	0.2043	0.9514	0.1705	0.9571
15	36s	0.1192	0.9514	0.2591	0.9429
20	36s	0.0925	0.9784	0.0644	0.9571
25	36s	0.0757	0.9784	0.0236	0.9857
30	35s	9.3065e-04	1.0000	4.6639e-05	1.0000
35	35s	8.4819e-07	1.0000	2.2389e-06	1.0000
40	35s	2.2942e-06	1.0000	1.2312e-06	1.0000
45	35s	4.2259e-07	1.0000	5.8786e-07	1.0000
50	35s	7.4016e-07	1.0000	3.3890e-07	1.0000
55	36s	2.3546e-06	1.0000	9.1678e-08	1.0000
60	36s	4.8171e-07	1.0000	1.7699e-07	1.0000
65	36s	7.5054e-07	1.0000	3.6083e-08	1.0000
70	36s	1.0656e-07	1.0000	1.0284e-07	1.00001
75	35s	1.4218e-07	1.0000	4.9360e-08	1.0000
80	36s	2.7106e-07	1.0000	3.7226e-08	1.0000

When the research is completed, we will feed the tested images to the model that we have trained using known and unknown face's label. The predicted image in Fig. 16 and 17 is well identified by the model as we trained the model data, which is the Fig. 16 predicted to known faces and Fig. 17 is predicted unknown faces. The prediction images are shown in Fig. 16 and Fig. 17.

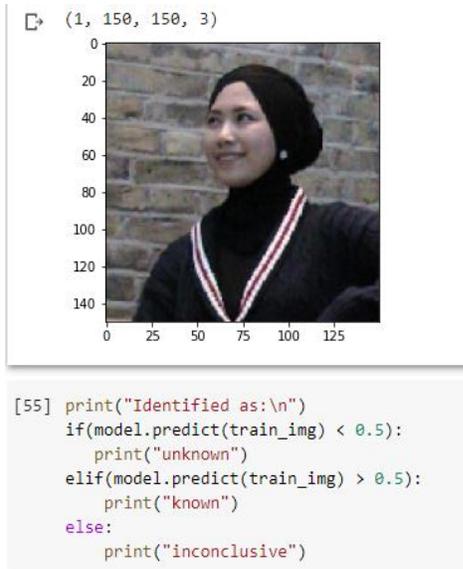


Fig. 16. The Prediction Image Result from Set A.

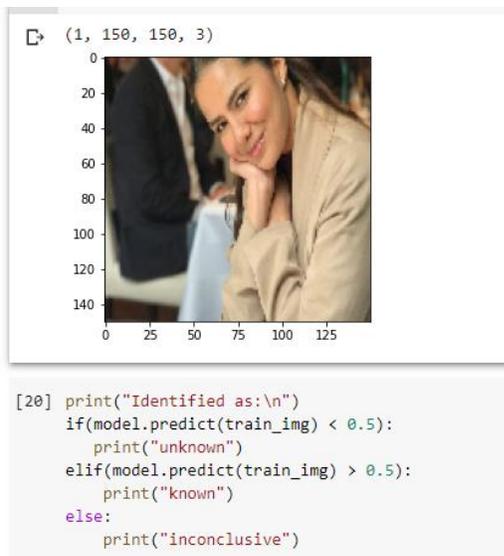


Fig. 17. The Prediction Image Results from Set B.

Based on the comparison of face recognition approach in the Table V, it is clear that the all mentions methods capable to recognize face recognition but the accuracy is differed. Author from [68] mention that the highest percentage by using ANN

approach is 80%. Meanwhile a study did by [69] had mentions that the experiment by using Multi-class SVM achieve until 96%. Other than that, a study did by [70], had mention their approach got the 77% similarities by using PCA integrated with Eigenface approach. From those comparisons, our proposed approach shows that the CNN can achieve a higher face recognition accuracy than others. As such, it can be concluded that the CNN can promote the performance of face recognition due to the availability of the many features.

TABLE V. COMPARISON OF FACE RECOGNITION ACCURACY

Method	Accuracy (%)
CNN	98.5
ANN	80%
Multi-class SVM	96%
PCA + Eigenface	77%

## VI. CONCLUSIONS

Convolution neural networks have become the main technique in the field of face recognition. In this research paper, implements a CNN, which automatically trained the given dataset to predict the classification of images. These models predict an accurate output result by using every face angle from the front, right (30-45 degrees) and left (30-45 degrees). and give significant performance. On the other hand, it will lead to further development for face recognition using deep learning. From the model training experiment point of view, we can conclude that our data set can produce good results and through the data set the model can differentiate between two different data in high accuracy prediction. Hence CNN is a good technique for face recognition technology.

However, we can have a better result if we divide our data set into 70: 20: 10 ratios. 70 % is for training folder data set, 20% is for validation folder data set and 10% for the test folder data set. We are using 255 images for this experiment. We can have a better prediction if we use the bigger data set.

## VII. FUTURE WORK

The research should be further developed in a large dataset to make sure this research can be implemented in real vehicles for safety purposes. Moreover, this paper aims to use face recognition technology in scientific and daily life applications for locking and unlocking autonomous vehicles. In the near future, face recognition technology will become a common approach in many applications. With the Covid-19 pandemic that happens in this world right now where all people are wearing mask wherever they go outside to public area, its hard to identify a person with a mask covering half of their face. The researcher should consider the user in pandemic situation. Furthermore, additional algorithms need to be used and conducted to improve user experience especially for disabled users.

## ACKNOWLEDGMENT

This research was supported by Ministry of Education (MOE) through Fundamental Research Grant Scheme (FRGS/1/2021/ICT10/UTM/02/3). We also want to thank to

the Government of Malaysia which provide MyBrain15 program for sponsoring this work under the self-fund research grant and L00022 from Ministry of Science, Technology and Innovation (MOSTI).

This research also was supported by UTM Encouragement Research Grant Q.J130000.3851.19J08.

#### REFERENCES

- [1] Kramp, T., R. van Kranenburg, and S. Lange, Introduction to the Internet of Things, in *Enabling Things to Talk: Designing IoT solutions with the IoT Architectural Reference Model*, A. Bassi, et al., Editors. 2013, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 1-10.
- [2] Mehta, R., J. Sahni, and K. Khanna, Internet of Things: Vision, Applications and Challenges. *Procedia Computer Science*, 2018. 132: p. 1263-1269.
- [3] Sadique, K.M., R. Rahmani, and P. Johannesson, Towards Security on Internet of Things: Applications and Challenges in Technology. *Procedia Computer Science*, 2018. 141: p. 199-206.
- [4] Ray, P.P., A survey on Internet of Things architectures. *Journal of King Saud University - Computer and Information Sciences*, 2018. 30(3): p. 291-319.
- [5] Bassi, A., Bauer, M., Fiedler, M., Kramp, T., van Kranenburg, R., Lange, S., Meissner, S. (Eds.), *Enabling Things to Talk*. 2013.
- [6] Morgenstern, L. and S.A. McIlraith, John McCarthy's legacy. *Artificial Intelligence*, 2011. 175(1): p. 1-24.
- [7] Nguyen, G., et al., Machine Learning and Deep Learning frameworks and libraries for large-scale data mining: a survey. *Artificial Intelligence Review*, 2019. 52(1): p. 77-124.
- [8] Barenkamp, M., J. Rebstadt, and O. Thomas, Applications of AI in classical software engineering. *AI Perspectives*, 2020. 2(1): p. 1.
- [9] Westera, W., et al., Artificial intelligence moving serious gaming: Presenting reusable game AI components. *Education and Information Technologies*, 2020. 25(1): p. 351-380.
- [10] Hrastinski, S., et al., Critical Imaginaries and Reflections on Artificial Intelligence and Robots in Postdigital K-12 Education. *Postdigital Science and Education*, 2019. 1(2): p. 427-445.
- [11] Mellakh, M., D. Petrovska-Delacrétaz, and B. Dorizzi, Using Signal/Residual Information of Eigenfaces for PCA Face Space Dimensionality Characteristics. Vol. 4. 2006. 574-577.
- [12] Keding, C., Understanding the interplay of artificial intelligence and strategic management: four decades of research in review. *Management Review Quarterly*, 2021. 71(1): p. 91-134.
- [13] Smids, J., S. Nyholm, and H. Berkers, Robots in the Workplace: a Threat to—or Opportunity for—Meaningful Work? *Philosophy & Technology*, 2020. 33(3): p. 503-522.
- [14] Roberts, F.S., The Challenges of Multidisciplinary Education in Computer Science. *Journal of Computer Science and Technology*, 2011. 26(4): p. 636-642.
- [15] Zaleha, S., et al., Microsleep Accident Prevention for SMART Vehicle via Image Processing Integrated with Artificial Intelligent. 2021.
- [16] Bagloee, S.A., et al., Autonomous vehicles: challenges, opportunities, and future implications for transportation policies. *Journal of Modern Transportation*, 2016. 24(4): p. 284-303.
- [17] Thomopoulos, N. and M. Givoni, The autonomous car—a blessing or a curse for the future of low carbon mobility? An exploration of likely vs. desirable outcomes. *European Journal of Futures Research*, 2015. 3(1): p. 14.
- [18] Khayyam, H., et al., Artificial Intelligence and Internet of Things for Autonomous Vehicles, in *Nonlinear Approaches in Engineering Applications: Automotive Applications of Engineering Problems*, R.N. Jazar and L. Dai, Editors. 2020, Springer International Publishing: Cham. p. 39-68.
- [19] Seuwow, P., E. Banissi, and G. Ubakanma, The Future of Mobility with Connected and Autonomous Vehicles in Smart Cities. 2020. p. 37-52.
- [20] Felemban, E. and A.A. Sheikh, A Review on Mobile and Sensor Networks Innovations in Intelligent Transportation Systems. *Journal of Transportation Technologies*, 2014. Vol.04No.03: p. 9.
- [21] Braun, R. and R. Randell, Futuramas of the present: the “driver problem” in the autonomous vehicle sociotechnical imaginary. *Humanities and Social Sciences Communications*, 2020. 7(1): p. 163.
- [22] Norma Jean Mattei, 2017 Infrastructure Report Card. 2017.
- [23] Othman, K., Public acceptance and perception of autonomous vehicles: a comprehensive review. *AI and Ethics*, 2021.
- [24] Hancock, P.A., I. Nourbakhsh, and J. Stewart, On the future of transportation in an era of automated and autonomous vehicles. *Proceedings of the National Academy of Sciences of the United States of America*, 2019. 116(16): p. 7684-7691.
- [25] Gruel, W. and J.M. Stanford, Assessing the Long-term Effects of Autonomous Vehicles: A Speculative Approach. *Transportation Research Procedia*, 2016. 13: p. 18-29.
- [26] Yoneda, K., et al., Automated driving recognition technologies for adverse weather conditions. *IATSS Research*, 2019. 43(4): p. 253-262.
- [27] Gusland, D., et al. Imaging radar for navigation and surveillance on an autonomous unmanned ground vehicle capable of detecting obstacles obscured by vegetation. in *2019 IEEE Radar Conference (RadarConf)*. 2019.
- [28] (Ed.), A.E., *handbook of intelligence vehicles*. 2012. 2.
- [29] Ren, K., et al., The Security of Autonomous Driving: Threats, Defenses, and Future Directions. *Proceedings of the IEEE*, 2020. 108(2): p. 357-372.
- [30] Nagendran, N. and A. Kolhe. Security and Safety With Facial Recognition Feature for Next Generation Automobiles. 2019.
- [31] Realpe, M., B. Vintimilla, and L. Vlacic, Sensor Fault Detection and Diagnosis for autonomous vehicles. *MATEC Web of Conferences*, 2015. 30: p. 04003.
- [32] Venkatesh. Safety Locking System of Car Door Using Sensors. 2016.
- [33] Vinil Kumar.V, D.N., Mr. K.S.Vairavel, Smart Door Lock Opening In Cars Using Face Recognition. 2017.
- [34] Sarker, I.H., Machine Learning: Algorithms, Real-World Applications and Research Directions. *SN Computer Science*, 2021. 2(3): p. 160.
- [35] Bohr, A. and K. Memarzadeh, The rise of artificial intelligence in healthcare applications. *Artificial Intelligence in Healthcare*, 2020: p. 25-60.
- [36] Sharma, N., R. Sharma, and N. Jindal, Machine Learning and Deep Learning Applications-A Vision. *Global Transitions Proceedings*, 2021.
- [37] Di Franco, G. and M. Santurro, Machine learning, artificial neural networks and social research. *Quality & Quantity*, 2021. 55(3): p. 1007-1025.
- [38] Zhai, J., et al., A Review of the Evolution of Deep Learning Architectures and Comparison of their Performances for Histopathologic Cancer Detection. *Procedia Manufacturing*, 2020. 46: p. 683-689.
- [39] Said, Y., M. Barr, and H.E. Ahmed, Design of a Face Recognition System based on Convolutional Neural Network (CNN). *Engineering, Technology & Applied Science Research*, 2020. 10(3): p. 5608-5612.
- [40] Yong Li , Z.W., Yang Li , Xu Zhao , Hanwen Huang, Design of face recognition system based on CNN. *Journal of Physics: Conference Series* 2020.
- [41] Krizhevsky, A., I. Sutskever, and G.E. Hinton, ImageNet classification with deep convolutional neural networks. *Communications of the ACM*, 2012. 60: p. 84 - 90.
- [42] Najafabadi, M.M., et al., Deep learning applications and challenges in big data analytics. *Journal of Big Data*, 2015. 2(1): p. 1.
- [43] Dibaei, M., et al., Attacks and defences on intelligent connected vehicles: a survey. *Digital Communications and Networks*, 2020. 6(4): p. 399-421.
- [44] González-Lozoya, S.M., et al., Recognition of facial expressions based on CNN features. *Multimedia Tools and Applications*, 2020. 79(19): p. 13987-14007.

- [45] Moraes, T.G., E.C. Almeida, and J.R.L. de Pereira, Smile, you are being identified! Risks and measures for the use of facial recognition in (semi-)public spaces. *AI and Ethics*, 2020.
- [46] Wang, M. and W. Deng, Deep face recognition: A survey. *Neurocomputing*, 2021. 429: p. 215-244.
- [47] Galterio, M.G., S.A. Shavit, and T. Hayajneh, A Review of Facial Biometrics Security for Smart Devices. *Computers*, 2018. 7(3).
- [48] Tawalbeh, L.a., et al., IoT Privacy and Security: Challenges and Solutions. *Applied Sciences*, 2020. 10(12).
- [49] Fuad, M.T.H., et al., Recent Advances in Deep Learning Techniques for Face Recognition. *IEEE Access*, 2021. 9: p. 99112-99142.
- [50] Yang, X., et al. Face Anti-Spoofing: Model Matters, so Does Data. in 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR). 2019.
- [51] Li, L., et al., A Review of Face Recognition Technology. *IEEE Access*, 2020. 8: p. 139110-139120.
- [52] Brnabic, A. and L.M. Hess, Systematic literature review of machine learning methods used in the analysis of real-world data for patient-provider decision making. *BMC Medical Informatics and Decision Making*, 2021. 21(1): p. 54.
- [53] Qiao, Q. and P.A. Beling, Decision analytics and machine learning in economic and financial systems. *Environment Systems and Decisions*, 2016. 36(2): p. 109-113.
- [54] Lai, Y., A Comparison of Traditional Machine Learning and Deep Learning in Image Recognition. *Journal of Physics: Conference Series*, 2019. 1314: p. 012148.
- [55] Janiesch, C., P. Zschech, and K. Heinrich, Machine learning and deep learning. *Electronic Markets*, 2021.
- [56] Nguyen, D., et al. Joint network coding and machine learning for error-prone wireless broadcast. in 2017 IEEE 7th Annual Computing and Communication Workshop and Conference (CCWC). 2017.
- [57] Turkoglu, B. and E. Kaya, Training multi-layer perceptron with artificial algae algorithm. *Engineering Science and Technology, an International Journal*, 2020. 23(6): p. 1342-1350.
- [58] Marthon, S.A., C.J.F. Cameron, and S.C. Kremer, Recurrent Neural Networks, in *Handbook on Neural Information Processing*, M. Bianchini, M. Maggini, and L.C. Jain, Editors. 2013, Springer Berlin Heidelberg: Berlin, Heidelberg. p. 29-65.
- [59] Alzubaidi, L., et al., Review of deep learning: concepts, CNN architectures, challenges, applications, future directions. *Journal of Big Data*, 2021. 8(1): p. 53.
- [60] Buber, E. and B. Diri, Web Page Classification Using RNN. *Procedia Computer Science*, 2019. 154: p. 62-72.
- [61] Abiodun, O.I., et al., State-of-the-art in artificial neural network applications: A survey. *Heliyon*, 2018. 4(11): p. e00938.
- [62] Khalaf, M., et al. Recurrent Neural Network Architectures for Analysing Biomedical Data Sets. in 2017 10th International Conference on Developments in eSystems Engineering (DeSE). 2017.
- [63] Montúfar, G., Restricted Boltzmann Machines: Introduction and Review. *ArXiv*, 2018. abs/1806.07066.
- [64] Kim, K.P. and F. Yusof. Multi-dimensional reduction using self-organizing map. in *American Institute of Physics Conference Series*. 2014.
- [65] Baldi, P., Autoencoders, unsupervised learning and deep architectures, in *Proceedings of the 2011 International Conference on Unsupervised and Transfer Learning workshop - Volume 27*. 2011, JMLR.org: Washington, USA. p. 37-50.
- [66] C A Padmanabha Reddy, Y., P. Viswanath, and B. Eswara Reddy, Semi-supervised learning: a brief review. 2018, 2018. 7(1.8): p. 5.
- [67] Okereke, C., M. Mohamad, N. Abdul Wahab, S. Zaleha. H, A Review of Machine Learning Path Planning Algorithms for Autonomous Underwater Vehicles (AUV) in *Internet of Underwater Things (IoUT)*. 2020.
- [68] Mukhaiyar, R. and R. Safitri. Implementation of Artificial Neural Network: Back Propagation Method on Face Recognition System. in 2019 16th International Conference on Quality in Research (QIR): International Symposium on Electrical and Computer Engineering. 2019.
- [69] Pk, A.M.N., X. Ding, and T. Page. An Integrated Approach for Face Recognition Using Multi-class SVM. in 2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA). 2020.
- [70] Ramadhani, A.L., P. Musa, and E.P. Wibowo. Human face recognition application using pca and eigenface approach. in 2017 Second International Conference on Informatics and Computing (ICIC). 2017.

# A Case Study on Social Media Analytics for Malaysia Budget

Ahmad Taufiq Mohamad, Nur Atiqah Sia Abdullah\*

Faculty of Computer and Mathematical Sciences  
Universiti Teknologi MARA, Shah Alam  
Selangor, Malaysia

**Abstract**—Malaysia citizen always looks forward to the budget announcement, which is presented by the government each year. Due to the direct effect on the economy, the citizens' opinions are crucial in understanding what they want and whether the budget satisfies them or not. Social media analytics can gather netizens' opinions on Twitter and conduct sentiment analysis. Most of the corpora in previous sentiment analysis research use English-based corpus. However, the current scenario of tweets in Malaysia uses a combination of English-Malay words. Therefore, this study uses a hybrid of the corpus-based and support vector machine approach. Semantic corpus-based combines the Malay and English words. Then, the domain-specific corpus on Malaysia Budget is constructed, which is budget corpus. Two separate analyses include category classification and sentiment analysis. Overall, most netizens have a positive sentiment about Malaysia's Budget with 56.28% of the tweets being positive sentiments. The majority of the netizens focus on social welfare and education that have the highest tweets. The discussion highlights the suggestion to improve the accuracy of this study.

**Keywords**—Malaysia budget; twitter; social media analytics; sentiment analysis; category classification; budget corpus

## I. INTRODUCTION

Social media platforms allow people to share content quickly, efficiently, and in real-time. There are numerous social networking services available to be utilized. Netizen intends to discuss current issues include politics, budget, products, and others using these social networking services. Budget is one of the important issues for a government. A government has annually presented the national budget plan for the next part of the year. The allocation and utilization of public funds in an efficient and prudent manner have always been a key concern in most of the budgets, including the Malaysia Budget. For this case study, the focus is on the Malaysia Budget 2020, which has been announced on 11 October 2019.

The budget consists of all aspects such as education, national defense, agriculture, transportation, and many more. This concern caused the government to reform its budget and finance to gain greater rationality and effectiveness in public financial management [1]. Therefore, the budget announcement is crucial for the ruling government.

Netizen shares their opinions through social media platforms about the budget before and after the budget presentation in Parliament. The government can use these

opinions as an evaluation of their budget allocation and citizens' satisfaction. Sentiment analysis can help in opinion mining. It makes use of natural language processing and text analytics to identify and quantify subjective information systematically. After the budget announcement, there is a need to conduct a social media analytic on these opinions to evaluate the peoples' sentiments towards the budget. It can be the guidelines for improving future budget analysis.

This paper aims to conduct a case study on social media analytics for the Malaysia Budget. The processes in the case study can be a guideline for future budget analysis. The paper continues with Section II that focuses on a literature review on social media analytics, sentiment analysis, and data visualization. Then, Section III shows the methodology for the study. It follows by the results and discussion in Section IV. It ends with the conclusion in Section V.

## II. RELATED WORK

### A. Twitter

Twitter has gained popularity among scholars, students, leaders, politicians, and the general public. It is one of the ideal public platforms for the rapid and comprehensive dissemination of political information and opinions [2], with an average of 330 million monthly active users and 500 million tweets. Retweeting is also a big part of Twitter, where people retweet or share other tweets with everyone else. The activity on Twitter involves the use of hashtags to aggregate tweets about the same subject.

### B. Social Media Analytics

The use of social media and the web creates a source of data that can be mined for new insights into how people communicate and behave, what they think and feel, and how they connect to each other [3]. Typically, retailers use social media in a few ways to promote their products. However, with people not only sharing content but also sharing their opinions, retailers or organizations find these opinions useful.

Gathering netizens' opinions about a topic or product or something in general, organizations can analyze their opinions and find ways to capitalize on them. If the netizens complain about a product of a rival company, organizations can use those opinions in creating a new product that will satisfy the netizens' needs. That is what social media analytics is all about; a practice of gathering data from social media websites and analyzing that data using social media analytical tools to make better decisions.

\*Corresponding Author.

### C. Data Preparation

Data preparation is crucial in social media analytics. It includes data scraping, data cleaning, data pre-processing, and stemming.

1) *Data scraping*: One of the ways to gather data from Twitter is through data scraping. The author in [4] describes scraping as getting the online data collection from social media and other websites in the form of unstructured data. Scraping has shown its capabilities in social media analytics, allowing new ways to collect and analyze social data [5].

2) *Data cleaning*: This process removes repeated data that are unrelated to the topic, removing typographical errors [4]. If there is incorrect or inconsistent data, it can lead to false conclusions, thus misdirecting the solutions. For example, this study analyzes the netizens' opinions if the data are incorrect, and the result could show netizens agrees with the budget allocation. However, the actual result could be the other way around.

3) *Data pre-processing*: Multiple steps of pre-processing [6] include removing stop words and stemming. However, it depends on the kind of analysis and expected output. Stop words are the most frequent words like articles (a, an, the), auxiliary verbs (be, am, is, are), prepositions (in, on, of, at), conjunctions (and, or, nor, when, while) that does not provide any information to the analysis. Therefore, stop words can be removed [7].

4) *Stemming*: In pre-processing, stemming is defined as coding multiple forms of a linguistic object into a 'rudimentary' shape with the same meaning [8] or obtaining the root, the stem of derived words [9]. Another part of data pre-processing is the categorization of data. It aims at classifying documents into a variety of pre-defined categories [10]. It is a process of assigning tags or categories to text according to its contents.

### D. Sentiment Analysis

Sentiment analysis is evolving rapidly as an automated linguistic relation and context review process [11] that involves a process of extracting attitudes, emotions, and feelings [4]. Social sentiment indicates how a person states his opinion and attitude towards an object [12]. The strength of sentiment or opinion is associated with the intensity of some emotions [13] such as joy and anger.

The evaluations can be based on consumer behavior research: rational evaluations and emotional evaluations. Rational evaluations are tangible beliefs and utilitarian attitudes, for example, "This house is worth the price". While emotional evaluations are based on non-tangible and emotional responses to events that go deep into the state of mind of individuals. For example, "This is the best house in the neighborhood". After evaluation, the polarity of the statements needs to be defined. Classification of polarity can be binary, ternary, or ordinal [11] depending on the aim of the sentiment analysis.

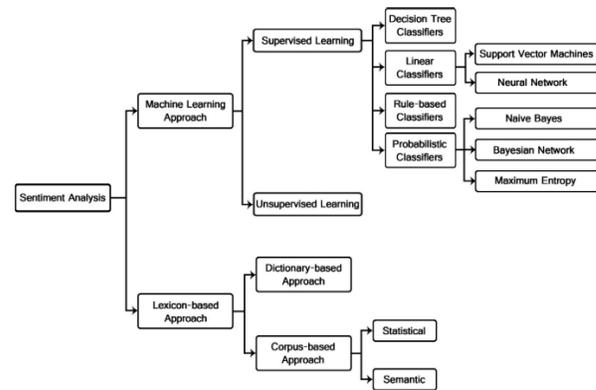


Fig. 1. Sentiment Analysis Techniques [15].

Fig. 1 shows the multiple techniques used for sentiment analysis. Sentiment detection approaches can be divided into the lexicon-based approach and the machine-learning approach [14]. The lexicon-based approach is divided into dictionary and corpus approaches. The machine learning approach (ML) uses popular algorithms such as Support Vector Machine (SVM) and Naïve Bayes (NB), which use linguistic features. ML approaches for sentiment analysis can be unsupervised or supervised machine learning.

Multiple articles on sentiment analysis are studied to gain knowledge on the performance of the classifiers mentioned. Table I shows numerous papers on sentiment analysis. The purpose of this comparison is to find the classifier that performs the best among others. From the review, SVM is the best as it performs better than other classifiers in terms of sentiment classification. There is a Malay Opinion Corpus [16] used as a data source. It is similar to this study, where the extracted tweets are Malay words with a combination of English words.

After a literature review of the sentiment analysis techniques, this study uses a hybrid of semantic corpus-based and machine learning SVM. The semantic corpus-based was chosen because it gives the sentiment values directly and suitable for domain/context-specific data. The SVM was chosen as the classifier as it is the best among others.

### E. Data Visualization

Data visualization can express data in a visual form that finds blind spots [27], which helps users acquire knowledge about the data. Data can be observed from different perspectives and used more in-depth observation and analysis. Because there are different degrees of data, the zoom feature should be implemented in data visualization [28].

Many researchers agree that data visualization can improve decision-making [29-31]. It helps an organization to view where they are and the process carried by an organization. An organization views and analyses the visualized data and can identify the problems for adjustments. Therefore, the organizations improve their decision-making through systematic data analysis to make changes to their process flow.

TABLE I. COMPARISON OF SENTIMENT ANALYSIS TECHNIQUES

Study	Technique	Feature Selection	Data Source/ Domain	Performance
[16]	SVM, Naïve Bayes, KNN	Information Gain (IG), Gini index, Chi-squared	Malay Opinion Corpus	IG-based performed best, SVM performed best (85.33%)
[17]	Naïve Bayes, KNN, and Decision Tree	Word tokens	Roman-Urdu opinions	Naïve Bayes highest accuracy (97.50%)
[18]	SVM, Naïve Bayes, Rocchio, C4.5, KNN	Word tokens	Reuters-21578, Ohsumed	SVM outperforms other classifiers
[19]	SVM, Artificial NN	Words, TF-IDF, IG	Amazon.com	ANN produce better or at least comparable results to SVM
[20]	Convolutional NN	Uses filters to produce features	Movie reviews, SST-1 SST-2, Subj, TREC, CR, MPQA	CNN achieve the highest accuracy for 4 out of 7 tests
[21]	Rule-based	Lexical features	Social media text	Performed as well as other techniques
[22]	Hybrid of Rule-based with supervised learning	N-gram, POS Tags, @USER, Hashtag, URL, Discourse	Twitter	Hybrid improve SVM Predictions
[23]	Bayesian Network	Chi-square	Twitter	Precision: 55.57%
[24]	KNN, Random Forest, Naïve Bayes, Bayesian Network	Words	Twitter	KNN highest accuracy for with stop words (99.65%) and without stop wards (96.64%)
[25]	Maximum Entropy	Words	Chinese online product reviews	Accuracy: 80.87%
[26]	Unsupervised learning	POS tagging	Korean language	F1 score: 71.8%

#### F. Types of Data Visualization

There are five data visualization categories, namely temporal, network, geospatial, hierarchical, and multidimensional.

1) *Temporal visualization*: It is one of the simplest and quickest ways to represent important time-series data. Temporary datasets usually include location and time datasets. Sometimes, these datasets may contain different characteristics [32], depending on the data sources. Temporal data have items that have a start and finish time with possibilities of data overlapping with each other.

2) *Network visualization*: A network dataset comprises an arrangement of a set of known connections among entities [33]. Network visualization shows complex relationships between several elements. A network visualization displays undirected and directed graph structures. This kind of visualization sheds light on the relationships between entities. Round nodes represent entities, while lines indicate their relationships. The vivid display of network nodes can reveal non-trivial data discrepancies.

3) *Geospatial visualization*: techniques supporting the analysis of geospatial data using interactive visualization. One of the earliest forms of information visualization is geospatial visualization. There exist a substantial number of applications these days, in which it is crucial to analyze relationships that include geographic location [34]. Geospatial visualization takes place in several real-world situations such as wildland fire fighting, forestry, archaeology, environmental studies, and urban planning that call for decision-making and processes for information formation.

4) *Hierarchical visualization*: Hierarchical visualization is suitable for numerous data types that are automatically hierarchical or ideal for a recursive grouping [35]. Hierarchical data are organized in a tree structure in which each data element identifies a node in the tree. At the same time, each

node can have child nodes. Hierarchical data visualization allows the user to drill down through multiple levels.

5) *Multidimensional visualization*: It manages datasets with several variables to correspond to the visual structure of one-dimension, two-dimension, or higher dimensions [36]. Usually, this technique can represent data depending on one or two variables [37].

### III. METHODOLOGY

There are several phases in the methodology include business understanding, data understanding, data preparation, modeling, evaluation, and deployment. The data preparation phase covers all activities to construct the final dataset from the initial raw data. After the data extraction, the data preparation phase focuses on cleaning the data before the modeling phase. The result of this phase produces a new dataset for the modeling phase.

#### A. Data Collection

RapidMiner software is used for data collection as it is easy to use and without coding. Using the “search Twitter” node in RapidMiner, an access token is needed from Twitter to gain access for extraction. After getting the access token, it sets the keywords for extracting tweets. The related keywords are Budget2020 and “Belanjawan 2020”, which obtain through Google Trends. The process of data extraction continues in 22 days (2 to 23 October 2019). The extraction happens at around 11.30 pm every single day and saves in separate excel files. At the end of data extraction, there are a collection of 9,638 tweets with 12 columns.

#### B. Data Cleaning

Dataset needs to be cleaned from unwanted data such as repetition of data and not related to the topic. Each data is scanned to remove noise, which is unrelated data. For the repetitive data, using the excel function of removing duplicates proves to be enough for removing repetitive data, keeping only the unique texts.

### C. Data Classification

As the budget covers various topics, netizens' tweets also diversify according to the categories in the budget. Therefore, there are nine budget categories with different keywords. The tweets are processed according to the words in the nine categories. Table II shows the sample of related terminologies for nine categories. The nine categories are selected because they are the most talked-about topic by netizens. After analyzing the tweets, the keywords used by the netizens are captured.

After thoroughly going through all the tweets and identifying the keywords, a corpus is created for category classification. The corpus is saved as a CSV file. Each row contains the words and the category. The related words are as follows: 26 words for agriculture, 151 words for the economy, 46 words for education, 41 words for general, 22 words for health, 45 words for others, 19 words for public services, 52 words for social welfare, and 36 related words for transportation. There are 438 words in the budget corpus.

Besides categorizing the words in the budget, the polarity of each tweet is assigned. There are three polarities in this study, positive, negative, and neutral. There are different words according to the polarity. Due to the multilingual comments by the netizen, the words are in Malay and English. Table III shows the related words for the three different polarities. The polarity represents the emotion and feeling of the netizen towards the budget categories. Positive words represent happiness and satisfaction in the budget category. The negative words show the dissatisfaction with the budget.

The processes of classification for the polarity are the same as the category classification. All the sentiment words are used to train the model to identify the sentiment of each tweet. After the classification processes, there are 114 words for the positive polarity, 90 words for neutral polarity, and 92 words for negative polarity. The corpus is used to train the model to classify the sentiment for each tweet.

### D. Modeling

For this modeling phase, there are a few steps to be taken. The first step is selecting a suitable model. For this study, the model focused on sentiment analysis. There are two approaches for sentiment analysis, which are machine learning and lexicon-based models. Machine learning models belong to supervised classification. Two sets of documents, training, and testing, are needed for classification purposes. The training set is used in an automatic classifier to differentiate the characteristics of tweets. The testing set is used to check the performance of the classifier.

For lexicon-based models, it employs dictionaries of words annotated with their semantic polarity and sentiment strength. It uses a corpus to help in the sentiment classification process. Then, the corpus is used to calculate a score for the polarity of the document or dataset. After comparing the techniques for sentiment analysis models, a hybrid of corpus-based and Support Vector Machine (SVM) is selected as the technique in this study. Fig. 2 shows the designed process of sentiment analysis for this study.

TABLE II. WORDS IN SELECTED CATEGORIES

Category	Related Words
Agriculture	Pertanian, sawit, getah, padi, peladang, pesawah, farmer
Economy	M40, B40, gst, tax, cukai, pekerjaan, gaji, ekonomi, epf
Education	Pendidikan, education, TVET, pendidikan tertiary, biasiswa
General	Menteri, Belanjawan, Budget, government, kerajaan, Malaysia
Health	Perubatan, patients, vaccines, medical, kesihatan, disease
Public Services	MINDEF, polis, tentera, kebombaam, pertahanan, TLDM, defence
Social Welfare	Bumiputra, disabled, OKU, wanita, children, orang asli
Transportation	Pengangkutan awam, tol, kereta, minyak, BSH, fuel, Petrol
Others	Persiaran, hiburan, seni, pelancongan, budaya, belia, sukan

TABLE III. SAMPLE WORDS IN THREE POLARITIES

Polarity	Related Words
Positive	best, sokong, satisfying, love, agree, baik, happy, excited, glad, uplifting
Negative	#pakatanhancing, malap, garbage, rugi, bodoh, worse, keburukan
Neutral	not sure, entah, unfortunately, why, but, cadangan, diharapkan

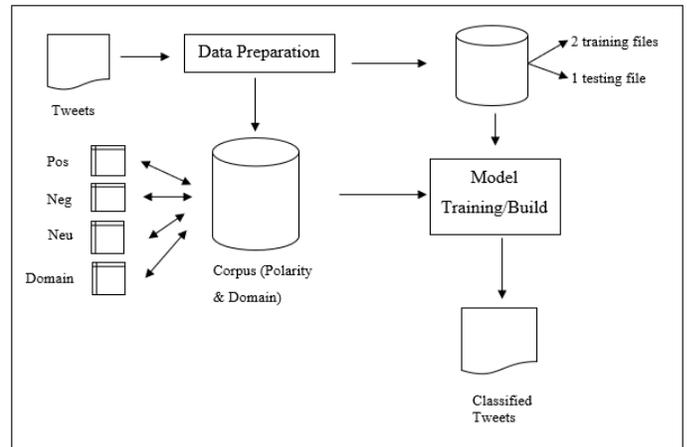


Fig. 2. Sentiment Analysis Techniques [15].

After pre-processing and the preparation of the data, the results of the classifications are set into a corpus. The corpus is used for modeling, where the extracted dataset is trained by two training files and tested using a single file using Support Vector Machine (SVM). The two training files are files containing the category keywords and sentiment keywords. The result of the testing is then compared with the benchmark sentiment dataset to check the accuracy.

The result of both analyses is visualized in a dashboard form. The visualization is presented using PowerBI software based on a dashboard approach where multiple charts are in a single view. As the visualizations have different techniques, multidimensional visualization is more suitable for this study due to the data types. Table IV shows the types of visualizations and data representations for the dashboard.

TABLE IV. DASHBOARD VISUALIZATION

Chart	Data Representation
Pie chart	Percentage and number of polarity
Column chart	Total of tweets in each category
Column chart	Total of tweets in each category with sentiment

The pie chart is used to show the percentage and amount of polarity. The column chart is used to show the total tweets in each category, and sentiments. As SVM has many parameters to experiment with, this study finds the best parameter that produces the best score. GridSearch function is used to find the best value for each parameter. To summarize, the best parameters for this SVM model are:

- Best C: 1000.
- Best Kernel: rbf.
- Best Gamma: 0.001.

These parameters are used for the category and sentiment classification as training files used in the GridSearch function yield the same result.

#### IV. RESULTS AND DISCUSSION

This study explains the processes of gathering and creating a budget corpus for analysis. A hybrid of SVM and corpus-based approaches is proposed for category classification and sentiment analysis. The modeling uses two training files and one testing file for both analyses. Based on the results, social welfare and education are the most popular category in Malaysia Budget 2020 (see Table V).

The netizen talked about the welfare of disabled people, natives, senior citizens, and people from different religions and races. On the topic of education, netizen comment about education issues ranging from kindergarten to university. The other categories in the tweets are agriculture, economy, health, and others. Table V shows the actual number of tweets in each category in the budget.

For sentiment classification, the result of the model training using the parameters achieved a score of 46.59%. The result of the testing model achieved an accuracy of 31.04%. Table VI shows the classification report of the sentiment classification.

Based on Table VI, the accuracy for the sentiment classification is 31.04%. Among the sentiments, neutral sentiment has the highest accuracy of 39.30%, f1-score of 32.54%, precision of 75.37% but the lowest recall score of 20.75%. For the negative sentiment, the model achieved 28.57% accuracy, 28.30% for f1-score, 19.79% in precision, and 49.60% for recall. Lastly, for positive sentiment, it achieved an accuracy of 27.53%, f1-score of 30.31%, precision of 19.48%, and recall of 68.21%.

Fig. 3 shows the noticeable gap between the actual and result of sentiment classification.

There are 843 actual positive tweets, but 2,951 tweets are predicted positive. For the negative sentiment, it is about 502 tweets, but 1,258 tweets are predicted negative. Lastly, neutral has the most sentiment tweets (n=3,952), but the model only

predicted 1,088 neutral tweets. The difference between the classification results is because of the lacking of words in the budget corpus.

With category and sentiment classification, the result is visualized in a dashboard. It helps the analysts in making a more in-depth critical analysis of the study.

Fig. 4 shows a dashboard for the social media analytics in Malaysia Budget 2020. There are three charts in the dashboard. A pie chart displays the tweets based on the sentiment. The column charts illustrate the tweets by time and category. A slicer function is also added to the dashboard to filter the visualization based on a specific category.

The dashboard is evaluated using convenience sampling. From the survey, the dashboard is understandable for the users. The majority of the users agreed that the dashboard is simple and useful for quick insight into the budget.

TABLE V. ACCURACY OF CATEGORY CLASSIFICATION

Category	Actual Number	Result
economy	856	746
education	261	3263
transportation	129	0
health	63	111
agriculture	89	1521
public services	532	0
social welfare	138	3284
general	1361	0
others	2206	94

TABLE VI. REPORT OF SENTIMENT CLASSIFICATION

Item	Accuracy (%)	f1-score (%)	Precision (%)	Recall (%)
negative	28.57	28.30	19.79	49.60
neutral	39.90	32.54	75.37	20.75
positive	27.53	30.31	19.48	68.21
accuracy		31.04	31.04	31.04
macro avg		30.38	38.22	46.19
weighted avg		31.78	61.21	31.04

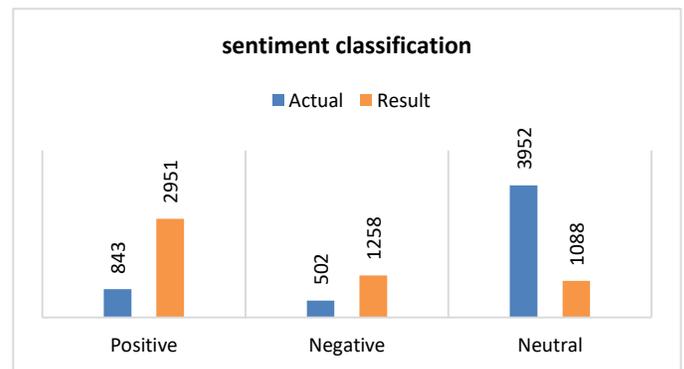


Fig. 3. Bar Chart of Sentiment Classification.

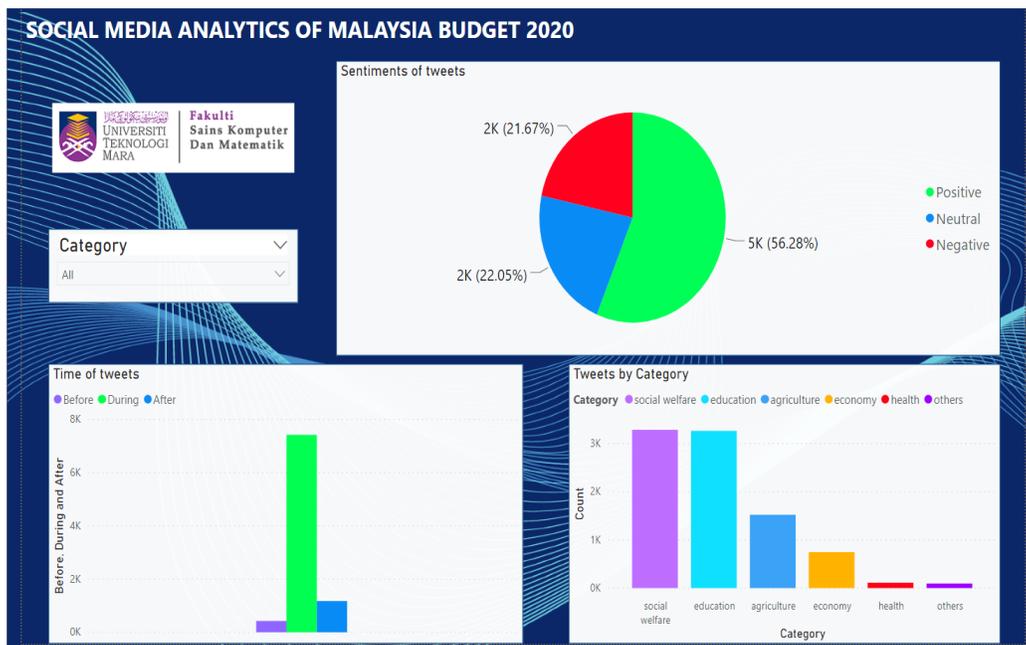


Fig. 4. Social Media Analytics Dashboard for Malaysia Budget 2020.

With only 5,297 tweets used out of 9,638 raw tweets, the data collection for the analysis is insufficient. As the study focuses on Twitter for data collection, perhaps using other social media platforms like Facebook can increase the data collection related to the budget. Thus, it will lead to higher accuracy of category and sentiment classification of tweets. Furthermore, the study only explored a narrow range of possible parameters values. A recommendation is to explore the SVM parameters such as kernels, shrinking, tolerance for stopping criterion, and class weight. Moreover, a more complex model for analysis would be an opportunity to be explored.

## V. CONCLUSION

The budget presentation has a direct impact on the economy of the country. Therefore, the citizens' opinions are crucial in understanding the actual needs and their satisfaction. Social media analytics can process opinions with sentiment analysis. This study chose a corpus-based approach to extract the Malay and English words that focus on Malaysia's Budget. A hybrid of SVM and corpus-based approaches is used for category classification and sentiment analysis. Overall, the netizens are positive about Malaysia's Budget with 56.28% of the overall tweets. The netizens are more concerned about the social welfare and education aspect of the budget as both categories have the highest tweets. Further exploration of the SVM parameters and complex model for analysis is the potential area to be studied.

## ACKNOWLEDGMENT

The authors express their gratitude to the Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA, Shah Alam, Selangor, Malaysia for supporting this study.

## REFERENCES

- [1] N. A. Siddiquee, "Managing for results: Lessons from public management reform in Malaysia," *Int. J. Public Sect. Manag.*, vol. 23, no. 1, pp. 38–53, 2010.
- [2] S. Stieglitz, L. Dang-Xuan, A. Bruns, and C. Neuberger, "Socialmedia analytics," *Bus. Inf. Syst. Eng.*, vol. 6, no. 2, pp. 89–96, 2014.
- [3] G. Moss, H. Kennedy, S. Moshonas, and C. Birchall, "Knowing your publics: The use of social media analytics in local government," *Inf. Polity*, vol. 20, no. 4, pp. 287–298, 2015.
- [4] B. Batrinca and P. C. Treleaven, "Social media analytics: a survey of techniques, tools and platforms," *AI Soc.*, vol. 30, no. 1, pp. 89–116, 2014.
- [5] N. Marres and E. Weltevrede, "SCRAPING THE SOCIAL?: Issues in live social research," *J. Cult. Econ.*, vol. 6, no. 3, pp. 313–335, 2013.
- [6] M. Ghiassi, J. Skinner, and D. Zimbra, "Twitter brand sentiment analysis: A hybrid system using n-gram analysis and dynamic artificial neural network," *Expert Syst. Appl.*, vol. 40, no. 16, pp. 6266–6282, 2013.
- [7] A. Fahrmi and M. Klenner, "University of Zurich Old wine or warm beer : target-specific sentiment analysis of adjectives Old Wine or Warm Beer : Target-Specific Sentiment Analysis of Adjectives," no. April, pp. 60–63, 2008.
- [8] Z. Xiang, Z. Schwartz, J. H. Gerdes, and M. Uysal, "What can big data and text analytics tell us about hotel guest experience and satisfaction?," *Int. J. Hosp. Manag.*, vol. 44, pp. 120–130, 2015.
- [9] N. Zainuddin and A. Selamat, "Sentiment analysis using Support Vector Machine," *I4CT 2014 - 1st Int. Conf. Comput. Commun. Control Technol. Proc.*, no. I4ct, pp. 333–337, 2014.
- [10] Y. Ko and J. Seo, "Automatic text categorization by unsupervised learning," 2000, pp. 453–459.
- [11] A. R. Alaei, S. Becken, and B. Stantic, "Sentiment Analysis in Tourism: Capitalizing on Big Data," *J. Travel Res.*, vol. 58, no. 2, pp. 175–191, 2019.
- [12] Y. Mejova, "Sentiment Analysis : An Overview Comprehensive Exam Paper," *Science (80-. )*, pp. 1–34, 2009.
- [13] Y. Lin, X. Wang, and A. Zhou, "Opinion spam detection," *Opin. Anal. Online Rev.*, no. May, pp. 79–94, 2016.
- [14] D. Maynard and A. Funk, "Automatic detection of political opinions in tweets," *CEUR Workshop Proc.*, vol. 718, pp. 81–92, 2011.

- [15] W. Medhat, A. Hassan, and H. Korashy, "Sentiment analysis algorithms and applications: A survey," *Ain Shams Eng. J.*, vol. 5, no. 4, pp. 1093–1113, 2014.
- [16] T. Al-Moslmi, S. Gaber, A. Al-Shabi, M. Albared, and N. Omar, "Feature selection methods effects on machine learning approaches in Malay sentiment analysis," *1st ICRIL-International Conf. Innov. Sci. Technol. (IICIST 2015)*, no. April, pp. 2–5, 2015.
- [17] M. Bilal, H. Israr, M. Shahid, and A. Khan, "Sentiment classification of Roman-Urdu opinions using Naïve Bayesian, Decision Tree and KNN classification techniques," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 28, no. 3, pp. 330–344, 2016.
- [18] T. Joachims, "Text Categorization with SVM: Learning with Many Relevant Features," pp. 2–7.
- [19] R. Moraes, J. F. Valiati, and W. P. Gavião Neto, "Document-level sentiment classification: An empirical comparison between SVM and ANN," *Expert Syst. Appl.*, vol. 40, no. 2, pp. 621–633, 2013.
- [20] Y. Kim, "Convolutional neural networks for sentence classification," *EMNLP 2014 - 2014 Conf. Empir. Methods Nat. Lang. Process. Proc. Conf.*, pp. 1746–1751, 2014.
- [21] J. Wilson and C. Hernández-Hall, "Physics laboratory experiments," *Eighth Int. AAAI Conf. Weblogs Soc. Media*, p. 18, 2014.
- [22] P. Chikersal, S. Poria, and E. Cambria, "SeNTU: Sentiment Analysis of Tweets by Combining a Rule-based Classifier with Supervised Learning," no. *SemEval*, pp. 647–651, 2015.
- [23] M. S. Asriadi, M. S. Mubarak, and Adiwijaya, "Classifying emotion in Twitter using Bayesian network," *J. Phys. Conf. Ser.*, vol. 971, no. 1, pp. 0–14, 2018.
- [24] A. P. Jain and V. D. Katkar, "Sentiments analysis of Twitter data using data mining," *Proc. - IEEE Int. Conf. Inf. Process. ICIIP 2015*, pp. 807–810, 2016.
- [25] H. Wu, J. Li, and J. Xie, "Maximum entropy-based sentiment analysis of online product reviews in Chinese," no. *May*, pp. 559–562, 2017.
- [26] Y. Ko and J. Seo, "Automatic text categorization by unsupervised learning," pp. 453–459, 2000.
- [27] Q. Fu, W. Liu, T. Xue, H. Gu, S. Zhang, and C. Wang, "a Big Data Processing Methods for Visualization," pp. 571–575, 2013.
- [28] F. Bao and J. Chen, "Visual framework for big data in d3.js," *Proc. - 2014 IEEE Work. Electron. Comput. Appl. IWCA 2014*, pp. 47–50, 2014.
- [29] Y. Zheng, W. Wu, Y. Chen, H. Qu, and L. M. Ni, "Visual Analytics in Urban Computing: An Overview," *IEEE Trans. Big Data*, vol. 2, no. 3, pp. 276–296, 2016.
- [30] H. Yan, J. Wang, and C. Xia, "Research and Application of the Test Data Visualization," *Proc. - 2017 IEEE 2nd Int. Conf. Data Sci. Cyberspace, DSC 2017*, pp. 661–665, 2017.
- [31] A. Lodde, "Network Visualisation," *Network*, 2009.
- [32] A. Shrestha, "Visualizing Spatio-Temporal data," 2014.
- [33] J. Madadhain, D. Fisher, P. Smyth, S. White, and Y. Boey, "Analysis and visualization of network data using JUNG," *J. Stat. Softw.*, vol. 10, no. 2, pp. 1–35, 2005.
- [34] D. A. Keim, "Information Visualization: Scope, Techniques and Opportunities for Geovisualization," in *Exploring Geovisualization*, 2005, pp. 21–52.
- [35] P. Neumann, S. Schlechtweg, and S. Carpendale, "Arctrees: Visualizing Relations in Hierarchical Data," *Proceeding EUROVIS'05 Proc. Seventh Jt. Eurographics / IEEE VGTC Conf. Vis.*, pp. 53–60, 2005.
- [36] R. M. Pillat, E. R. A. Valiati, and C. M. D. S. Freitas, "Experimental study on evaluation of multidimensional information visualization techniques," *ACM Int. Conf. Proceeding Ser.*, vol. 124, no. April 2014, pp. 20–30, 2005.
- [37] H. Pohlheim, "Visualization of Evolutionary Algorithms - Set of Standard Techniques and Multidimensional Visualization," *GECCO'99 - Proc. Genet. Evol. Comput. Conf. San Fr. CA*, pp. 533–540, 1999.

# A Pattern Language for Class Responsibility Assignment for Business Applications

Soojin Park

Graduate School of Management of Technology  
Sogang University  
Seoul, Korea

**Abstract**—Assigning class responsibility is a design decision to be made early in the design phase in software development, which bridges requirements and an analysis model. In general, assigning class responsibility relies heavily on the expertise and experience of the developer, and it is often ad-hoc. Class responsibility assignment rules are hard to be uniformly defined across the various domains of systems. Thus, the existing work describes general stepwise guidelines without concrete methods, which imposes the limit in deriving an analysis model from requirements specification without any loss of information and providing sufficient quality of the analysis model. This study tried to grasp the commonality and variations in analyzing the business application domain. By narrowing the subject of the solution, the presented patterns can help identify and assign class responsibilities for a system belonging to the business application domain. The presented pattern language consists of six segmented patterns, including 19 variations of relationship type among conceptual classes. Each sequence of a use case specification could be analyzed as the result of weaving a set of the six segmented patterns. A case study with a payroll system is presented to prove the patterns' feasibility, explaining how the proposed patterns can develop an analysis model. The coverage of the proposing CRA patterns and enhancement of implementation code quality is discussed as the benefit.

**Keywords**—Class responsibility assignment; analysis pattern; business application; sequence diagram

## I. INTRODUCTION

Developing an analysis model is the first phase in software development where abstract solutions are contrived. In the analysis model development, the task that is the most challenging and requires high creativity is assigning class responsibilities. Due to the nature of the task, responsibility assignment has heavily relied on the developer's experience and knowledge about the application domain. The class responsibility assignment (CRA) is hard to teach and apply [1]. On the other hand, it is hard to revise the wrong assignment of responsibilities to classes by adding other design patterns or architectural styles in successive phases.

The GRASP pattern [2] is remarkable and traditional among several approaches introduced to solve the CRA problem. However, it provides several fragmentary solutions and still requires lots of ad-hoc decision-makings to implement the patterns in a specific system. Since introducing the GRASP pattern, several approaches [3-5] that try to lessen the heuristic aspect of the CRA problem have been proposed. Nevertheless, their limitation is that they propose a way to evaluate the CRA

results rather than assign responsibility itself. The posterior evaluation cannot reduce developers' efforts which are already exerted for CRA.

This study presents a pattern-based approach for assigning responsibility, which bridges analysis modeling and design modeling. CRA problems for business applications can eventually be decomposed into a set of CRUD operations on information: creating (C), reading (R), updating (U), and deleting (D). Thus, a data transaction is decomposed into six fragments and designed a CRA pattern for each fragment. This study also provides a way to compose the six fragmented CRA patterns for realizing a sequence diagram for each scenario in use case specifications. According to the given scenario, the sequence diagram can be composed of 2~6 CRA patterns. The links and messages that appeared in sequence diagrams are reflected as relationships between classes and responsibilities of each class. Each CRA pattern is represented by a uniformed template similar to the Gang of Four (GoF) pattern template [6] and composed of predefined variables and constants. The information developers extract from use case specifications is used to substitute variables in the CRA pattern and decide which patterns compose a complete sequence diagram for a scenario. In other words, developers can make an analysis model from the requirements model by mapping the information from use case specifications into each CRA pattern in developing an analysis model from the requirements model.

Compared with other related studies, the differentiated point of the proposed CRA pattern is as follows: the most assignment result of class responsibility is not a set of the tentative candidates but a final decision itself. The limit of the other existing work on class responsibility problems is that developers must select one among multiple candidate responsibilities or revise the candidates even after applying proposed methods. The reason is that most methods do not have a limit on the scope of their application. A solution proposed by the approach to solving the CRA problem of all domains cannot embed the properties for each domain. As a result, even if it is a solution that automatically supports class responsibility assignment, developers must tailor it to fit the characteristics of the domain after applying the methods. This study limits the proposed CRA pattern's application scope to the business application domain to substantially reduce those kinds of developers' efforts. Instead, by embedding the inherent features of the business application domain into the patterns, most of the responsibilities extracted from the CRA pattern

application are included in the final version of an analysis model without any revise.

A case study is conducted to adopt a payroll management system to show the feasibility of using the proposed CRA patterns in developing an analysis model. The coverage of the responsibilities extracted from the CRA patterns is measured to show the benefit of the proposed patterns. The result explains that a considerable portion of the responsibilities can be systematically extracted by applying the CRA patterns and included in the final version of the analysis model. And, the enhancement of the code quality derived from the analysis model constructed by applying the CRA patterns is also evaluated.

The rest of the paper is organized as follows: Section 2 presents related works on the class responsibility assignment problem. Section 3 gives an overview of the presented CRA pattern language, and Section 4 introduces the representation of each CRA pattern. Section 5 demonstrates a case study using a payroll management system, and section 6 shows the evaluation result. Section 7 concludes the paper with future work.

## II. RELATED WORK

Most of the analysis patterns [7-12] tended to focus on providing a way to identify classes that abstract domain knowledge. The main objective of design patterns [7] published up to now is to solve specific problems for successive implementation steps or enhance specific software quality. Contrary to this trend, [2] designated designing objects with responsibilities step as the heart of developing an object-oriented system and introducing the GRASP pattern. GRASP presents nine design principles as patterns: information expert, creator, low coupling, protected variations, indirection, polymorphism, high cohesion, pure fabrication, and controller. The GRASP pattern addresses fundamental, common questions and fundamental design issues on assigning class responsibilities. However, the questions defined by the GRASP are too general, and some principles are more fundamental than others. Their solutions are rather guidelines than patterns that define constants and variables of a model.

Since the introduction of the GRASP, several studies have been dealt with the CRA problem. Bowman et al. introduced a solution for the CRA problem, which is based on a multi-objective genetic algorithm (MOGA) and uses class coupling and cohesion measurement [3][13]. The MOGA takes as input a class diagram to be optimized and suggests possible improvements to it. They implemented a case study that showed that the multi-objective genetic algorithm could fix various artificially seeded assignment problems. However, the result of the MOGA application is limited to fixing the information included in classes. It does not help to construct sequence diagrams that explain dynamic behaviors based on the fixed responsibilities.

In [4], another metaheuristic algorithm for detecting wrong assigned responsibilities and making an optimized CRA is introduced. The proposed four different algorithms (simply genetic algorithm, hill-climbing, simulated annealing, and particle swarm optimization) use the same class coupling and

cohesion metrics. They transformed the CRA problem into a search problem by encoding the problem and defining the fitness function. Like the MOGA, they chose a multi-objective approach, normalizing and combining three different coupling and cohesion measurements into a single aggregated fitness function and implemented a case study on the ATM Simulation domain model. Thus, their pros and cons are similar to MOGA's ones. Although they provide a way to evaluate already completed CRA results and enhance the quality of a design model, the contribution is limited to the conceptual model. Moreover, enhancement opportunities are given after the end of the developers' CRA step. Thus, it is hard to reduce the effort of developers on the responsibility assignment step itself.

Unlike the formerly described two approaches using some algorithm for detecting errors after the end of whole CRA steps, [5] proposed a technique to detect any error in every CRA step. For every step in CRA, the editor automatically detects bad smells of the current CRA and suggests refactored CRAs as alternatives. Designers can accept or reject the suggested CRAs. By repeating the steps of the responsibility assignment and refactoring, designers can construct the more appropriate CRA. This study's contribution is that they suggest formal representation for informal guidelines in GRASP and automatic detection rules for finding bad smells, which is violating the guidelines. However, like other approaches, the developers should create any CRA result before detecting the CRA errors and refactoring, and the application scope is limited on conceptual models.

Whereas the studies mentioned above mainly want to automatically detect errors as a follow-up to the developer's class responsibility identification results, the studies in [14-16] take an approach to automatically extract and present design elements from use case specification. [14] proposes an automated method that extracts domain classes from parsing use case specification using the Natural Language Processing (NLP) technique. [15], like [14], creates a parsed use case description (PUCD), an intermediate step product, from parsing the sentences of the use case specification, and then proposes candidates to construct a class model. The final decision to construct a class model remains to developers. [16] presents an automatic generation of a conceptual model from requirements written in a natural language, English, and proves the quality of the generated models against human works. However, their work has limited in that the coverage of the proposed method over all kinds of natural language is not comprehensive. And, the inherent ambiguity in the natural language occurs, hesitating the decision if a specific noun is an attribute, class, or association. Extracting a conceptual model from requirements needs an abstraction phase and heuristic insights for a specific domain area. Thus, it still requires experts' decisions on the details of the automatically generated conceptual model. Considering the effort of the experts' confirmation on the results, the benefit from the automatic generation of a conceptual model is skeptical. For this reason, this study does not include a conceptual model in the scope of automatically generated modeling artifacts. The conceptual model extracted by experts is used as input knowledge for automatic class responsibility assignments.

As mentioned above, although such NLP-based approaches have partial benefits, there is a limit to replacing the abstraction process that indicates the properties of the application domain, with only parsing the use case specification as a natural language sentence and interpreting it grammatically.

As the different approaches to solving class responsibility assignments, [17-18] attempt to determine responsibilities automatically between classes by using a class diagram as an input. [17] introduces a method that proposes an appropriate number of classes using three hierarchical agglomerative clustering algorithms and two criteria (aggregation metrics and CRA-Index) in the class diagram. And a comparison of the result applying their solution and the MOGA application result is presented. On the other hand, [18] presents a strategy for automatically generating a basic behavior schema from the static view represented by a class diagram. Through the analysis of the relationships between classes, the basic operations required for each class are identified. However, [17-18] has a limit in that the automatically generated operations are specified in too general terms, which requires the final decision of developers on every generated responsibility. Thus, the generated result can be utilized as a guide or reference to decide each responsibility of classes. Still, the automatically generated responsibility, i.e., operation, is hard to participate in an analysis model without a final update from developers.

Consequently, the existing studies on the CRA problem succeeded in enhancing the quality of a design model by providing various evaluation methods. However, most of the current work provides class responsibility assignments as a reference artifact or a candidate artifact for software developers. The result requires developers' final decision or update. It means that they still have a limit in relieving the developers of the CRA step's painful and challenging decision-making burden.

### III. A PATTERN LANGUAGE FOR CLASS RESPONSIBILITY ASSIGNMENT FOR BUSINESS APPLICATIONS

Most pattern-based approaches are subject to questions regarding the completeness of the patterns used. The answer to the question can be found in the definition of the business applications of [19]: "a business application is an application with structured logic and transaction-based database which supports simultaneous access by other applications." From the definition of a business application, an idea that a business flow can finally be disassembled into atomic CRUD(Create/Read/Update/Delete) operations can be captured. Most of the complex business services provided by the domain are readily broken down into a series of CRUD operations.

For example, Fig. 1 shows that the four different business flows from different systems can be decomposed to the identical combination of a read data pattern and an update data pattern. Besides the CRUD operations, interactions with the environment in which the system is driven are also needed to realize a business flow in the applications. In this study, the atomic collaboration between classes for realizing each CRUD operation and interaction with the environment is designed as each CRA pattern. The objective of the proposed CAR pattern language is to provide a way to build an analysis model by

generating a sequence diagram of the system belonging to the business application domain combining the atomically designed CRA patterns. In this study, the syntax to utilize the CRA patterns is also provided. So, for this reason, the proposed set of the CRA patterns is named a "CRA pattern language." First, this section presents an overview of the CRA pattern language.

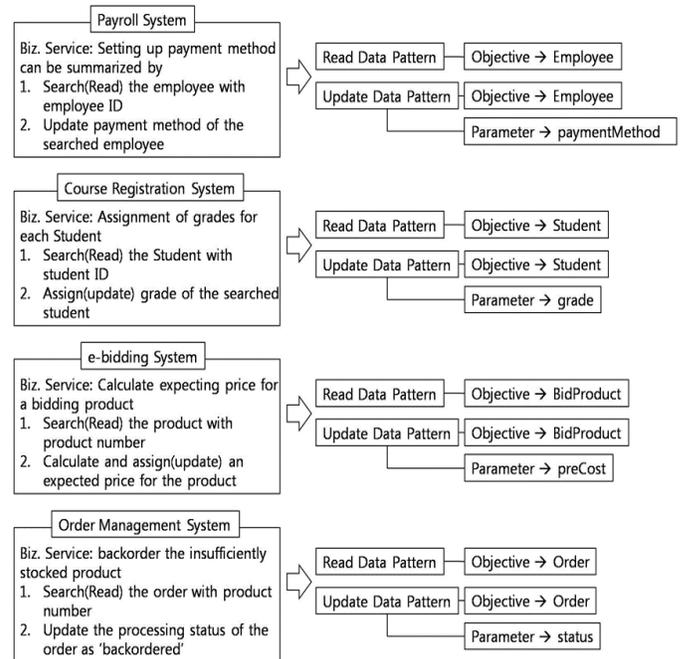


Fig. 1. Examples of Different Business Services Decomposed into the Same Atomic Collaboration Patterns.

#### A. Domain Model

A domain model for assigning class responsibilities for the business application contains all classes participating in the proposed pattern set. This study follows the Model-View-Controller (MVC) [20] pattern in identifying the role of participating classes in realizing a scenario of a use case specification. The participating classes that are divided into three analysis class stereotypes: << boundary >>, << control >> and << entity >>. These three stereotyped classes are arranged in separate packages that represent the basic three layers of business applications. The BizApplication package contains GUI form classes and <<boundary>> classes to interface with external systems. The BizProcess package contains <<control>> classes for managing flows in individual use cases. The BizLogic package contains <<entity>> classes to include actual business logic.

Fig. 2 depicts the whole class composing domain model for assigning class responsibilities of business applications. In Fig. 2, the question marks (?) in class names or operation names indicate pattern variables. The '+' mark, shown in class, operation, and parameter names, is an operator for concatenating two strings. Pattern variables are substituted with data values elicited from requirements documents to generate instantiated class or operation names during the pattern instantiation stage. For example, '?UCNm+ApprvlForm' is instantiated as RgstrCrsApprvlForm if the string value of



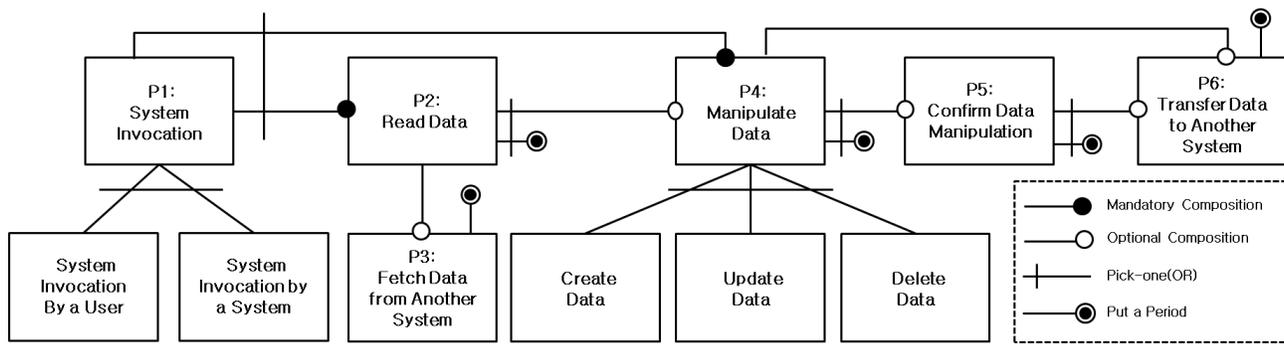


Fig. 3. Pattern Language Application Graph.

The firstly applicable pattern in order is the System Invocation pattern which gives a solution on how the system can be invoked. After applying the System Invocation pattern, the Read Data pattern can be successively applied as users usually check data before changing it. If the data is located in other systems, Fetch Data from Another System pattern can be applied. To be composed as a design fragment for reading some data, the possible pattern sequence is “System Invocation → Read Data” or “System Invocation → Read Data → Fetch Data from Another System.” If the data source to be read is the system itself, the first pattern sequence will be applied. Otherwise, the second option should be applied. So, a typical pattern application sequence is “System Invocation → Read Data → Manipulate Data” patterns. But users could manipulate data without reading anything in some cases, which is also a typical sequence. Thus, the Read Data pattern can be an optional pattern like Fetch Data from Another System pattern.

After applying a pattern belongs to the data manipulation pattern, Confirm Data Manipulation pattern could be optionally applied if it requires any specific actions to reflect the result of data manipulation on the system. The other applicable pattern is Transfer Data to Another System pattern, applied when the data manipulation result should be reflected to another related system.

To sum up, the proposed pattern language is composed of 2 required patterns (System Invocation, Manipulate Data) and four optional patterns (Read Data, Fetch Data from Another System(s), Confirm Data Manipulation, Transfer data to another system(s)). The Read Data pattern is an optional pattern when it is applied with other data manipulation patterns. However, it can be a mandatory pattern when it is used to implement a scenario to show some information to users without any change on data. The minimum number of the patterns composing a scenario is two as the shortest sequence is “System Invocation → Read Data” or “System Invocation → Manipulate (Create/Update/Delete) Data.” The maximum number of the applied patterns for realizing a scenario is six as the most extended pattern sequence is “System Invocation → Read Data → Fetch Data from Another System → Manipulate (Create/Update/Delete) → Confirm Data Manipulation → Transfer data to another system.”

### C. Process of Building an Analysis Model using CRA Pattern Language

With the CRA patterns, a sequence diagram to identify class responsibility from a scenario in a use case specification can be composed through three phases – use case analysis, CRA pattern weaving, CRA pattern instantiation. Fig. 4 shows each step of constructing an analysis model using the proposed CRA patterns, and the detail of each step is the following.

Use Case Analysis: (a) the reference artifacts are use case model and initially identified conceptual key classes. (b) The process starts with analyzing input use cases to identify the necessary information to populate CRA patterns through questions and answers. (c) A set of predefined questions is presented to the developer to decide patterns to be applied and elicit pattern variables to instantiate the chosen patterns.

CRA Pattern Weaving: Use case analysis results in a set of CRA patterns chosen to apply. Six patterns are presented in this study. Each selected pattern defines a segmented collaboration among participating classes, and the number of the selected patterns for a scenario is between two and six. (d) To realize a given scenario as an analysis model, the patterns to compose a complete sequence diagram should be weaved into a sequence diagram. The identically appeared lifeline between two CRA patterns becomes the connection point of the two patterns. From the P1 pattern to the P6 pattern, the required patterns are weaved step by step. At the end of CRA pattern weaving, we can get a skeleton of a complete sequence diagram for the target scenario.

CRA Pattern Instantiation: The skeleton of a sequence diagram resulting from the CRA pattern weaving step still has uninstantiated pattern variables. The value for each pattern variable is extracted in the previous use case analysis step. (e) From the answers to the questions, the values for pattern variables can be extracted. The instantiation of the composed pattern results in an analysis model with responsibilities of CRUD operations and other supporting operations for each analysis class. All of the responsibilities that appeared in the sequence diagram are registered as the operations of the key classes. Besides adding the operation to the existing key classes, new classes are also defined by applying CRA patterns.

The details of each phase will be explained with a tangible application case of a payroll management system in Section 5.

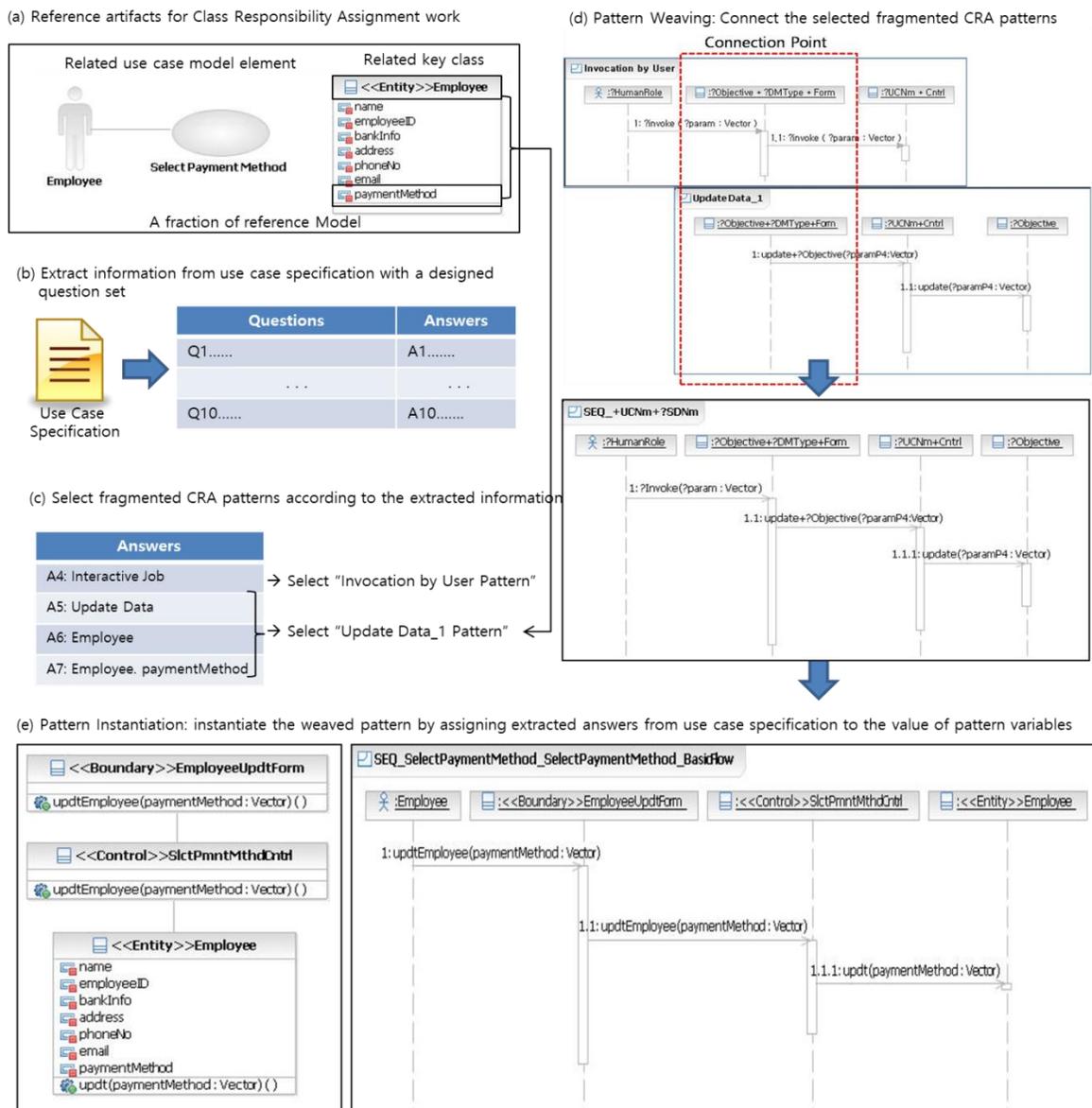


Fig. 4. Building an Analysis Model using CRA Pattern Language.

#### IV. REPRESENTATION OF A CRA PATTERN

The GoF pattern template [6] is utilized to represent each CRA pattern. However, all of the compartments of the GoF pattern template are not used. Also Known As, Motivation, Known Uses, and Sample Code sections are not used as they are out of the concern of the CRA pattern. The followings are the sections and their brief descriptions of the CRA pattern.

- 1) *Problem*: The question to be solved with the pattern regarding the class responsibility assignment aspect.
- 2) *Forces*: The conditions be satisfied by applying the pattern.
- 3) *Solution*
  - a) *Structure*: The static view of the newly defined classes or their properties (operations and relationships), which participate in the interactions in the pattern.

b) *Participants*: The specification of roles of the classes participating in the interactions in the pattern.

c) *Interaction*: The dynamic view showing the collaboration among the classes specified in section 3.2 Participants. More than one interaction could be defined according to the relationship format of the <<Target>> role class and other classes.

4) *Consequences*: The guaranteed benefit from the application of the pattern.

5) *Following patterns*: Another CRA pattern connected to the next to build a complete sequence diagram.

6) *Example*: Simple application example is presented. The finally generated sequence diagram and the corresponding class diagram are provided for understanding the pattern.

Fig. 5 shows the specification of the “Create Data” pattern documented according to the template above. The “Create Data”

pattern has three different interactions, and each sequence diagram defines the collaboration among the participating classes according to the given condition.

As specified in Fig. 5, the P4 patterns (Create/ Read/ Update/ Delete Data patterns) define several interaction

variants according to class relationships and attributes. Table I lists up all interactions embedded in each CRA pattern. There are a total of 19 interactions that can be used to construct a sequence diagram, as shown in Table I.

### Create Data Pattern

#### 1. Problem

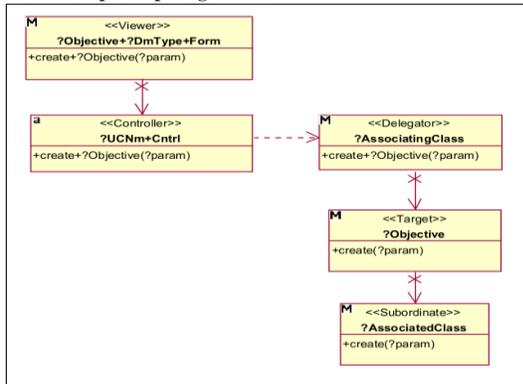
Who should be responsible for creating a new instance of some classes?

#### 2. Forces

- Input data from a user should be created as an instance of a class.
- Responsibility assignment with high cohesion and low coupling should be accomplished.

#### 3. Solution

##### 3.1 Structure: participating classes



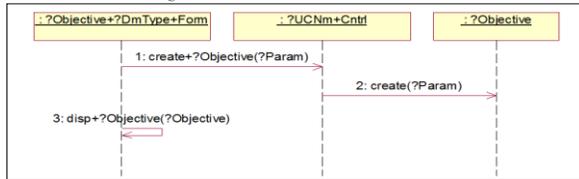
##### 3.2 Participants

Role	Description
Viewer	A UI (User Interface) form class for accepting data required to be newly created.
Controller	A control class for conducting collaboration among classes for the realization of a given business flow.
Target	A newly created entity class as the result of the given business flow.
Delegator	An entity class including the <<Target>> class as a data member.
Subordinate	An entity class defined as a data member of <<Target>>.

##### 3.3 Interaction

###### Create Data 1: Simple Creation

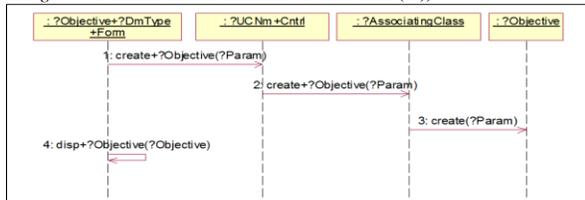
Use WHEN a <<Target>> class does not exist in the current static view.



1. Input data from a viewer is passed to a controller
2. The controller creates a target object.

###### Create Data 2: Creation through an Associating Class

Use WHEN (a <<Target>> class exists in the current static view) AND (a <<Target>> is an associated attribute of other class(es))

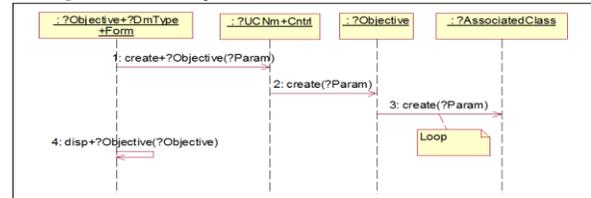


1. Input data from a viewer is passed to a controller

2. The controller delegates create() responsibility to a delegator of the target object.
3. The delegator creates a target object.

###### Create Data 3: Successive creation of Associated Classes

Use WHEN (a <<Target>> class exists in the current static view) AND (a <<Target>> has (an) object(s) other class (es) as (an) associated attribute(s))



1. Input data from a viewer is passed to a controller
2. The controller creates a target object.
3. The controller delegates creation of subordinate to the target object.
4. The target creates subordinates object(s) as many as defined.

#### 4. Consequences

A fragment of sequence diagram which is instantiated by the pattern conforms to the guidelines of the GRASP pattern. Thus, the instantiated design model can guarantee high cohesion and low coupling.

#### 5. Following Patterns

Confirm Data Manipulation, Transfer Data to Another System

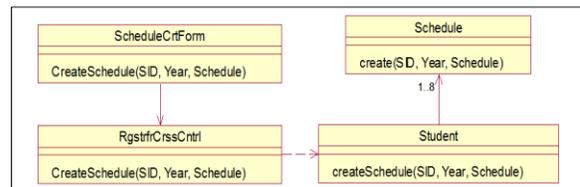
#### 6. Example

- The flow of Event: Create a Schedule

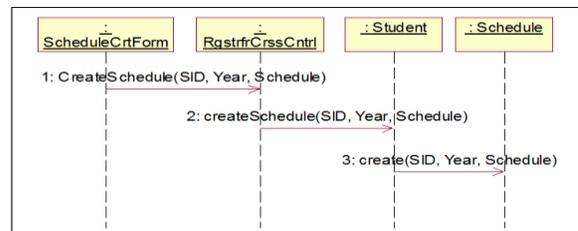
In the given conceptual model of a course registration system, Student class is associated with Schedule class. To compose a sequence diagram for the "creation of a schedule" flow, Create Data 3 is selected and applied. The values elicited from requirements are as the following:

Pattern Variable	Input Value
?Objective	"Schedule"
?AssociatingClass	"Student"
?UCNm	"RgstrfrCrss" (abbreviation of RegisterforCourses)
?DMType	"Crt"
?paramP4	"SID, Year, Semester"

The design model fragment resulting from applying to Create Data 3 is depicted in the following. The Student that is instantiated from ?AssociatingClass (Delegator) is the owner of createSchedule() responsibility and creates an instance of the Schedule which is instantiated from ?Objective(Target) class.



Instantiated Class Diagram for "Create a Schedule" Flow



Instantiated Sequence Diagram for "Create a Schedule" Flow

Fig. 5. CRA Pattern Specification: Create Data Pattern.

TABLE I. THE LIST OF THE CRA PATTERNS AND THEIR INTERACTIONS

Pattern	Interaction	Applicability
System Invocation (P1)	Invocation by User	Use when a user invokes a flow of events
	Invocation by System	Use when a software system periodically accomplishes a flow of events
Read Data (P2)	Read_Data_1	Use when all retrieved data items are attributes of ?objective class
	Read_Data_2	Use when(Retrieved data item(s) is(are) distributed into more than two classes) AND (there exist association relationships among the classes)
	Read_Data_3	Use when retrieved data item(s) which is(are) not attributes of ?objective class belong to the class(es) that has(have) no association relationship with ?objective class
	Read_Data_4	Use when retrieved data item(s) which is(are) not attributes of ?objective class belong to ?AssociatedClass class and the others belong to the class(es) that has(have) no association relationship with ?objective class
	Read_Data_5	Use when an ?objective class is an associated attribute of other class(es)
Transfer Data from Another System (P3)		Use when the reading data from another interface system is needed
Create Data (P4)	Create_Data_1	Use when an ?objective class does not exist in the current static view
	Create_Data_2	Use when (an ?objective class exists in the current static view) AND (an ?objective is an associated attribute of other class(es))
	Create_Data_3	Use when (an ?objective class exists in the current static view) AND (?objective has (an) object(s) other class (es) as (an) associated attribute(s) )
Update Data (P4)	Update_Data_1	Use when (an ?objective class does not exist in the current static view) OR ((an ?objective class exists in the current static view) AND (it is not the applicability of Update Data Pattern_2 and Update Data Pattern_3))
	Update_Data_2	Use when updated data item(s) that is(are) not an attribute(s) of ?objective class belong to ?AssociatedClass class
	Update_Data_3	Use when updated data item(s) which is(are) not an attribute(s) of ?objective class belong to the class(es) that has(have) no association relationship with ?objective class
Delete Data (P4)	Delete_Data_1	Use when (an ?objective class does not exist in the current static view) OR ((an ?objective class exists in the current static view) AND (it is not the applicability of Delete Data Pattern_2 and Delete Data Pattern_3))
	Delete_Data_2	Use when an ?objective class is an associated attribute of other class(es)
	Delete_Data_3	Use when (an ?objective class has another class as an associated attribute) AND (the relationship between the classes is an aggregation by value)
Confirm Data Manipulation(P5)		Use when an acquisition of higher leveled user for the reflection of data status changes is needed
Transfer Data to Another System(P6)		Use when the transformation of a data manipulation results to other system is needed

### V. CASE STUDY: BUILDING AN ANALYSIS MODEL USING CRA PATTERN LANGUAGE FOR A PAYROLL MANAGEMENT SYSTEM

The proposed CRA patterns impose many constants and parameters(variables) in participating classes' attributes and responsibilities, confusing unintimate readers. So, this paper will explain the details of each phase of adopting CRA patterns in building an analysis model from a scenario of a use case with a specific system, a payroll management system, rather than discuss with a set of general constants and variables. The chosen scenario of the payroll management system is the basic flow of "Select a payment method," as shown in Fig. 6.

#### A. Use Case Analysis

First, a set of generic questions is presented for applying the proposed CRA patterns, as shown in Table II. The developer answers the questions based on use case specifications and already defined key classes. Each question is used for the developer to select a set of appropriate fragmented patterns and identify parameter values in each CRA pattern.

- Q1~Q2: Questions for extracting the name of the target use case and flow of events.

This question is for composing the name of the sequence diagram from a flow of events in a use case specification. The blanks in the answer strings to Q1 and Q2 are excluded when used as values for pattern variables, '?UseCaseNm' and '?SeqNm'. For example, if the answer to Q1 is "Select Payment Method" and the answer to Q2 is "Basic Flow," the values for '?UseCaseNm' and '?SeqNm' are "SelectPaymentMethod" and "BasicFlow," respectively. Thus, the newly constructed sequence diagram name is "SelectPaymentMethod BasicFlow."

The value of variables, '?UCNm' and '?SDNm' are decided by excluding vowels from '?UseCaseNm' and '?SeqNm'. The values for '?UCNm' and '?SDNm' are used to name classes and operations.

- Q3: Question for selecting a type of the *System Invocation* patterns.

The available answers to the question Q3 are "Interactive Job" or "Batch Job." If the answer for Q3 is "Interactive Job," System Invocation by a user behavior is selected as the second segmented collaboration pattern. In that case, additional question Q3.1 is given to designate the active actor of the target flow of event. The answer to Q3.1 is denoted as an actor, as

described in Table II. If the answer to Q3 is “Batch Job,” System Invocation by a system behavior is selected, which describes a kind of automatic invocation of the target system according to predefined schedules. As it does not require an active actor, Q3.1 is skipped in this case.

The “Select payment method” flow is a kind of interactive job. Thus, the answer to Q3 is “Interactive Job.” According to the use case specification, the flow starts with an event from the Employee. The answer to Q3.1 is “Employee,” and it will be mapped to the active actor denoted as the pattern variable, ‘?humanRole’ of the sequence diagram.

- Q4~Q6: Questions to select proper *Manipulate Data* pattern and extract required values for pattern variables.

To realize a flow as a sequence diagram, not all of the CRUD operations are used. Depending on the event description of a use case, a different set of CRUD patterns are used. Questions Q4~Q6 are designed for developers to help determine the CRUD operations set and extract values of pattern variables.

## Use Case 5 : Select Payment Method

### 1. Brief Description

This use case allows an Employee to select a payment method. The payment method controls how the Employee will be paid. The Employee may choose to either: pick up his check directly, receive it in the mail, or have it deposited directly into a specified bank account.

### 2. Flow of Events

#### 2.1 Basic Flow

This use case starts when the Employee wishes to select a payment method.

1. The system requests that the Employee specify the payment method he would like (either : “pick up”, “mail”, or “direct deposit”).
2. The Employee selects the desired payment method.
3. If the Employee selects the “pick-up” payment method, no additional information is required.  
If the Employee selects the “mail” payment method, the system requests that the Employee specify the address that the paycheck will be mailed to.  
If the Employee selects the “direct deposit” method, the system requests that the Employee specify the bank name and account number.
4. Once the Employee provides the requested information, the system updates the Employee information to reflect the chosen payment method.

Fig. 6. Use Case Specification of “Select Payment Method.”

TABLE II. QUESTIONS AND ANSWERS FOR “SELECT PAYMENT METHOD” FLOW ANALYSIS

No	Generic Questions	Answer	Pattern Variable	Selected Pattern
FLOW LEVEL				
Q1	What is the Use Case Name?	“Select Payment Method”	?useCaseName	N/A
		“SlctPmntMthd”	?UCNm	
Q2	What is the name of the flow of events?	“BasicFlow”	?seqNm	N/A
		“SlctPmntMthdBsc”	?SDNm	
Q3	What is the job characteristic?	“Interactive Job”	invocationType	P1: Invocation by a User
Q3.1	If it is an interactive job, what is the name of the active actor?	“Employee”	?humanRole	N/A
DATA MANIPULATION LEVEL				
Q4	What is the data manipulation type? (select 1 among creation/read/update/deletion)	“Update Data”(Updt)	?DMType	P4: Update Data
Q5	What is the objective data of the data manipulation?	“Employee”	?objective	
Q6	What are the data items to be changed after this update?	“paymentMethod”	?paramP4	
Q7	Is there any other data for an <i>Employee</i> to retrieve for the update of the <i>paymentMethod</i> ?	“No”	needData	P2, P3 is not selected
Q8	Is the retrieved data located on another system? If it is, what is the system?	“No”	?interfaceSystem	P3 is not selected
Q9	To accomplish this flow of events, is it need to take any approval from someone?	“No”	NeedApproval	P5 is not selected
Q10	After completing this data manipulation, should the changed data be transformed to another system(s)?	“No”	NeedAnotherSystem	P6 is not selected

Q4 asks which data manipulation is needed to realize the target flow among creating/updating/deleting data. The abbreviation (Cr/Rd/Updt/Dlt) of the answer to Q4 is mapped to the value of the variable, '?DmType,' included in CRA patterns. After '?DmType' is designated, the next question, Q5, asks the objective of the designated data manipulation. The objective data of CRUD manipulation should be one of the key classes already given as an input artifact for building an analysis model. The next question, Q6, is applied only if the answer to Q4 is "Update Data." However, it does not mean that Q6 is differently designed according to the answer to Q4, in other words, the type of data manipulation. Q6 is designed to ask the property of the selected data manipulation. If the selected data manipulation type is "Delete Data," Q6 asks which property of the target class should be deleted. Therefore, while the answer of Q5 is one of the given key classes, the answer of Q6 should be one of the attributes in the selected class as the answer to Q5.

For example, in the case of the "Select payment method" flow of events, after all, the flow changes the value of the 'payment Method,' of the key class, 'Employee.' So, it is a kind of update manipulation. Thus, "Update Data" is the answer to Q4, and the abbreviation, 'updt,' is mapped as the value of '?DmType'. The objective data is the class, 'Employee.' The updated attribute is 'paymentMethod' as the answer to Q6, and it is mapped to the value of "?paramP4.'

- Q7: Questions to select *Read Data* pattern or not.

As depicted in Table II, for analyzing the "Select payment method" scenario, Q7 asks if an additional "Read Data(P2)" pattern is needed before the "Manipulate (Create/Update/Delete) Data" pattern. According to the given flow of events, the answer to Q7 is "No" as a user selects his preferred payment method without retrieving any additional data from the system. Consequently, the "Read Data(P2)" pattern is not selected to compose a sequence diagram.

However, in the case that require additional retrieving data before creating/updating/deleting data or the case that main flow is for retrieving data (answer to Q4 is "Read Data"), answering the additional questions Q7.1 and Q7.2 are needed for extracting data for the "Read Data" pattern. The additional questions Q7.1 and Q7.2 are specified in Table III. Those questions ask the name of retrieving data and the retrieval conditions.

- Q8: Questions to select *Fetch Data from Another System* pattern or not.

If the answer to Q7 is "Yes," the answer to Q8 is required. In applying Read Data(P2) pattern to compose a sequence diagram, one of the checkpoints is the location of the data to be retrieved. Suppose the data location is not the target system, message.

Sequences to request the data to the system that is the source of the retrieved data. The required collaboration with the other system is defined in Fetch Data from Another System(P3) pattern. Thus, in this case, the P3 pattern should be weaved with the already selected P2 pattern. For the given example scenario, selecting the P3 pattern is not considered

because it is not required to retrieve other data to update the payment method as the data resource is a user.

TABLE III. SUPPLEMENTAL QUESTIONS NOT APPLIED TO "SELECT PAYMENT METHOD" FLOW ANALYSIS

No	Generic Questions	Pattern Variable
Q7	Is there any other data for an '?humanRole' to retrieve to update the '?objective'?	?DmType
Q7.1	What is the name of the retrieving data?	?objective
Q7.2	What is the search condition for the retrieval of '?objective'?	?Condition
Q7.3	What are the retrieving attributes?	N/A
Q8	Is the retrieved data located on another system? If it is, what is the system?	?interface System
Q8.1	What data should be transferred from ?InterfaceSystem?	?objective
Q8.2	What is the search condition for the retrieval of ?objective?	?condition
Q9	To accomplish this flow of events, is it need to take any approval from someone?	NeedApproval
Q9.1	Who is responsible for the data confirmation?	?actorNm
Q10	After completing this data manipulation, should the changed data be transformed to another system(s)?	NeedAnotherSystem
Q10.1	What is the destination system of the data transfer?	?interface System
Q10.2	What is the additional data to be transferred except ?objective data?	?addData

- Q9: Questions to select *Confirm Data Manipulation* pattern or not.

If the answer Q4 is one of the "create/ update/ delete data," the Manipulate Data(P4) pattern is selected, question Q9 should be considered. Q9 asks if any approval is needed to save data manipulation results or not. As the given example, if it is required to get a confirmation from any actor after updating the payment method of an employee, the answer to Q9 should be "Yes," and Confirm Data Manipulation(P5) pattern will be selected. P5 pattern defines the message sequences to request confirmation to an actor responsible for the approval of the data manipulation and to approve it into the target system.

In the case of payment method update, however, it is not required any other confirmation to select the payment method of own Employee. So, the answer to Q9 is "No," and the P5 pattern will not be selected.

- Q10: Questions to select *Transfer Data to Another System* pattern or not.

The other question to be considered when Manipulate Data(P4) pattern has been selected is Q10. In some cases, changes in data in the target system should be reflected in another system. The change should be propagated to the data source system when the changed data source is not the target system but the other system. In that case, the data source system should already have been identified as a passive actor in the given use case model. The transformation of the changed data to the passive actor is defined in Transfer Data to Another System(P6) pattern. Q10 asks if the changed data should be

transformed to another system after the completion of data manipulation. The P6 pattern will be selected and weaved with the P4 pattern to compose a sequence diagram when the answer to Q10 is "Yes."

In the given example case, the changed data, "payment Method" is an attribute of the class, "Employee," saved in the target system itself. The answer to Q10 is "No." Consequently, the P6 pattern will not be selected.

### B. CRA Pattern Weaving

A set of CRA patterns necessary to implement the given flow is selected from among the six segmented CRA patterns by analyzing the given flow of the use case specification and answering each predefined generic question introduced above. Most CRA patterns define several variations in the assignment of responsibilities. As the result of the use case analysis step, the needed collaboration variation in each CRA pattern is selected.

Among CRA patterns, the Manipulate Data(P4) patterns define several interaction variations in each pattern, as shown in Fig. 5. Once a specific pattern is selected from the use case analysis step, proper interaction variation should be selected in several variations. The factor determining a specific interaction variation is the class's relationship to the '?objective' variable in the use case analysis stage has with other classes. The relationship between classes can be grasped through the conceptual class model.

Fig. 7 shows that UpdateData\_1 is selected among the three interaction variations of the Update Data (P4) pattern according to the predefined rule. As shown in Fig. 8, the '?objective' class (Employee) has the updated item '?paramP4'(paymentMethod) as its attribute. So, the

relationship between '?objective' class and '?associatedClass' or '?AssociatingClass' is not required to be considered. Thus, the condition highlighted by the red square is satisfied with the given relationship between the 'objective' class and the updated item, '?paramP4'. For this reason, UpdateData\_1 is finally selected.

In connecting two collaboration patterns, the most left one among the same lifelines in the two patterns is the connection point, and it is named as "weaving point." By overlapping the lifeline that becomes the weaving point, the two patterns are connected. While repeatedly weaving the selected patterns, the segmented CRA patterns are composed into a sequence diagram to realize the given flow of events.

Fig. 8 depicts the weaving of two patterns to compose a sequence diagram for the given example flow of events. The patterns selected according to the answers to each question described in Table II are Invocation by a User pattern in P1 pattern and Update Data\_1 collaboration pattern among P4 patterns. As shown in Fig. 8, the most left one among the object's lifeline commonly included in the two collaboration patterns is '?objective+?DMType+Form', which becomes a weaving point. The pattern variables marked with the prefix '?' still are denoted in the object names on the top of the diagram or the messages between lifelines as value assignment is not done in this step.

The 'invoke(param)'message in the Invocation by a User pattern is designed to be substituted by the first message in the firstly connected pattern to the Invocation by a User pattern. Therefore, the 'invoke(param)'message is substituted by 'update + ?objective (?paramP4)' in the weaved sequence diagram in the lower part of Fig. 8.

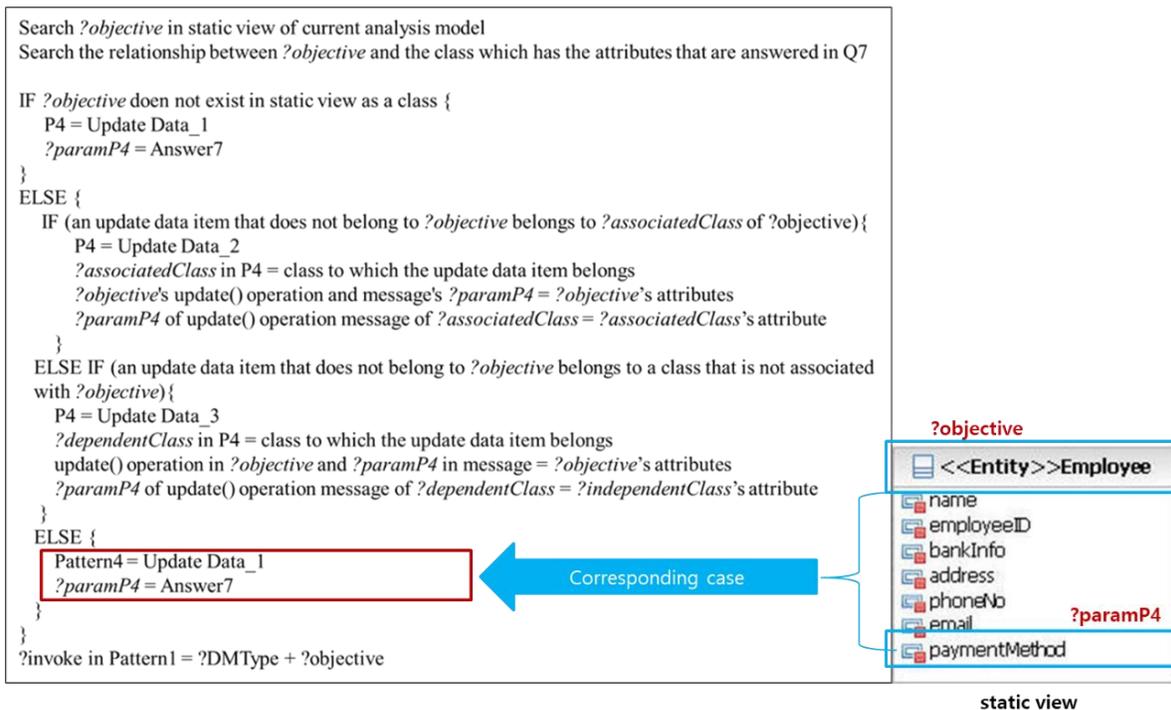


Fig. 7. Rule for Selecting an Interaction Variation in Update Data Pattern.

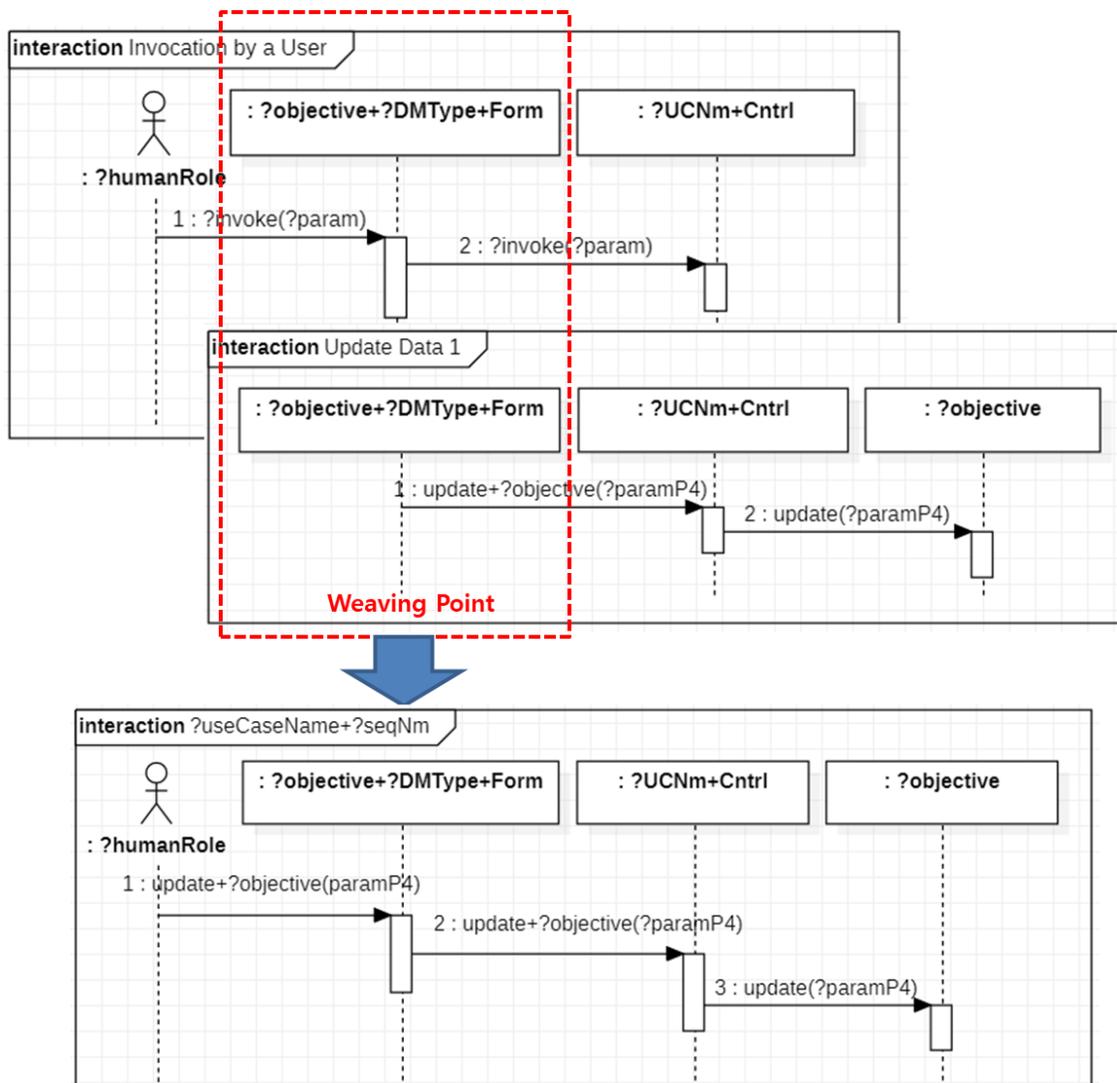


Fig. 8. An Example of CRA Pattern Weaving for Composing a Sequence Diagram for the “Select Payment Method” Flow.

### C. CRA Pattern Instantiation

The skeleton of the sequence diagram that realizes the given flow is completed through the CRA pattern weaving step. This step is called CRA pattern instantiation. The upper diagram in Fig. 9 is the weaved sequence diagram for the "Select payment method" flow. Although the sequence of messages is composed, uninstiated variable patterns exist in the names of an actor, lifelines, and messages. The values to be substituted for the pattern variables included in the skeleton of the sequence diagram are the answers to each question identified in the previous use case analysis step. For example, the name of the control class of this sequence is '?UCNm+Cntrl' is instantiated to 'SlctPmntMthdCntrl' because the extracted value of '?UCNm' is 'SlctPmntMth' according to the values in the table of use case analysis. In the same way, all the pattern variables are instantiated with the values in the table. As a result, the lower diagram in Fig. 9 is completed, with no uninstiated pattern variable.

The identified responsibility denoted on each message of the sequence diagram should be an operation of the class, which is the message's destination. The developer should keep the consistency between the static view represented by a class diagram and the dynamic view specified by a sequence diagram by adding the identified responsibilities to the proper classes as operations. Fig. 10 shows that the newly identified responsibilities in defining the sequence diagram for the "Select payment method" flow are added to the classes. In building the sequence diagrams with CRA patterns, the newly <<Boundary>>, and the <<Contoller>> stereotyped classes are additionally identified. Comparing the analysis model in Fig. 10 before and after the creation of the sequence diagram, it can be confirmed that the "<<Boundary>>EmployeeUpdtForm" class and the "<<Contoller>>SlctPmntMthdCntrl" extracted by the "Update Data" pattern are added to the analysis model.

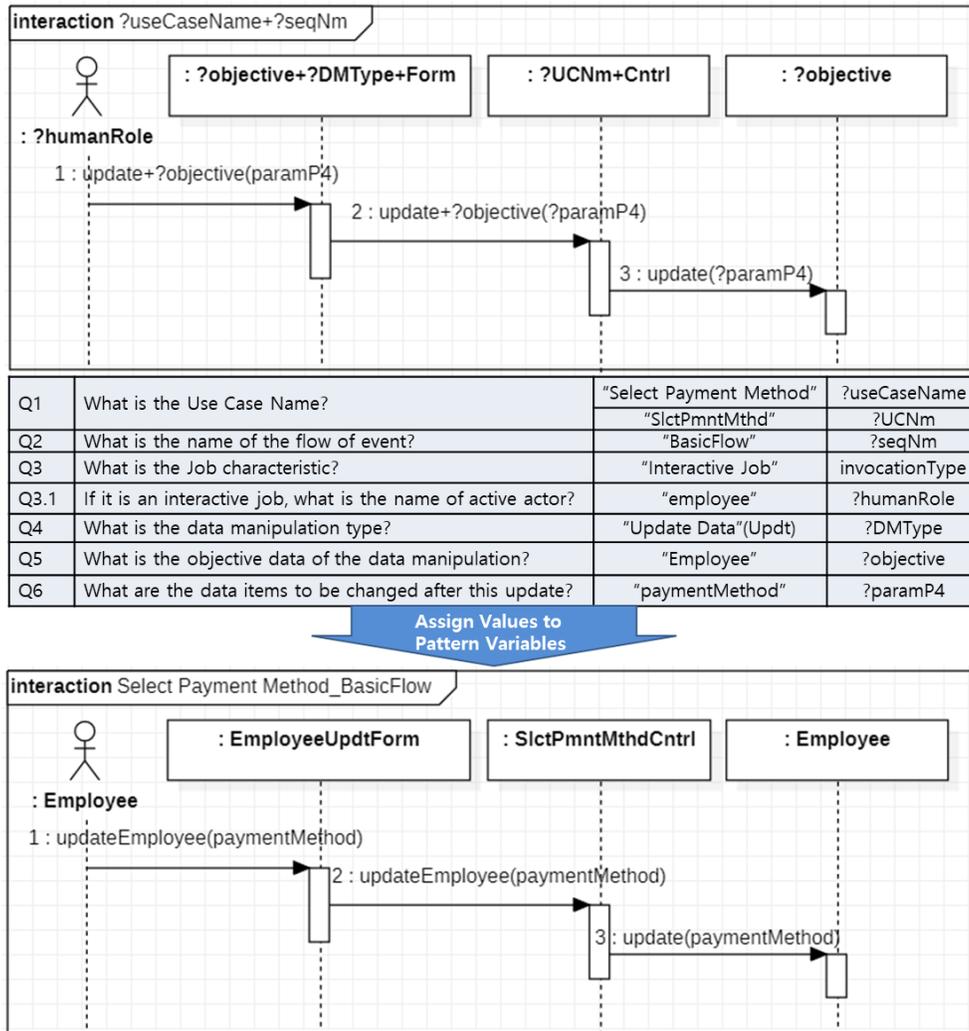


Fig. 9. An Example of CRA Pattern Instantiation to Build the Sequence Diagram for the "Select Payment Method" Flow.

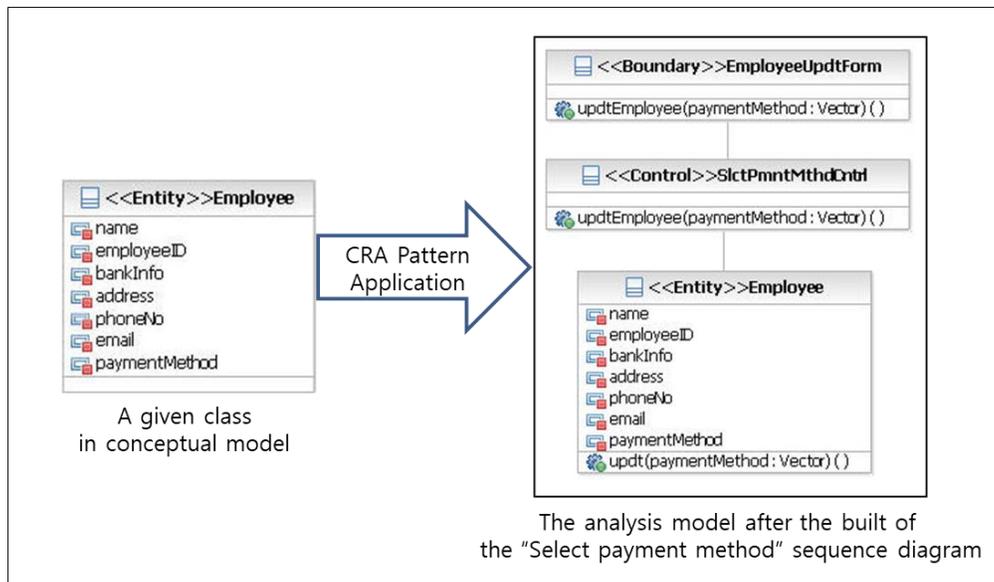


Fig. 10. The Changes of the Static View of the Payroll Management System.

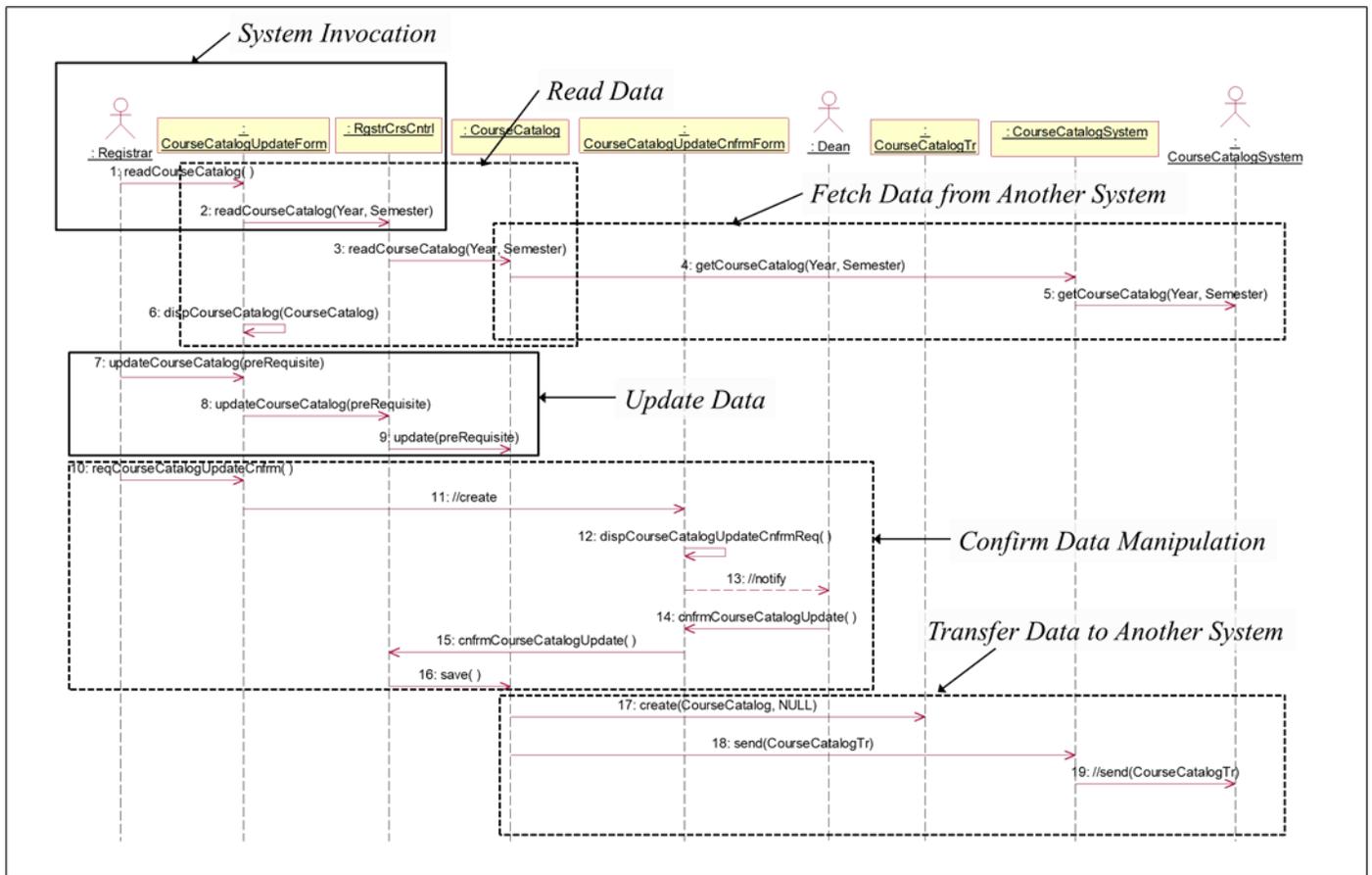


Fig. 11. Applying the six CRA Patterns in Building a Sequence Diagram: the Sequence Diagram for the "Register for Courses" Scenario of the Course Registration System.

D. An Example of Sequence Diagram Built by Applying All the Six CRA Patterns

In proving the feasibility of the proposed CRA patterns, it is necessary to show an example of the sequence diagram to apply all the six CRA patterns. However, unfortunately, in the payroll management system, the target system of this case study, there is no scenario to require all the six segmented CRA patterns. Thus, this study picked one of the scenarios of another system, the "Course Registration System," referenced as an example system in object-oriented analysis textbooks. The selected scenario is the basic flow of the "Register for courses" use case. By weaving the proper set of CRA patterns and instantiating pattern variables with the values from the use case analysis, the sequence diagram in Fig. 11 is built. Similar to the sequence diagram for "Select payment method", Fig. 11 is the sequence diagram with the two required CRA patterns: System Invocation pattern and Update Data pattern. However, in Fig. 11, all of the supporting CRA patterns are also participating. The responsibilities denoted on all messages have been identified from the application of the selected six CRA patterns. This example confirms that the flow composed of considerably long interactions can be realized by applying the proposed CRA pattern language.

VI. EVALUATION

Although the case study result shows the feasibility of the proposed CRA pattern language, it is needed to prove how much responsibilities could be extracted from system behaviors in use case specifications by utilizing it. First, this study applied the CRA pattern language to other scenarios in the use case specification of the payroll management system, besides the scenario presented as the case study in Section 5. Those scenarios realized by utilizing the CRA pattern language are: Select Payment Method / Maintain Timecard / Create Employee Report / Maintain Purchase Order / Create Administrative Report/ Maintain Employee Info / Run Payroll / Login.

TABLE IV. COMPARISON OF THE NUMBER OF ELEMENTS IN AN ANALYSIS MODEL

Elements #	Conceptual Model	Instantiated Model	Analysis Model
<b>Type</b>			
<b>Class</b>	7	35	38
<b>Operation</b>	0	44	51
<b>Attribute</b>	23	27	27
<b>Relationship</b>	6	37	42
<b>Total</b>	36	143	158

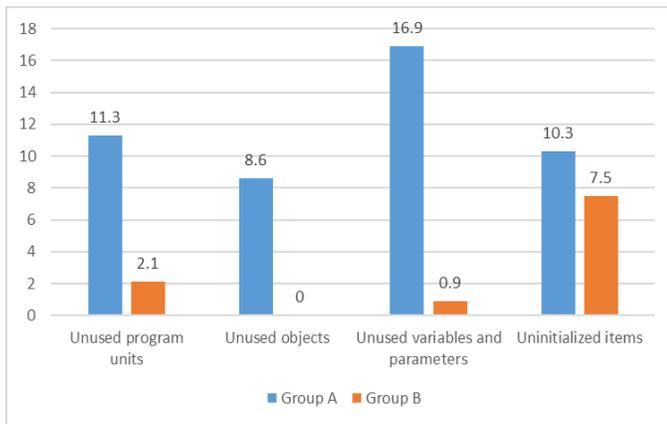


Fig. 12. Comparison of the Bad Symptoms Detected on the Implementation Code.

Table IV compares the number of identified operations (responsibilities) from the CRA pattern application on the scenarios above and the number of all operations in the finalized analysis model to prove the proposed CRA patterns' coverage. The number of design elements extracted purely by the CRA patterns is the value obtained by subtracting the # of elements of the conceptual model from the # of elements of the instantiated model in Table IV. The instantiated model refers to the model obtained as a result of pattern instantiation. The conceptual model is a model that is given as an input, including entity classes identified before applying the CRA patterns. The number of operations included in the conceptual model is 0. After that, the number of operations extracted through pattern application is 44, which is only seven less than 51 operations included in the model at the end of the analysis phase. It means that only seven operations that the developer additionally identified and added to the operation set. Other 86%  $((44-0)/51*100)$  of the class responsibilities of the entire analysis model were identified through CRA pattern application. Likewise, considering the number of whole elements, including classes and relationships, it can be confirmed that 67%  $((143-36)/158*100)$  of the elements are defined as the instantiation of the CRA pattern.

The fact that 67% of the elements of the entire analysis model can be extracted by applying uniform patterns means that, on another axis, 67% of the elements of the analysis model pose the same level of quality. Moreover, applying the proposed CRA patterns implies that GRASP guidelines like high cohesion and low coupling are assured. Thus, it implies that 67% of the analysis model built by the CRA patterns can provide a good and uniform quality even without a separate quality assurance task.

To confirm the effect of applying CRA patterns in the quality of the analysis model, we conducted a controlled experiment. The subjects who participated in the experiment were 4th-year undergraduate students who took the Object-Oriented Analysis and Design course. Students teamed up with 4-5 students to experience from identifying the requirements of the payroll management system to building the application. In constructing the analysis model, only 5 out of 10 teams (group A) provide only use case specifications. To the remaining five teams (group B), a questionnaire for identifying use case

specification, CRA pattern specifications, and pattern variables (Table II and Table III) was provided together. That is, in group A, students arbitrarily built an analysis model, and in group B, the CRA pattern language provided in this study was applied to build an analysis model. Both groups completed the development of their payroll management system for ten weeks.

For comparing the quality of the codes written by group B that applied the CRA pattern language to construct an analysis model and group A that did not apply the CRA pattern language, this study conducted static analysis on the implementation code using Understand [22]. As a result, as shown in Fig. 12, it can be confirmed that the number of detected bad symptoms of the source code is significantly smaller in group B than in group A. Among the bad symptom items, the notable result is the number of unused objects/variables and parameters, and those numbers of group B are close to 0. Since the analysis model is constructed by filling the pattern parameters defined in the given CRA patterns with the values extracted from the use case specification, there exists the effect of fundamentally preventing the inclusion of design elements that are not based on the requirements in the analysis model. It is the reason why the number of bad symptoms found in group B is minimal.

The benefits of the proposed CAR pattern language confirmed through the evaluation results can be summarized as follows. The CAR pattern language help that (1) a significant part of the analysis model can be completed by applying the CAR pattern language itself, and (2) developers with little design experience can also be expected to create an analysis model that guarantees consistent quality.

## VII. CONCLUSION AND FUTURE WORK

The assignment of responsibilities to classes is hard to teach and acquire in practice as many considerations should be taken. Several approaches are proposed to lessen heuristic factors and relieve the efforts to decide which responsibilities are required for a specific class. However, up to now, the existing works, regardless of the used technology, give too general assignment results or too many candidates for one responsibility for developers, which cannot reduce much effort in designing classes.

This study narrows the scope of the proposed CRA pattern language into the business application domain to solve the generality problems. It provides the responsibility assignments results not requiring further revision. The proposed CRA pattern language comprises the six segmented patterns, including several interaction variants according to the relationship format among the conceptual classes.

The six CRA patterns result from vertically decomposing one data transaction performed by a business application into one atomic sequence block. Manipulate Data patterns, which can be seen as the main pattern, contain several interaction variations that specify various collaboration aspects. While searching for the answer to the standardized question set for each flow described in the use case specification, the developers assign values to the variables existing in each pattern. The answers to the questions also determine the set of patterns needed to realize a given flow. The selected pattern

creates a sequence diagram while overlapping the lifeline corresponding to the predetermined weaving point, and this step is called pattern weaving. As a result of pattern weaving, the skeleton for one sequence diagram is completed, and instantiated sequence diagram can be obtained by substituting the values of pattern variables identified in advance.

This study shows the feasibility and the coverage of the proposed CRA pattern language in constructing an analysis model with a case study for constructing an analysis model of a payroll management system. In particular, the results showing that 67% of the operations identified in the final analysis model can be extracted only by applying the proposed CRA pattern proves the differentiation of this study. And, the enhancement of code quality shown through the designed experiment is another benefit of applying the proposed CRA patterns.

The questions for extracting information from use case specifications and the rules for selecting an interaction among the provided interaction variations in a CRA pattern are designed to consider the automation tool development. As for now, the development of the automation tool integrating with a UML authoring tool and Microsoft Word is under construction. With the automated tool, developers just select a proper word to answer a question from use case specifications written in Microsoft Word. And, then, automatically, a proper set of the CRA pattern will be selected, and each word selected by developers will substitute each pattern variable. Consequently, the sequence diagram will be created in a UML authoring tool automatically. Besides constructing the automated tool that supports the CRA patterns, we also plan to extend the case studies to more diverse applications.

#### REFERENCES

[1] D. Svetinovic, D. M. Berry, and M. Godfrey, "Concept Identification in Object-Oriented Domain Analysis: Why Some Students Just Don't Get It," in *Proceedings of the 13th IEEE International Conference on Requirements Engineering (RE'05)*, pp. 189-198, 2005.

[2] C. Larman, *Applying UML and Patterns: An Introduction to Object-Oriented Analysis and Design and Iterative Development*, 3rd Edition, Pearson Education India, 2004, pp.736.

[3] M. Bowman, L. C. Briand, and Y. Labiche, "Solving the Class Responsibility Assignment Problem in Object-oriented Analysis with Multi-Objective Genetic Algorithms," *IEEE Transactions on Software Engineering*, vol. 36, no. 6, pp. 817-837, 2010.

[4] G. Glavas, and K. Fertalji, "Metaheuristic approach to class responsibility assignment problem," in *Proceedings of the ITI 2011, 33rd International Conference on Information Technology Interfaces*, pp.591-596, 2011.

[5] M. Akiyama, S. Hayashi, T. Kobayashi, and M. Saeki, "Supporting Design Model Refactoring for Improving Class Responsibility Assignment," in *Proceedings of the ACM/IEEE 14th International*

*Conference on Model Driven Engineering Languages and Systems (MODELS 2011)*, pp. 455-469, 2011.

[6] E. Gamma, R. Helm, R. Johnson, and J. Vlissides, "Design Patterns: Elements of Reusable Object-Oriented Software," Addison-Wesley, 1995.

[7] M. Fowler, *Analysis patterns: reusable object models*, Addison-Wesley, vol. 10, pp. 357, 1997.

[8] S. Purao, V. C. Storey, and T. Han, "Improving analysis pattern reuse in conceptual design: Augmenting automated processes with supervised learning," *Information Systems Research*, vol. 14, no. 3, pp.269-290. 2003.

[9] M. E. Fayad, J. Rajagopalan, and A. Ranganath, *Stable Analysis Patterns: A True Problem Understanding with UML*, 2004.

[10] G. Shu-Hang, L. Yu-Qing, J. Mao-Zhong, G. Jing, and L. Hong-Juan, "A requirement analysis pattern selection method for E-business project situation," in *Proceedings of the IEEE International Conference on eBusiness Engineering ICEBE07*, pp. 347-350, 2007.

[11] X. U. Jin-song, and S. H. I. Lei, "Web application analysis pattern based on recursive MVC structure [J]," *Computer Engineering and Design*, vol. 12, 2005.

[12] H. S. Hamza, and M. E. Fayad, "The Negotiation Analysis Pattern," in *Proceedings of the EuroPLoP*, 2003.

[13] M. Bowman, L. C. Briand, and Y. Labiche, "Multi-Objective Genetic Algorithms to Support Class Responsibility," in *Proceedings of the 2007 IEEE International Conference on Software Maintenance*, pp. 124-133, 2007.

[14] C. Arora, M. Sabetzadeh, L. Briand, and F. Zimmer, "Extracting domain models from natural-language requirements: approach and industrial evaluation," in *Proceedings of the ACM/IEEE 19th International Conference on Model Driven Engineering Languages and Systems*, pp. 250-260, 2016.

[15] M. Elbendak, P. Vickers, and N. Rossiter, "Parsed use case descriptions as a basis for object-oriented class model generation," *Journal of Systems and Software*, vol. 84, no. 7, pp.1209-1223, 2011.

[16] V. B. R. V. Sagar, and S. Abirami, "Conceptual modeling of natural language functional requirements," *Journal of Systems and Software*, vol. 88, pp. 25-41, 2014.

[17] H. Masoud, and S. Jalili, "A clustering-based model for class responsibility assignment problem in object-oriented analysis," *Journal of Systems and Software*, vol. 93, pp.110-131, 2014.

[18] M. Albert, J. Cabot, C. Gómez, and V. Pelechano, "Automatic generation of basic behavior schemas from UML class diagrams," *Software & Systems Modeling*, vol. 9, no. 1, pp. 47-67, 2010.

[19] A. Leff, and J. Rayfield, "Programming model alternatives for disconnected business applications," *Internet Computing*, vol. 10, no. 3, pp. 50-57, 2006.

[20] M. Veit, and S. Herrmann, "Model-view-controller and object teams: A perfect match of paradigms," in *Proceedings of the 2nd international conference on Aspect-oriented software development*, pp. 140-149, 2003.

[21] R. T. V. Braga, R. Ré, P. C. Masiero, and C. C. Mourão, "A Process to Create Analysis Pattern Languages for Specific Domains," in *Proceedings of the SugarLoafPLoP*, 2007.

[22] Understand. Available at: <https://www.scitools.com/> (accessed 25/08/2021, 2021).

# Implementing Flipped Classroom Strategy in Learning Programming

Rosnizam Eusoff, Syahanim Mohd Salleh, Abdullah Mohd Zin  
Center for Software Technology and Management  
Universiti Kebangsaan Malaysia  
Bangi, Malaysia

**Abstract**—Novice students encountered many difficulties and challenges when learning to program. They face problems in terms of high cognitive load in learning and lack of prior programming knowledge. Various strategies and approaches are implemented to overcome the difficulties and challenges in programming. A flipped classroom is an active learning strategy implemented in many subjects and courses, including programming. The flipped classroom strategy consists of three phases, namely, pre-class, in-class, and post-class. A focus group discussion is conducted involving 13 participants from various learning institutions. The purpose of the study is to discuss the implementation of flipped classroom strategy in programming. The study also identifies a technique for monitoring students' involvement in activities outside the classroom and proper motivation to engage students in programming. Related research questions are constructed as guidelines for the discussion. The deductive thematic analysis is performed on the transcripts of the discussion. As a result, four pre-determine codes and two codes were generated from the analysis. This study identifies suitable activities, tools, monitoring strategies, and motivation to support the implementation of a flipped classroom in programming. There is good potential through flipped classrooms in learning programming with a systematic and careful planned implementation.

**Keywords**—*Flipped classroom; learning programming; cognitive load; active learning; focus group discussion*

## I. INTRODUCTION

Programming is a complex subject that requires high concentration and focuses from the students. The process of learning programming requires a tremendous amount of exposure to understand the logic in each programming solution using the basic concepts despite the overwhelming syntax it might carry [1][2]. Novice students in learning the subject face difficulties and challenges. Challenges and difficulties are identified through studies in programming [3]–[7]. Among the challenges in programming are high cognitive workload [1][8], inappropriate learning strategies, time constraints, and lack of preparation before entering the classroom [2][9]. Novice students with limited knowledge need a strategy or method to help them in programming [10][11]. Active participation of the students in the learning process is one of the essential aspects of learning programming [12][13]. The difficulties experienced by students in learning can be attributed to the passive role played by them during traditional lectures [14].

Among the new strategies used in programming is flipped classroom (FC), where lecturers employ this strategy in the

learning session to enhance and improve the student learning experience [14]–[16]. The main advantages of FC are providing students with prior knowledge and preparing them before class; give extra learning time; experience active and collaborative learning in class, and strengthening the understanding of new knowledge and skills after class [17]–[19]. There are three phases of the learning process in the FC, namely pre-class, in-class, and post-class. Pre-class activities focus on theory, initial information, and preparation before entering the classroom. In-class sessions emphasize active learning activities for developing new knowledge and skills. Active learning requires students to engage in meaningful learning activities in class [20]. At the same time, post-class activities focus on strengthening knowledge and skills. Programming involves various cognitive activities and structures of multiple skills to learn [21]. FC can create a new learning environment with a practical session and enhance students' learning experience [22]. FC also enhances student satisfaction and their level of engagement in learning [23]. Besides, the implementation of FC also positively impacts students' self-efficacy and intrinsic motivation [24]. In a traditional classroom, educators allocate ample time to convey information to students to read and learn the information by themselves.

On the other hand, FC promotes pre-class activity whereby some knowledge is learned before class. This situation will give sufficient classroom time to lecturers as some of the topics are covered during the pre-class activity. Thus, lecturers can utilize the extra classroom time to focus more on impactful learning activities in programming [25]. The use of FC in programming strategy is reported to be more effective at the tertiary institution level than at the school level. Although more research on FC is increasingly conducted by researchers for various subjects [26], implementing FC in programming is not much discussed in the reports [27]. Instructors who want to use FC in their learning need to understand the implementation strategies to ensure the method's success and achieve its objectives [28]. In this regard, there is a need to conduct more research in FC [23], especially studies that describe the implementation of FC in programming.

## II. METHODOLOGY

Researchers have utilized a focus group discussion (FGD) technique to obtain qualitative data, which involved discussions in small groups [29]. FGD is a suitable technique for generating new ideas compared to individual interviews

because the participants can brainstorm ideas during the ongoing discussion [30]. Besides, the FGD method is an excellent option to understand the views and opinions of others regarding the discussed subject [31]. Further, FGD is a flexible method that can be performed in a variety of conditions. There are seven steps of FGD involved in this study, as listed in Fig. 1.

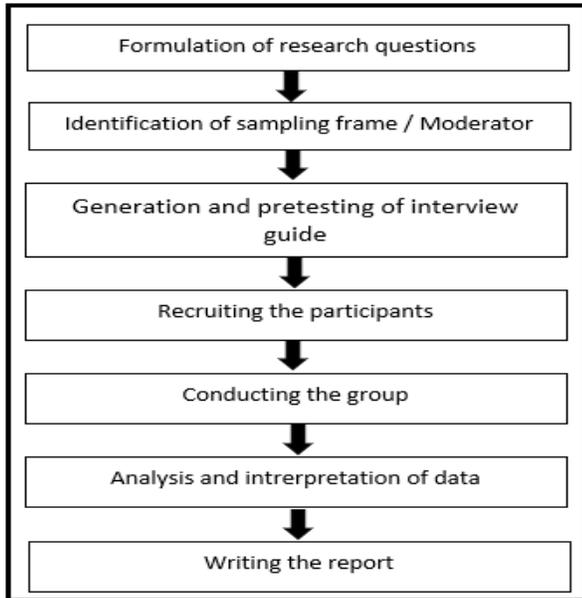


Fig. 1. Steps in Conducting a Focus Group Discussion Study. Adapted from [32], "Focus Groups Theory and Practice," p. 50.

#### A. Research Questions

A good research question (RQ) will guide the implementation of the study to be smoother and more efficient. Four research questions are posed in this study as follows:

RQ 1. What are the appropriate activities to implement FC strategy in programming?

RQ 2. What are the suitable tools that can support FC strategy in programming?

RQ 3. How to monitor students' participation in FC activities outside the classroom?

RQ 4. How to motivate students in learning programming?

#### B. Participants

The implementation of FGD requires two critical elements; the recruitment of participants and the design of the interview guide [32]. Research questions in the study are used as the design of the interview guide. Next, the researchers conducted a pilot test involving five participants. The purpose of the pilot test is to identify the weaknesses and provide improvements to the actual FGD. According to [33], the appropriate number of FGD is about six to twelve participants. The optimal time for each session is between one to two hours. Participants in the FGD are 13 senior lecturers who have been experienced in teaching programming at institutions of higher learning in Malaysia for about 12 to 32 years. According to [34], teachers with five to seven years of teaching experience can be considered expert teachers. FGD is conducted online by using

Zoom application. Participants were split into two groups to facilitate the online discussion effectively. The first group discussion was attended by six participants, and the second group was accompanied by seven participants.

#### C. Transcribing and Member Checking

The recording of the discussion is transcribed in a clean verbatim manner. Participants checked the transcript for the member checking process. Submission of the transcripts to the respective participants improves the accuracy of the data [35]. Furthermore, the checking process permits the participants to confirm or deny the interpretation made by the researchers on the views and suggestions of the participants during the discussion [36].

#### D. Coding and Analysis

Code is the smallest unit of analysis with exciting features about the data considered relevant to the research question. The data contained in the transcript is in the form of excerpts generated from the discussion. There are four predefined codes at the initial stage of the analysis process: Activity, Tools, Monitoring, and Motivation code. Two additional codes are produced when the analysis process is carried out, namely Learning Strategy and Evaluation. In total, there are 232 passages produced from the transcripts. Learning Strategy code has 91 passages which is the code that has the highest passages.

Meanwhile, the Activity code consists of 53 passages, and the Tools code consists of 36 passages. The Motivation code consists of 31 passages, while the Monitoring consists of 15 passages. Lastly, the Evaluation code consists of 6 passages. Thematic analysts are used to analyzing these coded passages. Thematic analysis analyses and translates qualitative data to form a specific theme [37].

### III. FINDINGS

#### A. Activities to Implement FC Strategy in Programming

In general, the findings in this section are made through passages grouped under the Learning Strategies, Activity and Motivation codes. As mentioned, FC comprises three phases, namely pre-class, in-class, and post-class. The learning activities involved can be regarded as the same or slightly different for each of these phases. However, students may encounter issues when learning to program in FC strategy. The problems are caused by students' failure to understand FC requirements. Hence, during the first face-to-face class meeting with the students, a sufficient explanation regarding the implementation of FC in learning should be given to the students. Students are informed about the three essential phases involved in FC: pre-class, in-class, and post-class. In the early stages of the course, students must participate in the learning session and eliminate their anxiety about programming. Lecturers can share exciting videos about programming with students in the class as a first insight for them. "The first topic is crucial to attracting students to programming. If students think that the first topic is difficult, most probably, students will have problems engaging with other topics. Students should not be addressed with difficult questions, but instead, the lecturer may opt for intermediate questions when asking questions to the respective students."

Ensuring students' participation in learning activities outside the classroom is the biggest challenge the educators face when implementing FC strategy [38]–[42]. A participant suggested that allocation of marks should be given to students who are actively involved in the pre-class and post-class activities. According to the participant, extra marks will motivate students to engage in activities outside the classroom actively. Thus, lecturers should consider allocating marks for students who show good involvement during the pre-class and post-class activities. This initiative will attract students' interest and boost their motivation in the learning process. "From my experience all this while, students will only do extra assignments outside class if there are only marks given for those assignments. I believe some extra marks will motivate them well."

Although students may view videos about programming online, lecturers need to guide their students on which video they should watch. A meaningful learning environment should be created as much as possible in learning activities. For example, the teacher should design the questions and problems based on students' daily life experiences, such as using ATMs and vending machines or developing a smartphone application's software. Most students have anxiety based on the information they have obtained about the difficulties of programming. "Lecturers need to create a meaningful learning environment for students. These novice students may have zero knowledge of programming. Most of them are worried about programming."

Programming is known as one of the subjects that has a high percentage of failures among students. The learning activities in programming should gradually develop students' skills from easy to challenging levels. The aim for each activity will focus only on one new skill so that students will not experience a high cognitive load. In the early stages of learning, students are exposed to videos from various sources to inform them about the importance of programming and its application in daily life. The video viewing activities can also be assigned to students as pre-class activities. Next, as in the class session, students are divided into several groups, and they are asked to discuss the videos they have watched and present the results of their discussions in class.

Lecturers can prepare several sets of questions for the students to discuss in their groups. Every two groups will receive a similar question for discussion. Then, each group should present the results of the meeting to all. Through this method, two different solutions can be generated from the same question. Based on this, students will be able to perceive that a problem that occurs in programming has various solutions. Post-class activities focus on exercises and tasks to strengthen students' new knowledge and skills. As a guide, the lecturer may provide students with examples of complete solutions to the assigned questions. Next, students will receive questions that are similar to the given example as post-class activity. Students can refer to the provided examples as a guide to answer the questions. These activities can be assigned as individual or group assignments. Thus, students will not feel burdened to carry out post-class activities through this method, especially for challenging problems.

### *B. Suitable Tools to Support FC in Programming*

The findings in the section are based on passages grouped under the Tools and Motivation codes. In supporting a learning process, lecturers can incorporate myriad choices of tools and supporting materials. Hence, to implement the FC strategy in the learning session, lecturers must prepare and choose suitable tools and learning materials for the class, especially for the pre-class and post-class activities, as the lecturer's supervision is absent. Video is the most widely used material in FC at the pre-class level [39]. The videos can be self-produced by lecturers or taken from various sources on the internet, such as YouTube. The optimum period for video viewing is between five to ten minutes [39] [43]. An appropriate video screening period will ensure that students are not burdened with such activity. Lecturers may assign quizzes or short questions to students while watching the video or after finishing the video. The task will ensure that students will pay attention to the details in the video as they need to answer the quiz or short questions. Besides that, lecturers can provide the students with a worksheet to record the pre-class and post-class activities. These worksheets can also be used to assess students' involvement in activities and class discussions. The worksheets are applicable in a lab, so students can use them to mark errors they have encountered while running a program.

Apart from providing students with questions, lecturers can ask students to look and solve the problems by themselves. The problem-solving tasks can be regarded as project work. For example, students are asked to identify the business needs of specific companies through the company's advertising catalogue. Students must identify the problem and suggest a solution using programming. In the early stages, lecturers can help students by providing ideas and input. Once students already have solid knowledge, they are encouraged to figure out their solutions without the intervention of the lecturer. The use of infographic notes should be given priority on technical topics in programming. The infographic form notes are easier to understand than text notes, especially in specialized topics such as control structures, arrays and method. "After the introduction topic, I think infographic notes are more suitable to be used because it will be easier for students to see the whole process in programming through infographics as compared to usual text-based notes."

### *C. Monitoring Students' Participation in FC*

The discussion of the findings in this section is based on the passages grouped under the Monitoring and Evaluation codes. Class management is a critical aspect of a physical classroom, while learning materials are essential online [44]. The biggest challenge in FC is to ensure that student engagement in activities outside the classroom [38][45]. The outside classroom's activities will occur without supervision from lecturers. In this situation, lecturers can measure students' involvement in the pre-class activities by judging students' responses in the class. Usually, students who have prepared before class will be more ready and able to answer questions while in-class compared to students who don't prepare. At the beginning of class, lecturers can ask some questions that are related to the pre-class activity. Students who have not completed their pre-class activities will be unable to answer the question. Monitoring students' involvement in activities is also

more accessible through a LMS platform such as Moodle. Log-in records into the LMS can be regarded as proof of students' participation outside of the classroom. A short quiz can be embedded in the video to ensure students will watch the entire video without skipping. In this way, students are required to watch the whole video to answer the quiz.

Besides, monitoring also can be done by students themselves in group activities. Every group has an appointed leader, and the leader is responsible for reminding the group members about the assigned task. Most of the students are more receptive to reprimands from their peers compared to lecturers. "From my experience, students have more of a sense of guilt towards their friends than lecturers. Most of their daily life is with their friends in the hostel. They would be embarrassed if they did not participate in the activities with their group."

Monitoring students' involvement in pre-class and post-class activities is vital in the implementation of the FC strategy. However, participants' opinion that students should be allowed to do activities outside the classroom at their convenience. In this regard, lecturers need to determine the appropriate monitoring method to be applied to the students accordingly. The most important thing is to make sure students carry out the activities they should do and complete outside the classroom.

#### D. Motivating Students in Learning Programming

The discussion of this section's findings is based on the passages grouped under the Motivation and Evaluation codes. Motivation is a crucial element in determining success in learning. Successful students are usually students who are highly motivated in their learning. Researchers have conducted various studies that show a connection between motivation and success in learning programming [5][46][47]. The different approaches and strategies introduced in the learning increase student motivation and make programming more exciting and relevant to real-life situations [48]. There are two types of motivation: intrinsic motivation from internal factors and extrinsic motivation from external factors [49]. Most of the motivational methods that are given to students are extrinsic forms of motivation. However, the best motivation is the intrinsic type of motivation, which comes from the students themselves. However, intrinsic motivation can also be developed from extrinsic motivation. For example, when students always achieve high marks in tests or quizzes, their interest in programming will subsequently increase, and this is where intrinsic motivation will indirectly appear. A study by [41], found that at the early stages of the implementation of FC in learning, students are more motivated to do assignments or quizzes as activities outside the classroom. These two activities are considered as extrinsic motivation for students. Gradually, intrinsic motivation will be formed when students are motivated to engage with any FC's activities outside the classroom. The success of new approaches in learning will occur if students are instilled with more intrinsic motivation. Lecturers also need to constantly motivate students about the importance of programming in student's daily lives. However, based on experience, most students will carry out activities directed by their extrinsic motivation. For example, students will only complete an assignment when they are informed that the marks will be awarded for the work. In this regard, it is

advisable if the allocation of marks is given for outside classroom activities. "My experience with students so far, if they knew there would be no marks for an activity, they would not do it."

As the most crucial factor in determining the success of flipped classroom strategies introduced to students, the motivational element needs attention in learning. Lecturers need to be creative in finding suitable methods to increase the motivation of their students.

#### IV. DISCUSSION

In general, FC is a technology-based strategy in providing early exposure to students outside the classroom. Students, in turn, will gain in-depth exposure during the classroom session [50][51]. Comparison of four learning strategies used in [52] study has found that FC strategy produced students with best performance achievement compared to other strategies. There are various methods of FC strategies that can be implemented in the learning process. The main goal of the FC strategy is to provide students with ample learning time and the opportunity to gain early exposure to the learning content before the class session [53]. The use of FC strategies does not mean eliminating the role of the instructor or any form of direct instruction that occurs in a learning process. Instead, this strategy maximizes meeting time between instructor and student with strategic activities that have a higher impact on learning programming. FC can also meet the individual needs of different students without having to reduce the material and filling in the learning [54]. According to [51], students who received FC exposure are more sensitive to their learning processes than students exposed to the traditional strategy. Several essential elements need to be presented in the FC implementation model for programming. The main elements are strategic planning of activities according to the FC phases, preparation of appropriate tools for learning activities, and an effective monitoring strategy for outside classroom activities. Student motivation is a key element in determining the success of the FC strategy used. Therefore, lecturers need to provide motivation to attract students to programming. Intrinsic motivation is best, although it is quite difficult to establish in the student. However, extrinsic motivation can turn into intrinsic motivation gradually as students begin to take an interest in programming. A flipped classroom model in programming is illustrated in Fig. 2.

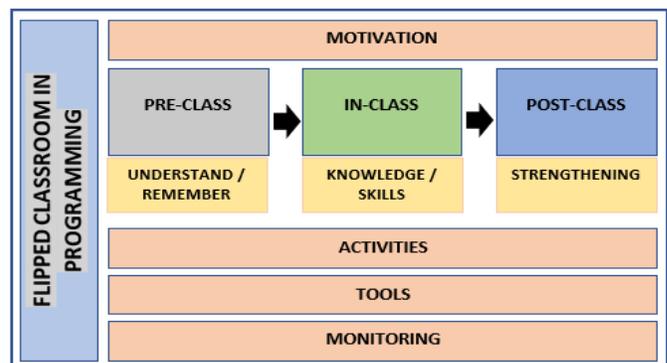


Fig. 2. A Flipped Classroom Model in Programming.

## V. CONCLUSION

There are myriad advantages gained through the implementation of FC in learning programming. Among the benefits are that students will be well prepared before entering the classroom as they must conduct a pre-class activity. This condition will aid the learning process in the classroom to be more efficient because students are equipped with basic knowledge. An extra-time earned can be used to conduct strategic active and collaborative learning in the classroom. The main goal of FC is to create a student-centred active learning environment. The lecturer only serves as a moderator who monitors the learning activities in the classroom. Post-class activities will focus on strengthening new knowledge that has been learned in class. However, the implementation of this FC strategy needs to be planned carefully and strategically to get the full advantage of this strategy.

## ACKNOWLEDGMENT

The authors acknowledge Universiti Kebangsaan Malaysia and the Ministry of Education Malaysia for their support. This study was funded by the UKM Research Grant (GGPM-2020-027).

## REFERENCES

- [1] S. M. Salleh, Z. Shukur, and H. M. Judi, "Scaffolding Model for Efficient Programming Learning Based on Cognitive Load Theory," *Int. J. Pure Appl. Math.*, vol. 118, no. 7 Special, pp. 77–82, 2018.
- [2] K. M. Yusoff, N. S. Ashaari, T. S. M. T. Wook, and N. M. Ali, "Validation of the Components and Elements of Computational Thinking for Teaching and Learning Programming using the Fuzzy Delphi Method," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 1, pp. 80–88, 2021.
- [3] S. M. Shuhidan, M. Hamilton, and D. D'Souza, "Understanding novice programmer difficulties via guided learning," *Proc. 16th Annu. Jt. Conf. Innov. Technol. Comput. Sci. Educ. - ITiCSE '11*, p. 213, 2011.
- [4] B. Özmen and A. Altun, "Undergraduate Students' Experiences in Programming: Difficulties and Obstacles," *Turkish Online J. Qual. Inq.*, vol. 5, no. 3, pp. 9–27, 2014.
- [5] A. Gomes and A. Mendes, "A teacher's view about introductory programming teaching and learning: Difficulties, strategies and motivations," *Proc. - Front. Educ. Conf. FIE*, vol. 2015-Febru, no. February, 2015.
- [6] Y. Qian and J. Lehman, "Students' Misconceptions and Other Difficulties in Introductory Programming," *ACM Trans. Comput. Educ.*, vol. 18, no. 1, pp. 1–24, 2017.
- [7] M. Rahmat, S. Shahrani, R. Latih, N. F. M. Yatim, N. F. A. Zainal, and R. A. Rahman, "Major Problems in Basic Programming that Influence Student Performance," *Procedia - Soc. Behav. Sci.*, vol. 59, pp. 287–296, 2012.
- [8] R. Duran, J. Sorva, and S. Leite, "Towards an analysis of program complexity from a cognitive perspective," *Proc. 2018 ACM Conf. Int. Comput. Educ. Res. - ICER '18*, pp. 21–30, 2018.
- [9] E. Lahtinen, K. Ala-mutka, and H.-M. Jarvinen, "A Study of the Difficulties of Novice Programmers," *ACM ITiCSE'05*, pp. 14–18, 2005.
- [10] F. Layth Khaleel, N. Sahari Ashaari, and T. S. M. Tengku Wook, "An Empirical Study on Gamification for Learning Programming Language Website," *J. Teknol.*, vol. 81, no. 2, 2019.
- [11] A. R. Mohamad Gobil, Z. Shukur, and I. A. Mohtar, "Novice difficulties in selection structure," *Proc. 2009 Int. Conf. Electr. Eng. Informatics, ICEEI 2009*, vol. 2, no. August, pp. 351–356, 2009.
- [12] S. B. Ho, S. L. Chean, I. Chai, and C. H. Tan, "An Assessment of Learning Content Model for Introductory Programming in Higher Education," *ASM Sci. J.*, vol. 14, no. 1, pp. 55–62, 2021.
- [13] C. Stöhr and T. Adawi, "Flipped Classroom Research: From 'Black Box' to 'White Box' Evaluation," *Educ. Sci.*, vol. 8, no. 1, p. 22, 2018.
- [14] M. N. Giannakos, J. Krogstie, and D. Sampson, "Putting Flipped Classroom into Practice: A Comprehensive Review of Empirical Research," *Digit. Technol. Sustain. Innov. Improv. Teach. Learn.*, pp. 27–44, 2018.
- [15] S. R. Sobral, "Flipped classrooms for introductory computer programming courses," *Int. J. Inf. Educ. Technol.*, vol. 11, no. 4, pp. 178–183, 2021.
- [16] K. Thongkoo, P. Panjaburee, and K. Daungcharone, "Integrating inquiry learning and knowledge management into a flipped classroom to improve students' web programming performance in higher education," *Knowl. Manag. E-Learning*, vol. 11, no. 3, pp. 304–324, 2019.
- [17] J. L. Jensen, E. A. Holt, J. B. Sowards, T. Heath Ogden, and R. E. West, "Investigating Strategies for Pre-Class Content Learning in a Flipped Classroom," *J. Sci. Educ. Technol.*, vol. 27, no. 6, pp. 523–535, 2018.
- [18] W. Kelly, "Flipping the Classroom to Solve the Time Problem," 2017. [Online]. Available: [https://flippedlearning.org/flexible\\_environment/flipping-classroom-solve-time-problem/](https://flippedlearning.org/flexible_environment/flipping-classroom-solve-time-problem/). [Accessed: 20-Nov-2018].
- [19] J. Herala, A. Vanhala, E. Knutas, A., & Ikonen, "Teaching programming with flipped classroom method: a study from two programming courses," *15th Koli Call. Conf. Comput. Educ. Res.*, pp. 165–166, 2015.
- [20] B. Sohrabi and H. Iraj, "Implementing flipped classroom using digital media: A comparison of two demographically different groups perceptions," *Comput. Human Behav.*, vol. 60, pp. 514–524, 2016.
- [21] R. P. Medeiros, G. L. Ramalho, and T. P. Falcao, "A Systematic Literature Review on Teaching and Learning Introductory Programming in Higher Education," *IEEE Trans. Educ.*, pp. 1–14, 2018.
- [22] K. Siripongdee, P. Pimdee, and S. Tuntiwongwanich, "A blended learning model with IoT-based technology: Effectively used when the COVID-19 pandemic?," *J. Educ. Gift. Young Sci.*, vol. 8, no. 2, pp. 905–917, 2020.
- [23] G. Akçayır and M. Akçayır, "The flipped classroom: A review of its advantages and challenges," *Comput. Educ.*, vol. 126, no. January, pp. 334–345, 2018.
- [24] T. N. T. Thai, B. De Wever, and M. Valcke, "The impact of a flipped classroom design on learning performance in higher education: Looking for the best 'blend' of lectures and guiding questions with feedback," *Comput. Educ.*, 2017.
- [25] J. Elmaleh, "Improving Student Learning in an Introductory Programming Course Using Flipped Classroom and Competency Framework," in *IEEE Global Engineering Education Conference, EDUCON, 2017*, no. April, pp. 49–55.
- [26] C. K. Lo and K. F. Hew, "A critical review of flipped classroom challenges in K-12 education: possible solutions and recommendations for future research," *Res. Pract. Technol. Enhanc. Learn.*, vol. 12, no. 1, p. 4, 2017.
- [27] Hendrik and A. Hamzah, "Flipped Classroom In Programming Course: A Systematic Literature Review," *Int. J. Emerg. Technol. Learn.*, vol. 16, no. 2, pp. 220–236, 2020.
- [28] Z. Turan and B. Akdag-cimen, "Flipped classroom in English language teaching: a systematic review Flipped classroom in English language teaching: a systematic review," *Comput. Assist. Lang. Learn.*, vol. 0, no. 0, pp. 1–17, 2019.
- [29] A. J. Onwuegbuzie, W. B. Dickinson, N. L. Leech, and A. G. Zoran, "A Qualitative Framework for Collecting and Analyzing Data in Focus Group Research," *Int. Inst. Qual. Methodol.*, pp. 1–21, 2009.
- [30] R. L. Breen, "A practical guide to focus-group research," *J. Geogr. High. Educ.*, vol. 30, no. 3, pp. 463–475, 2006.
- [31] S. Wilkinson, "Focus group methodology: a review," *Int. J. Soc. Res. Methodol.*, vol. 1, no. 3, pp. 181–203, 1998.
- [32] D. W. Stewart and P. N. Shamdasani, *Focus Groups Theory and Practice*, Third. SAGE Publications Inc, 2014.
- [33] A. Nili, M. Tate, and D. Johnstone, "A framework and approach for analysis of focus group data in information systems research," *Commun. Assoc. Inf. Syst.*, vol. 40, no. December, pp. 1–21, 2017.

- [34] D. C. Berliner, "Expert Teachers : Their Characteristics , Development and Accomplishments," pp. 13–28, 2001.
- [35] L. Birt, S. Scott, D. Cavers, C. Campbell, and F. Walter, "Member Checking: A Tool to Enhance Trustworthiness or Merely a Nod to Validation?," *Qual. Health Res.*, vol. 26, no. 13, pp. 1802–1811, 2016.
- [36] A. G. Candela, "Exploring the function of member checking," *Qual. Rep.*, vol. 24, no. 3, pp. 619–628, 2019.
- [37] V. Clarke and V. Braun, "Thematic analysis," *J. Posit. Psychol.*, vol. 12, no. 3, pp. 297–298, 2017.
- [38] A. Mohamed, "Designing a CS1 Programming Course for a Mixed-Ability Class," in *WCCCE '19*, 2019, pp. 10–15.
- [39] T. Ishak, R. Kurniawan, Z. Zainuddin, and C. M. Keumala, "The role of pre-class asynchronous online video lectures in flipped-class instruction : identifying students ' perceived need satisfaction," *J. Pedagog. Res.*, pp. 1–11, 2019.
- [40] Y.-H. Chang, A.-C. Song, and R.-J. Fang, "Integrating ARCS Model of Motivation and PBL in Flipped Classroom: a Case Study on a Programming Language," *EURASIA J. Math. Sci. Technol. Educ.*, vol. 14, no. 12, 2018.
- [41] V. Gupta, "Blended SPOC Teaching and Learning Model for Computer Programming Course: Insights and Defeating Challenges," *IEEE TALE2020 - An Int. Conf. Eng. Technol. Educ.*, pp. 251–257, 2020.
- [42] H. Y. Durak, "Modeling Different Variables in Learning Basic Concepts of Programming in Flipped Classrooms," *J. Educ. Comput. Res.*, 2019.
- [43] K. Zeuch, S. Kaven, and V. Skwarek, "Evaluation of a re-designed introductory course " Programming in C " with video support," in 2019 18th International Conference on Information Technology Based Higher Education and Training (ITHET), 2019, pp. 1–6.
- [44] F. A. Albrahim, "Online Teaching Skills and Competencies," *TOJET Turkish Online J. Educ. Technol.*, vol. 19, no. 1, pp. 9–20, 2020.
- [45] H. Y. Durak, "Flipped learning readiness in teaching programming in middle schools : Modelling its relation to various variables," *J. Comput. Assist. Learn.*, no. July, pp. 939–959, 2018.
- [46] S. Alhazbi, "Using flipped classroom approach to teach computer programming," *Proc. 2016 IEEE Int. Conf. Teaching, Assess. Learn. Eng. TALE 2016*, no. December, pp. 441–444, 2016.
- [47] S. Nikolic, M. Ros, and D. B. Hastie, "Teaching programming in common first year engineering: discipline insights applying a flipped learning problem-solving approach," *Australas. J. Eng. Educ.*, pp. 1–12, 2018.
- [48] R. A. Alturki, "Measuring and improving student performance in an introductory programming course," *Informatics Educ.*, vol. 15, no. 2, pp. 183–204, 2016.
- [49] E. L. Deci and R. M. Ryan, "Self-determination theory: A macrotheory of human motivation, development, and health," *Can. Psychol.*, vol. 49, no. 3, pp. 182–185, 2008.
- [50] J. L. Bishop and M. A. Verleger, "The Flipped Classroom A Survey Of The Research," in 120th ASEE Annual Conference & Exposition, 2013.
- [51] J. F. Strayer, "How learning in an inverted classroom influences cooperation, innovation and task orientation," *Learn. Environ. Res.*, vol. 15, no. 2, pp. 171–193, 2012.
- [52] N. T. T. Thai, B. De Wever, and M. Valcke, "The impact of a flipped classroom design on learning performance in higher education: Looking for the best 'blend' of lectures and guiding questions with feedback," *Comput. Educ.*, vol. 107, pp. 113–126, 2017.
- [53] C. E. Davenport, "Evolution in Student Perceptions of a Flipped Classroom in a Computer Programming Course," *J. Coll. Sci. Teach.*, vol. 47, no. 4, pp. 30–35, 2018.
- [54] N. Hamdan, P. McKnight, K. McKnight, and K. M. Arfstrom, "A Review of Flipped Learning," vol. 15, no. 5, pp. 86–87, 2013.

# High Density Impulse Noise Removal from Color Images by K-means Clustering based Detection and Least Manhattan Distance-oriented Removal Approach

Aritra Bandyopadhyay<sup>1</sup>, Kaustuv Deb<sup>2</sup>, Atanu Das<sup>3</sup>, Rajib Bag<sup>4</sup>

Department of Computer Science and Engineering<sup>1,2</sup>

Supreme Knowledge Foundation Group of Institutions, Chandannagar, India<sup>1,2</sup>

Department of Masters of Computer Applications, Netaji Subhash Engineering College, Kolkata, India<sup>3</sup>

Principal, Indas Mahavidyalaya, Bankura, India<sup>4</sup>

**Abstract**—Removal of impulse noise from color images is a stringent job in the arena of image processing. Impulse noise is fundamental of two types: Salt and pepper noise (SAPN) and Random valued impulse noise (RVIN). The key challenge in impulse noise removal from color images lies in tackling out the randomness in the noise pattern and in handling multiple color channels efficiently. Over the years, several filters have been designed to remove impulse noise from color images, but still, the researchers face a stringent challenge in designing a filter effective at high noise densities. In this study, a combination of K-means clustering-based detection followed by a minimum distance-based approach for removal is taken for high-density impulse noise removal from color images. In the detection phase, K-means clustering is applied on combined data consisting of elements from designated  $5 \times 5$  windows of all the planes from RGB color images to segregate noisy and non-noisy elements. In the removal phase, noisy pixels are replaced by taking the average of medians of all non-noisy pixels and non-noisy pixels under  $7 \times 7$  windows residing at least Manhattan distance from the inspected noisy pixel. Performance of the proposed method is evaluated and compared up against the latest filters, on the basis of well-known metrics, such as Peak signal to noise ratio (PSNR) and Structural similarity index measurement (SSIM). Based on these comparisons, the proposed filter is found superior than the compared filters in removing impulse noise at high noise densities.

**Keywords**—Impulse noise; color image; salt and pepper noise; random valued impulse noise

## I. INTRODUCTION

Digital images are susceptible to be corrupted by noise while in transmission. There are certain procedures involved in image registering which captures the digital images by multi sensor imaging. During this type of image acquisition, transmission and recording events, different type's noise [1] can be incorporated into images. One of the noise types is impulse noise, which affects images by generating fixed or random changes in the pixel's intensities in the range of '0' to '255'. These sudden intensity changes not only degrade the images but also hamper the successive image processing

procedures like morphological processing, segmentation, object recognition etc. Impulse noise is of two types: salt and pepper noise (SAPN) [2] and random valued impulse noise (RVIN) [3]. Both the types of noises disturb the homogeneity of the pixel's intensities of images. Salt and pepper noise is categorized as fixed valued impulse noise, as it creates sudden dots in images by '0' (pepper noise) and '255' (salt noise) intensities. Due to these fixed but sudden fluctuations in pixel's intensities produces spikes in images. It may be possible that some '0' and '255', which are actual values may reside in the images. Those are either edge or texture pixels. On the other hand, random valued impulse noise degrades the images in arbitrary ways. RVIN can have any changed value in the range of 0 to 255. It is very tough to remove both the noise categories as it needs efficient detectors to find impulse-noise-like pixels and a removal mechanism to remove those noises without impeding the minute features of the images.

Fundamentally, a lot of filters [1 – 3] have been designed for removing impulse noise from grayscale images, but occasionally there are filters [1 - 23] designed for color images. The challenges in dealing with the multiple color panels and emulating a solution that integrates all those said channels have laid the way for further researches in this field. In this paper, an amalgamation of k-means clustering oriented detection trailed by least distance-based removal method is proposed for high density impulse noise removal from color images. The different clustering methods are found to be doing generously well in noise detection. It sorts out the noisy pixels effectively by applying K-Means clustering on each window of color images and the replacement of the noisy pixel is being performed by the combined average of non-noisy pixels at minimum distance from the designated noisy pixel and median of all detected non-noisy pixels within a certain window. Typically, the proposed work accentuated its superiority in producing excellent qualitative and quantitative outcome at high noise densities; however it yields moderate performance at low noise densities. Investigational results show the preeminence of the proposed method over the other recent methods.

The next section is oriented as follows. Section II exemplifies the literature review part. Section III illustrates the proposed methodology consisting of a detection algorithm followed by a removal algorithm. In Section IV, results of the proposed work are portrayed and discussed all over. The paper ends with a Section V on conclusion.

## II. LITERATURE REVIEW

Over the years, several linear and non-linear filters [1-24] were projected to remove impulse noise from grayscale and color images. The linear noise removal filters followed the convolution procedure with a window of coefficients. Later non-filters were proposed, out of which the median filter was the most popular one. The filter used median operation of surrounding pixels to restore every pixel which produced blurry outputs. But, in the restoration procedure, subtle features of images were lost. In the upcoming years adaptive median filters [4, 5] and weighted median filters [7, 8] were proposed. In those filters adaptive and weighted pixel-oriented approaches were taken respectively. Moreover, only the noisy pixels were restored leaving out the non-noisy ones. This approach created a revolution in image restoration. One of the established traditional switching filters among those, having the similar approach with boundary discriminative noise detection [4] created massive impact in the noise restoration arena. It was later reformed by amending with elimination tactics to form BDNDE [5]. Challenges came with designing noise restoration for color images as the complexity of the images increased with different color panels having diverse intensities. In a very recent approach, a switching filter [6] with fast processing speed was designed. The filter used the analogous neighborhood pixels in least distance as a measure of precipitateness and the replacement of noisy pixels were done by a practical fast processing switching algorithm.

Vector median filter (VMF) [7] was one of the most proven filters, having effective noise removal capability for color images by using vector median approach for reinstatement operation. It was improvised later, amalgamated with center weighted approach to form Center Weighted Vector Median Filter (CWVMF) [8]. With further research, an adaptive non-causal linear prediction-based vector median filter [9] was designed based on adaptive error prediction-oriented approach which was a further advancement of the VMF. Recently, another modification was performed on VMF where the researchers came up with an idea to integrate adaptive VMF with weighted median filter method [10]. This approach was equally effective at both low- and high-density noises. In vector median filtering approach [11] another used quaternion depiction to find out color distances based on which the filter classified noisy and non-noisy pixels using four directional criteria. That was followed by weighted median filter for removal operation. This approach was improvised with the previous filter's upgradation [12] by using a weighted adaptive approach in the quaternion depiction for finding out more justified color distances which, thereby vividly enhanced the outcomes. One more adaptive vector median filter (ANCLPVMF) [13] was proposed in the similar timeframe which used the concept of linear estimation to calculate error components and thereby compare it with a defined threshold to sort out noisy pixels. The removal phase used an adaptive

VMF for carrying out replacement of detected noisy pixels. Quaternion approach became popular as it combined three color planes into a single unit. Here, a rank-based approach [14] was proposed in recent times using quaternion theory which had segregated noisy pixels by rank criteria, along with edge detection mechanism and thereafter substituted those noisy pixels by weighted vector median filter. In the meantime, a relatively new filter [15] came up with a thought-provoking awareness by using statistical Moran's I (MI) index for noise detection operation, which was followed by VMF for carrying-out noise removal activity. In the same time, a support vector machine (SVM) oriented fuzzy filter [16] has been proposed. The approach used SVM in training phase and thereby, the testing phase segregated noisy and non-noisy pixels. Thereafter, fuzzy filtering was applied on the noisy pixel elements in removal operation. In the category of fuzzy filters, histogram fuzzy color (HFC) filter [17] was introduced where the association amid the planes was measured to estimate the original histogram and thereby rebuild the image by fuzzification. This approach was revised in Modified HFC [18] to scale up the performance for both RVIN and SPN. It was further restructured by using support vector machine-based approach to produce Multiclass support vector machine adaptive filter (MSVMAF) [19]. In the equivalent period an adaptive iterative fuzzy filter (AIFF) [20] was proposed that worked based on a trimming approach which created a new insight in fuzzy filtering. Among the recent approaches [21], a fuzzy averaging oriented noise detection and removal was carried out where detection was based on fuzzification of renowned ROD statistics and removal mechanism followed a thresholding based fuzzy oriented noise removal. In most recent times a method used deep convolution neural network for impulse noise removal. The method [22] first trained a classifier for noise detection and it was followed by putting the noise detected images into a denoiser for carrying out denoising operation. In current times a new filter [23] was designed which has used trimmed median filter, decision based median filter and unsymmetric trimmed mean filtering in circumstances based on the impulse values. The combined effect of those filters shaped virtuous outcome.

## III. PROPOSED METHODOLOGY

In this paper, it has been primarily concentrated on removal of high-density impulse noise from RGB color images. An amalgamation of k-means clustering based noise detection tactic followed by a minimum distance-oriented removal mechanism is portrayed here (see Fig. 1 and 2). A  $5 \times 5$  window is used here in the detection trailed by a  $7 \times 7$  window in removal method to process the whole image pixel wise. These local windows are formed by centering each designated pixels in the image. Let us define the center pixel as  $C_{m,n}$  and the window by  $WD_{5 \times 5}$ . Then the window criterion is outlined like below where:

$$WD_{5 \times 5} = [C_{row, col}], \text{ where } m - 2 \leq row \leq m + 2, n - 2 \leq col \leq n + 2$$

Here  $C_{row, col}$  denotes all the pixel elements under the local window where each of those pixels have corresponding red, green and blue components, well-defined in RGB color images.

### A. Detection Method

In the beginning of the detection procedure, red, green and blue planes are extracted from the input noisy RGB color image (CLIM). A binary flag matrix FCLIM of the same size as the RGB image CLIM is created and is filled by '0'. The center pixel of a window is denoted as CE and its intensity is denoted as  $PINT_{CE}$ . The proposed detection algorithm is applied on each  $5 \times 5$  window shaped surrounding the pixels obeying window criteria residing at each of the red, green and blue planes independently.

1) Primarily the designated local  $5 \times 5$  window elements are skimmed and put into an array. By this process, the respective  $5 \times 5$  window elements of each red, green and blue plane are stored in three independent arrays ARYRED, ARYGREEN, ARYBLUE.

2) The elements of each of the above defined three arrays are chronologically put into three successive columns to form a new  $3 \times 25$  matrix MATRGB. Thereby the 1st, 2nd and 3rd column of MATRGB represents ARYRED, ARYGREEN, ARYBLUE elements in unchanged order.

3) K-Means clustering method has been employed on MATRGB having combined data from each red, green and blue plane. K-Means clustering would engender four different clusters  $Cl_1, Cl_2, Cl_3, Cl_4$  and group the analogous elements having similar properties into an equivalent cluster. K-Means clustering is performed on combined data to get the overall impact of a particular pixel at identical position on the red, green, blue planes and thereby putting the designated pixel into a proper cluster. The work is primarily focused on detecting random valued impulse noise affected pixel elements from noisy images. This implies that the noisy pixel elements of despoiled images are having random or arbitrary intensity value, whereas the non-noisy pixel elements have non-arbitrary values. So, after the application of K-Means algorithm on the combined data there is more likelihood that the non-noisy pixels having similar properties are likely to fall in the same cluster, while the noisy pixels, having dissimilar properties will be falling in random clusters.

4) The cluster having maximum number of elements is marked as maximum cluster (MC). The maximum cluster is most likely to be formed by non-noisy elements, as the non-noisy pixels having homogenous properties are most likely to fall in a same cluster although the noisy pixels having heterogeneous properties are likely to be scattered in different clusters. So, there is a mere chance for the randomized noisy pixels to group together to form a superlative cluster that can surpass a non-noisy element-contained cluster based on the component count.

5) All the elements in the maximum cluster are marked as non-noisy and the corresponding marked pixels intensities in the flag image FCLIM is filled by '0' and others are filled by '1'.

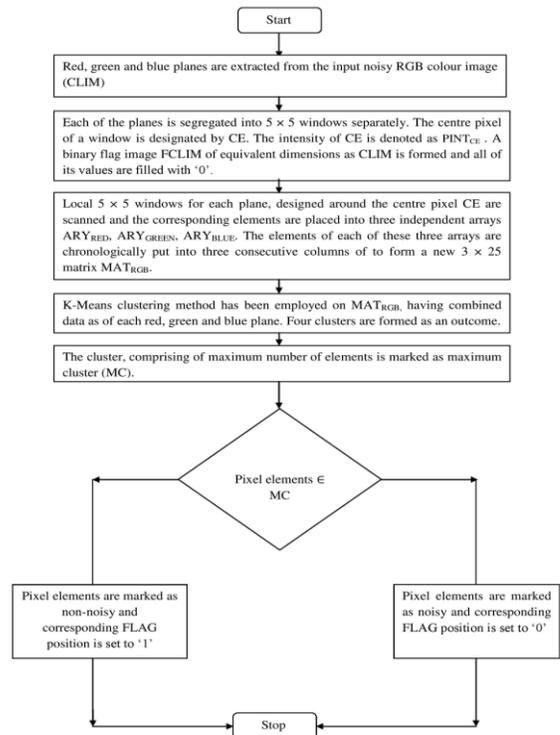


Fig. 1. Flowchart of Noise Detection Methodology.

### B. Removal Method

In the noise removal process, the output flag image FCLIM is segregated into  $7 \times 7$  windows, where each window's center element CE is noisy.

The following section portrays the removal algorithm for individual windows:

1) Primarily, for each  $7 \times 7$  window, the detected non-noisy pixels are kept on an array DRR. Instantaneously the array is sorted in ascending order to find out the median MD. The median value can effectively take part in the removal procedure as it brings out the overall impact of all of the non-noisy pixels in the DRR array. Furthermore, as the median value is a part of the non-noisy array, it can be more effective in removal.

2) Then, the non-noisy pixel or pixels in the DRR, partaking least Manhattan distance from the noisy center pixel CE is or are accumulated. Manhattan distance is calculated by taking the absolute difference between the center noisy pixel CE and the designated non-noisy pixel. If only such one-pixel value or multiple non-noisy values is or are present at minimum distance, then that value or those values are accrued in an array MDRR.

3) In a  $7 \times 7$  window, the maximum Manhattan distance possible is 6, whereas the minimum Manhattan distance possible is 1. Let DS be the Manhattan distance from CE. DS is initialized to 1. If any non-noisy pixel or pixels is or are found at DS from CE, then that or those non-noisy pixel or pixels are put in MDRR and we stop. If no non-noisy pixel is found at

DS, then DS is incremented and again non-noisy pixel or pixels is or are tried to be found. This process of finding non-noisy pixel at least distance is carried out up to the DS value of 6, until found. By this procedure, MDRR is formed with the non-noisy pixel or pixels at a least Manhattan distance of DS from CE.

4) Finally, the pixel intensity of center noisy pixel CE is replaced by using the equation below:

$$PINT_{CE} = \frac{(MD + \sum_{i=1}^n MDRR[i])}{1 + n}$$

Here, n is the number of elements in MDRR.

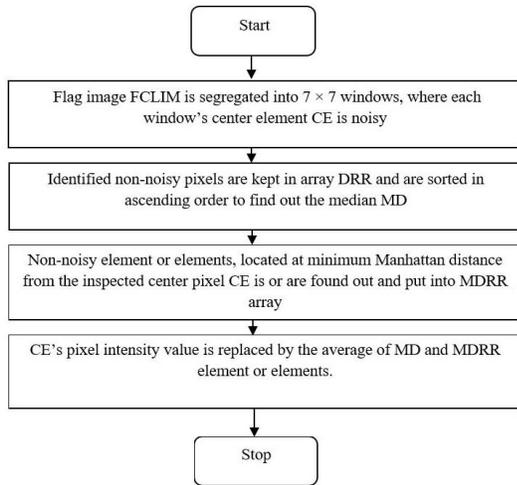


Fig. 2. Flowchart of Noise Removal Methodology.

MDRR[i] is the  $i^{th}$  element in MDRR.

#### IV. RESULT AND DISCUSSION

This section portrays the simulation results of the proposed method executed in MATLAB R2018a installed on a Windows PC having core i5 processor and 8 GB of RAM. Experiment has been carried out on 10 color test images at various noise densities for both salt and pepper and random valued impulse noise. Experimental results of 4 images: Lena, Baboon, Tower and Barbara, out of those 10 test images are shown in this paper. Seven different filters have been compared against the proposed filter at various noise densities. Qualitative results are portrayed by three figures. Two images: Lena and Baboon are used to show visual output and comparison of the proposed filters in contrast to different filters. Peak signal to noise ratio (PSNR) and Structural similarity index measurement is used to measure the quantitative performance of the proposed filter.

Visual performance of the proposed filter is portrayed by two established test images: Lena and Baboon. The filter has been tested on 20 images but only these two images are shown in this paper. Fig. 3 displayed the qualitative performance comparison of the proposed filter with the existing established recent filters in terms of Baboon image and from the said Fig. 3 it is pertinent that the proposed filter outpaced the compared state-of-the-art filters with respect to habitual human viewpoint. The performance variety of the proposed filter is

depicted in Fig. 4 and Fig. 5 using standard Lena image. The proposed filter is tested on both salt and pepper and random valued impulse noise effected images. Fig. 4 and Fig. 5 interpret the visual output of the proposed filter at diverse noise densities on the Lena image affected by RVIN and SAPN respectively. From the visual perspective, the proposed filter has shown notable result for both the types of impulse noise patterns. Quantitative performance of the proposed filter is judged by Peak signal to noise ratio and Structural similarity index measurement. Definition of Peak signal to noise ratio (PSNR) in 'dB' is demonstrated below:

$$PSNR = 10 \log_{10} \frac{255^2}{MSE} \quad (1)$$

$$MSE = \left( \sum_{A,B} \frac{\sum_{A,B} (Bi(a,b) - De(a,b))^2}{A \times B} \right) \quad (2)$$

Here, Bi = Base Image, De = De-noised image, A = Count of rows, and B = Count of Columns.

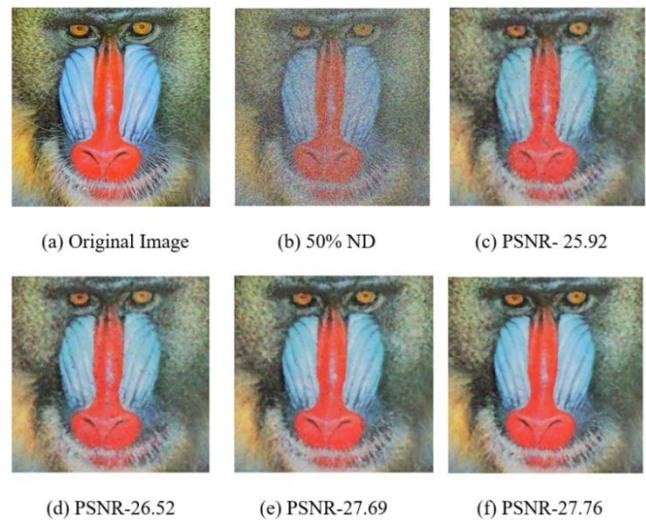


Fig. 3. Visual Performance Comparison of Proposed Filter Outcome against Recent Filters for Baboon Image in Terms of RVIN.

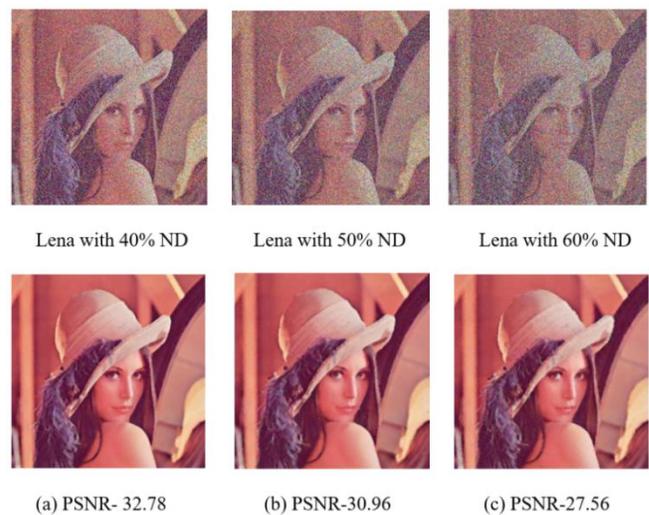


Fig. 4. Visual Performance of Proposed filter at Varied Noise Densities for Lena Image in Terms of RVIN.

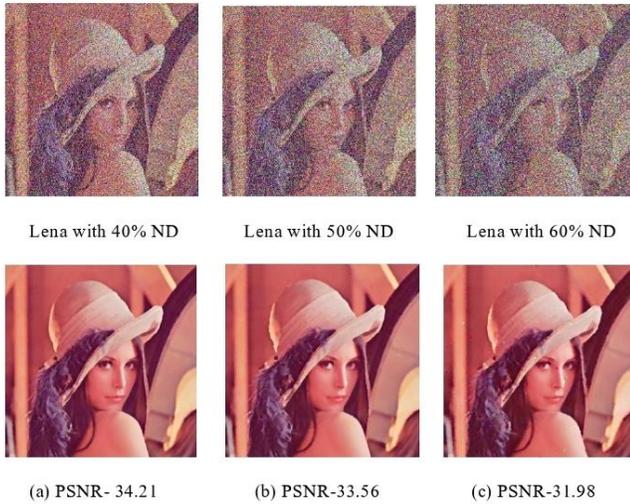


Fig. 5. Visual Performance of Proposed Filter at Varied Noise Densities for Lena Image in Terms of SAPN.

The structural semblance amid the base and restored image is quantified by Structural similarity index measurement (SSIM) and is defined as follows:

$$SSIM(i, j) = \frac{(2\Phi_i + \Phi_j + C_1)(2\beta_{ij} + C_2)}{(\Phi_i^2 + \Phi_j^2 + C_1)(\beta_i^2 + \beta_j^2 + C_2)} \quad (3)$$

Here,  $\Phi_i$  and  $\Phi_j$  are the mean of image  $i$  and image  $j$  correspondingly. The standard deviation of image  $i$  and image  $j$  is portrayed by  $\beta_i$  and  $\beta_j$  correspondingly.  $C_1, C_2$  are the defined constants.  $\beta_{ij}$  is the co-variance of  $i$  and  $j$ .

Table I assesses the proposed filter’s efficiency by means of PSNR for both RVIN and SAPN for standard Lena image. These two noise patterns create fixed and random dots on images thereby generating distorted images. The proposed algorithm takes care of both the noise patterns effectively as shown in Table I. Some recent filters are compared to the proposed filter to showcase its competence. It can be seen that at various noise densities, especially at higher noise densities the filter works superior to the recent reputable filters.

TABLE I. COMPARISON OF DIFFERENT FILTERS WITH PROPOSED FILTER IN TERMS OF PSNR (DB) FOR LENA IMAGE

Noise	Filters	Noise Density		
		40% ND	50% ND	60% ND
SAPN	HFC [17]	37.47	25.82	22.25
	BDND [4]	25.04	24.80	24.12
	BDNDE [5]	27.77	27.23	26.12
	AIFF [20]	30.11	29.58	27.72
	MHFC [18]	38.83	30.63	24.82
	MSVMAF [19]	34.10	30.69	25.52
	CAVMFWMF [10]	37.44	34.63	31.92
	ROY [16]	30.54	28.43	26.38
	CHANU [14]	32.54	31.56	29.61
	GREGORI [21]	29.21	28.04	27.33
	KARTHIK [22]	31.49	31.01	30.53
	PROPOSED	34.21	33.56	31.98

RVIN	VMF [7]	25.20	23.60	22.80
	CWVMF [8]	18.72	16.51	14.92
	HFC [17]	27.32	26.12	24.35
	MSVMAF [19]	31.92	28.76	24.84
	MHFC [18]	28.05	25.66	22.29
	SINGH [9]	32.14	30.27	26.43
	CAVMFWMF [10]	34.44	30.71	26.34
	MALINSKI [6]	31.35	29.58	27.56
	JIN [11]	28.54	26.58	24.72
	JIN [12]	32.67	30.58	27.19
	ANCLPVMF [13]	32.21	30.32	26.65
	MIVMF [15]	28.86	26.58	24.69
	ROY [16]	30.09	27.65	26.03
	GREGORI [21]	28.67	27.64	25.71
	ZHANG [22]	32.68	29.40	27.21
	PROPOSED	32.78	30.96	27.56

TABLE II. PERFORMANCE EVALUATION OF PROPOSED FILTER UP AGAINST RECENT FILTERS IN TERMS OF SSIM FOR DIFFERENT IMAGES

Noise	Image	Noise Density	Filters		
			MHFC [18]	CAVMFWMF [10]	PROPOSED
SAPN	Lena	10%	0.9942	0.9905	0.9901
		30%	0.9793	0.9809	0.9794
		50%	0.9016	0.9586	0.9612
		80%	0.2567	0.8178	0.8235
	Baboon	10%	0.9893	0.9811	0.9804
		30%	0.9759	0.9699	0.9679
		50%	0.9012	0.9485	0.9495
		80%	0.2426	0.7635	0.7965
	Tower	10%	0.9896	0.9935	0.9924
		30%	0.9801	0.9777	0.9712
		50%	0.9065	0.9585	0.9587
		80%	0.2510	0.8156	0.8191
RVIN	Lena	10%	0.9923	0.9883	0.9876
		30%	0.9782	0.9778	0.9761
		50%	0.9002	0.9515	0.9545
		80%	0.2334	0.8112	0.8129
	Baboon	10%	0.9811	0.9774	0.9758
		30%	0.9682	0.9651	0.9641
		50%	0.8925	0.9443	0.9456
		80%	0.2113	0.7551	0.7586
	Tower	10%	0.9864	0.9825	0.9818
		30%	0.9751	0.9706	0.9701
		50%	0.8994	0.9503	0.9516
		80%	0.2215	0.8117	0.8137

Table II portrays the performance comparison of the proposed filter counter to some of the recent filters with respect to another metric SSIM, to judge the efficacy of the filter to embrace the shape and structure of the investigated images while going through the restoration procedure. Three different images Lena, Baboon and Tower are used to depict the result. As seen from the comparison, the proposed filter holds over

80% resemblances for all those images at a high noise density of 80% with respect to both SAPN and RVIN and also embraces 99% alikeness at a minimum 10% noise density. These results point toward the potential of the proposed algorithm to reinstate the structure of the images to a commendable extent post restoration.

One more imperative factor of the proposed filter was to choose the window size to be applied all over the image on both detection and removal stages. As the method is applicable for color image restoration, the same window size was applicable for all the red, green and blue color planes. Trial and error method was used to find the window size for the proposed method. After implementing the algorithm with different odd numbered window sizes,  $5 \times 5$  and  $7 \times 7$  size was found suitable for the proposed detection and correction method respectively. The PSNR outcome of the proposed filter using different odd numbered window sizes is demonstrated in Table III and it can be seen that, our method produced a superlative PSNR result for the selected window sizes.

It is intrinsic that, detection is the primary aspect for a filtering before applying a removal mechanism. While applying K-Means in the proposed method to cluster the least variant non-noisy elements, a cluster size has to be selected. As,  $5 \times 5$  window size is used in the detection procedure, we have 25 elements, which will be segregated into different clusters after applying the K-means method to the data. If higher cluster size is taken, that could invalidate the objective of clustering as several small cluster would be created and it will be hard to find a maximum cluster having non-noisy elements. So, smaller cluster sizes were taken and investigation was performed on a trial-and-error basis. From Table IV, it can be perceived that, cluster size 4 yielded maximum output for the proposed method after being tested on different images.

TABLE III. PERFORMANCE OF THE PROPOSED FILTER FOR VARIED WINDOW SIZES

Noise	Window Size		Noise Densities		
	Detection	Removal	40% ND	50% ND	60% ND
SAPN	3 * 3	3 * 3	34.06	33.19	31.64
		5 * 5	34.11	33.38	31.73
		7 * 7	34.15	33.45	31.75
	5 * 5	3 * 3	34.07	33.21	31.59
		5 * 5	34.17	33.49	31.82
		7 * 7	34.21	33.56	31.98
	7 * 7	3 * 3	33.97	32.98	31.23
		5 * 5	33.91	32.89	31.12
		7 * 7	34.09	33.12	33.33
RVIN	3 * 3	3 * 3	31.98	30.22	26.23
		5 * 5	32.59	30.74	27.32
		7 * 7	32.61	30.79	27.41
	5 * 5	3 * 3	31.97	30.20	26.14
		5 * 5	32.67	30.84	27.47
		7 * 7	32.78	30.96	27.56
	7 * 7	3 * 3	31.99	30.17	26.33
		5 * 5	32.65	30.81	27.29
		7 * 7	32.45	30.61	27.11

TABLE IV. PERFORMANCE OF THE PROPOSED FILTER FOR VARIED CLUSTER SIZES

Noise	Images	Cluster Size		
		3	4	5
SAPN	Lena	31.75	31.98	31.61
	Baboon	29.51	29.68	29.30
	Barbara	25.01	25.69	24.46
RVIN	Lena	27.36	27.56	26.91
	Baboon	26.81	26.96	25.97
	Barbara	23.98	24.65	22.96

By all the results shown and analyzed above, the proposed emerged to be superior to all the compared state-of-art filters. In the work, the key aspect of the enhancement lies in the K-means clustering-oriented detection. K-means clustering of size 4 is used here on each of the  $5 \times 5$  kernels to generate four clusters having respective pixel intensities based on the randomized clustering method. As the non-noisy pixels have more propensity to have the least variant values within the defined small kernels, it is more likely that those pixels will be grouped by the clustering procedure and will belong to the same cluster. On the other hand, the noisy pixels are more probable to have scattered values and least possible to belong to the same cluster and also very occasional to form a cluster having the greatest number of elements. This creates the foundation of the proposed work followed by captivating the least Manhattan distance criteria in removal operation which has strengthened the proposed algorithm. Here, the non-noisy pixels, residing at least distance from the evaluated noisy pixel are taken as the key element in the removal operation. Because these non-noisy pixels at least distance are having the most influence on the assessed noisy pixel for each kernel. Altogether, these crucial facets of the proposed work justify its groundwork and showcase the reason behind the enhancement.

## V. CONCLUSION

This paper demonstrates a high-density noise removal scheme from color images. The proposed method is fabricated on K-means clustering based detection followed by least distance criteria-oriented removal. Applying K-means clustering on the collective data, formed by elements of each defined windows of a color image, extracts the mutual effect of all color planes for individual pixels, residing at identical positions in each plane and thereby categorizing each pixel into a specific cluster. Clustering is applied in the conjecture that, the non-noisy pixels from each window having similarity are categorized into a specific cluster while noisy elements having variations will be scattered into different clusters and thus can easily segregate non-noisy and noisy pixels effectively. Then the non-noisy pixels, found at least distance from the inspected noisy pixel, are used along with all over median criteria of segregated non-noisy pixels from each window, for the replacement operation. This removal scheme uses the impact of closest non-noisy pixels, because these pixels are having maximum influence on the inspected noisy pixel. The overall work is justified by the superior qualitative and quantitative results up against the recent reputable filters. It can be seen that; the proposed algorithm works brilliantly at high noise densities and effectively at lower middle noise densities. Our

future objective is to design a filter that is equally capable at both low and high noise densities.

#### ACKNOWLEDGMENT

We would like to express our heartfelt gratitude to Ms. Sonali Banerjee and Ms. Koyel Chakraborty for their relentless inspiration and motivation that abetted us to conduct this work in this tough time around.

#### REFERENCES

- [1] K. Kondo, M. Haseyama and H. Kitajima, "An accurate noise detector for image restoration," Proceedings. International Conference on Image Processing, pp. I-I, 2002, doi: 10.1109/ICIP.2002.1038025.
- [2] S. Banerjee, A. Bandyopadhyay, R. Bag and A. Das, "Sequentially combined mean-median filter for high density salt and pepper noise removal," 2015 IEEE International Conference on Research in Computational Intelligence and Communication Networks (ICRCICN), pp. 21-26, 2015, doi: 10.1109/ICRCICN.2015.7434203.
- [3] S. Banerjee, A. Bandyopadhyay, A. Mukherjee, A. Das, and R. Bag, "Random Valued Impulse Noise Removal Using Region Based Detection Approach," Eng. Technol. Appl. Sci. Res., vol. 7, no. 6, pp. 2288–2292, Dec. 2017, doi: 10.48084/etasr.1609.
- [4] P. E. Ng and K. K. Ma, "A switching median filter with boundary discriminative noise detection for extremely corrupted images," IEEE Transactions on Image Processing, vol. 15, no. 6, pp. 1506-1516, June 2006, doi: 10.1109/TIP.2005.871129.
- [5] A. Nasimudeen, S. N. Madhu, and T. Rao, "Directional switching median filter using boundary discriminative noise detection by elimination." Signal, Image and Video Processing vol. 6, no. 4, pp. 613-624, 2012.
- [6] L. Malinski and B. Smolka, "Fast adaptive switching technique of impulsive noise removal in color images," Journal of Real-Time Image Processing, vol. 16, no. 4, pp. 1077-1098, Aug 2019.
- [7] J. Astola, P. Haavisto and Y. Neuvo, "Vector median filters," Proceedings of the IEEE, vol. 78, no. 4, pp. 678-689, April 1990, doi: 10.1109/5.54807.
- [8] S. J. Ko and Y. H. Lee, "Center weighted median filters and their applications to image enhancement," IEEE Transactions on Circuits and Systems, vol. 38, no. 9, pp. 984-993, Sept 1991, doi: 10.1109/31.83870.
- [9] K. M. Singh, "Vector median filter based on non-causal linear prediction for detection of impulse noise from images," International Journal of Computational Science and Engineering, vol. 7, no. 4, pp. 345-355, 2012.
- [10] A. Roy, J. Singha, L. Manam, and R. H. Laskar, "Combination of adaptive vector median filter and weighted mean filter for removal of high-density impulse noise from colour images," IET image processing, vol. 11, no. 6, pp.352-361, 2017.
- [11] L. Jin, Z. Zhu, X. Xu and X. Li, "Two-stage quaternion switching vector filter for color impulse noise removal," Signal Processing, vol. 128, pp. 171-185, Nov 2016.
- [12] L. Jin, Z. Zhu, E. Song and X. Xu, "An effective vector filter for impulse noise reduction based on adaptive quaternion color distance mechanism," Signal Processing, vol. 155, pp. 334-345, Feb 2019.
- [13] A. Roy and R. H. Laskar, "Non-casual linear prediction based adaptive filter for removal of high density impulse noise from color images," AEU-International Journal of Electronics and Communications, vol. 72, pp. 114-124, Feb 2017.
- [14] P. R. Chanu and K. M. Singh, "A two-stage switching vector median filter based on quaternion for removing impulse noise in color images," Multimedia Tools and Applications, vol. 78, no. 11, pp. 15375-15401, Jun 2019.
- [15] C. C. Hung and E. S. Chang, "Moran's I for impulse noise detection and removal in color images," Journal of Electronic Imaging, vol. 26, no. 2, 023023, April 2017.
- [16] A. Roy, J. Singha, and R. H. Laskar, "Impulse noise removal from color images: An approach using SVM classification based fuzzy filter," In TENCON 2017-2017 IEEE Region 10 Conference, pp. 929-934, Nov 2017.
- [17] S. Schulte, V. D. Witte, M. Nachtegael, D. V. D. Weken, and E. E. Kerre, "Histogram-based fuzzy colour filter for image restoration," Image and Vision Computing, vol. 25, no. 9, pp. 1377-1390, 2007, ISSN 0262-8856, <https://doi.org/10.1016/j.imavis.2006.10.002>.
- [18] S. Masood, A. Hussain, A. Jaffar, and T. S. Choi, "Color differences based fuzzy filter for extremely corrupted color images," Applied Soft Computing, vol. 21, pp. 107–118, 2014, 10.1016/j.asoc.2014.03.006.
- [19] A. Roy, and R. H. Laskar, "Multiclass SVM based adaptive filter for removal of high density impulse noise from color images," Applied Soft Computing, vol. 46, pp. 816-826, 2016.
- [20] F. Ahmed, and S. Das, "Removal of High-Density Salt-and-Pepper Noise in Images With an Iterative Adaptive Fuzzy Filter Using Alpha-Trimmed Mean," IEEE Transactions on Fuzzy Systems, vol. 22, no. 5, pp. 1352-1358, Oct 2014, doi: 10.1109/TFUZZ.2013.2286634.
- [21] V. Gregori, S. Morillas, B Roig and A. Sapena, "Fuzzy averaging filter for impulse noise reduction in colour images with a correction step," Journal of Visual Communication and Image Representation, vol. 55, pp. 518-528, Aug 2018.
- [22] W. Zhang, L. Jin, E. Song and X. Xu, "Removal of impulse noise in color images based on convolutional neural network," Applied Soft Computing, vol. 82, 105558, Sep 2019.
- [23] B. Karthik, T. K. Kumar, S. P. Vijayaragavan and M. Sriram, "Removal of high density salt and pepper noise in color image through modified cascaded filter," Journal of Ambient Intelligence and Humanized Computing, vol.12, no. 3, pp. 3901-3908, Mar 2021.
- [24] A. Bandyopadhyay, K. Deb, A. Das, and R. Bag, "Random Valued Impulse Noise Detection Using Fuzzy c-Means Clustering Technique," Smart Computing Techniques and Applications, Springer, Singapore, pp. 397-405, 2021.

# MultiStage Authentication to Enhance Security of Virtual Machines in Cloud Environment

Anitha HM<sup>1</sup>

Department of ISE  
BMS College of Engineering  
Affiliated to VTU, Bengaluru, India

Dr.P Jayarekha<sup>2</sup>

Department of ISE  
BMS College of Engineering  
Bengaluru, India

**Abstract**—The adoption of cloud computing in different areas has shown benefits and given solutions to applications. The cloud provider offers virtualized platforms through virtual machines for the cloud users to store the data and perform computations. Due to the distributed nature of cloud, there are many challenges and security is one of the challenges. To address this challenge, verification method is implemented to achieve high level security in the cloud environment. Many researchers have provided different authentication mechanisms to safeguard virtual machines from attacks. In this paper, Multi Stage Authentication is proposed to overcome the threats from attackers towards virtual machines. In order to authorize and access the virtual machine, multistage authentication incorporating the factors like username, email id, password and OTP is carried out. Mealy Machine model is applied to analyze the state changes with factors supplied at multiple stages and trust built with each stage. Experimental results prove that system is safe achieving data integrity and privacy. The proposed work gives the protection against unauthorized users, provides secure environment to the cloud users accessing the virtual machines.

**Keywords**—Authentication; multi stage authentication; one time password; finite state machine; mealy machine

## I. INTRODUCTION

In cloud environment, many users deploy the applications. These applications are accessed by several users. Dependability of users on the cloud is increasing day to day[1] as the investment is lesser. Hence cloud environment is prone to security issues[2]. Illegal access, misuse of data and assets hacking by the malicious users are some of the threats that has to be addressed with more importance. Proper authentication has to be in place to safeguard against these attacks[3]. Traditional authentication mechanisms such as password-based login suffer with security problems. Password hijacking, stealing and phishing attacks[4] are some of the threats which create burden on cloud environment. Hence the resource access from the attackers has to be protected by good authentication.

Many well-known cloud computing environments such as Google, Amazon and Microsoft have already adopted the multifactor authentication. The major usage constraint is with respect to the users as they need to use the extra effort to login providing more factors. There is one more main concern to safeguard the user's credentials as they are shared with cloud environment to access the services from the cloud. Cloud users perform computations using virtual machines where they store the data and continue working till completion. Virtual

machines belonging to different users are stored in the same host. Hence security of the virtual machine (VM) has to be taken care with almost importance. Before the VM is granted or accessed by the cloud user, authentication has to be carried out. Authentication [5] helps in proving the trustworthiness of the cloud users. Single factor authentication suffered with the problems such as if the user forgets the password and losing of password will completely avoid the legitimate user to access the resources in the cloud. Multistage Authentication (MSA) gives an additional layer of security to access the resources in the cloud and cloud provider is sure of extra security along with service level agreement. First step for cloud users is signing the service level agreement with cloud provider, next step is multistage authentication to access the cloud. Hence using this multistage authentication avoids attacks by the compromised users. There are advantages of choosing multistage authentication when compared with normal authentication such as increased security in the cloud environment and prohibiting the unauthorized users in to the system.

### A. Motivation

The main objective of the paper is to protect the VMs in the cloud environment from illegal access and theft of data using MSA. MSA in cloud environment considers more than one factor from cloud users side credentials so that authentication is stronger. Even though the attacker tries with any one factor, gathering all the factors is not an easy measure to enter the system. MSA offers robust method of authentication cloud users and benefits with effective solution to the authentication. To provide high degree of security in the virtualized cloud environment and protect against several cyber-attacks that happen. Using multiple factors [6] provides an additional step towards accessing sensitive and confidential data stored in the cloud provider's domain. It is normally common that most of the users will accessing the virtual machines from the same host. Hence, it's the cloud provider's responsibility to meticulously provide the access to the virtual machines with appropriate authentication mechanism. Its observed number of incidents happening in the cloud regarding the data theft and DOS attacks.

Some of the research questions to be considered are:

- Access to the virtual machines in the cloud environment by the registered users without hassles.

- Will the MSA approach recognize the unauthorized users?
- The security features such as integrity, confidentiality and authenticity are achieved or not?

### B. Contribution

The paper starts with theoretical concept of authentication, state machine to provide strong model to overcome illegal access and protect the virtual machines from attacks. The paper includes

- Authentication requirement and different authentication approaches with pros and cons are explored in the paper.
- Mealy Machine is presented to analyze the authentication process performed by the legitimate user to build the trusted environment and prevent the unauthorized user at all states.
- The approach uses MSA to allow users to access VMs for completing the tasks assigned by their organization.
- To protect every user's credential in the cloud provider's domain, robust MSA approach is applied guaranteeing the integrity and privacy.

This paper is organized as Section 2 gives background, Section 3 describes the related work, Section 4 presents the proposed approach, Section 5 gives the evaluation of the algorithm, Section 6 explains the results and discussions and Section 7 concludes the paper.

## II. BACKGROUND

### A. Traditional Authentication

Authentication [7] is a technique of proving the identity of the user in accessing the system by providing the details such as password and username. Traditionally single factor authentication was used to enter the system with an access card. It is observed that every user obtaining any services from any provider normally uses password-based authentication [3]. This password-based approach is usually used across different applications on hosts. Password is a widely accepted mechanism as it does not involve any major complications, users have to memorise the password and apply whenever the authentication is required. Passwords can be plaintext, combination of various characters involving special characters, numbers and so on. Users have suffered with many attacks due to weak passwords. There are cases where random passwords are selected and attackers can crack passwords. The different types of password attacks are dictionary attack, brute force attack, session hijacking and so on. Attacks disrupt the normal functioning of the cloud environment. The usage scenario of any environment is the users register for the service with certain password, which gets stored in the cloud server. Claimant has to provide the password in order to prove that he is authorized user. If the password matches with the stored password, then the claimant users are authenticated. The systems usually advice to choose the strong password.

### B. Authentication

User has to prove that he is legitimate and this can be done using authentication. Usual methods are username and password to prove identity of the user. With the advancements in the security measures of any network, two factor and multifactor authentication [8] was applied to defend against illegal users.

Authentication avoids unauthorized access [5] to the sensitive information. There are all possibilities that the attacker gains access to virtual machines and tampers the information [9] stored, which leads to integrity threat.

There are five types of authentication mechanisms type [10] [11] [12].

- Password authentication: This method involves the password given by the users with a combination of characters, symbols and numbers. Users have to create strong passwords to avoid attacks. Many users keep simple passwords to avoid remembering long and cryptic passwords. Hence users are at the risk of password attacks.
- Certificate Authentication: User identity is confirmed by the digital certificate issued by the certification authority. The best example is Aadhar card to identify the user. Users provide the digital certificate when they are using the services or resources from the server. Once the server verifies digital certificate, user is decided as the legitimate.
- Biometric Authentication: User identification based on the biological characteristics of the user. Using the biometric factors, access doors or login to the system is granted in some of private firms. Biometric feature can be added as one of the factors with multifactor authentication.
- Token generated method: User credentials are maintained and users receive the tokens on one of the credentials. They provide the tokens to prove their identity.
- Multi factor authentication: Users add more than one factor to authenticate himself with server to access the resources. Multifactor authentication (MFA) can take more than one factor at the same time or multilevel. Due to this method of authentication, system is protected with various threats.

Among these different authentication [13] mechanisms multifactor authentication is applied as it is one of the most promising approaches. Multi factor authentication [6] mechanism defends against the attacks with extra care. Factor is the one which user provides to claim who he is. Suppose an employee enters the organization. He can enter the organization by swiping the card. How will the doors get to know that he is authorized person? It's because he has the smart access card which can be used for authentication. In this smart card, there is integrated chip which controls the access to the office environment. Normally chip stores the user

authentication data, user identification and data used by the users with respect to applications.

The different types of factors are collected [14] from the user to authenticate are:

- Knowledge factor: Aspects that users know like passwords. This factor is normally shared between the user and the provider. Once the user chooses the factor, it will be stored in the provider’s database server and each time the user enters his factor, it has to be validated.
- Possession factor: Aspect that user has such as mobile phone or any other device. It can be the one-time password, smart cards or security tokens. If the user happens to lose the device, it is difficult to authenticate the legitimate user.
- Inherence factor: Feature that user is like biometric feature, voice or fingerprint. This factor is the one that the user is and the biometric factors are unique to each and every user.

Table I below represent the different factors which users are aware of to make use.

TABLE I. DIFFERENT FACTORS THAT ARE CONSIDERED FOR AUTHENTICATION

Knowledge factor	Possession factor	Inherence factor
User Knows- PIN, Password, security question related to his DOB or anything which user is aware of.	User possesses- Mobile phone, Smart card or tablet on which receives one time password(OTP), random password, etc	User is identified with biometric features: Iris, finger print or face recognition

The advantages of multi factor authentication [15] are:

- Improved Security: System security is enhanced by introducing the multifactor authentication. Additional Layers of authentication will add on to the security.
- Compliance: Necessary conditions of the organization are satisfied.
- Flexibility: Options for authentication is improved with more factors compared to traditional password authentication.

### III. RELATED WORK

Ometov et al [15]., has discussed about multifactor authentication right from single factor authentication. They have explored different authentication methods, applications and challenges involved in implementing the multifactor authentication. The authors have identified operational concerns such as usability, robustness, integration and security. They have provided the benefits of MFA towards security. The authors have proposed the reversed approach in which the factors obtained from the users have secrets such fingerprint or pin. Considering  $n$  as sum and  $I$  factors with  $S_e$  secrets provided to them.

Factors and correspondingly secrets can be written as

$$I_1: S_{e1}$$

$$I_2: S_{e2}$$

$$\dots$$

$$\dots$$

$$I_n: S_{en}$$

Secrets are provided by the user to authenticate so that they can enter the system. Assume there are four factors and user forget any one factor to enter, then there is a trusted cloud party, which will aid to recover factor so that the user will be able to enter the system. Some of the biometric factors such as fingerprint, face change over the time, for which there is support by trusted party to update the feature in the database. There is decision policy which helps in deciding whether the user is authenticated or not.

B. B.Gupta et al [16], have proposed a model for access control based on the identity and mutual authentication using smart cards. The approach has five different phases right from the registration to authentication including updation of credentials. Hash functions are used towards the data. The approach mitigates unauthorized access, eaves dropping and single sign on with smart cards. It also defends against DoS attacks, fake identity and illegal use of smart cards.

C. Singh and T. Deep Singh [17] have proposed MFA with three levels based on the three levels of authentication. At the first level the login and password are stored with double encryption such as SHA-1 and AES. Second level of authentication uses the out of band authentication technique. After the first level, server provides the OTP to registered mail. User has to prove that he is legitimate by providing the OTP to the server. Third level user has to click certain number of images and buttons on the screen to get authenticated. The approach provides the protection against various attacks like man-in middle, brute force and password guessing.

A. Bhanushali et al [18], have given a good input about different authentication algorithms with respect to security, usability, space and storage. They have described the algorithms such as draw a shape, grid selection and déjà vu authentication algorithm based on the images. In order draw a secret, technique user is provided with a drawing and user has to reproduce same by redrawing. In grid selection the user is provided with small grid and needs to draw the pattern for authentication. Déjà vu is based on the seed value generated by the trusted server towards the user and at the time of authentication, user has to prove using this value. The inference provided by the authors is graphical based approach is better than the textual approach with respect to security.

Multilevel authentication [19] is presented by the authors to enhance security for electronic devices. Three levels of security checks are performed to authenticate the legitimate user. First level of security check is done with normal password. Biometric authentication is carried out in the second level. Last level of security check is performed by the accelerometer.

The proposed approach in the paper does not need any trusted third party and the interaction is between the cloud

provider and cloud user. There is no need for the user to go through the sequence of images with MSA approach.

Some users might not be well versed with drawings and user has to go with stages and provide input. Hence the proposed work is friendly to the users and provides security with features such as confidentiality and privacy. The approaches implemented by the various researchers along with the security parameters are given in Table II.

TABLE II. IMPLEMENTED AUTHENTICATION APPROACHES WITH SECURITY PARAMETERS

Authors	Description	Security Parameters addressed
Ometov et al[15]	Multifactor Authentication	Highlighted the operational concerns robustness, security and integration.
B. B.Gupta et al[16]	Smart Cart Authentication	Protection against unauthorized access, eavesdropping and DoS attacks.
C. Singh and T. Deep Singh [17]	MFA based on three level authentications	Defends man-in- middle, brute force and password attacks.
A. Bhanushali et al[18]	Survey about authentication algorithms	Graphical based approach provides better security.
A.Dinakar et al[19]	Multilevel authentication	Three levels of security checks for authentication.

IV. PROPOSED APPROACH

The objective of the proposed work is to implement secure access to the virtual machines using Multistage Authentication. In Multistage Authentication more than one factor is considered. As per the authentication mechanisms, using multiple factors, system is less prone to attacks.

A. Adversary Scenario

Attacks are possible from the attackers to gather the information stored in the cloud server [20]. Attacker might also try to spoof and access the VMs from the cloud provider. In the Fig. 1 shown below, legitimate users are the authenticated users and attacker [21] is the one trying to intrude the system. In normal authentication, login and password are used to provide the VMs. The traditional approach will give opportunities for attackers to damage the security features such as data integrity, confidentiality and availability [22].

A formulation is obtained for the minimization of attacks on the virtual machines with automata theory. The model used to realize the approach is mealy machine. Given below are the details of the state machine and use case of mealy machine.

B. Introduction to State Machine

State Machine is the machine which works based on the behavior of the system. The output of the system depends on the user’s input. The machine which has finite number of states is known as finite state machine. Let us consider the simple example of tube light. When the user switches on the button, the state changes to on and otherwise it is off. There are two states in this machine namely switch on and switch off which is depicted in the Fig. 2.

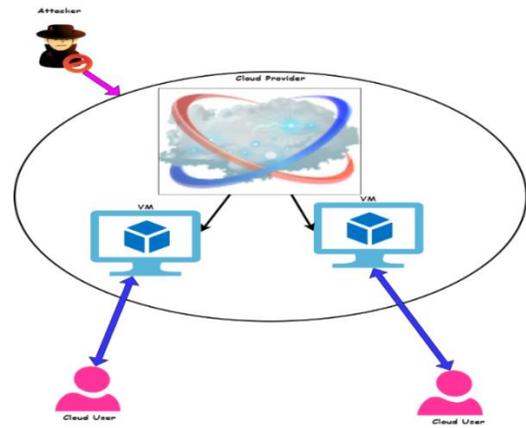


Fig. 1. Scenario of Risks.

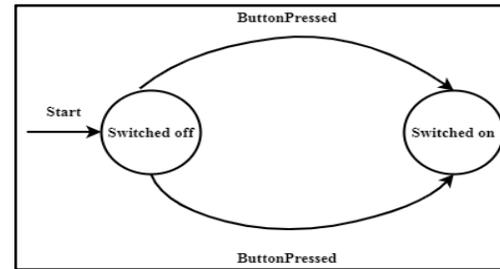


Fig. 2. State Machine of Tube Light.

C. Finite State Machine

Finite State machine is a computational model [23] with defined number of states. States always present the status of the system at the given instance. Consider the example traffic signal. As per the light shown, pedestrians cross the road and vehicles navigate through the traffic. This is one of the classic examples of Finite State machine. Finite state machine contains starting state, accepting states and final state. The output is either accept or reject. With specific input transition of state takes place. All these input symbols are represented in the alphabet.

Formal definition of finite state machine: It is represented with set of three entities shown in the equation 1:

$$F = (V, I, t_r) \tag{1}$$

V & I are non-empty finite groups

t<sub>r</sub>: V x I → V is a state transition function.

v<sub>0</sub>: Initial state where v<sub>0</sub> ∈ V

I: input alphabet contains input symbols

To summarize the concept of the FSM as

- Has finite number of states
- Either zero or more accepting states
- Has at least one state
- Set of symbols for transition
- Has alphabet which has the set of input symbols.

Next followed by this topic, mealy machine is FSM depending on the present state and input symbol. The system is modeled with Mealy machine.

D. Overview of Mealy Machine

Mealy Machine is a finite state machine [24][25] in which output state depends on the current input symbol and state.

Let us find out (V, v<sub>0</sub>, I, O, t<sub>r</sub>, F):

V: Finite Set of States

v<sub>0</sub>: Initial state

I: Set of symbols for transition

O: Output Symbol

t<sub>r</sub>: Function of transition mapping V x I → V

F: Output function mapping to V→O

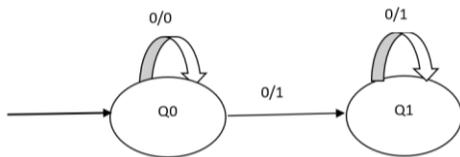


Fig. 3. State Transition in Mealy Machine.

Mealy Machine [25] has simple one input upon which transition to the next state shown in Fig. 3. Only two states are presented Q<sub>0</sub>, Q<sub>1</sub>. Input symbols are 0 and 1. Output is represented as 0 and 1. Mealy machines have fewer states compared to that of Moore machine. Mealy machines are secure to use; response for the inputs with mealy machines are faster. Mealy machines are used so that each level the trust is increased and only legitimate users are granted with the VMs.

E. Use case with Mealy Machine

The factors considered for the authentication are Email-id, password, Phone Number and One Time Password. Using mealy machine trust chain can be seen. In any of the stage the input is wrong, trust is broken. When the trust is broken by any of the user, it is very clear that it is the attack performed by the intruder. These factors are provided as the input symbols to the system. As per the factor and present state, the user progresses to the next state shown in the Fig. 4.

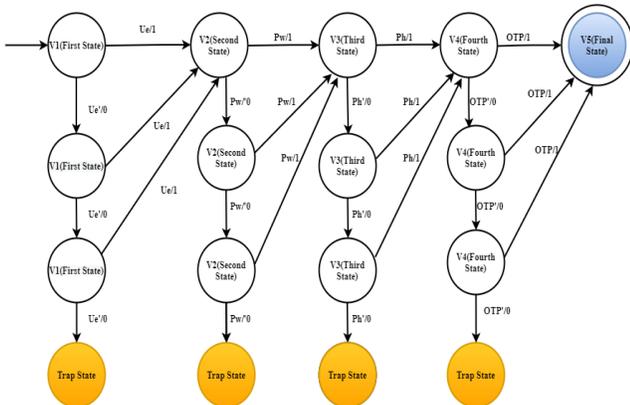


Fig. 4. Multistage Authentication System State Changes Depicted with Mealy Machine.

Here as per the input, the change in the state is seen. First user name and email id are the input symbol for state change. Next input symbol considered is password, followed by phone number and OTP. The system is multistage or multi-level where there are stages which legitimate user will be able to clear and succeed. Upon correct entry of email, password is generated to the valid email. User can login using the password generated. User has to go through the four stages in order to reach the final stage as shown in the Fig. 4. Every stage input and current stage important to advance to the next stage.

Let us represent the details of machine with the multifactor authentication

$$V = \{V_1, V_2, V_3, V_4, V_5\}$$

V<sub>1</sub>: Initial State or first state

I = { Ue, Pw, Ph, OTP }

O = { 0, 1 }

T<sub>r</sub> is the transition function.

Upon receipt of matching symbols like email id, phone number, password and OTP, transition takes place to the next level in the system. The output states are 0 and 1. 0 represents failure and no transition and 1 depicting success along with transition to next state. Three attempts are considered in the proposed approach. As shown in the Fig. 4 the intruder at any stage tries to perform attack, cannot advance further and access the virtual machine.

F. Security Analysis with Mealy Machine

Attacks can be viewed and analyzed based[26][27] on the automata theory. The proposed MSA approach protects against attacks[28] which are discussed below:

- **Replay Attack:** If an attacker somehow gathers the email id and user name, guessing the secret password and gathering the OTP is not possible. Attacker cannot penetrate the cloud environment and access the virtual machines. With the mealy machine, if at any stage input is wrong, state change will not happen. Between V<sub>1</sub> and V<sub>5</sub>, if the attacker tries to gather any factor and apply that in between randomly, successful authentication is not possible as mealy machine depends on current state also.
- **Spoofing Attack:** Attacker tries to impersonate in order to avail the virtual machines. Every time OTP is generated and it is not easy for attacker to get the OTP. There are multiple factors for attacker to guess, it is not just login and password compared to traditional systems. Intruder trying to capture Ue, Pw, User name and random password to authenticate himself is not accepted as password is received to legitimate user's email.
- **Data theft resistant:** The approach implemented overcomes the data theft as illegal access is not happening. If an attacker tries to intrude in any stage, there are only three attempts and third attempt being the last one, upon failure goes to trap state.

- Brute force attack: If any intruder tries to attack the system in any stage gathering some information, intruder cannot succeed in entering the system. As there are different levels and at each level if wrong input is raised, state change will not take place.
- Man in Middle attack: This system is resistant for man in middle attacks.

Intermediately in any state  $V_i \in V$  where  $i \rightarrow 1,2,3,4,5$  it is not possible enter the system. In order to validate the mealy machine model, simulation is performed and evaluated. The factors considered, algorithm steps and implementation details are presented below.

G. Methodology

Cloud user credentials are collected by the cloud provider during the registration phase. When users want to access the resources, authentication is performed. Here multistage authentication is used by the cloud provider. The factors considered for authentication in this approach are presented below.

- Email id: The user registers with his or her username and email ID. A unique hash code is created for each user using MD5 algorithm. MD5 algorithm [29] is used to encrypt the 4-digit random passwords generated for the user. The username and 4 digit non encrypted password are sent to the registered email ID. The user logs into his or her email account and must take note of the unique password provided in the body of the message. A link is sent to the registered email id. The user must click on the link included in the email to activate his account and get access to the login page.
- User name and password: Once the login page appears, the user enters the username and password sent via email. At this point they must also enter their contact number for the next level - OTP verification. If the username and password authenticate correctly, that is, if it matches with the information stored in cloud provider's database, the second factor is verified.
- One Time Password (OTP): Once the user clicks on the generate OTP button after providing the phone number, a random 5-digit OTP is generated and sent to the respective phone number. The user is required to enter the OTP. The entered OTP is verified with the temporarily stored OTP. If verification is successful, the user is granted access to the VM.

Multistage authentication shown in the Fig. 5 is explained step by step in the algorithm provided below. There are stages here in the approach. In the first stage, the email id and user name are provided. Cloud provider verifies in the database and sends the password to email. Using the password, user can login and provide the phone number for receiving OTP. This phone number is validated in the database and the OTP is sent. All these steps are shown in the Fig. 5.

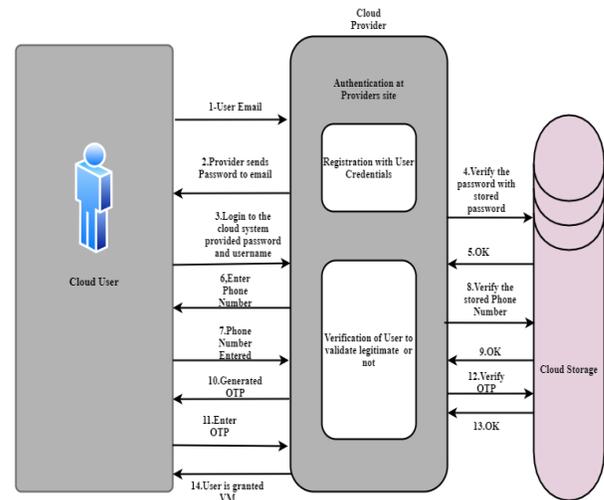


Fig. 5. Multistage Authentication Depicting Authentication Process.

Algorithm: Multi stage Authentication

Input: Username & Email-id

Output: Valid User is able to enter the cloud Environment

1. Begin
2. for each n users in the cloud provider Cp do
3. Enter Email-id Ue and User\_name Un
4. Cloud Server Generates 4-digit password PW4 and sent to user's email-id Ue
5. Enter the user\_name Un and Password PW4 in to the system
6. If (Un && PW4 with Cp server database)
7. Ask user to enter phone\_no Ph
8. Send OTP to Ph
9. If (entered OTP == Cp Server Value)
10. Grant the user request
11. Else
12. Generate Alert to the Cloud Provider about illegal access
13. End

Notations used in the MFA approach are described in the Table III.

TABLE III. NOMENCLATURE OF THE TERMS USED IN THE PROPOSED MFA APPROACH

Notation	Description
Cu	Cloud user
Un	User Name
Rn	Random Number
Act. link	Activation link
Cp	Cloud Provider
Ue	User email id
PW4	Four-digit password
Ph	Phone number
OTP	One time password
H(.)	One way hashing
X->Y: A	Send A from X to Y

The stages of authentication are login, authentication and verification phase in order to grant user with virtual machines requested. This is depicted in the Fig. 6.

1) Login Phase

Step 1: Cloud user requests to allocate the virtual machine to the cloud provider with whom he is signed the SLA. Cloud user sends user name and email id.

Step 2: Cloud Provider generates four-digit hash and sends to the cloud user. Along with this activation link is also sent to the cloud user's mail id.

Step 3: User clicks the link to activate his account in the cloud environment.

2) Authentication Phase

Step 1: User enters the password provided by the cloud provider in to the cloud system.

Step 2: Cloud Provider asks the user to enter the valid phone number.

Step 3: Cloud User Provides the phone number.

Step 4: Cloud Provider generates the randomly five-digit password as one time password valid for 60 seconds to the cloud user's phone.

Step 5: Cloud User has to enter the OTP to access the virtual machine allocated for him by the cloud provider.

3) Verification Phase

Step 1: OTP generated is stored in cloud provider's database.

Step 2: Cloud User entered OTP is compared with stored OTP.

Step 3: Both are same, cloud user is granted virtual machine.

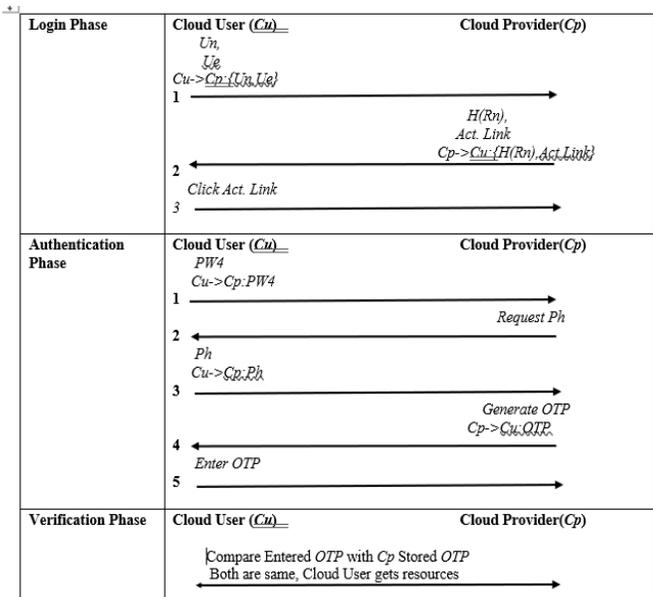


Fig. 6. Stages of Authentication.

V. EVALUATION OF ALGORITHM

Simulation is performed considering the many users and cloud provider. The authentication system is implemented using php, html and CSS at the front end, backend Mysql and XAMPP web server [30] solution stack. The backend database stores the user details. System has three modules viz. registering user credentials such as user name and email id, login page and OTP page. The algorithm has different factors for authentication. If the user is able to guess any of factor, it is not an easy mechanism for adversary to retrieve all factors. OTP is valid only for limited time and attacker breaking the OTP with in time duration is not easy. User has to sign up to access the cloud provider shown in the Fig. 7.

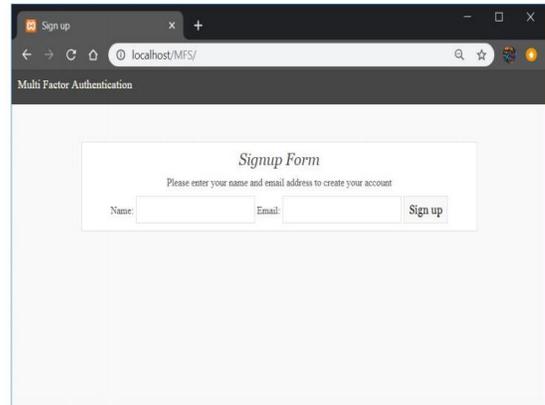


Fig. 7. User Sign up with cloud Server.

After the registration the username and unique password is sent to the user on his/her registered email id shown in Fig. 8.



Fig. 8. Reception of Username and Password by the user.

The user now knows his/her unique password and can access the login page, as shown in Fig. 9.

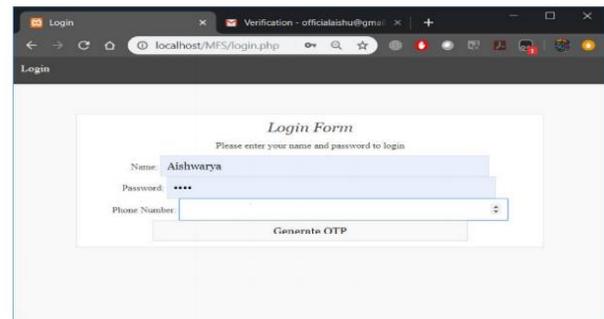


Fig. 9. Login Form.

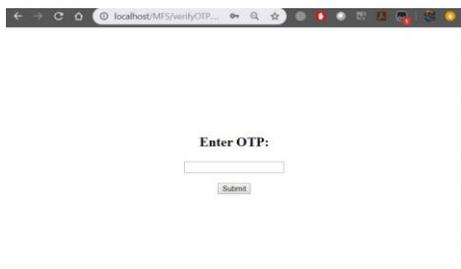


Fig. 10. OTP Confirmation.

User receives the OTP on valid phone number and enters OTP as shown in Fig. 10.

When the user submits the OTP, it is verified with value stored in the cloud provider database and once it is confirmed the multistage authentication is complete. User has passed all authentication checks. Every time the OTP is generated and there is no chance of gaining the access to the cloud environment.

### VI. RESULT AND DISCUSSION

Multistage authentication is checked for different time slots and recorded the successful attempts and failure attempts. In these number of successful logins is legitimate users. Testing is carried out using JMeter [31]. Login analysis is performed using JMeter. JMeter is opensource java-based tool used to test load and performance. Failure attempts some of them are intruders trying with brute force method to enter the system. The system is tested for the varying number of users right from 10 to 100. It is found that the system has provided resistance towards the attacks. Accuracy of system is calculated using the formula given below.

$$Accuracy = \frac{Sl}{Tl}$$

Where *Sl* is successful logins and *Tl* specifies total logins. The graph representation is shown in the Fig. 11.

The experiment is run for one hour, three hours and six hours. Overall Login statistics of users are depicted in Table IV.

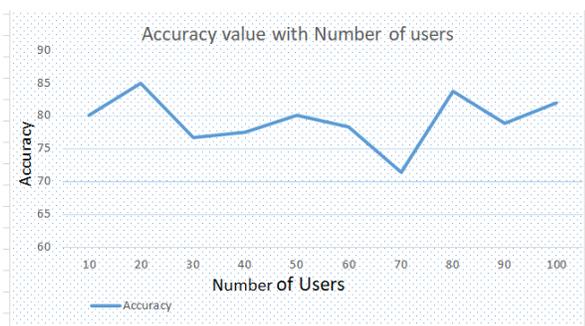


Fig. 11. Accuracy Depiction.

TABLE IV. OVERALL STATISTICS

Duration	60	180	360
Failure Login	33	42	77
Successful Login	63	88	95

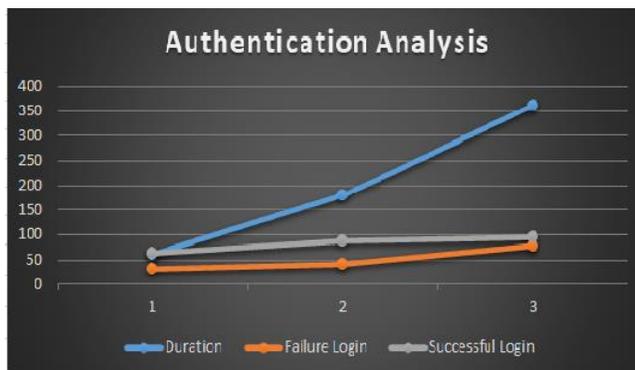


Fig. 12. Overall Login Statistics.

The graph in Fig. 12 indicates that MSA approach provides the legal access to cloud environment. The cloud users after the SLA contract with cloud providers can request for resources using MSA. MSA adds one more layer of security after SLA. The system does not allow the unauthorized access; hence approach provides privacy and protection against intruders who are trying to access the resources illegally.

### VII. CONCLUSION

Cloud computing is technology which has lot of benefits to the cloud users in terms of cost, accessibility and scalability. In spite of these advantages, there are many challenges and security is one of the challenges to be addressed. In order to protect against the attacks launched by illegal users, MSA mechanism is used in the applied. Different authentication mechanisms are discussed. Adversary scenario is presented and how attacker gains access to cloud resources to disrupt the regular functioning of cloud environment. The approach is validated with mealy machine theory. Mealy machine representation provides the stage changes along with trust flow from one stage to another to evaluate if any unauthorized access is carried out. MSA uses the factors viz user name, email id, phone number and OTP. Though user is registered, authentication mechanism has to be carried out every time user wants to access the virtual machines. The proposed approach protects against the attacks such as spoofing, replay and data theft. The results clearly depict how strong the authentication mechanism with respect to number of authenticated logins and time duration. With the observation of the approach implemented, it is quite unlikely to get the access by unauthorized users to the virtual machine which is meant for legitimate users. With the benefit of security, there is an overhead experienced by the user in passing through multiple stages to authenticate and access the VM whenever it is required.

In future, it is planned to consider the roles and grant the access to the virtual machines in cloud environment.

### REFERENCES

- [1] G. Kaur and R. Kumar, "A Review on Reliability Issues in Cloud Service," *Int. J. Comput. Appl.*, no. Icaet, pp. 975–8887, 2015, [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.736.1442&rep=rep1&type=pdf>.
- [2] R. Buyya, "Introduction to the IEEE transactions on cloud computing," *IEEE Trans. Cloud Comput.*, vol. 1, no. 1, pp. 3–21, 2013, doi: 10.1109/TCC.2013.13.

- [3] I. E. Liao, C. C. Lee, and M. S. Hwang, "A password authentication scheme over insecure networks," *J. Comput. Syst. Sci.*, vol. 72, no. 4, pp. 727–740, 2006, doi: 10.1016/j.jcss.2005.10.001.
- [4] M. Kazim, "A survey on top security threats in cloud computing," vol. 6, no. 3, 2015.
- [5] N. Veeraragavan and L. Arockiam, "Enhanced Authentication Mechanism for Securing the Cloud Services using AaaS," vol. 3, no. 3, pp. 171–175, 2016, doi: 10.17148/IARJSET.2016.3336.
- [6] B. Macleij, E. F. Imed, and M. Kurkowski, "Multifactor Authentication Protocol in a Mobile Environment," *IEEE Access*, vol. 7, pp. 157185–157199, 2019, doi: 10.1109/ACCESS.2019.2948922.
- [7] M. Wazid, A. K. Das, R. Hussain, G. Succi, and J. J. P. C. Rodrigues, "Authentication in cloud-driven IoT-based big data environment: Survey and outlook," *J. Syst. Archit.*, vol. 97, no. September 2018, pp. 185–196, 2019, doi: 10.1016/j.sysarc.2018.12.005.
- [8] A. Acar, W. Liu, R. Beyah, K. Akkaya, and A. S. Uluagac, "A privacy-preserving multifactor authentication system," *Secur. Priv.*, vol. 2, no. 5, pp. 1–19, 2019, doi: 10.1002/spy2.88.
- [9] A. Jesudoss and N. P. Subramaniam, "A Survey on Authentication Attacks and Countermeasures in a Distributed Environment," *Indian J. Comput. Sci. Eng.*, vol. 5, no. 2, pp. 71–77, 2014.
- [10] Lal, Nilesh A., Salendra Prasad, and Mohammed Farik. "A review of authentication methods." vol 5 (2016): 246-249.
- [11] W. Li and L. Ping, "Trust model to enhance security and interoperability of cloud environment," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 5931 LNCS, pp. 69–79, 2009, doi: 10.1007/978-3-642-10665-1\_7.
- [12] D. D. Kumar, K. Vijay, S. Bhavani, E. Malathy, and R. Mahadevan, "A study on different types of authentication techniques in data security," *Int. J. Civ. Eng. Technol.*, vol. 8, no. 12, pp. 194–201, 2017.
- [13] B. D. Deebak, F. Al-Turjman, and L. Mostarda, "Seamless secure anonymous authentication for cloud-based mobile edge computing," *Comput. Electr. Eng.*, vol. 87, p. 106782, 2020, doi: 10.1016/j.compeleceng.2020.106782.
- [14] D. Dasgupta, A. Roy, and A. Nag, "Toward the design of adaptive selection strategies for multi-factor authentication," *Comput. Secur.*, vol. 63, pp. 85–116, 2016, doi: 10.1016/j.cose.2016.09.004.
- [15] A. Ometov, S. Bezzateev, N. Mäkitalo, S. Andreev, T. Mikkonen, and Y. Koucheryavy, "Multi-Factor Authentication: A Survey," *Cryptography*, vol. 2, no. 1, p. 1, 2018, doi: 10.3390/cryptography2010001.
- [16] B. B. Gupta and M. Quamara, "An identity based access control and mutual authentication framework for distributed cloud computing services in IoT environment using smart cards," *Procedia Comput. Sci.*, vol. 132, pp. 189–197, 2018, doi: 10.1016/j.procs.2018.05.185.
- [17] C. Singh and T. Deep Singh, "Article ID: IJCET\_10\_01\_020 Cite this Article: Charanjeet Singh and Dr. Tripat Deep Singh, A 3-Level Multifactor Authentication Scheme for Cloud Computing," *Int. J. Comput. Eng. Technol.*, vol. 10, no. 1, pp. 184–195, 2019,
- [18] A. Bhanushali, B. Mange, H. Vyas, H. Bhanushali, and P. Bhogle, "Comparison of Graphical Password Authentication Techniques," *Int. J. Comput. Appl.*, vol. 116, no. 1, pp. 11–14, 2015, doi: 10.5120/20299-2332.
- [19] A. G. Dinker, V. Sharma, Mansi, and N. Singh, "Multilevel authentication scheme for security critical networks," *J. Inf. Optim. Sci.*, vol. 39, no. 1, pp. 357–367, 2018, doi: 10.1080/02522667.2017.1374745.
- [20] S. Milad Dejamfar and S. Najafzadeh, "Authentication Techniques in Cloud Computing: A Review," *Int. J. Adv. Res. Comput. Sci. Softw. Eng.*, vol. 7, no. 1, pp. 95–99, 2017, doi: 10.23956/ijarcsse/v7i1/01105.
- [21] A. Ahmad, W. S. Zainudin, M. N. Kama, N. B. Idris, and M. M. Saudi, "State of the Art Intrusion Detection System for Cloud Computing," vol. 10, no. 3, pp. 480–495, 2018.
- [22] A. Narang and D. Gupta, "A review on different security issues and challenges in cloud computing," 2018 *Int. Conf. Comput. Power Commun. Technol. GUCON 2018*, no. October, pp. 121–125, 2019, doi: 10.1109/GUCON.2018.8675099.
- [23] N. Rasouli, M. R. Meybodi, and H. Morshedlou, "Virtual machine placement in cloud systems using Learning Automata," 13th *Iran. Conf. Fuzzy Syst. IFSC 2013*, no. May 2019, pp. 7–12, 2013, doi: 10.1109/IFSC.2013.6675616.
- [24] Aarts, Fides, et al. "Improving active Mealy machine learning for protocol conformance testing." *Machine learning* 96.1-2 (2014): 189-224.
- [25] Mavridou, Anastasia, and Aron Laszka. "Designing secure ethereum smart contracts: A finite state machine based approach." *International Conference on Financial Cryptography and Data Security*. Springer, Berlin, Heidelberg, 2018.
- [26] T. R. Thamburu and A. V. A. V., "International Journal of Advanced Research in A Survey on Trust Management Models in Internet of Things Systems," vol. 7, no. 1, pp. 15–21, 2017, doi: 10.23956/ijarcsse/v7i1/0115.
- [27] Q. W. Shang, K. Cao, and F. Wang, "The study on network attacks based on automaton theory," *Procedia Eng.*, vol. 23, pp. 653–658, 2011, doi: 10.1016/j.proeng.2011.11.2561.
- [28] P. Kumar, "Cloud Computing: Threats, Attacks and Solutions," *Int. J. Emerg. Technol. Eng. Res.*, vol. 4, no. 8, pp. 24–28, 2016, [Online]. Available: [www.ijeter.everscience.org](http://www.ijeter.everscience.org).
- [29] L. Khakim, M. Mukhlisin, and A. Suharjono, "Security system design for cloud computing by using the combination of AES256 and MD5 algorithm," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 732, no. 1, 2020, doi: 10.1088/1757-899X/732/1/012044.
- [30] Mearaj, Insha, Piyush Maheshwari, and Maninder Jeet Kaur. "Data conversion from traditional relational database to MongoDB using XAMPP and NoSQL." 2018 *Fifth HCT Information Technology Trends (ITT)*. IEEE, 2018.
- [31] Shenoy, Srinivasa, Nur Asyikin Abu Bakar, and Rajashekara Swamy. "An adaptive framework for web services testing automation using JMeter." 2014 *IEEE 7th International Conference on Service-Oriented Computing and Applications*. IEEE, 2014.

# Computer Vision based Polyethylene Terephthalate (PET) Sorting for Waste Recycling

Ouiem Bchir, Shahad Alghannam, Norah Alsadhan, Raghad Alsumairy, Reema Albelahid, Monairh Almotlaq  
Department of Computer Science, College of Computer and Information Sciences  
King Saud University, Riyadh, Saudi Arabia

**Abstract**—Recycling plays a vital role in saving the planet for future generations as it allows keeping a clean environment, reducing energy consumption, and saving materials. Of special interest is the plastic material which may take centuries to decompose. In particular, the Polyethylene Terephthalate (PET) is a widely used plastic for packaging various products that can be recycled. Sorting PET can be performed, either manually or automatically, at recycling facilities where the post-consumed objects are moving on the conveyor belt. In particular, automated sorting can process a large amount of PET objects without human intervention. In this paper, we propose a computer vision system for recognizing PET objects placed on a conveyor belt. Specifically, DeepLabv3+ is deployed to segment PET objects semantically. Such system can be exploited using an autonomous robot to compensate for human intervention and supervision. The conducted experiments showed that the proposed system outperforms the state of the art semantic segmentation approaches with weighted IoU equals to 97% and Mean BFscore equals to 89%.

**Keywords**—PET; recycling; computer vision; machine learning

## I. INTRODUCTION

Over the last decade, people around the world have a rising concern about efficient waste management due to the yearly waste increase. In fact, according to the World Bank Group 2020 statistics, 2.01 billion tons of solid municipal waste are engendered every year worldwide [1]. Furthermore, according to the same source, it is predicted that this amount would increase to 3.4 billion tons by 2050. One way of processing this huge amount of waste is by incineration. However, it can be harmful to the environment because of greenhouse gas emissions. Another commonly used way to process waste is landfill. Nevertheless, it is not appropriate for certain materials that need a very long time to biodegrade. In particular, plastic material, which constitutes 14% of the total waste amount [2], takes over 100 years to biodegrade. Therefore, recycling, which consists of processing and reusing the waste, emerged as an alternative method suitable for waste processing. Since the way of processing the waste depends on its type, the waste needs to be sorted. To make the sorting process easier, there are sometimes specific waste bins for the most common waste types such as plastic, glass, and paper. Even though different types of plastic require specific methods of treatment. Therefore, plastic materials must be sorted according to their type since the quality of waste separation highly affects the quality of the recycled plastic. One of the most valuable types of plastic for recycling is Polyethylene Terephthalate (PET). It is widely used for plastic bottles. It is

recognized by the symbol “PET” or “PETE” imprinted in the container.

The wide use of PET is due to the fact that it is environmentally friendly and inexpensive. For that reason, recycling centers sort plastic waste into PET and non-PET plastics. It is even further sorted into transparent, blue and green, and mixed color PET since they do not have the same sale price. In fact, transparent PET is the most valuable one and the mixed color is the least valuable [3]. Manual waste sorting is exhaustive and time consuming. Moreover, it may be affected by the worker’s condition. On the other hand, the PET chemical sorting process is very delicate, dangerous, and generates chemical residue [4]. Electrostatic systems that disperse plastics according to their types are alternative solutions for plastic sorting [5]. Nevertheless, they are not cost effective. Thus, mechanical approaches have been used instead, as they are safe and less costly [6]. They mainly use visual sensors to localize the PET materials that would be moved to the appropriate waste bin. Typically, mechanical sorting systems use a conveyor belt to carry the waste. When the waste reaches the camera position, an image of the waste scene is captured. Then, a computer vision system localizes the PET object in the captured image and categorizes it using image processing and machine learning techniques. More specifically, the image is segmented into objects. Then, these objects are conveyed as input to a recognition system in order to categorize it as PET or non-PET. Nevertheless, suitable visual descriptors need to be extracted from the image in order to discriminate PET objects effectively. In this respect, considering the diversity of PET waste and the background clutter, the determination of such features is arduous and constitutes a hindrance for computer vision systems [7]. One way of alleviating the problem of choosing the appropriate visual features is through the use of deep learning techniques ability to semantically segment the waste image.

In this paper, we propose to localize and categorize PET plastics on the conveyor belt. The proposed approach will semantically segment the PET material. To achieve this, DeepLabv3+ deep neural network architecture [8] will be trained to learn PET containers’ visual characteristics.

## II. SEMANTIC SEGMENTATION

In the field of computer vision, image segmentation is the task of dividing the image into sets of pixels called segments. It is considered as a one of the most difficult and challenging problems in the computer vision field [9]. Image segmentation aims to represent the image at a higher level in a way that

facilitates its analysis by localizing objects and edges. Over the last decades, image segmentation has been used in several applications such as medical image analysis, scene understanding, robotic vision, and self-driving cars [10]. The image segmentation process can be supervised or unsupervised. Unsupervised image segmentation does not require a training phase, and thus previous knowledge of the object is not needed [11]. Alternatively, supervised segmentation requires a training phase that uses a set of labeled pixels. It can be perceived as a classification of the pixels that constitute the image [12]. While instance segmentation treats multiple instances of the same object as distinct objects [13], semantic segmentation treats multiple instances of the same object as a single one. It does not differentiate between two or more instances referring to the same object in the same image. In the last decade, semantic segmentation approaches were mainly based on the extraction of suitable engineered features fed to a classifier. However, the efficiency of these approaches depends heavily on the extracted features. This is considered a critical factor for the progress of semantic segmentation [14]. Recently, the boost of Deep Learning in the context of computer vision has also affected semantic segmentation [14].

The development of Deep Convolutional Neural Net (DCNN) led to a significant improvement in semantic segmentation [15]. One of the main characteristics that led to the success of DCNN is its ability to learn abstract data representation [16]. However, while the special abstraction is recommended for classification tasks, it impedes semantic segmentation. In fact, semantic segmentation approaches based on DCNN face three main problems. The first one is related to the repeated combination of the max-pooling layer and striding that yields a feature map with decreased feature resolution [17]. The second obstacle concerns the multi-scale challenge, where the objects may have different scales [18]. This induces increasing the number of computations since it requires training the network with different scale versions of the image. The third hindrance is due to the discard of the location information [19]. DCNN, designed for image classification and object detection, is invariant to special transformation. This results in inconsistent segmentation outcomes. Furthermore, as semantic segmentation implicates segmentation and classification processes, the key point is then how to adjoin the two processes. We distinguish three types of deep learning approaches for semantic segmentation. The first type starts by learning the object regions [20] [21]. These regions, integrating the shape information, are then conveyed to a DCNN classifier [22] [23]. This type of approach depends on the results of the segmentation phase which in its turn depends on the engineered features. Alternatively, the second type of approach uses the convolution layers of DCNN to extract the features to use them for the segmentation phase [19] [24] [25]. However, segmentation and classification tasks are still performed in cascade. Therefore, classification still depends on the segmentation phase and consequently, any segmentation error cannot be recovered by the classification task. The third type employs DCNN directly on the images to learn the pixels' categories [17] [26]. This eliminates the segmentation phase. In order to enhance the segmentation performance along the

edges, the Conditional Random Fields (CRFs) approach [23] has been integrated into the DCNN based approaches [24] [27]. In fact, by taking into consideration the neighboring pixels, the object boundaries are better localized. CRF has been used as a post-processing step [8]. It has also been integrated to the DCNN architecture in [23], [24], [25], [26] and [27].

### III. RELATED WORK

In the literature, several PET sorting approaches have been reported. Among the reported works, some works designed a handcrafted feature suitable for PET categorization [28] [29] [30]. Other works used available generic handcrafted features [31] [32].

#### A. PET Sorting Approaches based on Application Dedicated Handcrafted Features

The approach in [28] extracts the foreground object (the waste object) by employing background subtraction. After connecting the obtained objects and enhancing the border using morphological operations, small blobs are discarded according to a pre-defined size threshold. For the remaining blobs called "white strips", a contour box is determined along its eight surrounding boxes of the same size called "grey strips". After the detection of the plastic blobs, a visual descriptor is extracted. The authors in [28] designed a new handcrafted feature. It is based on modeling the color distribution of the "grey strips". Alternatively, the authors in [29] propose the "white pixel" approach. They first start by preprocessing the image by performing noise removal, background subtraction, and grey level transformation. Then, they employ the MATLAB function "regionprops" [33] to split the image into a set of disconnected objects. This results in reducing the problem to a classification problem where only one object is present in the image. From the obtained grey level image, the authors designed two handcrafted features. The first one is extracted from the whole image by computing the average of the last 106 entries of the 256-bin normalized color histogram. Assuming that the bottom of the container is not covered by a label and is transparent showing the black color of the conveyer belt, the second proposed feature divides the image into five parts and extracts the center of the fifth one. From the extracted Region of Interest, ROI, the mean and standard deviation of the first 100 entries of the normalized 256-bin color histogram are computed. The resulting two features are then fed to the Linear Discriminant Analysis (LDA) classifier [34]. On the other hand, the reported approach in [30] assumes that only one object is present in the scene. It starts by converting the RGB image to a greyscale one. Then, the Canny edge detector [35] is employed to detect the object in the image. The 256-bin histogram is computed from the detected object based on which the authors in [30] designed a new handcrafted feature. The proposed feature consists of two values. The first one is the sum of the first one hundred entries of the 256-bin histogram,  $v_1$ , and the second one is the sum of the last one hundred entries,  $v_2$ . Similar to the proposed approach in [29], the authors in [30] assume that PET objects are transparent. Thus, they will be perceived as black, like the color of the conveyer belt. Considering this assumption, they design a rule to classify PET and non-PET

objects. More specifically, an object is considered PET if  $v_1$  is greater than  $v_2$ .

### B. PET Sorting Approaches based on Generic Handcrafted Features

The authors in [31] proposed a PET sorting system. They assume that there is only one object in the captured image and propose to classify plastic bottles carried on a conveyor belt as PET or non-PET. Moreover, they propose to further classify non-PET plastic bottles as High Density Polyethylene (HDPE) or Polypropylene (PP). The preprocessing step starts by segmenting the image using Otsu's thresholding method [36] in order to locate the object. It is followed by background subtraction and segmentation enhancement using morphological operators. The authors suggest working directly on the pixels of the considered object. However, due to the image's size, the obtained feature has a high dimension and the system would then be prone to the curse of dimensionality. That is why they propose to reduce the dimensionality using five techniques. Namely, they used Principal Component Analysis (PCA) [[37] [38], Kernel PCA [39], Fisher's Linear Discriminant Analysis (FLDA) [40], Singular Value Decomposition (SVD) [41], and Laplacian Eigenmaps (LEMAP) [42]. The resulting feature vectors are fed separately to the Support Vector Machine (SVM) classifier [43]. Then, the classification results obtained using each feature are combined using the majority vote approach. Alternatively, the system proposed in [32] treats each object present in the image separately. First, edges are detected. Then, standard shape features are extracted. These are the length, the width, the area, the aspect ratio, and the filling fraction. The Cartesian and polar coordinates of the 90 equally spaced points of the perimeter are also considered. The authors in [32] considered three classifiers. Namely, the K-Nearest Neighbor (KNN) [34] with  $K=1$ , Kohonen map [44], and Artificial Neural Net (ANN) [45]. For the KNN classifier they used the geometric feature, the Cartesian coordinates of the perimeter, and its polar coordinates separately. On the other hand, the geometric feature is used with Kohonen map, and the polar coordinate of the perimeter is used with ANN. Moreover, the authors designed a "factor-of-merit" measure to decide on the final category of the object. In fact, the "factor-of-merit" is computed for the different considered system results in order to combine them. The system is assessed in a 50-instance dataset.

### C. Convolutional Neural Net based Approaches

In [46], the authors developed a system that sorts four kinds of waste: glass, paper, plastic, and metal, based on a pre-trained ResNet-50 architecture [47]. ResNet was pre-trained using ImageNet dataset [48]. It is used to extract the feature automatically from the whole image. In fact, a single object is considered per image. A multi-class soft kernel SVM [43] is used instead of softmax for the classification task. In [49], the authors proposed a waste management system using ResNet-34 deep learning architecture. The system assumes the presence of a single object in the captured image. The work in [49] classifies the waste into six categories which are cardboard, glass, metal, plastic, paper, and trash. Nevertheless, the proposed system aims to classify the waste as digestible and indigestible. In fact, cardboard, glass, metal, plastic, and

paper categories are considered indigestible while the remaining waste is considered digestible. A computer vision waste sorting approach is proposed in [50]. It considers a single object per image. The authors adopted AlexNet [51] deep learning architecture to categorize various types of waste material. However, this system performed poorly compared to the system based on extracting Scale Invariant Feature (SIFT) [52] and feeding it to the SVM classifier [43]. The authors in [53] proposed a waste sorting system for all types of materials. It is based on DenseNet-121 [54] deep learning architecture. The choice of DenseNet was motivated by the small size of the dataset [53]. In an attempt to improve the performance, data augmentation is employed by considering vertical, horizontal, and random 25° rotations. To further improve the system's performance, a genetic algorithm is utilized to optimize the hyper-parameters of the fully connected layers.

As stated above, various vision-based recognition approaches have been proposed in the literature. The extracted features differ between these approaches. Some papers focus on designing handcrafted features suitable for the PET sorting application [28] [29] [30]. However, these approaches assumed that PET materials are transparent. The designed features are based on the fact that PET containers appear black like the conveyor belt color. Nevertheless, this is not the case. PET containers can be transparent, blue and green, and mixed colors. This infers that these approaches addressed only the problem of sorting transparent PET materials. Other approaches used existing generic features [31] [32]. One of them used dimensionality reduction on the image pixels as a feature. The other one employed the shape feature. However, in addition to using only 50 instances as a dataset, the shape feature would not be able to recognize crashed containers. These feature-based approaches face the challenge of feature choice or feature design. Moreover, the images need to be preprocessed and segmented in order to separate the object from the background. This makes the system performance sensitive to the performance of these preprocessing and segmentation techniques. Convolutional Neural Nets, CNN, would alleviate these problems by learning the appropriate feature without the need of preprocessing and segmentation techniques. However, the only approach that used deep learning to classify PET bottles did not classify plastic as PET or non-PET [55]. Rather, only PET bottles are fed to their system, which identifies the state of the PET bottles. Namely, it checks if the PET bottle has a cap, a seal, or content. Thus, to the best of our knowledge, no reported work addressed the problem of PET sorting using CNN. Alternatively, sorting all kinds of waste approaches based on various Deep CNN have been reported [46] [49] [50] [53]. Among these approaches, two are based on ResNet architecture [46] [49]. Another is based on AlexNet [50] and performed poorly. While the other is based on DenseNet [53] and would be practical only for small datasets.

## IV. PROPOSED APPROACH

We propose to segment the images captured from the conveyor belt semantically. Three categories need to be localized and identified. These are transparent PET, blue and green PET, and mixed color PET. For this purpose, we employ DeepLabv3+ [8]. Fig. 1 displays the architecture of

the proposed system. DeepLabv3+ [8] is designed to overcome the limitations of existing semantic segmentation approaches based on DCNN. More specifically, DeepLabv3+ [8] adopts an encoder-decoder architecture and uses Resnet as a backbone for the encoder. Nevertheless, as shown in Fig. 2, it introduces modifications to the Resnet through the use of atrous convolution. Moreover, Atrous Spatial Pyramid Pooling (ASPP) and fully connected Conditional Random Fields (CRF) are incorporated.

Fig. 2 shows a simplified structure of DeepLabv3+ model. As shown, the Resnet model reduces the size of the input image by a factor of 16. Nevertheless, DeepLabv3+ discards the striding of the last convolutional layer and replaces it by atrous convolution with rate equal to 2, and appends it by the Atrous Spatial Pyramid Pooling (ASPP) module. The output of ASPP is then up-sampled by 4 in the decoder module. The obtained feature map is concatenated with a feature map from the encoder module that has the same size, specifically the one down-sampling the input by a factor of 4. Next, it is convoluted using a set of 3X3 filters, and then up-sampled by 4 to engender an output of the same size of the input. Recurrent pooling and convolution layers decrease the resolution of the obtained feature. To remedy that, atrous convolution is introduced. Its idea comes from the wavelet decomposition. It up-samples the filter by inserting holes that are filled with zeroes to enlarge the receptive field. This is called Atrous convolution, or dilated convolution. Moreover, DCNNs are able to handle objects with different scales by using the Atrous Spatial Pyramid Pooling (ASPP) method.

The latter performs four parallel operations. These are one convolution with kernel 1X1 and three atrous convolutions with kernel 3X3 and rates equal to 6, 12 and 18, respectively. This results in extracting 4 features at different scales. The feature map learned at the end of the encoder is a stack of the obtained 4 features. To alleviate the localization problem, fully connected Conditional Random Field (CRF) [23] is employed. It is a statistical approach that models the relation between pixels by estimating the cost of assigning a pair of labels to a pair of pixels (pairwise cost). Its main function is to clear out invalid predictions by coupling neighbor pixels and privileging same label assignment for nearby pixels.

This leads to refining the segmentation result. Furthermore, DeepLabv3+ adopts the encoder-decoder architecture. It aims to refine the edges obtained by the segmentation. More specifically, the encoder is responsible for extracting the features and the decoder allows retrieving the spatial resolution. The encoder consists of two modules which are ResNet with atrous convolution component and the ASPP. The decoder merges and up-samples the learned features and the result of the encoder after up-sampling. We train DeepLabv3+ using labeled captured images. Images captured from the conveyor belt are fed to DeepLabv3+ [8]. The corresponding mask images are provided at the output. Mask images indicate the label of each pixel of the input image. The label could be transparent, blue and green, mixed color, or others.

## V. EXPERIMENTS

In order to evaluate the performance of the proposed approach, a dataset is collected. It includes images of size 720X960X3 pixels captured from 420X594 mm scene using a camera. The scene contains PET and non-PET materials on a black background representing the conveyor belt. The waste materials can be overlapped or not. Three types of PET are considered. These are transparent, blue and green, and mixed color PET. The dataset is labeled manually accordingly. The performance of the proposed approach is assessed using five performance measures. These are the standard performance measures used for semantic segmentation that take into consideration both the categorization and localization performances [57]. Namely, we will use the Global Accuracy [58], Mean Accuracy [58], Mean Intersection over Union (Mean IoU) [10], Weighted Intersection over Union (Weighted IoU) [58], and Mean BFscore [59]. In order to assess the performance of the proposed system, we intend to conduct three experiments.

### A. Experiment 1

In this experiment, we try to empirically figure out the best hyperparameter configuration for both Resnet-50 and Resnet-18 [47] when they are used as backbone models for the DeepLabv3+ in the context of PET sorting. In this regard, we train two DeepLabv3+ models. Precisely, Resnet-50 and ResNet-18 are trained using 60% of the data, validated on 20%, and tested on the remaining 20%. For each considered model, various configurations were tested. In particular, the optimizer, the learning rate, and the L2 regularization parameter were tuned. This results in 6 configurations for each model. Table I and Table III report the details of each

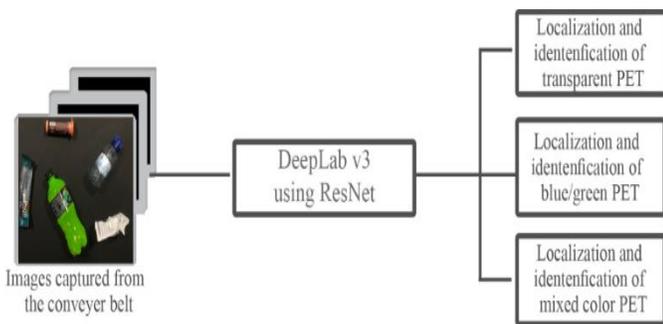


Fig. 1. Proposed System Architecture.

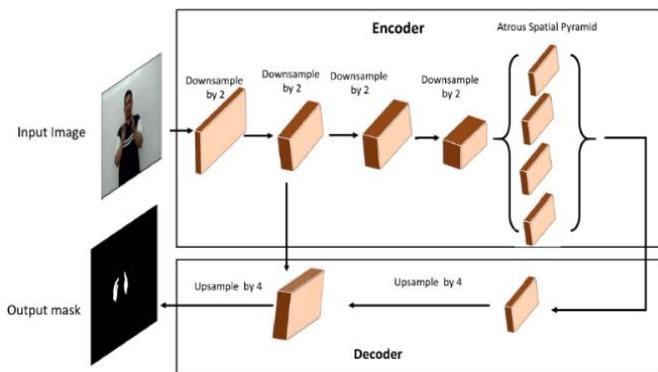


Fig. 2. Simplified Structure of DeepLabv3+ [56].

considered configuration with respect to Resnet-50 and Resnet-18 [47], respectively. Moreover, for this experiment the size of batch is set to 2 and the number of epochs is set to 30. In order to determine the best model, the testing performance results of each configuration are reported. These are Global Accuracy, Mean Accuracy, Mean IoU, Weighted IoU, and Mean BFscore.

TABLE I. THE CONSIDERED CONFIGURATIONS FOR RESNET-50

	Optimizer	Learning rate	L2 regularization
Configuration 1	SGDM	1e-3	0.005
Configuration 2	ADAM	1e-3	0.05
Configuration 3	SGDM	Initially:1e-3 Learn Rate Drop Period: 5 Learn Rate Drop Factor: 0.2	0.001
Configuration 4	SGDM	Initially:1e-3 Learn Rate Drop Period: 6 Learn Rate Drop Factor: 0.5	0.001
Configuration 5	SGDM	Initially:1e-3 Learn Rate Drop Period: 4 Learn Rate Drop Factor: 0.05	0.001
Configuration 6	SGDM	Initially:5e-2 Learn Rate Drop Period: 5 Learn Rate Drop Factor: 0.2	0.001

TABLE II. WEIGHTED IOU AND MEAN BFSCORE WHEN USING RESNET-50

	Weighted IoU	Mean BFscore
Configuration 1	0.9476	0.8744
Configuration 2	0.7539	0.7084
Configuration 3	0.9687	0.8933
Configuration 4	0.9233	0.8420
Configuration 5	0.9268	0.8146
Configuration 6	0.6333	0.6591

TABLE III. THE CONSIDERED CONFIGURATIONS FOR RESNET-18

	Optimizer	Learning rate	L2 regularization
Configuration 1	SGDM	1e-3	0.005
Configuration 2	SGDM	1e-4	0.001
Configuration 3	SGDM	Initially:5e-3 Learn Rate Drop Period: 5 Learn Rate Drop Factor: 0.2	0.001
Configuration 4	SGDM	Initially:1e-2 Learn Rate Drop Period: 6 Learn Rate Drop Factor: 0.03	0.001
Configuration 5	SGDM	5e-3	0.01
Configuration 6	SGDM	Initially:2e-2 Learn Rate Drop Period: 1 Learn Rate Drop Factor: 0.3	0.1

TABLE IV. WEIGHTED IOU AND MEAN BFSCORE WHEN USING RESNET-18

	Weighted IoU	Mean BFscore
Configuration 1	0.9252	0.8337
Configuration 2	0.9165	0.7698
Configuration 3	0.7863	0.6905
Configuration 4	0.8002	0.7077
Configuration 5	0.8122	0.7328
Configuration 6	0.7978	0.7012

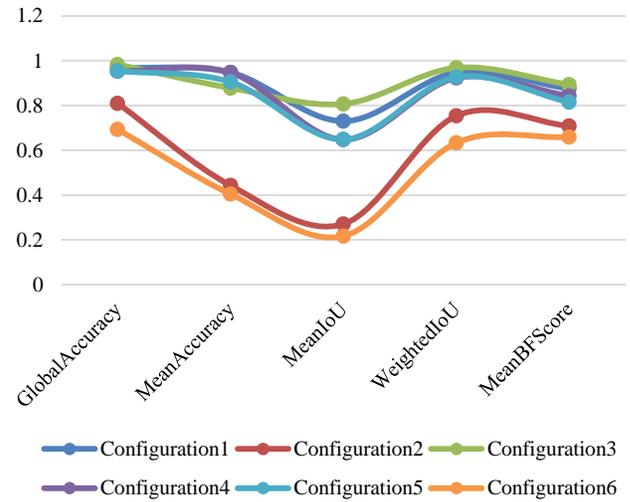


Fig. 3. Proposed System Performance when using Resnet-50 as Backbone.

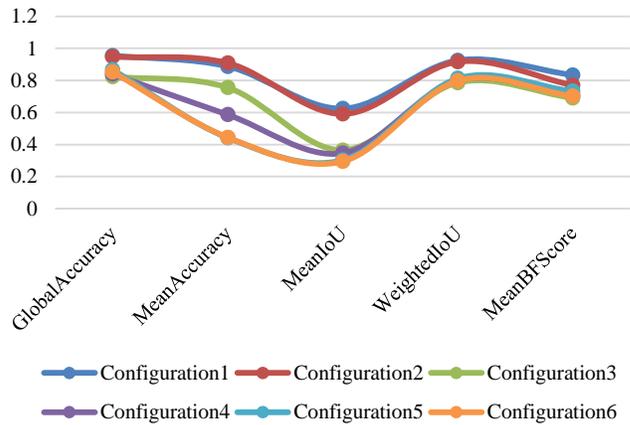


Fig. 4. Proposed System Performance when using ResNet-18 as Backbone.

Fig. 3 displays the performance measures of the system when using Resnet-50 as backbone for the DeepLabv3+ semantic segmentation approach. Similarly, Fig. 4 shows these performances when using Resnet-18. Table II and Table IV report Weighted IoU and Mean BFscore for Resnet-50 and Resnet-18, respectively.

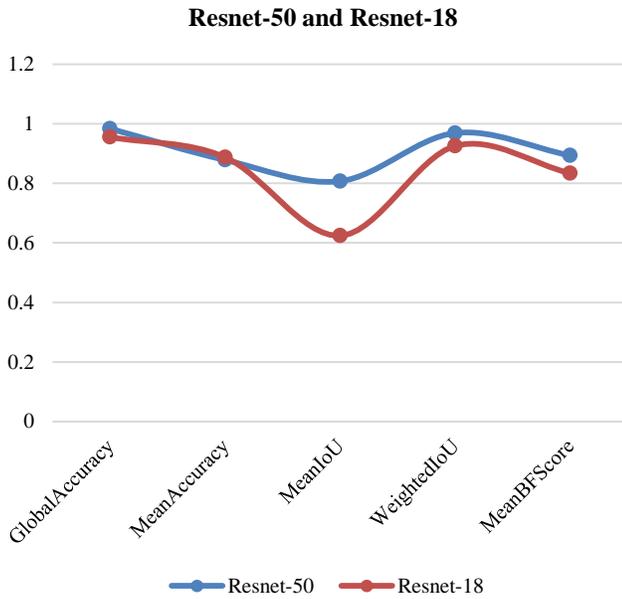


Fig. 5. Resnet-50 and Resnet-18 Models.

As shown in Fig. 3 and Fig. 4, configuration 3 allowed obtaining the best performance for Resnet-50. Actually, since the data is unbalanced Weighted IoU and Mean BFscore reflect better the performance of the system. Thus, configuration 3 outperformed the other configurations with a Weighted IoU of 0.9687, and Mean BFscore of 0.8933. This is confirmed by the results reported in Table II. More specifically, configuration 3 uses stochastic gradient descent (SGDM) as optimizer, a learning rate initially set to 0.001, and increasing by a factor of 0.2 every 5 epochs, and an L2 regularization of 0.001. According to [60], SGDM is expected to give better results. Moreover, the considered learning rate gave better result by avoiding missing the optimal weights while training the network. Furthermore, the L2 regularization of 0.001 avoided both over-fitting and under-fitting situations. In fact, in case of a large value, the model doesn't fit well, while in case of a small value, the training time is too long. Concerning Resnet-18, the best performances in terms of Weighted IoU and Mean BFscore were obtained when adopting configuration 1 which consists of a constant learning rate of 0.001, and a L2 regularization of 0.005. In fact, by avoiding missing optimal values for the model, and not over-fitting it, these two hyperparameters yielded a Weighted IoU equal to 0.9252, and a Mean BFscore equal to 0.8337. This result is confirmed by Table IV where configuration 1 yielded better results.

### B. Experiment 2

In this experiment, we try to empirically determine which Deep Learning model, Resnet-50 or Resnet-18 [47] is more effective as backbone model for the DeepLabv3+ when used for PET sorting. In this regard, we take into consideration the best obtained results for both models according to experiment 1. Namely, we consider the results lead by configuration 3 for Resnet-50 and the one lead by configuration 1 for Resnet-18. Fig. 5 displays the performance measures of Resnet-50 and

Resnet-18 on the testing sets, respectively. As mentioned previously, since the data is unbalanced, Weighted IoU and Mean BFscore are more suitable to assess the performance of the system. Thus, in Table V, we report Resnet-50 and Resnet-18 performances in terms of Weighted IoU and Mean BFscore. To further investigate the obtained results, Fig. 6 shows the comparison between Resnet-50 and Resnet-18 in terms of Weighted IoU with respect to each considered class. Similarly, Fig. 7 displays the comparison between Resnet-50 and Resnet-18 in terms of Mean BFscore with respect to each considered class. Finally, Fig. 8 displays sample semantic segmentation results obtained using Resnet-18 and Resnet-50. Taking into account, the best obtained results for both Resnet-50 (configuration 3), and Resnet-18 (configuration 1), we compare the two models when used as backbone for deepLabv3+ semantic segmentation approach.

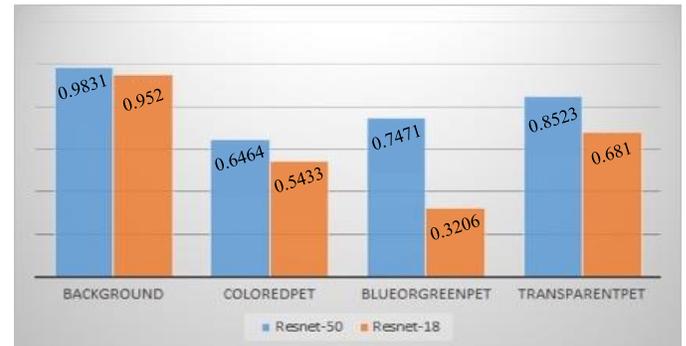


Fig. 6. Comparison between Resnet-50 and Resnet-18 in Terms of Weighted IoU with respect to each Considered Class.

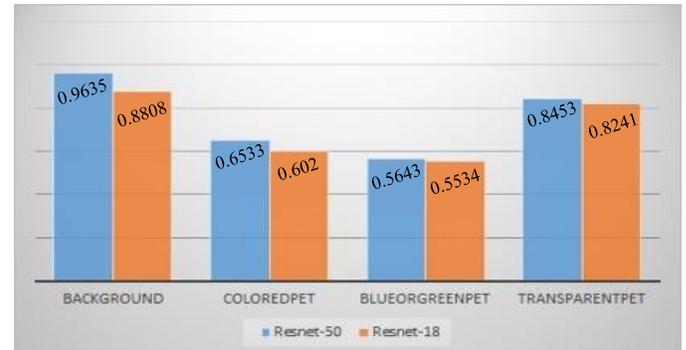


Fig. 7. Comparison between Resnet-50 and Resnet-18 in Terms of Mean BFscore with respect to each Considered Class.

TABLE V. TESTING WEIGHTED IOU AND MEAN BFSCORE COMPARISON BETWEEN RESNET-50 AND RESNET-18

	Resnet-50	Resnet-18
Weighted IoU	0.9687	0.9252
Mean BFscore	0.8933	0.8337

As shown, in Table V, Resnet-50 outperforms Resnet-18 with Weighted IoU equal to 0.97 and Mean BFscore equal to 0.89 for the testing results. The reason that Resnet-50 performs better than Resnet-18 can be explained by the fact that a deeper network learns more abstract features which yields better segmentation results.

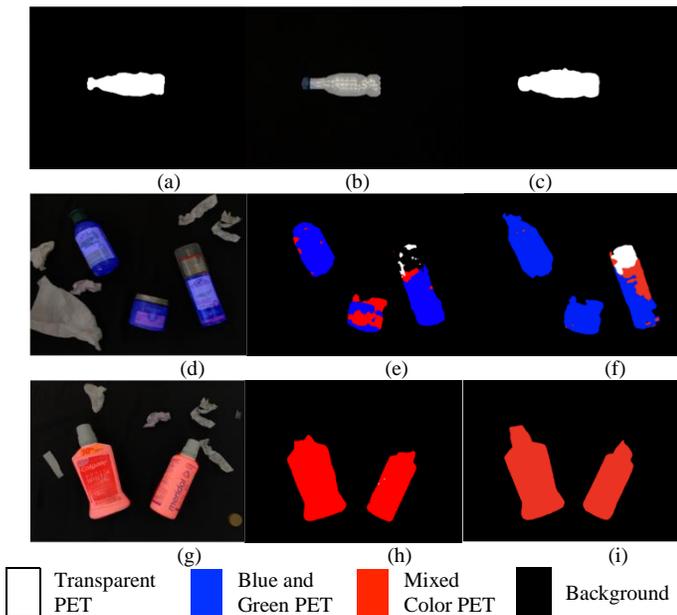


Fig. 8. Sample Semantic Segmentation Results Obtained using Resnet-18 and Resnet- 50. (a), (d), and (g) are the Original Images, (b),(e),and (h) The Segmentation Results Obtained when using Resnet-18, and (c), (f) and (i) The Segmentation Results Obtained when using Resnet-50.

As shown from Fig. 6 and Fig. 7, the performance is not the same for all considered categories. In fact, the background and Transparent PET classes have the higher performances. This is explained by the fact that background consists of black homogeneous color corresponding to the conveyor belt. Obviously, this is an easy segmentation problem. Concerning Transparent PET category, the obtained result can be attributed to the fact that this category is represented by a larger number of pixels in the dataset. In fact, if the model is trained with larger training set, the classification results are expected to be better. Alternatively, Blue or Green PET, and Colored PET are less represented in the training data. Furthermore, these two categories have large intra-class variance. In fact, in addition to the container shape variance, they are characterized by the color variance, whereas the background and the transparent PET categories have the same color per category. To better illustrate the obtained results, we can see from Fig. 8 (e) and Fig. 8 (f) that some blue or Green PET pixels are segmented as Mixed color PET or transparent PET. Similarly, from Fig. 8 (h) and Fig. 8 (i), we observe that some parts of the background are segmented as mixed color PET.

### C. Experiment 3

In this experiment, we intend to compare DeepLabv3+ semantic segmentation model to the state-of-the-art approaches on the waste sorting dataset. Namely, Fully Connected Network (FCN) [61], Unet [62], and Segnet [63] semantic segmentation approaches are considered. In this experiment, we consider Resnet-50 as backbone for DeepLabv3+ since it achieved better performance than Resnet-18. For the-state-of-the-art approaches, several hyperparameter configurations are considered. Moreover, in this experiment, the batch size is set to 2 for Unet [62], and Segnet [63]. It is the largest possible value due to the

memory size constraint. Alternatively, since FCN [61] uses a smaller size of the images (lower resolution), it is possible to increase the batch size 3. After considering the above mentioned configuration, the best obtained performance with respect to each approach is considered for the purpose of comparison with DeepLabv3+. Fig. 9 displays the performance comparison between DeepLabv3+ [47], FCN [61], Unet [62], and Segnet [63]. As depicted in Fig. 9, DeepLabv3+ outperforms the other deep learning segmentation approaches with weighted IoU equal to 0.9687 and a Mean BFscore of 0.8933. The second best is FCN, whereas Unet and Segnet perform poorly in terms of Mean BFscore.

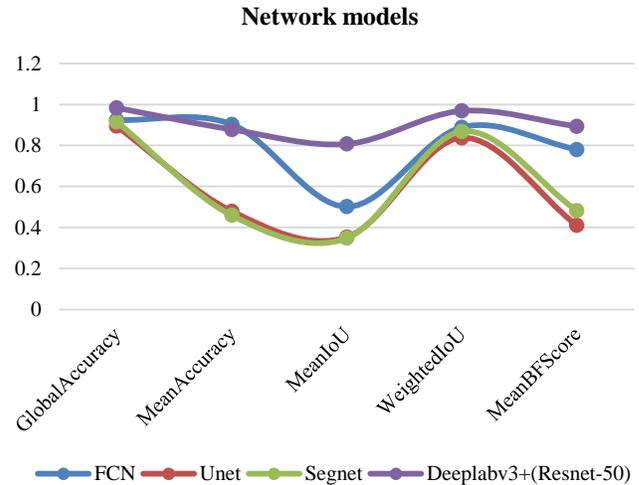


Fig. 9. Performance Comparison of DeepLabv3+ [47], FCN [61], Unet [62], and Segnet [63].

In order to better analyze the obtained results, a comparison of the four considered semantic segmentation approaches with respect to each category in terms of IoU and Mean BFscore is displayed in Fig. 10 and Fig. 11, respectively. As it can be seen from Fig. 10, DeepLabv3+ gives the best IoU performance with respect to all categories. This means that it is able to localize the PET container with respect to all categories better than the other approaches. Moreover, we can observe from Fig. 11 that DeepLabv3+ has the highest Mean BFscore with respect to most categories. However, the semantic segmentation performance is not the same with respect to all categories. This is the case for all considered segmentation approaches. For a better illustration of the results, we show sample segmentation results of DeepLabv3+ [47], FCN [61], Unet [62], and Segnet [63]. As shown in Fig. 12, Deeplabv3+ outperforms the other semantic segmentation approaches for the sample image representing the transparent PET. In fact, it localizes and identifies better the boundaries of the containers. This can be accredited to fully connected Conditional Random Field (CRF) module. Similar result can be observed from Fig. 13. In fact, although DeepLabv3+ miss - segmented some Blue and Green PET pixels as Mixed Color PET (Fig. 13(b)), it performs better than the other segmentation approaches. FCN is the second best (Fig. 13(c)). However, Unet (Fig. 13(d)) and Segnet (Fig. 13(e)) are not able to segment the Blue and Green PET image

shown in Fig. 13 (a). Actually, these two approaches classified the corresponding pixels as transparent PET. It means they were not able to capture the visual characteristics of the Blue or Green category.

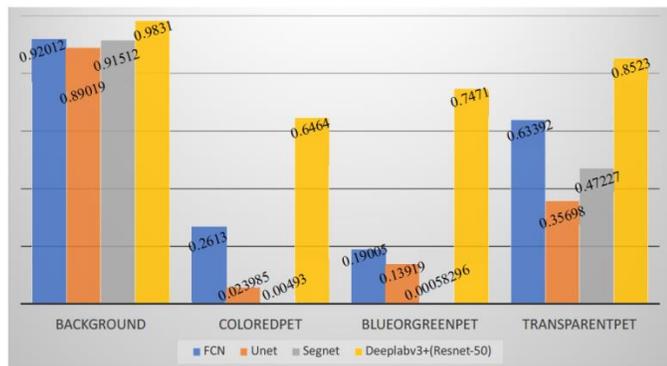


Fig. 10. Performance Comparison of the Four Considered Semantic Segmentation Approaches with respect to each Category in Terms of IoU.

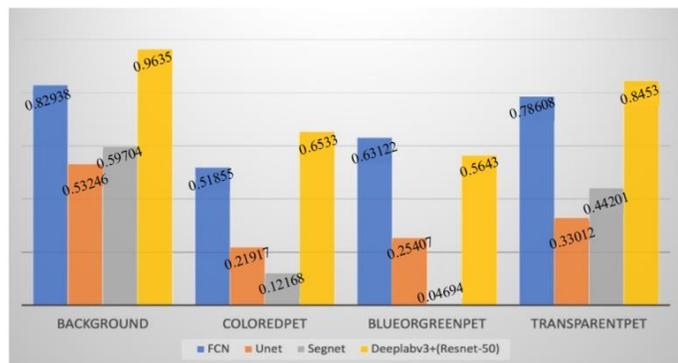


Fig. 11. Performance Comparison of the Four Considered Semantic Segmentation Approaches with respect to each Category in Terms of Mean BfScore.

FCN miss-segmented some pixels as transparent PET, and Unet and Segnet miss-segmented a large number of pixels as transparent PET. Actually, the confusion between the conveyor belt and the transparent PET can be explained by the fact that the transparency of this material makes them appear as black. Nevertheless, DeepLabv3+ is able to learn the appropriate visual feature that in engendered good segmentation result.

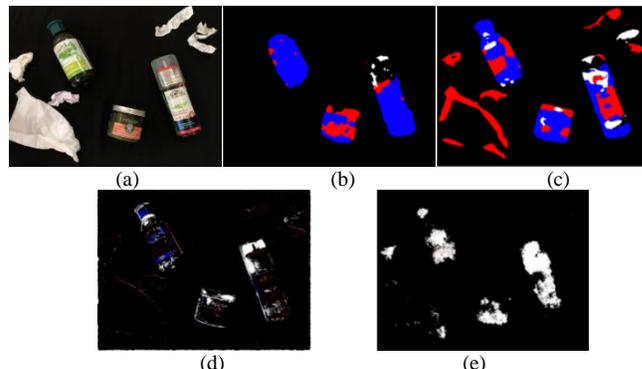


Fig. 13. Blue or Green PET Sample Image (a) Segmentation Results of (b) DeepLabv3+, (c) FCN (d) Unet, and (e) Segnet.

Legend: Transparent PET (white), Blue and Green PET (blue), Mixed Color PET (red), Background (black)

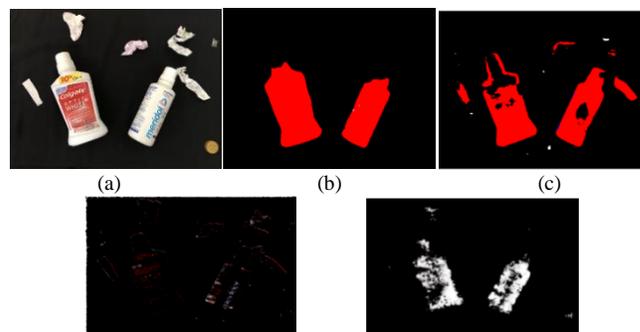


Fig. 14. Colored PET Sample Image (a) Segmentation Results of (b) DeepLab v3+, (c) FCN (d) Unet, and (e) Segnet.

Legend: Transparent PET (white), Blue and Green PET (blue), Mixed Color PET (red), Background (black)

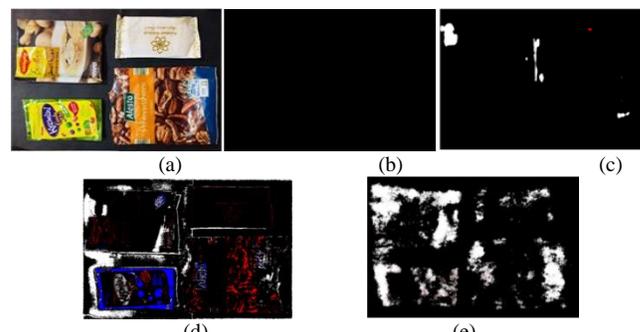


Fig. 15. Non-PET Sample Image (a) Segmentation Results of (b) DeepLab v3+, (c) FCN (d) Unet, and (e) Segnet.

Legend: Transparent PET (white), Blue and Green PET (blue), Mixed Color PET (red), Background (black)

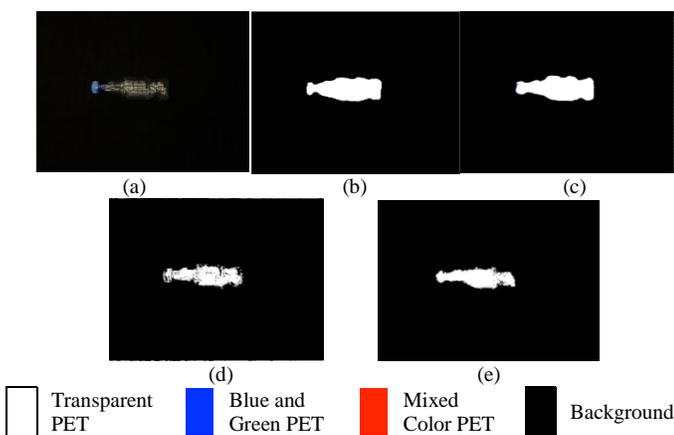


Fig. 12. Transparent PET Sample Image (a) Segmentation Results of (b) DeepLabv3+, (c) FCN (d) Unet, and (e) Segnet.

As showcased in Fig. 14, DeepLabv3+ yields better segmentation results than the other approaches. For this case too, FCN is the second best, and Unet and Segnet perform poorly. Similar analysis can be conducted on Fig. 15. Although the background (the black conveyor belt and other non-PET materials) is correctly segmented by DeepLabv3+,

## VI. CONCLUSION AND FUTURE WORK

Plastic containers are one of the most common types of waste. In order to be recycled, they need to be sorted according to their type since the quality of recycled plastic depends on the quality of waste separation. Of particular interest is Polyethylene Terephthalate (PET). In fact, recycling centers sort plastic waste into PET and non-PET, and further sort PET into transparent PET, blue and green PET, and mixed color PET. For this purpose, mechanical systems have been used. They need to recognize and localize PET materials in order to move them to the appropriate waste bin. In this context, we proposed to design a computer vision system to locate and recognize PET waste materials in a captured waste image using a deep learning network architecture called DeepLabv3+. The conducted experiments showed that increasing the number of layers of Resnet from 18 to 50 yields better semantic segmentation results. Furthermore, DeepLabv3+ outperformed the other considered approaches on the PET sorting dataset. As future works, we suggest to use Resnet with even larger number of layers, and to investigate ways to decrease the frame processing time.

### REFERENCES

- [1] "Trends in Solid Waste Management," 2020. [https://datatopics.worldbank.org/what-a-waste/trends\\_in\\_solid\\_waste\\_management.html](https://datatopics.worldbank.org/what-a-waste/trends_in_solid_waste_management.html) (accessed Oct. 10, 2020).
- [2] J. N. Hahladakis and E. Iacovidou, "Closing the loop on plastic packaging materials: What is quality and how does it affect their circularity?," *Sci. Total Environ.*, vol. 630, pp. 1394–1400, 2018, [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0048969718307307>.
- [3] "Polymer waste management: pet recycling." <http://polymerwastemanagement.blogspot.com/2007/11/pet-recycling.html> (accessed Oct. 10, 2020).
- [4] L. Bartolome, M. Imran, B. G. Cho, W. A. Al-Masry, and D. H. Kim, "Recent Developments in the Chemical Recycling of PET," in *Material Recycling - Trends and Perspectives*, InTech, 2012, pp. 65–84.
- [5] C. H. Park, H. S. Jeon, H. S. Yu, O. H. Han, and J. K. Park, "Application of electrostatic separation to the recycling of plastic wastes: Separation of PVC, PEL and ABS," *Environ. Sci. Technol.*, vol. 42, no. 1, pp. 249–255, 2008.
- [6] A. Picon, O. Ghita, P. F. Whelan, and P. M. Iriondo, "Fuzzy spectral and spatial feature integration for classification of nonferrous materials in hyperspectral data," *IEEE Trans. Ind. Informatics*, vol. 5, no. 4, pp. 483–494, 2009.
- [7] Y. Tachwali, Y. Al-Assaf, and A. R. Al-Ali, "Automatic multistage classification system for plastic bottles recycling," *Resour. Conserv. Recycl.*, vol. 52, no. 2, pp. 266–285, 2007, [Online]. Available: <https://dspace.aus.edu/xmlui/bitstream/handle/11073/106/35.232-2005.07.pdf?sequence=1&isAllowed=y>.
- [8] L. C. Chen, G. Papandreou, I. Kokkinos, K. Murphy, and A. L. Yuille, "DeepLab: Semantic Image Segmentation with Deep Convolutional Nets, Atrous Convolution, and Fully Connected CRFs," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 40, no. 4, pp. 834–848, 2017.
- [9] Z. Li, W. Yang, S. Peng, and F. Liu, "A Survey of Convolutional Neural Networks: Analysis, Applications, and Prospects," arXiv:2004.02806, 2020, [Online]. Available: <http://arxiv.org/abs/2004.02806>.
- [10] I. Ulku and E. Akagunduz, "A Survey on Deep Learning-based Architectures for Semantic Segmentation on 2D images," arXiv:1912.10230, 2019.
- [11] A. Kanezaki, "Unsupervised image segmentation by backpropagation," in *IEEE international conference on acoustics, speech and signal processing (ICASSP)*, Tokyo, 2018.
- [12] V. Lempitsky, A. Vedaldi, and A. Zisserman, "A pylon model for semantic segmentation," in *Advances in Neural Information Processing Systems 24: 25th Annual Conference on Neural Information Processing Systems*, Granada, 2011.
- [13] "A 2019 Guide to Semantic Segmentation | by Derrick Mwititi | Heartbeat." <https://heartbeat.fritz.ai/a-2019-guide-to-semantic-segmentation-ca8242f5a7fc> (accessed Sep. 29, 2020).
- [14] M. Siam, S. Elkerdawy, M. Jagersand, and S. Yogamani, "Deep semantic segmentation for automated driving: Taxonomy, roadmap and challenges," in *IEEE Conference on Intelligent Transportation Systems*, Proceedings, ITSC, Yokohama, 2018.
- [15] A. Garcia-Garcia, S. Orts-Escolano, S. O. Oprea, V. Villena-Martinez, and J. Garcia-Rodriguez, "A Review on Deep Learning Techniques Applied to Semantic Segmentation," arXiv:1704.06857, 2017.
- [16] M. D. Zeiler and R. Fergus, "Visualizing and understanding convolutional networks," in *European conference on computer vision*, Zurich, 2014.
- [17] Y. Zhang, Z. Qiu, T. Yao, D. Liu, and T. Mei, "Fully Convolutional Adaptation Networks for Semantic Segmentation," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, Salt Lake, 2018, [Online]. Available: <http://arxiv.org/abs/1804.08286>.
- [18] L. C. Chen, Y. Yang, J. Wang, W. Xu, and A. L. Yuille, "Attention to Scale: Scale-Aware Semantic Image Segmentation," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Las Vegas, 2016.
- [19] B. Hariharan, P. Arbeláez, R. Girshick, and J. Malik, "Hypercolumns for object segmentation and fine-grained localization," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Boston, 2015.
- [20] P. Arbeláez, J. Pont-Tuset, J. Barron, F. Marques, and J. Malik, "Multiscale combinatorial grouping," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Washington, 2014.
- [21] J. R. R. Uijlings, K. E. A. Van De Sande, T. Gevers, and A. W. M. Smeulders, "Selective search for object recognition," *Int. J. Comput. Vis.*, vol. 104, no. 2, pp. 154–171, 2013.
- [22] R. Girshick, J. Donahue, T. Darrell, J. Malik, U. C. Berkeley, and J. Malik, "Rich feature hierarchies for accurate object detection and semantic segmentation," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Washington, 2014, [Online]. Available: <http://arxiv>.
- [23] P. Kohli and V. Koltun, "Efficient Inference in Fully Connected CRFs with Gaussian Edge Potentials," in *Advances in Neural Information Processing Systems*, Granada, 2011.
- [24] C. Farabet, C. Couprie, L. Najman, and Y. Lecun, "Learning hierarchical features for scene labeling," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 8, pp. 1915–1929, 2013.
- [25] J. Dai, K. He, and J. Sun, "Convolutional feature masking for joint object and stuff segmentation," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Boston, 2015.
- [26] D. Eigen and R. Fergus, "Predicting Depth, Surface Normals and Semantic Labels with a Common Multi-Scale Convolutional Architecture," in *IEEE International Conference on Computer Vision (ICCV)*, Santiago, 2015.
- [27] M. Cogswell, X. Lin, S. Purushwalkam, and D. Batra, "Combining the Best of Graphical Models and ConvNets for Semantic Segmentation," arXiv:1412.4313, vol. 2, 2014, [Online]. Available: <http://arxiv.org/abs/1412.4313>.
- [28] M. A. Zulkifley, M. M. Mustafa, A. Hussain, A. Mustapha, and S. Ramli, "Robust identification of polyethylene terephthalate (PET) plastics through bayesian decision," *PLoS One*, vol. 9, no. 12, pp. 1–21, 2014.
- [29] S. Ramli, M. M. Mustafa, A. Hussain, and D. A. Wahab, "Histogram of intensity feature extraction for automatic plastic bottle recycling system using machine vision," *Am. J. Environ. Sci.*, vol. 4, no. 6, pp. 583–588, 2008.
- [30] J. Bobulski and J. Piatkowski, "PET waste classification method and plastic waste database WaDaBa," in *Advances in Intelligent Systems and Computing*, Ukraine, 2018.

- [31] K. Özkan, S. Ergin, S. Işık, and I. Işikli, "A new classification scheme of plastic wastes based upon recycling labels," *Waste Manag.*, vol. 35, pp. 29–35, 2015.
- [32] E. Scavino, D. A. Wahab, A. Hussain, H. Basri, and M. M. Mustafa, "Application of automated image analysis to the identification and extraction of recyclable plastic bottles," *J. Zhejiang Univ.*, vol. 10, no. 6, pp. 794–799, 2009.
- [33] MathWorks, *Image Processing Toolbox Use Guide*, 2nd ed. Natick: The Math Works Inc, 1997.
- [34] K. Fukunaga, *Introduction to statistical pattern recognition*, 2nd ed. San Diego: Academic Press, 1990.
- [35] J. Canny, "A Computational Approach to Edge Detection," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 8, no. 6, pp. 679–698, 1986.
- [36] N. Otsu, "A threshold selection method from gray-level histograms," *Automatica*, vol. 11, no. 3, pp. 285–296, 1975.
- [37] K. Pearson, "On lines and planes of closest fit to systems of points in space," *London, Edinburgh, Dublin Philos. Mag. J. Sci.*, vol. 2, no. 11, pp. 559–572, 1901.
- [38] H. Hotelling, "Analysis of a complex of statistical variables into principal components," *J. Educ. Psychol.*, vol. 24, no. 6, pp. 417–441, 1933.
- [39] B. Schölkopf, A. Smola, and K.-R. Müller, "Kernel principal component analysis," in *7th International Conference in Artificial Neural Networks (ICANN'97)*, Lausanne, 1997.
- [40] R. Fisher, "The Use Of Multiple Measurements In Taxonomic Problems," *Ann. Eugen.*, vol. 7, no. 2, pp. 179–188, 1936.
- [41] M. Lee, H. Shen, J. Z. Huang, and J. S. Marron, "Biclustering via Sparse Singular Value Decomposition," *Biometrics*, vol. 66, no. 4, pp. 1087–1095, 2010.
- [42] M. Belkin and P. Niyogi, "Laplacian Eigenmaps and Spectral Techniques for Embedding and Clustering," in *Neural Information Processing Systems Foundation (NIPS) 2001*, Vancouver, 2001.
- [43] V. Vapnik, *The Nature of Statistical Learning Theory*, 2nd ed. New York: Springer, 2000.
- [44] R. C. Gonzalez and R. E. Woods, *Digital Image Processing*, 2nd ed. New Jersey: Prentice-Hall, Upper Saddle River, 2002.
- [45] H. White, "Artificial Neural Networks: Approximation and Learning Theory," 1992.
- [46] O. Adedeji and Z. Wang, "Intelligent Waste Classification System Using Deep Learning Convolutional Neural Network," *Procedia Manuf.*, vol. 35, pp. 607–612, 2019, [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S2351978919307231>.
- [47] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, Las Vegas, 2016.
- [48] O. Russakovsky et al., "Imagenet large scale visual recognition challenge," *Int. J. Comput. Vis.*, vol. 115, no. 3, pp. 211–252, 2015.
- [49] M. W. Rahman, R. Islam, A. Hasan, N. I. Bithi, M. M. Hasan, and M. M. Rahman, "Intelligent waste management system using deep learning with IoT," *J. King Saud Univ. - Comput. Inf. Sci.*, 2020, doi: <https://doi.org/10.1016/j.jksuci.2020.08.016>.
- [50] M. Yang and G. Thung, "Classification of Trash for Recyclability Status," San Jose, 2016. [Online]. Available: <http://cs229.stanford.edu/proj2016/report/ThungYang-ClassificationOfTrashForRecyclabilityStatus-report.pdf>.
- [51] B. A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," in *Advances in Neural Information Processing Systems 25 (NIPS 2012)*, Lake Tahoe, 2012.
- [52] D. G. Lowe, "Distinctive image-features from scale-invariant keypoints," *Int. J. Comput. Vis.*, vol. 60, no. 2, pp. 91–110, 2004.
- [53] W. L. Mao, W. C. Chen, C. T. Wang, and Y. H. Lin, "Recycling waste classification using optimized convolutional neural network," *Resour. Conserv. Recycl.*, vol. 164, no. 105132, 2021, [Online]. Available: <https://doi.org/10.1016/j.resconrec.2020.105132>.
- [54] G. Huang, Z. Liu, L. van der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, Honolulu, 2017.
- [55] H. W. Mwangi and M. Mokoena, "Using Deep Learning to Detect Polyethylene Terephthalate (PET) Bottle Status for Recycling," *Glob. J. Comput. Sci. Technol.*, vol. 19, no. 4, pp. 27–31, 2019.
- [56] S. Aly and W. Aly, "DeepArSLR: A Novel Signer-Independent Deep Learning Framework for Isolated Arabic Sign Language Gestures Recognition," *IEEE Access*, vol. 8, pp. 83199–83212, 2020, doi: 10.1109/ACCESS.2020.2990699.
- [57] "Evaluate semantic segmentation," 2017. <https://www.mathworks.com/help/vision/ref/evaluatesemanticsegmentation.html> (accessed Nov. 07, 2020).
- [58] T. Ghosh, L. Li, and J. Chakareski, "Effective Deep Learning for Semantic Segmentation Based Bleeding Zone Detection in Capsule Endoscopy Images," *Proc. - Int. Conf. Image Process. ICIP*, no. September 2019, pp. 3034–3038, 2018.
- [59] E. Fernandez-Moral, R. Martins, D. Wolf, and P. Rives, "A New Metric for Evaluating Semantic Segmentation: Leveraging Global and Contour Accuracy," *IEEE Intell. Veh. Symp. Proc.*, vol. 2018-June, pp. 1051–1056, 2018.
- [60] L. Luo, Y. Xiong, Y. Liu, and X. Sun, "Adaptive gradient methods with dynamic bound of learning rate," *arXiv*, no. 2018, pp. 1–19, 2019.
- [61] J. Long, E. Shelhamer, and T. Darrell, "Fully convolutional networks for semantic segmentation," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, Boston, 2015.
- [62] O. Ronneberger, P. Fischer, and T. Brox, "U-net: Convolutional networks for biomedical image segmentation," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9351, pp. 234–241, 2015.
- [63] V. Badrinarayanan, A. Kendall, and R. Cipolla, "Segnet: A deep convolutional encoder-decoder architecture for image segmentation," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 39, no. 12, pp. 2481–2495, 2017.

# A New Approach for Training Cobots from Small Amount of Data in Industry 5.0

Khalid Jabrane, Mohammed Bousmah  
LTI Laboratory, National School of Applied Sciences  
Chouaib Doukkali University  
El Jadida, Morocco

**Abstract**—Machine learning is a vital part of today's world. Although the current Machine Learning slogan is “big data is required for a smarter AI”. All Artificial Intelligence learning techniques require the training of algorithms with huge data. Collecting and storing this data takes time and requires increasing computer memory. In Industry 5.0, human-robot collaboration is a challenge for artificial intelligence (AI) and its subdomains. Indeed, integration of its domains is required. Many AI techniques are needed, ranging from visual processing to symbolic reasoning, task planning to mind building theory, reactive control to action recognition and learning. Otherwise, the main two obstacles to this natural workflow interaction are big data memorization and time Learning that grows exponentially with the problem complexity especially. In this article, we propose a new approach for training Cobots from Small Amount of Data in the context of industry 5.0 based on common-sense capability inspired by human learning.

**Keywords**—Small data; industry 5.0; common-sense capability; machine learning

## I. INTRODUCTION

Despite its economic progress, all industrial revolutions had an impact on the labor market with the goal of replacing human labor with machines. The first industrial revolution replaced manual work with the invention of a steam engine and the second industrial revolution enabled mass production using electric energy. The tertiary industrial revolution started the automation era with informatization based on computers and the Internet. In the fourth industrial, the super intelligence revolution based on the Internet of things, cyber-physical system, and artificial intelligence (AI) will greatly change human intellectual labor. Fig. 1 depicts the five industrial revolutions.

Industry 5.0 will transform the labor market by emphasizing the central role of humans and encouraging collaboration between humans and a new generation of robots known as "collaborative robots" or "cobots". These cobots are designed to work alongside their human counterparts and, more importantly, help them accomplish common tasks in real world. They are user-friendly and their key function is to provide physical assistance to operators by performing unpleasant and risky activities. With the introduction of Cobots there should be no fear of losing the production line due to automation which has been a major concern of Industry 4.0, as a result better agility will be added to the smart factory.

In the context of Industry 5.0, AI and cobotics must play a central role to improve the capabilities of Cobot. The cobotics is a major discipline that focuses on collaborative robots and their uses as technical agents. Moreover, Cobotics seeks to extend beyond the isolated faculties of humans and robots. Synergy is an essential factor in increasing the respective capacities of man and machine.

However, this promising vision of cobot, driven by AI and cobotics, requires significant R&D progress. Many technical challenges remain in all subfields of AI application. The neural networks of deep learning models require exposure to huge amounts of data to learn a task. Training a neural network to recognize an object, for example, could require feeding it as many as 15 million images. Acquiring relevant datasets of this size can be costly and time-consuming, which slows the pace of training, testing and refining AI systems. Furthermore, some fields suffer from a lack of data to feed a starving deep learning model.

Researchers are working hard to find ways to train systems with less data and are optimistic that they will find a viable answer. As a result, AI specialists anticipate that the "big-data" variable's tendency will be reversed in the AI growth equation. Small data will supplant Big Data as fresh and innovative AI drivers in Industry 5.0.

The goal of this study is to present a novel approach for training cobots with small amounts of data. We place a premium on a framework built on common sense and on-the-fly multitasking techniques. As a result, this article presents a summary of current cobotics research. We define cobotics and provide a brief classification of cobotic systems. The second segment discusses the main challenges of artificial intelligence, while the third section looks for potential solutions. Finally, we'll present our model.

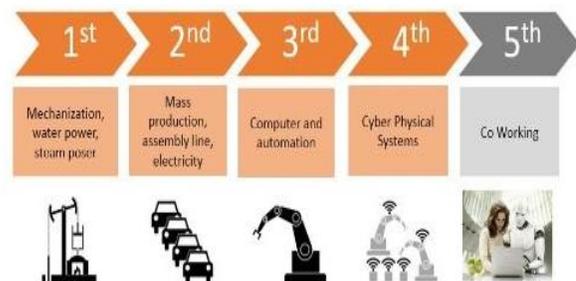


Fig. 1. The Five Industrial Revolutions.

## II. RELATED WORK

Cobotics is a transdisciplinary technology and is the intersection of three main fields such as robotics, ergonomics and cognitive. This new discipline focuses on studying the interaction of human and cobot.

Cobotics is not included in robotics because certain aspects, such as the human representation of the robot, ergonomics of the workstation, or operator acceptance, are the result of ergonomic and cognitive engineering studies.

At the end of the 1990s, the term "cobot" was describe as a passive effort-assistance device controlled directly by an operator [1]. Since then, the meaning of the term has evolved. It was only popularized in the 2010s. Current cobotics allow the extension of human gesture or behavior and is distinguished from simple robotics by the real, direct or remote interaction between a human operator and a controlled or pseudo-autonomous robotic system. This cooperative robotics is more "user-centric" [2].

While is still conceived today as a cooperative augmentative robotics, cobotics corresponds generically to the use of mechanical or artificial sensorimotor support systems developed specifically for a given task or relationship. It then becomes a form of parallel robotics or extension robotics, allowing an increase in performance, in strength, speed or precision [3].

Given the novelty of the theme, the majority of articles in the literature treat this new industrial revolution as being the era where Man and cobots will have to work side by side. Although this observation is part of our daily life in some pioneering industries in this field, this cooperation takes place for very specific and low-level tasks.

For some authors, Artificial Intelligence needs a theory based on the tasks [4], others think that to design new factories in Industry 5.0 with a human-centered perspective, technological engineering should be centered on values and ethics [5].

Other authors have even proposed probabilistic models to infer intention in human-robot interaction [6]. In this context, intention inference has been the subject of several studies and research based on the Markov model which predicts and models human behavior by a series of discrete states and actions.

Also, some studies explain an inspiring technique based on Reverse Reinforcement Learning (IRL) [7] [8]. Ordinary reinforcement learning involves the use of rewards and punishments to teach a behavior to an intelligent agent, in IRL the process is reversed, the robot observes a person's behavior to determine the goal that behavior appears to be aiming for. The problem in IRL is to determine the optimized reward function, by the agent, which best and in a transferable way defines the intended task. This approach has enabled state-of-the-art advances in several areas of robotics.

Although some articles suggest possible research avenues, finding a relevant issue linking artificial intelligence and Industry 5.0 seems philosophical if we move away from technical reflections based on the adoption of a stochastic

modeling approach, which also remain restrictive given the input hypotheses and the cases treated, which do not promise generalization.

In short, according to scientists and industry, the trend in the era of industry 5.0 is converging on the search for tools and technologies that propel the advancement of symbiotic interaction in the workplace.

In this context, recent advances in reinforcement learning have successfully combined deep learning to make significant improvements in the formation of an agent. Despite the impressive performance of Deep Reinforcement Learning (DRL) techniques on individual tasks, training a single DRL agent to perform multiple tasks remains difficult [9]. Traditional learning algorithms that consist of directly training a DRL agent for multiple tasks one by one have been shown to offer poor performance and may even fail on some tasks.

Unlike DRL which teaches an agent to perform a single task, the new multitasking DRL techniques advocate that the agent learns a single control policy that could work well on several different tasks.

The current AI approach is to train agents using as much data as possible while also blending real and synthetic data. Big data alone will not be able to overcome the difficulties of human-machine collaboration in real-world interactions.

We typically think of "big data" when we hear "artificial intelligence," because the most notable advancements in AI have been built on massive data sets. Image classification, for example, has made significant progress in the construction of ImageNet, while the GPT-3 language model has been trained on hundreds of billions of words of online text using deep learning techniques to produce human-like writing. It is therefore not surprising to see AI being closely linked to "big data" in the popular imagination. But AI is not just about big data sets, research on 'small data' approaches is being developed nowadays.

The common sense is the natural ability to make good judgment to behave in a practical and sensible way.

Common sense is the unconsciously acquired knowledge that all humans have since birth. This common-sense knowledge is gained through experience and curiosity, sometimes without the learner's knowledge.

According to John McCarthy, father of AI, Common sense knowledge includes the basic facts about events and their effects, facts about knowledge and how it is gained, facts about beliefs and desires. It includes the basic facts about material objects and their properties [10].

Common sense is the ability to interpret a situation in light of its context, based on millions of interconnected elements of common knowledge. The capacity to use this knowledge wisely qualifies the ability to perform common sense reasoning. Common sense reasoning is a central part of intelligent behavior.

In 1959, John McCarthy proposed common sense reasoning in the form of a theoretical program named Advice Taker. However, despite recent advances in machine learning,

there has been no progress in terms of true common sense reasoning skills. The recent surge in popularity of the subject can be attributed to recent advances in NLP and the importance of the task.

Since John McCarthy's hypothesis, proposed in the 1950's, that common sense programs could be developed using formal logic, Today's primary approaches to common sense reasoning in AI, as well as their taxonomies, are depicted in Fig. 2.

McCarthy's hypothetical proposition has sparked a flurry of research into logic-based approaches to commonsense reasoning. There are several research efforts; here are a few of them: situation calculus, naïve physics, default reasoning, non-monotonic logics, description logics, and qualitative reasoning, less formal knowledge-based approaches.

The 'Cyc' Project remains the most notable effort adopting the knowledge-based approach. The 'Cyc' Project spent 35 years codifying common sense into an integrated logic-based system. This awesome effort covers vast areas of common-sense knowledge and incorporates sophisticated logical reasoning techniques.

For a variety of reasons, including the fragility of symbolic logic, 'Cyc' was unable to realize its goal of delivering a generally useful common-sense service.

Artificial intelligence (AI) systems lack common sense knowledge. Furthermore, despite years of effort, developing common sense reasoning AI systems has always been a tedious task. Today's AI researchers agree that the most difficult problem in AI research is developing programs with common sense capabilities.

Formalizing common sense knowledge for any reasoning problem, no matter how simple, is a huge task. This is because common sense knowledge is implicit, whereas expert/specialist knowledge is usually explicit. As a result, developing an AI common sense reasoning system will necessitate explicitly expressing this knowledge.

An intelligent system lacking in common sense will struggle to understand its surroundings, interact naturally with people, respond appropriately in unexpected situations, or learn new experiences.

The concept of common-sense reasoning is still challenging for AI specially in the context of Human-Cobot collaboration in the industry 5.0 era. Progress in common sense applications for AI is insufficient. The difficulty lies in explicit formulations of what is common sense because it is an unstructured and very confused field.

### III. STATE OF THE ART AND TECHNICAL CHALLENGES OF AI IN THE ERA OF COBOT IN INDUSTRY 5.0

#### A. Classification of Cobot System

Cobotic systems are very diversified and their applications are numerous. Their classification is based on various and dispersed criteria. Many authors have tried to classify these cobotic systems to well structure this field.

First, the social-based classification of robot properties includes form, modality, social norms, autonomy, and interactivity [11]. Then safety-based classification of robot which was a major concern since the beginning of industrial robotics, standards and norms were established to regulate this field [12].

Moreover, Robots can be classified according to their architecture, degree of autonomy, mobility, transport capacity, handling, size, and distance from the operator. This approach disregards the human component of the cobotic system. Jean Scholtz proposes a role-based classification to more clarify the role and the nature of the Human-Robot Interaction (HRI) as described below [13]:

- Supervisor Interaction: The supervisor's role is to monitor and control the overall situation.
- Operator Interaction: The operator intervenes to change the internal model or to parameterize the software when the robot behavior is altered.
- Coworker: It works in the same environment as the robot, in parallel, and sometimes has some interactions with him, for example taking the piece he just processed.
- BYSTANDER: Present in the same environment as the robot and sometimes enters its working area, it has no real interaction with it. The robot is equipped with a presence sensor, as soon as a human enters its zone, it automatically switches to a slower mode or stops temporarily. Collaboration is reduced to a minimum.

#### B. Type of Human-cobot Industrial Collaboration

Human-robot collaboration in the industrial field can take several forms. Collaboration takes place either in a shared workspace without direct contact or in a shared workspace with direct contact. Tasks are executed with or without synchronization. The robot adapts its movement to meet the human workers, and in some cases, adjusting the movement is recommended in real time.

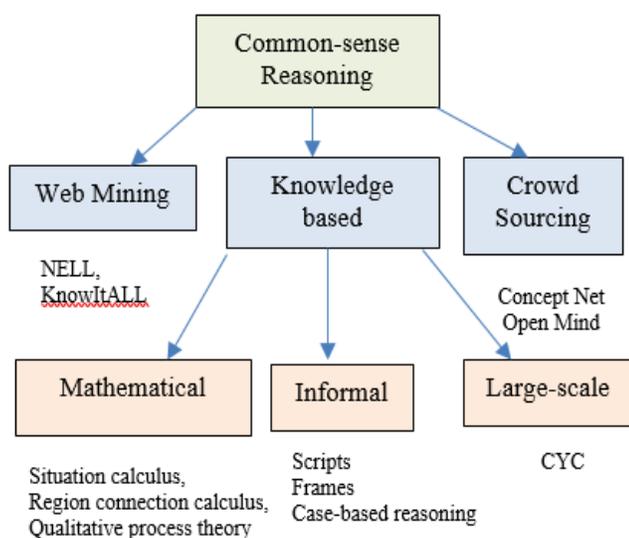


Fig. 2. Taxonomy of Approaches to Common Sense Reasoning.

According to the International Federation of Robotics (IFR), collaborative robotics today is characterized by applications where tasks run sequentially in shared workspaces, in which the robot and the employee work side by side.

Fig. 3 from IFR web site shows different types of industrial robots collaboration.

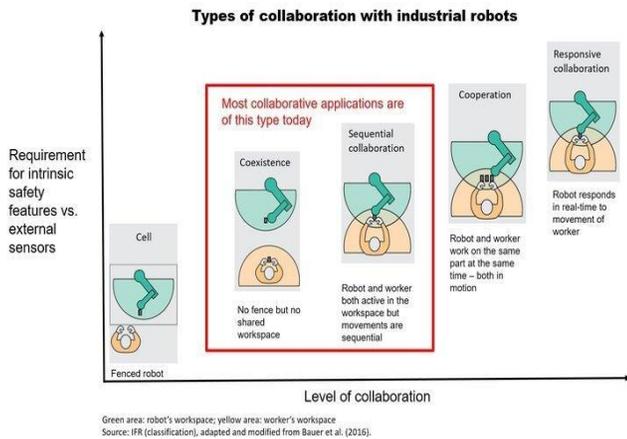


Fig. 3. Type of Collaboration with Robots Industry.

The robot frequently performs tedious or impractical tasks, such as lifting heavy parts or tightening screws. Otherwise, real-time applications in which the robot must react and expertly modify its actions to those of a worker are more technically challenging. However, robot movements are completely unpredictable; the user must ensure that the robot's potential setting meets safety requirements.

In fact, reactive human-robot collaboration will not be reachable so early in most manufacturing sectors where precision and repeatability are required to increase productivity. Otherwise, the most advanced research projects are all categorized as "sequential" or "support" collaboration scenarios [14]. Interdependent and collaborative scenarios between humans and machines require more sophisticated systems and solutions. Indeed, Cobots need a stronger semantic knowledge of the task's goal, as well as the behaviors and intentions of their human coworkers. Humans must also be able to communicate intuitively with the cobot.

### C. Technical Challenges of AI in the Era of Cobot in Industry 5.0

Today's researchers are trying to push the boundaries in order to create more advanced or complex forms of interaction by arming cobots with comprehension and anticipation skills aided by Artificial Intelligence.

Future cobots should be able to recognize human signals, movements and intentions, as well as distinguish between intentional and unintentional gestures related to the collaborative work. The natural collaboration between humans and cobots requires that cobot be able to capture, process and understand human demands with precision and robustness.

However, the technical challenges of AI lie in the interaction modalities such as speech, gaze or gesture planning

as well as motion control that must be performed in real time to ensure a natural workflow interaction. This natural workflow interaction will not be achieved only with both the classical sense-plan-act architectures and Reinforcement learning models that constitute the current state of the art in applied robotics.

Human-robot collaboration is a challenge for artificial intelligence (AI) and its subdomains. Indeed, AI's methods need to be further strengthened for a better integration of many techniques such as visual processing, symbolic reasoning, task planning, reactive control, recognition of actions and learning.

Otherwise, the main two obstacles to this natural workflow interaction are big data memorization and time learning that grows exponentially with the problem complexity especially.

1) *AI and big data*: The future of cobotics depends on artificial neural networks and deep learning which are designed to acquire advanced learning skills without the need for any type of programming. The goal of this extremely complex discipline is to enable robots to mimic the ability of humans to smoothly integrate inputs with motor responses, even as they undergo changes in their environment.

All Artificial intelligence learning techniques require the training of algorithms with huge data. Collecting and storing this data takes time and requires increasing computer memory. However, for cobotics, deep learning is a future goal rather than immediately achievable given that it requires truly massive amounts of processing power and data.

For example, deterministic problem optimization methods, including Q-learning, require recording important statistical data. Research has established that the convergence of the Q-Learning function has been proven for an infinite time. That's why it's inconceivable to teach a machine in 10 years what humanity has learned over millions of years.

One of the biggest problems of artificial intelligence is acquisition and storage. In the industry the input data comes from sensors. To validate the AI system, a mountain of sensor data must be collected. Irrelevant and noisy data sets can cause obstructions because they are difficult to store and analyze.

In addition, the AI algorithm becomes stronger and more powerful as the data collected is of good quality, relevant, and increases during its processing. The AI system fails badly when it is not fed with sufficient and good quality data; however, small variations in data quality have large consequences for results and predictions. Again, adoption of AI systems is limited for some industry sectors where data availability is insufficient.

2) *AI and multitask*: Deep reinforcement learning (DRL) has significantly improved the performance of intelligent agents. Although DRL approaches can improve agent performance to a greater extent, they were limited to systems that learned a specific task primarily through reinforcement learning algorithms.

DRL is a type of reinforcement learning and deep learning and can be defined as a crossroads between traditional and true

artificial intelligence, as illustrated in Fig. 4. The DRL combines action-based reward techniques from reinforcement learning with the concept of using a neural network to learn feature representation from deep learning.

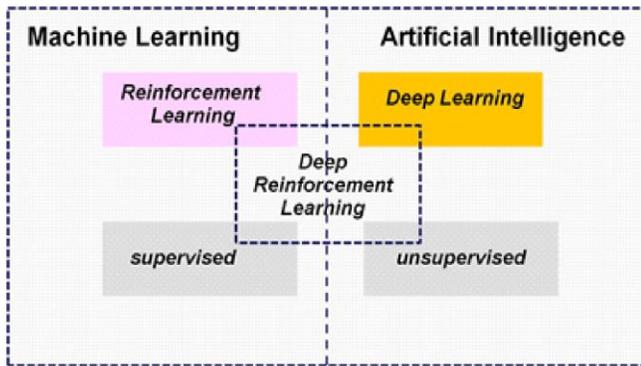


Fig. 4. Deep Reinforcement Learning.

Simultaneously, this method has proven to be inefficient in terms of data, particularly when reinforcement learning agents should interact with more sophisticated and rich data environments. This challenge emanates mostly from the limitations of deep reinforcement learning algorithm to deal with multiple scenarios of related tasks in the same environment.

Training reinforcement learning algorithms is typically time consuming, and processing requires high number of data samples to achieve an acceptable result. Second, reinforcement learning is a task-specific. Learning generalization to other tasks is practically impossible. The trained agent is deployed only on the task for which it was trained.

The section that follows provides an overview of the various challenges associated with multitasking learning in the context of deep reinforcement learning environment.

- Scalability

Scalability is a major issue in artificial intelligence when implementing multi-task learning via deep reinforcement learning [15].

One of the main shortcomings of traditional RL algorithms is their inability to extend their learning to other scenarios.

To converge to an acceptable result, RL algorithms often demand a larger number of training data samples and a longer training time [16]. There should be continuity and scalability in multitask learning by transferring the acquired knowledge to other tasks or processes. It should not take  $N$  times more samples or training time to learn  $N$  different tasks.

- The distraction problem

Balancing the demands of several tasks for the limited resources of a single learning system in a particular environment is one of the most challenging aspects of multitasking deep reinforcement learning.

Therefore, learning algorithms are often distracted to solve only a few tasks among others (a phenomenon known as the distraction dilemma) [17].

- Fractional observability

Observations made by an RL agent in many real-world scenarios are partial. Capturers only reflect a small part of the complete state of the environment [15]. When the state-action space is large, this challenge includes learning and remembering a compact representation of the environment with the most pertinent details from the environment.

- Real-world exploration

Continuous Reinforcement learning is generally based on trial and error. Exploration and exploitation are methods used by RL agents to learn by experimenting numerous possible actions from a given state in order to find the best action that delivers the best overall future reward [15]. When applying reinforcement learning to real-world problems, it is frequently difficult to achieve a higher level of exploration.

- Catastrophic interference

The goal of multitasking deep reinforcement learning (DRLM) is to train agents to learn a series of tasks with the ability to transfer knowledge from previous tasks to new tasks in order to improve the convergence speed [18]. This is a lifelong learning situation in which deep neural networks unexpectedly lose knowledge learnt in a previous task that is applicable to a new task.

The fundamental cause of this problem is changes in network parameters (weight) associated with a task that are overwritten to accomplish the goals of the following task [18]. This phenomenon is considered as a crucial obstacle to the development of a General Artificial Intelligence (AGI), as it has a negative impact on the ability to continual learning.

3) *AI and Human-Robot Interface (HRI)*: Human-Robot Interaction (HRI) is a field that studies, designs, and evaluates robotic devices for use by or with humans. The Human-robot interface (HRI) is related to the interaction modalities between the user and the robot. The sub-domains more concerned by AI research in robotics is the cognitive HRI (cHRI) that analyzes the information flow between the user and the robot and focuses mainly on multimodal interactions including textual, vocal and gestural interfaces.

Despite the advances of the AI, Human-Robot Interaction (HRI) continues to be a challenge for artificial intelligence (AI) and its subdomains. Human-robot interaction involves many technical challenges both on the technical level as well as human-centered aspects. The latter includes issues such as expectations, attitudes and perceptions.

HRI research deals with a wide range of issues, including the direct usage of robot systems that interact with humans in specific situations. The main research challenges in the field of HRI concern multimodal sensing and perception, design and human factors, and those related to developmental robotics:

- Multimodal perception

Real-time perception and management of uncertainty in detection are two of the most difficult challenges in robotics.

The need to perceive, understand, and respond to human activity in real time makes sensing and perception more complex and challenging in the field of HMI.

Human interaction sensors are far more diverse than those used in most other robotic fields today. The processing of real-time data from HRI inputs such as vision and speech poses significant challenges. Face expressions [19] and gestures [20] are examples of possible inputs that computer vision algorithms must be able to process. Correspondingly Language understanding and human-robot communication systems are still unsolved research difficulties [21, 22]. Understanding the relationship linking visual and linguistic inputs [23] then combining them to improve detection [24] and expression [25]. is even more difficult. The Fig. 5 below illustrates the information processing of cobot.

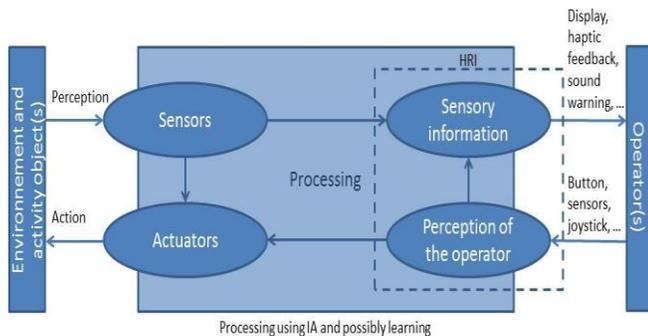


Fig. 5. Information Processing for the Cobot.

- Developmental Robotics

Developmental robotics is not a direct subset of the HRI field, but the two fields overlap significantly in their goals and have a lot in common when it comes to information acquisition techniques and multimodal perception.

The robot learns to model its environment, the objects that surround it, its own body, it learns elements of language, all this in strong interaction with the physical world but also through social interactions with humans or even other robots. The model that preoccupies the artificial intelligence researcher is no longer the chess player, but being able to learn and develop cognitively.

Developmental robotics, proposes to focus not on reproducing an immediately intelligent robot, but a robot that will be able to learn, starting with a reduced amount of innate knowledge.

#### D. Overview of Existing Solutions

DeepMind and OpenAI as research organizations have contributed significantly to the field of multi-task deep reinforcement learning (MTDRL). Their research efforts have resulted in three major MTDRL solutions, namely DISTRAL (DIStill & TRAnsfEr Learning), IMPALA (Importance Weighted Actor-Learner Architecture), and PopArt, which should be briefly mentioned in this paper as potential solutions to the issues listed in this part.

- DISTRAL (DIStill & TRAnsfEr Learning)

According to authors Nelson Vithayathil Varghese and Qusay H. Mahmoud [26]. The transfer-oriented method consists in sharing neural network parameters across related tasks in a given environment. This method has been considered as the reference for multitasking in reinforcement learning [27]. This approach encounters issues that have an impact on the learning process, such as negative knowledge transfer and ambiguity when designing a reward system for various tasks. [28]. The rewards system, in a multitasking context, should be built so that no task has to control or monopolize the shared model's learning.

DISTRAL was created as a framework for learning multiple tasks at once. DISTRAL is a novel approach to multitasking training that addresses the issues raised above.

The design's primary goal was to develop a general framework for distilling centroid policy and then transferring common behaviors into reinforcement learning across multitaskers rather than sharing parameters among the various workers in the environment [29].

Fig. 6 illustrates the Distill structure which provides a high-level view involving four tasks. The method is founded on the concept of shared policy (shown in the center), which distills common behaviors or representations from task-specific policies [30, 31]. The distilled policy is then regulated in order to direct the task-specific policies.

The knowledge gained in one task is distilled into the shared policy, which is then applied to other tasks.

The DISTRAL approach has proven to be very effective compared to the traditional method, transfer learning in multitasking therefore consists in sharing parameters over the neural networks.

DISTRAL algorithms learn faster and achieve better asymptotic performance. They are much more robust to the settings of the hyperparameters. Learning is more stable than with multi-tasking A3C baselines.

A3C was originally conceived as an extension of the actor-critic approach whose model is illustrated in Fig. 7. Two distinct neural network components are used: the actor and the critic, each having its own loss function. According to RL approaches such as Q-learning or REINFORCE, an actor can be considered as a function approximator that guides the way to act.

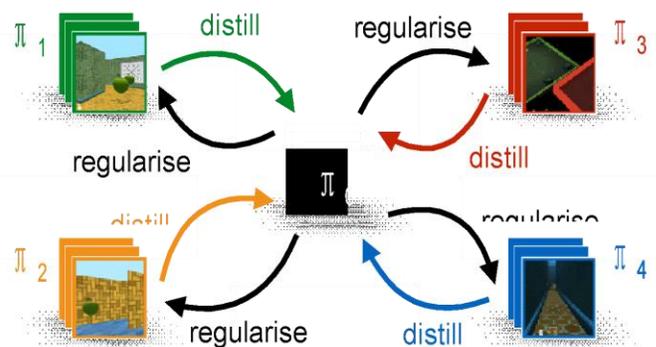


Fig. 6. Illustration of the DISTRAL Framework.

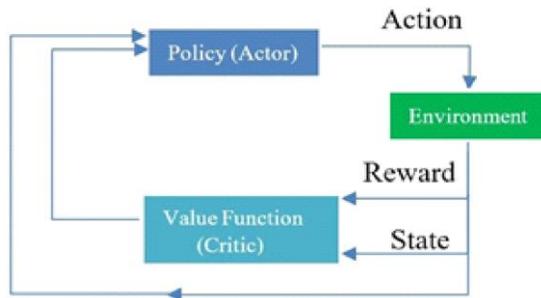


Fig. 7. Actor-Critic Model.

- Asynchronous Actor-Critic Advantage (A3C).

A3C (asynchronous actor-critical advantage) is an algorithm introduced by DeepMind. A3C offers a parallel training approach where multiple agents (called workers) run on multiple instances of the same environment [32].

Global value function is updated asynchronously by multiple workers operating in parallel environments. During the training, each parallel agents will experience a variety of different states at any time step  $t$ . The agents learning becomes nearly unique. This A3C uniqueness factor provides an effective and efficient way for agents to explore the complete state space in a given environment [33].

The role of the critic consists in evaluating the effectiveness of the policy put in place by the actor and contributes to its improvement [32].

Fig. 8 is the representation of a typical actor-critical model on which A3C is based.

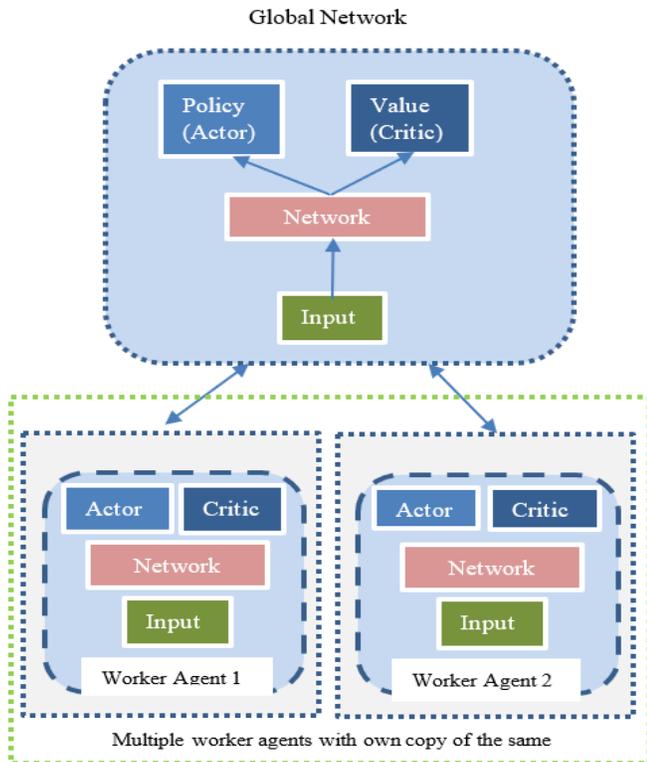


Fig. 8. Actor-Critic Model.

- IMPALA (Importance Weighted Actor-Learner Architecture).

Dealing with the increased amount of data an agent must handle, as well as the training time required, is one of the major issues in achieving functionality with a single reinforcement learning agent.

DeepMind has proposed an architecture called IMPALA to solve the abovementioned aspects of multitasking in the field of reinforcement learning. The IMPALA distributed agent architecture is based on a single reinforcement learning agent with a single set of parameters [30]. The main feature of the IMPALA approach is the ability to efficiently use resources in a single machine learning environment while scaling to many machines.

DeepMind also introduced a new correction policy based on a method known as V-trace, which enables relatively stable and fast learning by combining action and learning without compromising data efficiency or resource usage [30].

Generally, the architecture of a deep reinforcement learning model includes a single (critical) learner who is linked to several actors. Each individual actor in this ecosystem generates learning cycle parameters (also known as trajectories), which are sent as knowledge to the (critical) learner through a queue.

The learner collects the trajectories from all the other environmental actors to prepare a central policy. The policy parameters are updated with the learner (critical) and transmitted for each actor who retrieves them before the start of the new learning cycle (trajectory).

The IMPALA topology connects multiple actors and learners who should work together to build knowledge. Fig. 9 and Fig. 10 dropped from [34] depict, respectively the configurations of an IMPALA ecosystem architecture with a single learner and multiple learners.

- PopArt

Recent advancements have shown that reinforcement learning can outperform human performance in specific tasks. A specific aspect of reinforcement learning is training agents for one task at a time, learning an additional task requires instantiation of the agent [17].

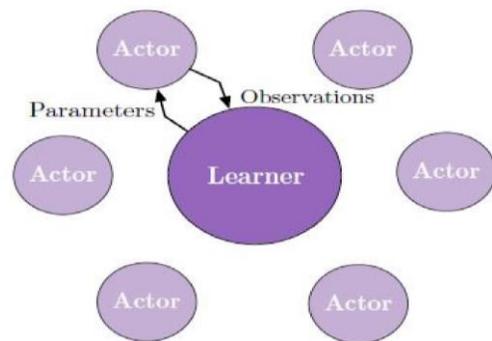


Fig. 9. IMPALA Single Learner Model.

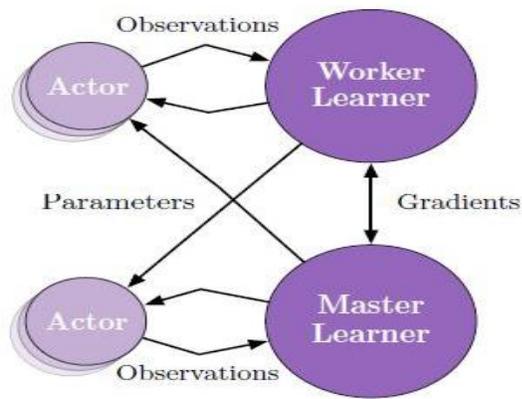


Fig. 10. IMPALA Multiple Synchronous Learners Model.

In order to overcome this limitation, much research has been carried out to improve RL algorithms by giving them the ability to carry out multiple sequential decision tasks at the same time. These research attempts that aim to support multitasking learning have often been faced with various challenges.

In general, this situation requires the establishment of a multitasking reinforcement learning (MTRL) system with strong immunity to the dilemma of distraction. Balancing the mastery of individual tasks is also important in order to achieve the ultimate goal of better generalization of learning [17]. The primary cause of the distraction scenario is that some tasks appear to be more important to the learning process due to the density or magnitude of the rewards given to them (rewards in the task).

As a result, the algorithm prioritizes these important tasks over others, sacrificing generality in the process [17].

PopArt is a new method proposed by DeepMind to improve reinforcement learning in multi-task environments. PopArt aims to reduce distractions and thus stabilize learning in order to facilitate the use of multitasking reinforcement learning (MTRL) techniques.

The PopArt method's main feature is the modification of the neural network's weights based on the results of all tasks in the environment. PopArt estimates mean and distribution of the ultimate targets for all tasks considered in the initial phase. The estimated values are then used to normalize the targets before updating the network weights. This method improves the stability and robustness of the learning process.

#### IV. PROPOSED MODEL

Artificial systems with common sense are generating a lot of interest in various fields of cognitive science and artificial intelligence to engineer common-sense reasoning into artificial agents in ways inspired by human reasoning.

Despite recent advances in many areas, artificial systems are still unable to comprehend and act on the world in a human-like manner, and are incapable of performing basic common sense thinking at the level of even young children.

So, how to concept a structure made of sense and common-sense blocks that allows cobots to understand, interact,

distinguish, and make decisions in order to overcome the challenges of the world around them. How to give cobots the intelligence and common sense they need to learn from raw and optimal representations of the scenes that fill the workplace with its objects, agents, events, and their properties.

So far, no approach has succeeded in implementing an intelligent, common-sense system. Isn't it time to reverse the trend and employ techniques and tools based on small data sets and the integration of a common-sense computational model tailored to each area of interest?

#### A. Small DATA is the Future of AI

Human intelligence has always been able to innovate and discover even before the advent of big data. All scientific discoveries throughout human history have been fueled by small amounts of data. It is estimated that 65% of these discoveries were the result of compiling a small amount of data in the form of rules, hypotheses and theories that were sophisticated and successful.

Today's biggest obstacle facing companies in developing AI systems is the lack of big data. These companies do not have the capacity of giants like Google or Facebook that rely on billions of data resources. Google, for example, benefits greatly from its massive amount of data. It can develop algorithms by processing over 130 trillion web pages, but a corporation may only have 30 relevant instances to automate an internal operation. The gap in AI adoption by companies is due in part to disparities in data resources.

Furthermore, developing a big data initiative within a company necessitates time, money, and expertise. The principles for implementing such a process include creating a data-driven program with architecture and infrastructure appropriate for the initiative's overall lifespan. The cost of this process is prohibitively expensive, and it grows in proportion to the scale of the issue and the complexity of the data.

Although it appears that current AI developments rely primarily on big data, we forget the value of observing small samples. AI becomes even smarter and more powerful if it can be trained with small amounts of data. The ultimate purpose of AI should be mastering knowledge rather than processing data. It is all about teaching a machine the knowledge it needs to complete a task.

In fact, small data mastery is essential to advance AI especially for specific industrial domains where man and robot have to collaborate by exchanging information although they are small quantities but relevant for the accomplishment of common tasks. As a result, the development of new AI techniques that do not rely on the well-known "big data" variable as input becomes critical.

The genesis of AI was to create machines capable of imitating human intelligence. However, Humans can learn from small amounts of information, they do not need to observe millions of examples of cars to learn to detect them correctly.

On the other hand, specialized learners have the ability to learn from small data because they have adequate inductive biases. Inductive biases represent knowledge of the world in

which learning will take place and are present in the model even before training begins. In other words, the model must already be capable of extracting meaning from a particular dataset. A In fact, machine learning model will learn successfully from small data only if it has a sufficient amount of this knowledge.

To summarize, small data has the advantage of being easy to collect, simple to process, ubiquitous and quickly exploitable by machine learning models. Furthermore, when applied to deep learning methods, the model can predict and converge rapidly towards an expected result even more in a narrow area, due to the ability to assign weights and rewards that will become less complex.

Investing in small data appears to provide a significant benefit because it increases the possibility of implementing alternative learning techniques.

To argue this point of view, we highlight some emerging AI tools techniques that rely only on small data and perform better than those that work with big data. These techniques appear to reinforce traditional machine learning modeling approaches and they include:

- Collaborative Machine Learning (CML).

As a distributed learning technology, collaborative machine learning (CML) trains multiple agents in a network to build a common and robust machine learning model without sharing data.

Similarly, to the synergy of heterogeneous human teams, task offloading allows agents to hold different, complementary and private representations of the training environment. The peripheral agents' joint learning is then achieved by parallelization and co-inference of distributed model learning.

The goal of collective machine learning is to create a unique predictive model that is more accurate than the sum of its parts.

- Few-Shot Learning

Few-Shot Learning is a technique that consists of performing supervised classification or regression based on a very small number of samples. Few-Shot Learning (FSL), also known as low intensity learning or spot learning, is a machine learning model that serves primarily as a tool for training machine learning algorithms with data relevant to the training context, even if it is small in number.

Else, Few-Shot Learning is different from standard supervised learning, which trains a model to recognize images in the training set and then generalize to the test set. In contrast, the goal of this technique is to distinguish similarities and differences between objects.

The idea of this approach is humans inspired; man can learn quickly by using what has been learned in the past. For example, a child can easily recognize the same person or animal in a large number of pictures.

Most approaches characterize few-shot learning as a meta-learning problem. To overcome the lack of data, a possible solution is to gain experience from other similar problems.

Meta-learning is a subfield of machine learning that is also known as learning to learn. In meta-learning, machine learning algorithms are applied to metadata related to machine learning experiments.

The main objective is to understand how machine learning can become flexible in solving learning problems and aims to improve the performance of existing learning algorithms or to learn (induce) the learning algorithm itself.

The small collection of labeled images used in meta-learning is called a support set as shown in Fig. 11. In contrast, the training set for conventional machine learning algorithms is large enough to learn a deep neural network, for example. Each class in the training set contains many samples.

The basic idea behind few-shot learning is that the support set has a limited number of classes and samples and can only provide additional information during the test. However, with a training set, if each class only has one sample, it is impossible to train a deep neural network.

The algorithm will be trained through a series of training tasks, each of which includes a support set with three different classes and two examples. The issue is a three-way-two-shot classification.

During training, the cost function will evaluate in turn for each task the performance on the query set taking into account the respective support set (Fig. 12). At test time, a completely different set of tasks is used to evaluate performance on the query set, given the support set.

As shown in Fig. 13, no overlap is existing between the classes in the two training tasks {cat, lamb, pig}, {dog, shark, lion} and between those in the test task {duck, dolphin, hen}. The algorithm will have to learn to classify image classes in general rather than focusing on classifying a particular set.



Fig. 11. Support Set Example.



Fig. 12. Query Set Example.



Fig. 13. Meta-Learning Framework.

The emphasis in FSL learning is on the quality of training data rather than the quantity. Furthermore, there is interest in designing and building AI machines or computer programs that improve automatically with experience.

The human-like learning allows FSL models to naturally advance robotics by improving robots capabilities that can at one-shot replicate or imitate human actions as well as enhancing their visual navigation.

- Zero-Shot Learning (ZSL)

Zero-shot learning is a learning model in which a machine is trained with an optimal minimum of labeled data during the learning phase. The machine learns to recognize a class of objects without having seen any previously labeled examples of that class. This method is also called on-the-fly learning.

Zero-shot learning relies on inference in order to reduce the requirement of the training phase for slightly different permutation masses.

The inference step in zero-shot learning is crucial: in this step, the algorithm attempts to predict and categorize classes of unseen data by analyzing its labeled data predictions to map the underlying attributes that have the highest probability of describing the data in general.

To solve Zero-Shot recognition problems, there are two popular ways. Fig. 14 depicts the anatomy of the first common method called “Embedding-Based Zero-Shot Learning”.

The input image is first processed by a feature extractor network (deep neural network (DNN)) to generate an N-dimensional feature vector for the image. This vector is fed into the main network, which produces a D-dimensional output vector.

The ultimate goal is to compute the weights of the projection network so that the N-dimensional input can be mapped to a D-dimensional output. Then, the loss compatibility module assesses the D-dimensional output's compatibility with the ground truth semantic attribute. The network's weights are tuned so that the D-dimensional output is as near as possible to the ground truth data.

The training seeks to develop a projection function from visual space to semantic space (word vectors or semantic embedding).

The Generative Model-Based Approach is the second Zero-shot Learning method. The generative method's goal is to use semantic attributes to generate image features for unobserved categories. At training time, the zero-shot classification model is trained on both seen and non-observed category images.

A general generative model-based zero-shot learning diagram is shown in Fig. 15.

The feature extractor network (deep neural network (DNN)) generates an N-dimensional feature vector for the image. The attribute vector is first fed into the generative model, as shown in the diagram. Based on the attribute vector, the generator creates an N-dimensional output vector. The generative model is trained in such a way that the synthesized feature vector resembles the original N-dimensional feature vector.

The generator's weights are fixed by the generative model, and the class attributes are used as input to generate non-observed category image features.

A basic image classifier is then trained by taking class image features (the training dataset) and non-observed category image features as the input and outputs the respective category label as shown in the Fig. 16.

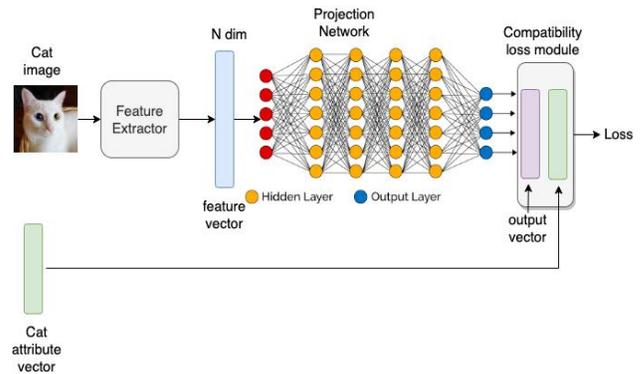


Fig. 14. Embedding-Based Zero-Shot Learning Model.

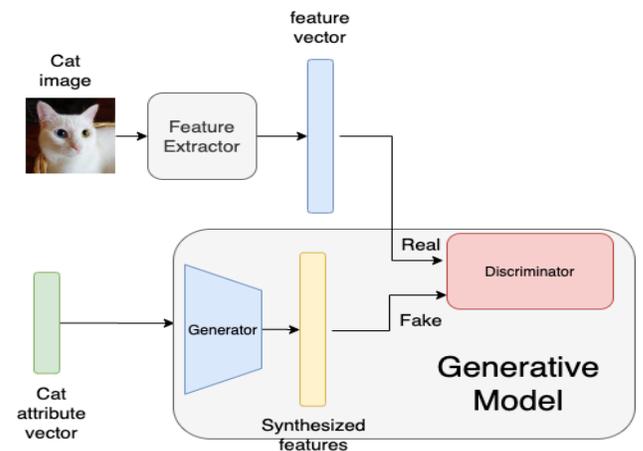


Fig. 15. Generative Model-Based Zero-Shot Learning.

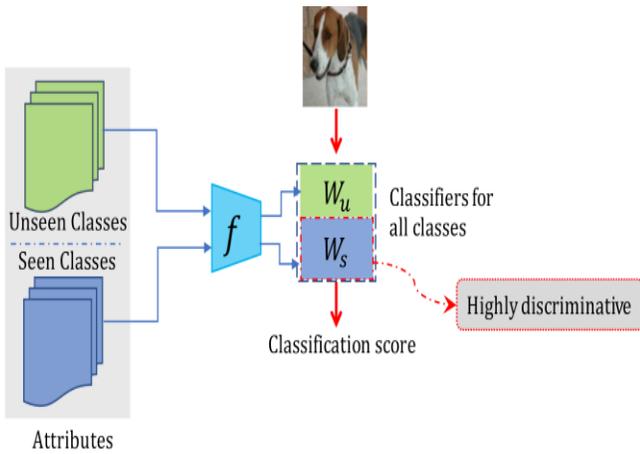


Fig. 16. Basic Image Classifier of Zero-Shot Learning Model.

**B. Proposed Model**

Our research aims to contribute to the growing literature on the new and novel theme that promises industrial revolution 5.0 in terms of collaboration between man and cobot. Our primary goal is to generate new ideas that will stimulate the interest of scholars in this subject.

According to our literature review, we have raised many challenges to overcome, especially when it comes to achieving effective collaboration between humans and machines. In this sense, the main problems that slow down the achievement of this goal largely concern big data.

Our approach consists of training a cobot by small amount of data using techniques discussed in this paper notably FSL and ZSL and MTDRL. An optimal common sense knowledge representation will be modeled and covers areas relating to human-machine collaboration in the context of Industry 5.0. These areas mainly concern actions and tasks, object recognition in the workplace and spatial navigation.

To compensate for the lack of the big data variable, research is continuing and focusing on strategies that rely simply on small data and allow for learning through collaboration or knowledge transfer.

In this order of thoughts, learning a cobot should be done as close to the human way as possible.

The cobot can collaborate and interact with its human counterpart only if it has a minimum of knowledge and common-sense background that allow it. The model will be able to learn at three levels: predictions against common-sense, human expectations and workers collaboration.

The cobot can act or accomplish a task in accordance with what has been pre-established in the model while remaining in permanent multimodal communication with the human collaborator who can correct it instantly to achieve the desired performance.

Like human learning, the cobot will be trained gradually from early stages of task completion, interaction, communication or decision making.

The model will be built around memory, computational units and three neural networks serving as training and correlating tools. The policies, rules and an optimal common-sense-knowledge repository will be stored at the memory level.

As shown in Fig. 17 our proposed model will be developed on three functions in order to calculate the action value, the policy and common-sense repository compliance value and finally the correlation function to assess the completion of multitasking based on the established policies and the repository of common-sense.

These functions will be implemented by three Deep Neural Network called:

- ZSL-DNN (Zero-Shot Learning Deep Neural Network).
- FSL-DNN (Few-Shot Learning Deep Neural Network).
- MTDRL-DNN (Multi-Task Deep Reinforcement Learning Deep Neural Network).

The Cobot's computational system will perform correlations between the objectives targeted by an action and what has been achieved by taking as reference the common-sense-knowledge repository, Human expectations and workers collaboration according to the algorithm illustrated in Fig. 18.

The algorithm's instructions will be carried out in the following sequence:

- Step 1: start of action;
- Step 2: correlation against common-sense;
- Step 3: return to step 2 if the outcome is unsatisfactory;
- Step 4: correlation against Human expectations;
- Step 5: return to step 4 if the outcome is unsatisfactory;
- Step 6: correlation against co-workers collaboration & correction;
- Step 7: return to step 6 if the outcome is unsatisfactory;
- Step 8: calculation of the action-value;
- Step 9: return to step 1 if the outcome is unsatisfactory;
- Step 10: reaction on the environment.

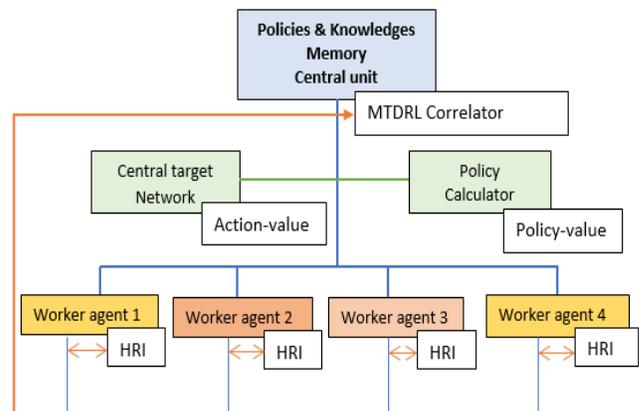


Fig. 17. Architecture of the Proposed Model.

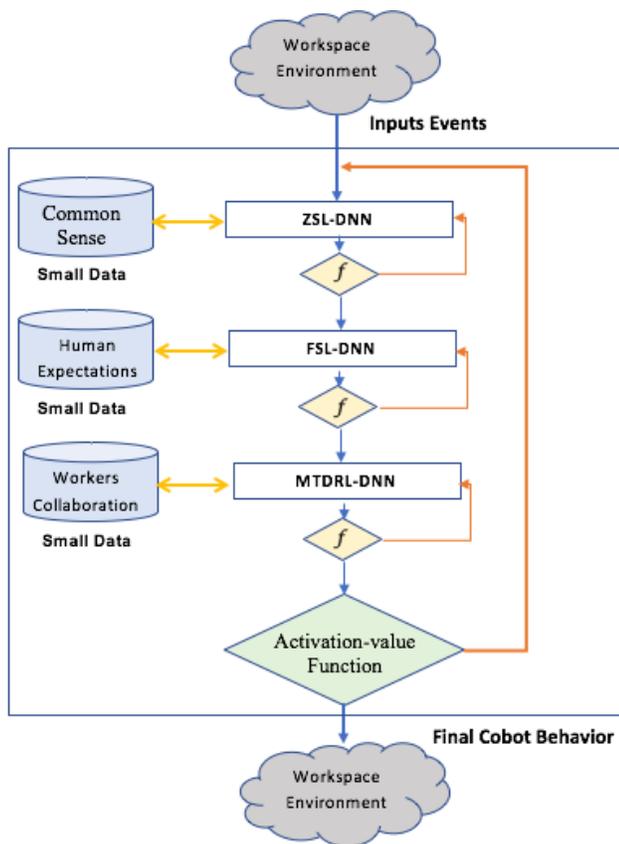


Fig. 18. Cobot Behavior Algorithm.

## V. CONCLUSION AND FUTURE WORK

The current trend in industry 5.0 is to be human-centered, the human and the cobot can interact safely and cooperate to accomplish the assigned tasks. The great progress of these systems is convincing, but the performance in this field is still far from being efficient. Artificial intelligence, while making great steps in many areas will have to overcome difficulties inherent to real-world environments.

Big data is critical to intelligence's success. On the other hand, the most significant constraint of deep learning is the requirement for enormous volumes of data; nevertheless, isn't it time to develop machines that can learn from little amounts of data?

In this paper, we have identified some of the technical challenges faced by researchers working on human-cobot collaboration. Current models of reinforcement learning for multi-tasking have many shortcomings that need to be addressed.

This study also highlights some of the existing solutions for addressing the key difficulties in the reinforcement area, such as DISTRAL, A3C, IMPALA, and PopArt.

Similarly, human-robot interaction has been briefly discussed given its importance in achieving Industry 5.0 goals. Human-robot interaction implies many technical challenges both in technical and human-centered aspects. Human-robot interaction is an open multidisciplinary field where current research is alive and growing.

Finally, we have proposed a new model and algorithm for training Cobots from small amount of data. Our model is based on three Deep Learning Neural Networks such as ZSL, FSL and MTDRL. The Cobot training will be gradually from early stages of task completion, interaction, communication or decision making.

In future work, we will try to deploy and experiment our model in a real industrial 5.0 context, in order to establish an appropriate Cobot collaboration.

## REFERENCES

- [1] M. Peshkin and J. Colgate, "Cobots," *Industrial Robot*, An International Journal, vol.26 n°5, pp. 335-341, 1999.
- [2] B. Claverie, B. Le Blanc and P. Fouillat, "La Cobotique," Presses universitaires de Bordeaux, 1 décembre 2013, DOI: 10.4000/communicationorganisation.4425.
- [3] Christoph. Bartneck, "A design-centred framework for social human-robot interaction," *University of Canterbury Conference Paper* October 2004.
- [4] Kristinn R.Thórisson, Jordi.Bieger, Thröstur.Thorarensen, Jona S. Sigurdardottir, "Why Artificial Intelligence Needs a Task Theory – And What It Might Look Like," *Conference Paper* July 2016, DOI: 10.1007/978-3-319-41649-6\_12.
- [5] Francesco. Longo, Antonio. Padovano and Steven. Umbrello, "Value-Oriented and Ethical Technology Engineering in Industry 5.0: A Human-Centric Perspective for the Design of the Factory of the Future," *applied sciences*, 18 June 2020.
- [6] Zhikun. Wang, Katharina. Mülling, Marc Peter. Deisenroth, Heni. Ben Amor, David. Vogt, Bernhard. Schölkopf, Jan. Peters, "Probabilistic Movement Modeling for Intention Inference in Human-Robot Interaction," Vol. 32, issue. 7, page(s). 841-858, *SAGE Journals*, April 2013.
- [7] Pieter. Abbeel and Andrew Y. Ng, "Apprenticeship Learning via Inverse Reinforcement Learning," *Computer Science Department, Stanford University: Stanford, CA 94305*, September 2004, DOI:10.1007/978-0-387-30164-8\_417.
- [8] Manuel. Lopes, Francisco S. Melo, Luis. Montesano, "Active Learning for Reward Estimation in Inverse Reinforcement Learning," *Conference: Machine Learning and Knowledge Discovery in Databases, European Conference, ECML PKDD 2009, Bled, Slovenia, September 7-11, 2009, Proceedings, Part II, September 2009*, DOI:10.1007/978-3-642-04174-7\_3.
- [9] Zhiyuan. Xu, Kun. Wu, Jian. Tang, Jieping. Ye, "Knowledge Transfer in Multi-Task Deep Reinforcement Learning for Continuous Control," *Conference Paper: 34th Conference on Neural Information Processing Systems (NeurIPS 2020), Vancouver, Canada, October 2020*.
- [10] John. McCarthy, "WHAT IS COMMON SENSE," *Computer Science Department, Stanford University : Stanford, CA 94305*, February 2002.
- [11] Antonio. Bicchi, Michael A. Peshkin, J. Edward Colgate, "Safety for Physical Human-Robot Interaction," *Springer Handbook of Robotics*, pp.1335-1348, Springer, Berlin, anuary 2008, DOI:10.1007/978-3-540-30301-5\_58.
- [12] Jean. Scholtz, "Theory and Evaluation of Human Robot Interactions," *Conference: 36th Hawaii International Conference on System Sciences (HICSS'03), January 2003*, DOI:10.1109/HICSS.2003.1174284.
- [13] Shirine. El Zaatari, Mohamed. Marei, Weidong. Li, Zahid. Usman, "Cobot programming for collaborative industrial tasks: An overview. Robotics and Autonomous Systems," *Publisher: Elsevier, Jun 2019*, DOI 10.1016/j.robot.2019.03.003.
- [14] Murtua, I., Fernandez, I., Tellaeché, A., Kildal, J., Susperregi, L., Ibarguren, A., Sierra, "Natural multimodal communication for human-robot collaboration. *International Journal of Advanced Robotic Systems*," July-August 2017, DOI: 10.1177/1729881417716043.
- [15] Ding. Z, Dong, H, "Challenges of Reinforcement Learning In Deep Reinforcement Learning," *Springer: Berlin/Heidelberg, Germany, 2020*.
- [16] Ruben. Glatt, Anna. Helena Reali. Costa, "Improving deep reinforcement learning with knowledge transfer," *In Proceedings of the*

- Thirty-First AAAI Conference on Artificial Intelligence, San Francisco, CA, USA, 4–9 February 2017.
- [17] Hessel. M, Soyer. H, Espeholt. L, Czarniecki. W, Schmitt. S, van Hasselt. H, “Multi-task deep reinforcement learning with popart,” In Proceedings of the AAAI Conference on Artificial Intelligence, Honolulu, HI, USA, 27 January–1 February 2019.
- [18] Matthew E. Taylor, Peter. Stone, “An introduction to intertask transfer for reinforcement learning,” *Ai Magazine* 32(1), March 2011, DOI:10.1609/aimag.v32i1.2329.
- [19] M. Betke, W. Mullally, and J. Magee, “Active detection of eye scleras in real time,” In Proceedings of the IEEE Workshop on Human Modeling, October 2001.
- [20] M. Betke, W. Mullally, and J. Magee, “Active detection of eye scleras in real time,” In Proceedings of the IEEE Workshop on Human Modeling, October 2001.
- [21] E. Horvitz and T. Paek, “Harnessing models of users’ goals to mediate clarification dialog in spoken language systems,” In Proc. of the Eighth International Conference on User Modeling, 2001.
- [22] Dagen. Wang and Shrikanth Narayanan, “An acoustic measure for word prominence in spontaneous speech,” *IEEE Transactions on Speech, Audio and Language Processing*, 15(2):690–701, Feb 2007, DOI:10.1109/TASL.2006.881703.
- [23] Rizzolatti. G, and Arbib. M.A, “Language within our grasp,” *Trends in Neurosciences*, 21(5):188–194, 1998.
- [24] B. Scassellati, “Investigating models of social development using a humanoid robot,” *Proceedings of the International Joint Conference on Neural Networks*, 4:2704–2709, July 2003.
- [25] C. Breazeal, A. Edsinger, P. Fitzpatrick, and B. Scassellati, “Active vision for sociable robots,” *IEEE Transactions on Systems Man and Cybernetics - Part A Systems and Humans* 31(5):443 – 453, DOI:10.1109/3468.952718.
- [26] Nelson Vithayathil. Varghese and Qusay H. Mahmoud, “A Survey of Multi-Task Deep Reinforcement Learning,” *Electronics* 9(9):1363, August 2020, DOI:10.3390/electronics9091363.
- [27] Yongyuan. Liang, Bangwei. Li, “Parallel Knowledge Transfer in Multi-Agent Reinforcement Learning,” arXiv, arXiv:2003.13085, March 2020.
- [28] Yee Whye. Tech, Bapst. V, Czarniecki . M, Quan. J, Kirkpatrick. J, Hadsell. R.; Heess. N, Pascanu. R, “Distral: Robust multitask reinforcement learning,” In Proceedings of the Thirty-first Annual Conference on Neural Information Processing Systems, Long Beach, CA, USA, 4–9, December 2017; pp. 4496–4506.
- [29] Liu. X, Li. L, Hsieh. P.C, Xie. M, Ge. Y, “Developing Multi-Task Recommendations with Long-Term Rewards via Policy Distilled Reinforcement Learning,” arXiv 2020, arXiv:2001.09595, January 2020.
- [30] Andrei A. Rusu, Sergio Gomez. Colmenarejo, Caglar. Gulcehre, Guillaume. Desjardins, James. Kirkpatrick, Razvan. Pascanu, Volodymyr. Mnih, Koray. Kavukcuoglu, and Raia. Hadsell, “Policy distillation,” *International Conference on Learning Representations (ICLR)*, 2016.
- [31] Emilio. Parisotto, Jimmy Lei. Ba, and Ruslan. Salakhutdinov, “Actor-mimic: Deep multitask and transfer reinforcement learning,” *International Conference on Learning Representations (ICLR)*, 2016.
- [32] Mnih. V, Badia. A.P, Mirza. M, Grave. A, Lillicrap. T, Harley. T, Silver. D, Kavukcuoglu. K, “Asynchronous methods for deep reinforcement learning,” In Proceedings of the International Conference on Machine Learning, New York, NY, USA, 19–24 June 2016.
- [33] Wang. Y, Stokes. J, Marinescu. M, “Actor Critic Deep Reinforcement Learning for Neural Malware Control,” In Proceedings of the AAAI Conference on Artificial Intelligence, New York, NY, USA, 7–12; Volume 34, pp. 1005–1012, February 2020.
- [34] Espeholt. L, Soyer. H, Munos. R., Simonyan. K, Mnih. V, Ward. T, Doron. Y, Firoiu. V, Harley. T, Dunning. I, “Impala: Scalable distributed deep-rl with importance weighted actor-learner architectures,” *ArXiv*. Feb 2018.

# Evaluation of using Parametric and Non-parametric Machine Learning Algorithms for Covid-19 Forecasting

Ghada E. Atteia<sup>1</sup>, Hanan A. Mengash<sup>2</sup>, Nagwan Abdel Samee<sup>3\*</sup>

Information Technology Department, College of Computer & Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 11461 Saudi Arabia<sup>1,3</sup>

Information Systems Department, College of Computer & Information Sciences, Princess Nourah bint Abdulrahman University, Riyadh, 11461 Saudi Arabia<sup>2</sup>

Computer Engineering Department, Misr University for Science and Technology, Giza, 12511 Egypt<sup>3</sup>

**Abstract**—Machine learning prediction algorithms are considered powerful tools that could provide accurate insights about the spread and mortality of the novel Covid-19 disease. In this paper, a comparative study is introduced to evaluate the use of several parametric and non-parametric machine learning methods to model the total number of Covid-19 cases (TC) and total deaths (TD). A number of input features from the available Covid-19 time sequence are investigated to select the most significant model predictors. The impact of using the number of PCR tests as a model predictor is uniquely investigated in this study. The parametric regression including the Linear, Log, Polynomial, Generative Additive Regression, and Spline Regression and the non-parametric K-Nearest Neighborhood (KNN), Support Vector machine (SVM) and the Decision Tree (DT) have been utilized for building the models. The findings show that, for the used dataset, the linear regression is more accurate than the non-parametric models in predicting TC & TD. It is also found that including the total number of tests in the mortality model significantly increases its prediction accuracy.

**Keywords**—Covid-19; parametric regression; non-parametric regression; linear regression; log regression; polynomial regression; generative additive regression; spline regression; k-nearest neighborhood; KNN; support vector machine; SVM; decision trees; DT

## I. INTRODUCTION

Once the coronavirus pandemic, Covid-19, broke out at the late of December 2019, in Wuhan, China, the virus has been spread all over the world by the Spring of 2020. The coronavirus pandemic has so far followed a wave pattern, with increases in new cases followed by reductions [1]. SARS-CoV-2, the coronavirus that causes Covid-19, has mutated since the beginning of the pandemic, resulting in variations of the disease symptoms [2]. The delta variation is one of these mutations. The delta coronavirus is one of the most contagious coronavirus strains to date [3]. Presently, some countries are suffering from the fourth wave of the pandemic with the severest mutated version of the virus, delta variant. The current total number of confirmed cases of Covid-19 approaches 245 million persons worldwide with nearly five million total deaths [4]. The unpredictable rapid spread of the pandemic all over the world has caused unprecedented global lockdowns and overwhelmed the healthcare systems. As no medicine has been

approved yet for this virus, the World Health Organization (WHO) has guaranteed the availability of Covid-19 clinical data for the majority of countries and encouraged the research community to provide support in this pandemic to “fight panic with information” [5][6]. This would certainly aid in directing governments toward proper crisis management and effective resource utilization to contain the pandemic.

Many recent studies have tackled the problem of forecasting the spread and mortality of the new coronavirus disease using various machine learning prediction methods. Based on the survey done in [7], most studies focused only on addressing the relationship between the numbers of confirmed and recovered cases and deaths to build models for predicting the spread of the coronavirus disease. However, there are other features that would significantly affect the prediction accuracy of these models.

In this paper, we propose a comparative study to evaluate the use of several parametric & non-parametric machine learning regression methods to model the two main folds of Covid-19 spread: the total number of confirmed cases and the total number of deaths. Within the study framework, we seek for the most significant input features of the models and investigate the impact of the number of tests on the prediction performance. The proposed framework has two phases: The Data Analytics & Modeling Phase and the Future Prediction Phase. In the first phase, Covid-19 time sequence dataset is preprocessed, and several significant predictors are selected according to a correlation criterion. These predictors are then used to build several regression models using several parametric & non-parametric methods using the training subset of the data. The model that shows the best prediction performance in terms of the least RMSE value will be considered for making the future predictions in the following phase. In the Future Prediction Phase, the values of the total deaths & the number of the total cases are to be predicted at future dates. In order to do so, the selected predictors should be estimated at the required future dates as well. Therefore, in this phase, each predictor is modeled individually against time (the day count referenced to an origin date) using a set of parametric & non-parametric methods. The best model is then used to estimate the value of the corresponding predictor at the required future date and predictor value is then substituted in

\*Corresponding Author

the total cases model as well as the total death model. The proposed framework has been applied on the Covid-19 dataset of Saudi Arabia over 116 days from April 25 till August 8, 2020 for training & testing the prediction models and these models have been used for estimating the future values of the total number of cases and total number of deaths.

## II. LITERATURE REVIEW

Several factors have influenced whether new Covid-19 cases are increasing or decreasing in specific locations during the pandemic. Some of these factors include the efficiency of vaccination, adhering the precautionary measures, the virus mutations, and the PCR tests. For instance, there was a huge surge in the number of Covid-19 confirmed cases during the winter of 2021 in the United States as a result of people not adhering to the COVID-19 precautions and regulations. Additionally, in many countries, vaccinating the citizens has aided in bringing new infection levels down until the spring season of 2021.

The number of PCR tests is one of the most important features that could significantly contribute to the prediction accuracy of the spread/ mortality models as it is explicitly affecting the number of confirmed cases. Nonetheless, no studies, to the best of our knowledge, have included the number of tests as an input feature to the Covid-related prediction models, nor have they examined its impact on the prediction accuracy of those models. For instance, the study of Yuanyuan et al. The work done in [8] utilized a linear regression analysis to create a model between the number of Wuhan roaming people and the cumulative number of Covid-19 cases in Henan province, China. Another study by Sansa et al. [9] conducted a correlation analysis and built a simple linear regression model between the numbers of confirmed cases and recovered cases in China over one month period. In another study[10], the epidemic peak in Saudi Arabia was predicted using the (Susceptible-Infected-Recovered) model [11], and the Logistic Growth model[12]. In that study, four variables were considered in the prediction models which are the number of daily confirmed, accumulated confirmed, recovered and deaths cases. Other studies utilized a number of non-parametric machine learning approaches to forecast the worldwide spread & death rate of Covid-19 and other pandemic-related variables as in [13][14][15]. The Naïve method, averaging, and Holt linear/winters method have been used in[14] to predict the value of the number of deaths in the next day based on the value of the present day. Another work in [16] has presented the application of linear and logistic regression for the prediction of the risk periods and survival of Covid-19 in different ages. However, the Decision Tree (DT)[17], K-Nearest Neighborhood (KNN) [18], and Support Vector Machine (SVM) [19] have been employed for the classification of patients (risk/mild) and hence the significant features have been extracted to distinguish between the classes of patients. In addition, DT, SVM, Random Forest, KNN, Naïve Bayes, and logistic regression were employed in [20] to predict the number of days needed to recover from Covid-19 and the age of patient that may result in risky outcomes of the disease.

## III. MATERIALS

In this work, a data set of COVID-19 records for Saudi Arabia [3] is used for building and evaluating the regression models. This dataset is published in the upstream repository at Johns Hopkins University Center for Systems Science and Engineering website [17]. The Covid-19 data set records the number of new confirmed cases, new deaths and recovered cases daily along with the corresponding accumulated total numbers. Other auxiliary entries like the median patient age, population, diabetes prevalence and others are also included in the data [2]. These auxiliary entries have constant values across the days. The number of new tests and total tests were recorded as well starting May 13th, 2020 for the Saudi Arabia data [2]. In this work, the entries with variable values are only used to model the number of the total confirmed cases and the total deaths using regression while the auxiliary entries were ignored as they do not contribute significantly to the models. There were four missing entries for the total tests and their values were estimated using the average of its two adjacent values. Day counts have been created to be used in reference to the required date. Day counts start from April 25th, 2020; i.e. Day 1 corresponds to April 25th, Day 2 to April 26th and so on. The available records are divided randomly into a training data set and a testing data set with a ratio of 8:2. The training data is used to estimate the regression coefficients of the prediction models while the testing set is used to evaluate the prediction accuracy of the proposed models. In order to unify the range of the input observations, the min-max normalization [18] is used to normalize the input features before building the models. All the codes of this work are created using the R programming language. For convenience, the following notations are used for the variables throughout the paper. TC, TR, ND, TD, TT, and DC denotes the number of the Total Confirmed Cases, the number of the Recovered Cases, the number of the New Deaths, the number of the Total Deaths, the number of the Total Tests, the Day Count.

## IV. METHODS

Regression is a supervised machine learning technique that is used for the prediction of a continuous quantitative outcome. For this purpose, the relationship between a dependent (response) variable and one or more independent variables (predictors) in a labeled dataset is estimated during the regression analysis process. Regression can be implemented using parametric and non-parametric algorithms. If a dataset is collected about a response variable  $Y$ , and predictor variables  $(x_1, x_2, x_3, \dots, x_m)$ , the relationship between  $Y$  and  $X$  can be modeled as in Eq. (1) [21].

$$Y = f(X, C) + C_0 \quad (1)$$

Where,  $C$  is a vector of  $m$  parameters,  $C_0$  is an error term that shows the deviation of the actual values from the model predictions and  $f(\cdot)$  is some function that maps the relationship between  $Y$  and  $X$ . The selection to use the parametric, semi-parametric or nonparametric method to implement the regression model depends mainly on the prior knowledge about the form of the function  $f(\cdot)$ . If  $f(\cdot)$  is known a priori, parametric methods is to be used; otherwise, non-parametric methods should be used. Semi-parametric methods can be used if  $f(\cdot)$  is known partially [21]. The function  $f(\cdot)$  could be

linear or non-linear function in the model parameters and accordingly the model becomes a linear or non-linear parametric model respectively. Parametric models require the estimation of the model parameters  $C$  and  $C_0$ . It is noteworthy mentioning that parametric models perform the best when the relational function is known and correct. In contrast, using the wrong function would result in larger bias when compared to the other competitive models [21] and would make inaccurate predictions. The most common parametric regression is the linear regression in which a linear model is composed of linear combination of the input predictors. Non-parametric regression methods do not require pre-knowing the form of  $f(\cdot)$  and consequently, they provide more flexibility in analyzing the relationship between the variables [21]. Many machine learning algorithms that are used for classification can be used as non-parametric regressors with some structural amendments when the response variable is continuous rather than discrete. The K-Nearest Neighborhood (KNN), Support Vector Machine (SVM) and Decision Tree (DT) algorithms are examples of such non-parametric regression methods.

**A. Parametric Machine Learning Regression**

To get sense of the relation between the dependent variable and each of the predictors, a set of scatter plots are provided in Fig. 1 for the total number of deaths and in Fig. 2 for the total number of confirmed cases. The scatter plots show that the

relationship between the response variables and all predictors, individually, are increasing and could be linearly modeled using the multivariate parametric linear regression.

**TD Linear Regression Models**

As the TD is highly correlated with the TC, TR & TT, the proposed prediction model of the TD in Experiment 1 is given in Eq. (2) while that of Experiment 2 after excluding TT, is given in Eq. (3) :

$$TD = C_0 + C_1 * TC + C_2 * TR + C_3 * TT \tag{2}$$

$$TD = C_0 + C_1 * TC + C_2 * TR \tag{3}$$

Where  $C_0, C_1, C_2, C_3$  are the regression coefficients of the model which represent the association of the model predictors to the dependent variable.

**TC Linear Regression Models**

The proposed prediction model of (TC, TT&TR) is given as in Eq. (4) and that of the (TC,TR) is given in Eq. (5):

$$TC = B_0 + B_1 * TR + B_2 * TT \tag{4}$$

$$TC = B_0 + B_1 * TR \tag{5}$$

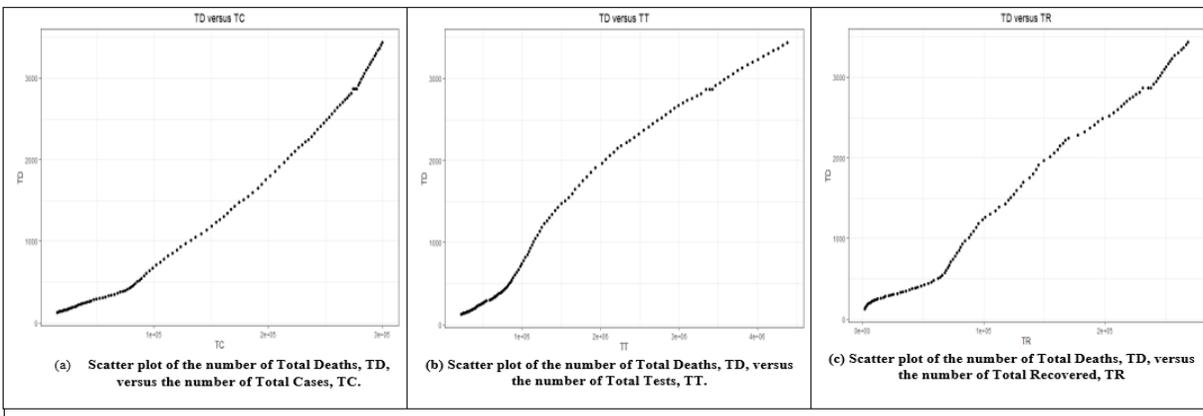


Fig. 1. Scatter Plot of the Total Deaths (TD) Versus Total Cases (TC), Total Tests (TT), and Total Recovered (TR).

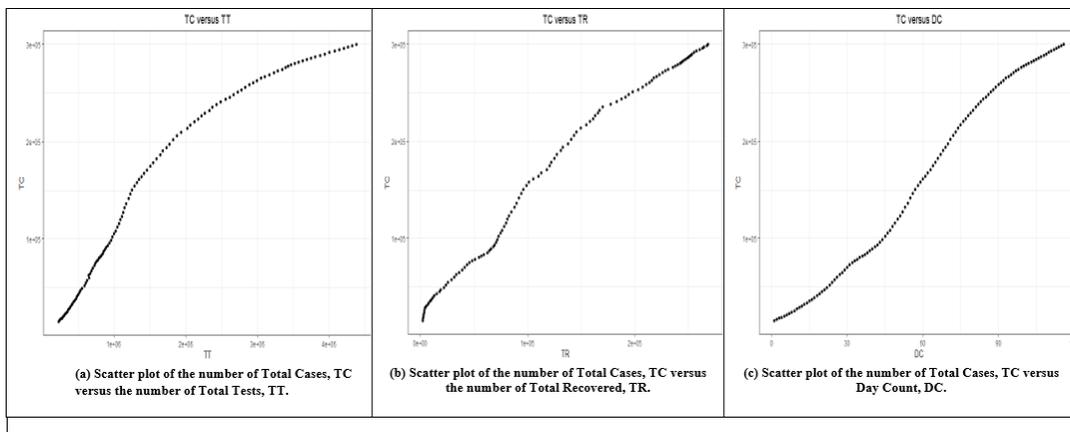


Fig. 2. Scatter Plot of the TC Versus Total Tests (TT), Total Recovered (TR), and Day Count (DC).

Where  $B_0, B_1, B_2$  are the regression coefficients of the model. The model coefficients for all of the linear models built in this study are estimated using the Least Squares Estimation algorithm.

### B. Non-Parametric Machine Learning Regression

In this part, the TC and the TD are modeled using a number of supervised learning non-parametric algorithms. Non-parametric algorithms do not make an assumption about the relationship between the response and predictors or the underlying distribution of the data and the model structure is configured from the data itself. In this study, the KNN, SVR and the DT algorithms are used for manipulating the regression problem.

KNN is a non-parametric supervised machine learning algorithm that is used for classification and regression. KNN approximates the association between the input features and the response variable using feature similarity[22]. In classification, KNN finds the majority votes of a number of neighbors (called k) of an input instance to select the appropriate class. However, in regression, the response variable is estimated by averaging the observations in the nearest neighborhood of the input instance based on a similarity measure. The similarity measure employed herein is the Euclidian Distance [23]. In order to select the optimal value of k, we run the KNN algorithm on the training dataset with k values starts from 3 up to 8 and calculate the RMSE at each k value then select the value that minimizes the root mean-squared error. k values of 1 & 2 are excluded as they cause unstable predictions. Also, k values greater than 8 are excluded as it has been observed that the RMSE values keep increasing as k increases.

Support Vector Machine (SVM) is a supervised machine learning algorithm that is used for classification and regression tasks. In a classification problem, SVM tries to find a hyperplane in the input feature space to distinctly classify the input data points[24]. Finding the hyperplane is an optimization problem to select the plane that achieves the maximum margin between the data points of two classes using the aid of kernel functions[25]. For a regression problem, SVM is known as SVR (Support Vector Regressor) and the problem then is to find a function that approximates input features to real numbers instead of discrete classes. This function itself defines the hyperplane in the regression problem and is used for the prediction of the response variable. This is again an optimization problem that aims to find the best hyperplane that passes through the maximum number of points within a given decision boundary at distance “ $\epsilon$ ” from the hyperplane. Let’s consider that the hyperplane is a straight line as in Eq. (6) [24]:

$$y = wx + b \quad (6)$$

Where  $w, b$  are the parameters of the line. Then the decision boundary can be defined as in Eq. (7), and Eq. (8):

$$wx + b = +\epsilon \quad (7)$$

$$wx + b = -\epsilon \quad (8)$$

So, any hyperplane that satisfies our SVR should satisfy Eq. (9) [24]:

$$-\epsilon < y - wx + b < +\epsilon \quad (9)$$

In this part of study, as no assumptions are made about the multivariate input or their relationships to the response variable, therefore, multiple kernel functions are used to adapt to the patterns in the data. The linear, polynomial, Gaussian radial basis and the sigmoid kernel functions [25] have been employed to non-linearly map the data from the original space into a higher dimensional space.

Decision Tree (DT) is a well-established supervised machine learning algorithm that can be used for classification and regression [26]. A decision tree makes decisions by splitting nodes into sub-nodes using the “if, then” condition multiple times until reaching the terminal homogeneous nodes. In this work, the Recursive partitioning has been employed to build the regression models of the response variables. The models are built against the predictors that show very high correlation with the response as depicted in Table I. As we are tackling a regression problem, we used the ANOVA splitting rule as the partitioning method of the tree. ANOVA rule is based on the Reduction of Variance concept to split the nodes. For each split, ANOVA calculates the variance of each node and then the variance of the split and then selects the split with the lowest variance. This process is repeated until all nodes with zero variance are reached and marked as the terminal nodes. At this end, no further splits are needed[26]. The ANOVA splitting rule is used as the partitioning methods of the tree. To pre-prune the Decision Tree, three hyperparameters are tuned and optimized. That is, the Complexity Parameter (CP), the Maximum Depth (MD) and the Minimum Split (MS). Complexity Parameter is used to save computing time by pruning off splits that does not improve the fit’s R-squared value by the value of (CP). The Maximum Depth indicates how deep the tree can be. The Minimum Split of the parent node which is the minimum number of observations in the parent node that can be split further[27]. To optimize the values of these hyperparameters, the R function “Rpart.tune” is used.

### C. The Study Framework

In this study, two models are to be built for the prediction of two response variables separately: the total number of confirmed cases (TC) and the total number of deaths (TD). Several parametric and non-parametric machine learning regression methods are utilized to build the models. The models will be evaluated based on some performance metrics and the best performing model will be considered for the future predictions of the response variables. The framework, shown in Fig. 3, is composed of two phases:

#### Phase 1: Data Analytics and Modelling

As a first step in this phase, data is explored to determine the significant predictors (the independent variables) to be used in building the models. A correlation analysis between all the input variables in the data has been conducted and the Pearson Correlation Coefficients (PCC)[28] are depicted in the correlation matrix in Table I. Only highly correlated variables (PCC>0.9) with the response variable are considered significant and used as predictors of the corresponding model. In Table I, highly correlated variables with the total confirmed

cases are highlighted in light grey while those highly correlated with the total deaths, are highlighted in dark grey.

After selecting the significant predictors, several parametric & non-parametric regression methods are used to model the total number of confirmed cases and the total number of deaths. At last, the model that shows the best prediction performance is selected for the future prediction in phase 2 of the framework.

The prediction model of the total number of deaths are built using the predictors that show high correlation with it which are the total number of tests, the total number of recovered cases and the total number of confirmed cases as shown in Table I. However, it was noted that the effect of the total number of tests on the Covid-19 prediction models is not investigated widely in the literature. Most probably this is because recording the TT on a daily basis was started late in most countries. Therefore, it has been decided in this study to figure out the impact of the total number of tests on the prediction accuracy of the proposed regression models. This is achieved by conducting two experiments for modeling the TD. In Experiment 1, all predictors that are highly correlated with the TD (which are TT, TR and TC) are used to build the model using the multivariate regression paradigm. On the other, the TT is excluded in Experiment 2 and the model is constructed using only TR and TC.

The prediction of the total number of confirmed cases is one main fold in tracing the spread of a pandemic. Therefore, an accurate model should be developed for the prediction of the total number of confirmed cases. In this study, two approaches are used to build and select the suitable TC model. In the first approach, a univariate prediction model is built for the TC using the day count as will be described later in this section. In the second approach, the multivariate regression is used to model the TC against the most significant predictors according to the high correlation criterion following the two experiments as in the TD model. In Experiment 1, according to the correlation criterion and as depicted in Table I, the TR and the TT achieve the highest correlation with the TC with  $PCC > 0.9$  and hence are used as the model predictors in this approach. Although, the TD shows high correlation with the TC, the former has been excluded while building the TC model. This has been decided to avoid any inaccuracy due to duplication as the TD model is considered the primary model and has already taken the TR and the TT in the prediction of TD. In Experiment 2, the TT is excluded from the model and the TR is the only predictor of the model.

After the TD & TC models from the two approaches are built by a set of parametric and non-parametric regressors, some performance metrics are then applied to evaluate the performance of the prediction models on the testing data set. The model that achieves the highest performance measures on the testing dataset are selected to be used for the prediction of the TC.

Phase 2: Future Prediction

As it is one of our objectives in this study to track the spread of Covid-19, values of the total number of confirmed cases and the total number of deaths are to be calculated at future dates. Given that the prediction models require the future values of their correspondent predictors, the values of these predictors are unknown apriori and need to be estimated beforehand at the required dates. Therefore, in this phase, each of the selected predictors is modeled individually against the day count. After that, the predictors' future values are substituted in the TC/TD forecasting models to find their corresponding future predictions. A number of parametric & non-parametric regressors are used to model the univariate predictors against the day count and the model with the least RMSE value is considered.

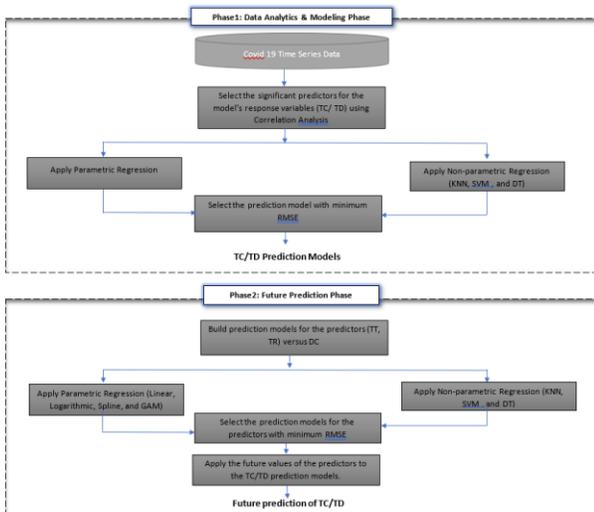


Fig. 3. The Study Framework for Predicting the Total Number of Cases & Total Number of Deaths of Covid-19 Outbreak.

TABLE I. CORRELATION MATRIX OF ALL VARIABLES INCLUDED IN THE STUDY

	DC	TR	TC	TT	TD	ND	NC
DC	1	0.99	0.994	0.969	0.982	0.658	0.032
TR	0.992	1	0.992	0.988	0.995	0.592	0.072
TC	0.994	0.992	1	0.965	0.989	0.658	0.034
TT	0.969	0.988	0.965	1	0.988	0.498	0.186
TD	0.981	0.994	0.989	0.988	1	0.580	0.083
ND	0.657	0.592	0.658	0.497	0.580	1	0.590
NC	0.033	0.072	0.034	0.186	0.083	0.59	1

V. RESULT AND DISCUSSION

In this section, the results related to the TC model are presented first followed by the results of the TD model. Within this arrangement, we present the models built using the parametric linear regression then those built using the non-parametric methods. To evaluate the performance of the regression models developed in this study, a number of well-known performance metrics are utilized. The Min-Max accuracy, MAPE, the Root Mean Squared Error (RMSE), the R-Squared, Error rate of the RMSE referenced to the mean of the actual values and the correlation accuracy are used to evaluate the accuracy of predictions on the testing data[29][30][31]. The model that achieves the highest significance and prediction accuracy will be used for making the future prediction of the total cases and deaths.

A. The Total Number of Confirmed Cases Prediction Model (TC Model)

Within the proposed framework for TC prediction, two approaches are used to model the total number of confirmed cases. In one approach, a univariate model that relates the TC with the DC is constructed. However, in the other approach, the highly correlated predictors with the TC (which are the TT & TR) are used to build the model. Under this approach, two experiments are conducted to investigate the effect of the TT on the TC prediction model. In Experiment 1, a model that relates the TC to both the TT & TR is built while in Experiment 2, the TT is excluded, and a univariate regression model is constructed using the TC & TR training data. Several regression models are built using the parametric linear regression and the KNN, SVR & DT non-parametric methods. The performance of each of the proposed models is assessed using the measures described in the Methods Section. The model that best fit the training data and that provides the highest prediction accuracy on the testing data is selected to be used in estimating the future value of the TC predictor required in the TD model.

1) Parametric Linear Regression

In this part, the relation between the predictors (TR, TT, DC) and the dependent variable (TC) is assumed to be linear. We have used two approaches in modeling TC. In the First Approach, TC is modeled versus predictors with high correlation with the response variable. And in the second approach TC is modeled only versus DC. In the first experiment under the first approach, we model TC versus TR & TT. To check the statistical significance of the estimated model coefficients, the standard error, p-value and the t-value are calculated after building the model using the training dataset as shown in Table II. The low values of these metrics reveal that the estimated coefficients are significant.

The accuracy of the TC model on the testing data has been evaluated using the Min-Max accuracy, the Mean Absolute Percentage Error (MAPE) and the R-Squared metrics. An average value between the maximum and minimum predictions has been retrieved as 94 % with a MAPE value of 0.063 which show a good accuracy of the prediction model over the testing data. The RMSE value of 6826 implies that there is an average alteration between the actual and the predicted values in the testing subset with an error rate of 5.27%. The value of the 0.99 for the R-squared reveals the high correlation between the actual and predicted values. This is consistent with the correlation accuracy of 0.9973 computed after predicting the TC for the test data. This implies that the actual and the predicted values have analogous directional movement in which the actuals values increase as the predicted values increase and vice-versa.

TABLE II. SUMMARY OF THE STATISTICAL SIGNIFICANCE OF THE ESTIMATED COEFFICIENTS OF THE (TC- TT& TR) PREDICTION MODEL

	Estimated Coefficient	STD Error	t-value	p-value
B <sub>0</sub>	25520	1560	16.36	< 2e-16
B <sub>1</sub>	-194135	18922	-10.26	< 2e-16
B <sub>2</sub>	464305	17319	26.81	< 2e-16

TABLE III. SUMMARY OF THE STATISTICAL SIGNIFICANCE OF THE ESTIMATED COEFFICIENTS OF THE (TC- TR) PREDICTION MODEL

	Estimated coefficient	STD Error	t.value	p-value
B <sub>0</sub>	1.084e+00	1.426e-02	75.98	<2e-16
B <sub>1</sub>	2.884e+04	2.091e+03	13.79	<2e-16

In the second experiment under this approach, the first approach, we model TC versus TR only. Like what has been done in Experiment 1, the statistical significance of the (TC, TR) model (given in Equation 4) are calculated and shown in Table III. The retrieved results of Min-Max accuracy, MAPE, RMSE, and R-squared are 91%, 0.1, 12812, and 0.98 respectively which are worse than the values for the (TC, TT&TR) model. The values of the performance measures depict that excluding the TT from the model reduces its statistical significance and reduces the prediction accuracy as well.

In the Second Approach, TC versus DC Model, the training dataset of the day count and the total number of cases (DC, TC) is used to fit a model for the TC. Five models have been built using the Linear, Logarithmic, Spline, Polynomial and the Generative Additive Regression. Scatter plots of these models are shown in Fig. 4. The R-squared values of these models vary from 0.8 to nearly 1. The Logarithmic regression provides the worst fit with the lowest R-squared value of (0.79) followed by the Linear regression model. The Spline regression and the Polynomial regression provide comparable R-squared values while the Generative Additive Model (GAM) provides the best fit in terms of the highest R-squared value. Therefore, the GAM model is considered here for further statistical significance analysis.

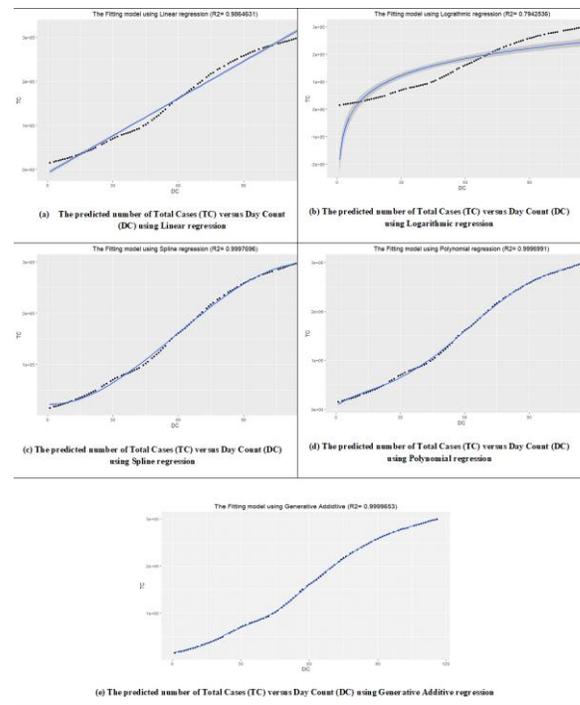


Fig. 4. The Predicted Total Cases (TC) Versus Day Count (DC) using: a) Linear Regression b) Logarithmic Regression c) Spline Regression d) Polynomial Regression e) Generative Additive Regression.

In an assessment of the prediction accuracy of the GAM model on the training data, the Adjusted and Multiple R-squared and the F-statistics are computed. The values of all R-squared measures are 1 which indicate that the variability in the TC is captured perfectly by the prediction model. This is supported by the very large value of the F-statistic (124906) and the very low p-value which reflect the high significance of the model. Therefore, this model was used to predict the TC values for the testing data and the performance metrics were computed to evaluate the prediction accuracy of the model. A Min-Max accuracy of 98.9% and a MAPE value of 0.011 were obtained for the model. The RMSE value of 1018 implies that there is a low average alteration between the actual and the predicted values in the testing subset with an error rate of 0.63%. The value of the 0.9999 for the R-squared reveals the high correlation between the actual and predicted values. This is consistent with the correlation accuracy of 0.9999 computed after predicting the TC for the test data.

2) *Non-parametric Machine Learning Regression*

In this part, no assumptions about the relation between the predictors (TR, TT, DC) and the dependent variable (TC) are made and the TC model is estimated from the data using the KNN, SVM and the DT regression methods. The performance measures calculated for all non-parametric methods are depicted in a table for each model and the model with the lowest RMSE is highlighted in light grey to facilitate the visual interpretation of the results. At the end, a comparison is conducted between the parametric and non-parametric models based on the RMSE measure to select the model that will be used for future predictions. Also, we have used two approaches in modeling TC as done in the Parametric regression.

In the First Approach, TC is modeled versus predictors with high correlation with the response variable. In the first experiment under this approach, we model TC versus TR & TT non-parametrically. Table IV shows the summary of the accuracy metrics for the models built by the KNN, SVM and the Decision Tree Regression. For the KNN, it is obvious that as the K increases, the larger the RMSE values are. Among all K values, the lowest RMSE & MAPE are achieved when the number of neighbor points equals 3. This k value also corresponds to the highest R-squared & Min-Max accuracy. For the SVM regression, the optimization tuning function “tune.svm” in the R language is used to deliver the best Gamma & cost parameters values for the Polynomial, Sigmoid & the Radial bases kernels for the SVM model. Values of the retrieved parameters are given in the caption of the table. It is noticed that the Radial kernel offers the least RMSE among the other kernels, yet still performing worse than the KNN. The Decision Tree Regressor has the worst performance over all non-parametric methods while the opposite is true for the KNN.

TABLE IV. SUMMARY OF THE ACCURACY OF THE (TC- TT & TR) PREDICTION MODEL ON THE TESTING DATASET USING THE KNN, SVM (GAMMA = 0.001, COST = 10 FOR POLYNOMIAL, RADIAL, SIGMOID KERNEL FUNCTION), AND DECISION TREE (BEST PARAMETERS: MAX DEPTH=3, CP=0.002, AND MINI SPLIT=10)

	Learning Parameters	RMS E	R2	Min-Max Accuracy	MAP E
KNN	k=3	1907.4	0.999	0.976	0.026
	k=4	2356.3	0.999	0.974	0.029
	k=5	2085.1	0.999	0.970	0.034
	k=6	2501	0.999	0.970	0.036
	k=7	2969.6	0.999	0.964	0.043
	k=8	3099	0.999	0.961	0.048
SVM	Linear Kernel	9349	0.991	0.907	0.118
	Polynomial Kernel	36644	0.85	0.77	0.29
	Radial Kernel	6326.7	0.996	0.927	0.099
	Sigmoid kernel	12713	0.649	0.38	0.778
DT	Anova Partitioning Method	11388.9	0.98	0.894	0.142

In the Second Approach, TC is modeled versus DC. Table V shows that the KNN with k=3 achieves the lowest error and the highest accuracy over all KNNs. Also, it has been found that the Radial kernel SVM is the best performer over all SVRs followed by the linear kernel. Decision tree performs comparably with the linear SVM and better than the Sigmoid SUM. However, again, the KNN with k = 3 is the best regressor over the other non-parametric algorithms and is highlighted in grey in Table V.

TABLE V. SUMMARY OF THE ACCURACY OF THE (TC-DC) PREDICTION MODEL USING KNN, SVM (GAMMA = 0.1, COST = 10 FOR POLYNOMIAL, RADIAL, SIGMOID KERNEL FUNCTION), AND DECISION TREE (BEST PARAMETERS: MAX DEPTH=3, CP=0.002, AND MINI SPLIT=10)

	Learning Parameters	RMSE	R2	Min-Max Accuracy	MAPE
KNN	k=3	2232	0.99	0.97	0.032
	k=4	2619	0.99	0.96	0.03
	k=5	2938	0.99	0.96	0.04
	k=6	2806	0.99	0.96	0.04
	k=7	3639	0.99	0.95	0.05
	k=8	4004	0.99	0.94	0.06
SVM	Linear Kernel	13143	0.98	0.87	0.18
	Polynomial Kernel	36607	0.85	0.76	0.31
	Radial Kernel	7913	0.99	0.94	0.06
	Sigmoid kernel	18408	0.96	0.86	0.16
DT	Anova Partitioning Method	12087	0.98	0.89	0.12

**B. The Total Number of Deaths Prediction Model (TD Model)**

In order to build the TD model, two experiments were conducted as aforementioned in Sec 3 in which the impact of the total number of tests on the prediction accuracy of the TD model is investigated. Several models are built using the parametric linear regression and the KNN, SVR & Decision Tree Non-parametric methods. The performance of each of the proposed models is assessed and the best fit will be used to estimate the total number of deaths.

**1) Parametric Linear Regression**

As a first Experiment, the TT, TR and the TC are used to model the TD using linear regression given in Equation 1. These predictors show very high correlation with the TD as illustrated in the scatter plots of Fig. 1. Table VI shows that the TC & TT coefficients have highest significance followed by the TR.

The accuracy of the TD model on the testing data has been evaluated. A Min-Max accuracy of 86% with a MAPE value of 0.13 is obtained for this model. The RMSE value of about 72 implies that there is very low average alteration between the actual and the predicted values in the testing data with an error rate of 4.25 %. A value of 0.995 for the R-squared and a correlation accuracy of 0.998 show that the actual and predicted values are highly correlated.

In the second Experiment, the TT is excluded, and the TR and the TC are used to model the TD using linear regression given in Equation 2. Table VII demonstrates the model significance over the training data. This table shows that the model coefficients have higher STD error, p-value & t-value than those obtained in Table VI for Experiment 1 using the TT as a model predictor. The accuracy of the TD model on the testing data has been computed. It has been found that the retrieved results of the Min-Max accuracy, MAPE, RMSE, and R-squared are 82%, 0.19, 97, 0.992 correspondingly which are worse than the values for the (TC, TT&TR) model.

TABLE VI. SUMMARY OF THE STATISTICAL SIGNIFICANCE OF THE ESTIMATED COEFFICIENTS OF THE (TD- TC& TR& TT) PREDICTION MODEL

	Estimated coefficient	STD Error	t-value	p-value
C0	-75.43	13.99	-12.378	5.32e-07
C1	2873.00	217.65	-5.212	< 2e-16
C2	-2218.01	377.07	12.933	6.47e-08
C3	2927.68	8.251e-04	203.60	< 2e-16

TABLE VII. SUMMARY OF THE STATISTICAL SIGNIFICANCE OF THE ESTIMATED COEFFICIENTS OF THE (TD- TC& TR) PREDICTION MODEL

	Estimated coefficient	STD Error	t-value	p-value
C0	-30.99	24.45	-1.268	0.208
C1	2741.32	273.18	10.035	<2e-16
C2	592.64	267.18	2.218	0.029

**2) Non-parametric Regression**

In the first Experiment, TD is modeled versus (TT-TR-TC). And as depicted in Table VIII, we can notice that the RMSE values for all KNN regressors used to build the (TD- TC& TR& TT) model is less than all other non-parametric models. Specifically, the least RSME is achieved by the KNN regressor with k =3 which is highlighted in grey in Table VIII. In contrast, it has been noticed that the Decision Tree has the worst performance metrics. For the SVMs, the radial kernel outperforms the linear & the sigmoid kernels.

TABLE VIII. SUMMARY OF THE ACCURACY OF THE (TD- TC& TR& TT) PREDICTION MODEL USING KNN, SVM (GAMMA = 0.01, COST = 10 FOR POLYNOMIAL, RADIAL, SIGMOID KERNEL FUNCTION), AND DECISION TREE (BEST PARAMETERS: MAX DEPTH=3, CP=0.015, AND MINI SPLIT=40)

	Learning Parameters	RMS E	R2	Min-Max Accuracy	MAP E
KNN	k=3	25.44	0.99	0.97	0.02
	k=4	27.25	0.99	0.97	0.02
	k=5	29.89	0.99	0.97	0.02
	k=6	36.65	0.99	0.97	0.03
	k=7	40.34	0.99	0.96	0.03
	k=8	43.94	0.99	0.96	0.03
SVM	Linear Kernel	85.25	0.99	0.81	0.19
	Polynomial Kernel	1131.2	0.83	0.45	1.69
	Radial Kernel	70.44	0.99	0.84	0.15
	Sigmoid kernel	91.22	0.99	0.80	0.19
DT	Anova Partitioning Method	232.82	0.95	0.78	0.32

TABLE IX. SUMMARY OF THE ACCURACY OF THE (TD- TR& TC) PREDICTION MODEL USING KNN, SVM (GAMMA = 0.01, COST = 10 FOR POLYNOMIAL, RADIAL, SIGMOID KERNEL FUNCTION), AND DECISION TREE (BEST PARAMETERS: MAX DEPTH=3, CP=0.015, AND MINI SPLIT=40)

	Learning Parameters	RMS E	R2	Min-Max Accuracy	MAP E
KNN	k=3	46.89	0.99	0.96	0.03
	k=4	48.42	0.99	0.96	0.03
	k=5	48.04	0.99	0.96	0.03
	k=6	45.89	0.99	0.97	0.027
	k=7	55.58	0.99	0.96	0.03
	k=8	53.15	0.99	0.97	0.03
SVM	Linear Kernel	117.7	0.99	0.78	0.23
	Polynomial Kernel	1188	0.87	0.44	1.75
	Radial Kernel	73.64	0.99	0.83	0.16
	Sigmoid kernel	125.2	0.98	0.75	0.25
DT	Anova Partitioning Method	269	0.94	0.83	0.22

In the second Experiment 2, TD is modeled versus (TR-TC). Table IX shows that the (TD- TR& TC) model also behaves like the (TD- TC& TR& TT) model in terms of the RMSE values but with larger values. It has been noticed that all KNN regressors has less RMSE values than all other non-parametric models. However, unlike the (TD- TC& TR& TT) model, the least RSME & MAPE and the highest accuracy & R-squared values are achieved by the KNN with  $k=6$  (highlighted in grey in Table IX). Moreover, it has been found that the Decision Tree has the worst performance metrics. For the SVMs, the radial kernel performs better than the linear & the sigmoid kernels.

C. Selecting the basic Models

In order to select the basic models that will be considered for the future prediction of the total number of confirmed cases & the total number of deaths, we compared the performance metrics for all the models created to the TC & TD variables using the parametric & non-parametric regression methods. The RMSE is selected to be used as the reference for the comparison as the R-squared values are convergent between most models, the Min-Max accuracy behaves consistently with it and the MAPE behaves consistently with the RMSE. The Bar graphs of Figures 5 & 6 are bar charts that show the lowest RMSE values for the parametric & non-parametric regression models built for the TC & the TD models respectively in this study. For the TC models, the RMSE values of only the KNN with  $k=3$  and the Gaussian radial kernel SVM along with the Decision Tree are depicted in Fig. 5. However, for the TD models, the records of the KNN with  $k=6$ , radial kernel SVM & the Decision Tree are shown in Fig. 6.

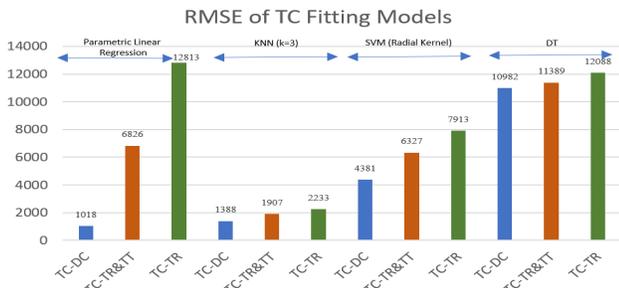


Fig. 5. Bar Chart for the Minimum RMSE retrieved for the TC Fitting Models.

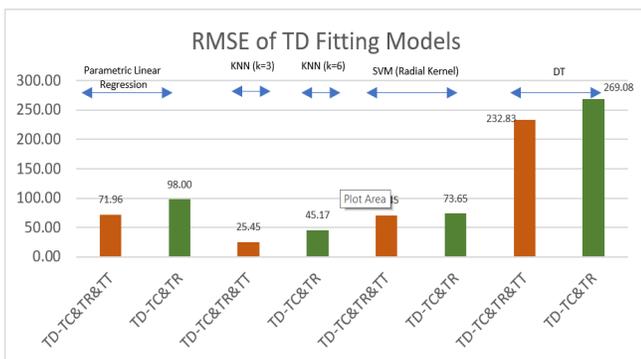


Fig. 6. Bar Chart for the Minimum RMSE retrieved for the TD Fitting Models.

For the TC, it is obvious that the (TC-DC) models have the best performance over all other models when estimated by both the parametric & non-parametric methods. Conversely, the (TC-TR) models are the worst consistently over all methods. Also, it has been observed that adding the TT as a predictor to the (TC-TR) model apparently improves the performance of the model but yet the (TC-TD) model outperforms the (TC-TR&TT) model. In order to select the best (TC-DC) model, we select the modeling method that provides the least RMSE. It has been found that the parametric linear regression model outperforms the KNN, SVM & DT non-parametric regressors. Therefore, it has been decided in this study to consider the linear regression model of the (TC-DC) model as the basic model for tracking the TC growth and for estimating the future values of the TC predictor in the TD model.

For the TD, we can see that adding the TT to the TC& TR reduces the RMSE for all parametric & non-parametric models. Although the reduction in RMSE is slight for almost all regression methods, for the KNN ( $k=6$ ), the presence of TT in the model reduces the RMSE by nearly 50%. However, we can see that TT has negligible effect for the SVM (Radial) Regressor. It is also noticed that the non-parametric KNN ( $k=6$ ) performs the best over the other non-parametric models and the parametric linear model followed by the SVM regressor. It is clear also that the linear regression & the SVM performs comparably for the (TD-TC&TR&TT) Nevertheless, it is decided in this study to consider the (TD-TC& TR&TT) build by the Radial Kernel SVM to be used for predicting the future values of the TD instead of the KNN. By finding the future prediction for the unseen data at multiple future dates, we found that all TD predictions have the same values. This could be explained in the light of knowing the nature of the KNN algorithm in associating the unseen data to its neighbors. That is, all upcoming future values appear in the neighborhood of the last training example (Day 116) in the training dataset which always uses this neighborhood to find the future prediction which will give surely the same value for the predictions for all days after Day 116.

D. Prediction of the Predictor's Future Values

The future predictions of the TD are estimated using the (TD-TC&TR& TT) model. However, the future values of the predictors TC, TR and TT are yet to be predicted against the Day Count. The (TC-DC) model has been previously built and its linear regression model will be used for predicting the future TC value. However, in this part, we model each of the predictors (TT and TR) with respect to the DC using parametric & non-parametric regression methods. Five parametric models have been built using the Linear, Logarithmic, Spline, Polynomial and the Generative Additive Regression [32][33][34]. However, the non-parametric models have been built using the KNN, SVM & DT regression. Afterward, we select the model that has the least RMSE value for the future prediction of the corresponding predictor. Fig. 7 & 8 show the parametric models of the predictors while Fig. 9 & 10 show the non-parametric models. The values of the RMSE corresponding to each model are depicted in Table X. It is clear from this table that the GAM models have the least RMSE over all other models therefore, they have been selected to find the future values of the predictors.

TABLE X. THE VALUES OF THE RMSE & R-SQUARED VALUES FOR THE (TT/TR VERSUS DC) MODELS BUILT USING SEVERAL PARAMETRIC AND NON-PARAMETRIC REGRESSION METHODS. LEAST RMSE VALUES ARE HIGHLIGHTED IN GREY

Predictor	Method	RMSE	R2
TT	linear	275906	0.94
	log	720572.8	0.59
	Splines	15480.06	0.99
	polynomial	31395.33	0.99
	GAM	12382.7	0.99
	KNN	15145.8	0.99
	DT	183297.9	0.98
	SVM	90788.64	0.99
TR	linear	11444.48	0.98
	log	48101.85	0.66
	Splines	2037.958	0.99
	polynomial	2585.802	0.99
	GAM	1247.912	0.99
	KNN	1295.82	0.99
	DT	11798.02	0.98
	SVM	5981.838	0.99

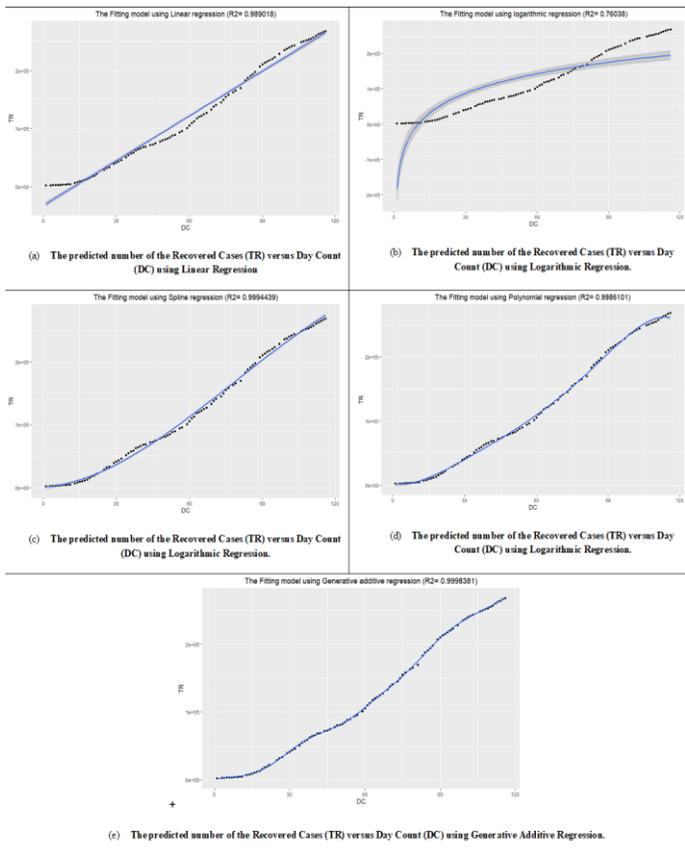


Fig. 7. The Predicted Number of the Recovered Cases (TR) Versus Day Count (DC) using: a) Linear Regression b) Logarithmic Regression c) Spline Regression d) Polynomial Regression e) Generative Additive Regression.

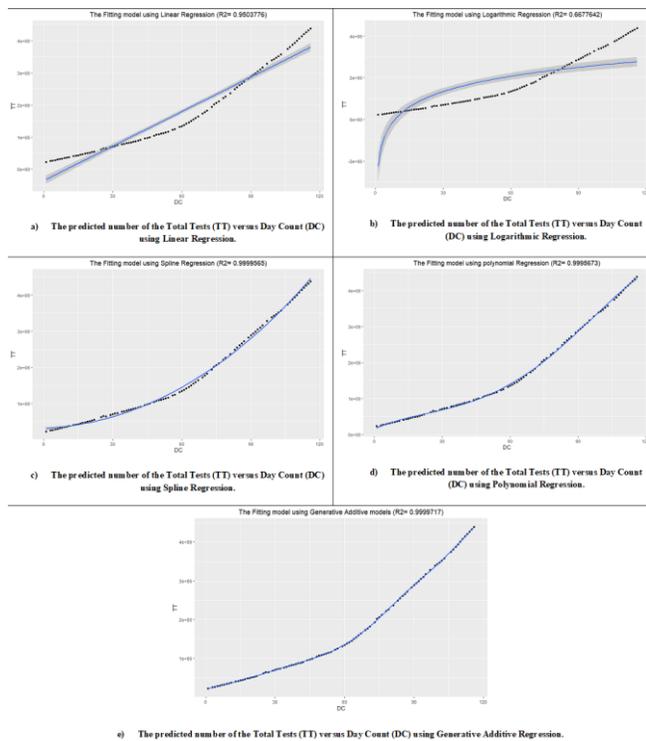


Fig. 8. The Predicted Number of the Total Tests (TT) Versus Day Count (DC) using: a) Linear Regression b) Logarithmic Regression c) Spline Regression d) Polynomial Regression e) Generative Additive Regression.

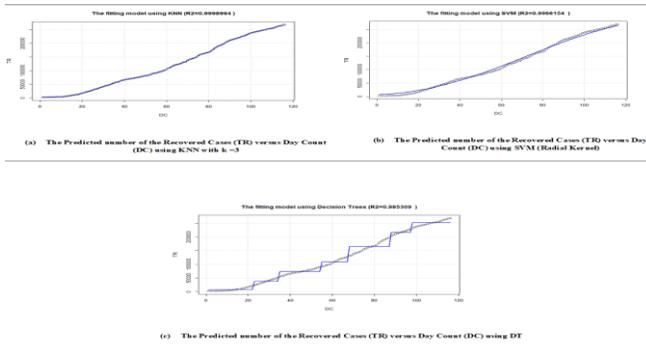


Fig. 9. The Predicted Number of the Recovered Cases (TR) Versus Day Count (DC) using Non-Parametric Regression: a) KNN with k =3 b) SVM (Radial Kernel) c) DT.

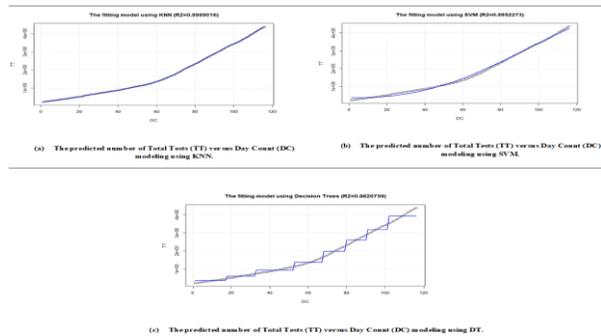


Fig. 10. The Number of Predicted Total Tests (TT) Versus Day Count (DC) using Non-Parametric Regression: a) KNN, K =3 b) SVM c) DT.

## VI. CONCLUSION

The main objective of this work is to investigate the power of the parametric and non-parametric machine learning methods in the accurate prediction of the spread and mortality of Covid-19 pandemic. Different features in the used Covid-19 dataset have been examined. Very high correlation between the models' response variable and the input predictors is used as the feature selection criterion. The significance of using the number of PCR tests as a model predictor has been investigated. Within the framework of this study, the data is preprocessed, and the most significant predictors are selected to build a number of regression models for the TC & TD separately. The parametric linear regression and the non-parametric KNN, SVM and DT are used for individually modeling the response variables against the selected predictors. The models that show the best prediction performance are considered the basic models to be used for the future prediction of the response variables. The predictors are modeled individually against a time variable using a variety set of parametric & non-parametric methods. The best model is then used to estimate the value of the corresponding predictor at the required future date. The findings show that, for the given dataset, the linear regression performs better than the non-parametric models for predicting TC & TD. It is also found that including of the total number of tests in the mortality model significantly increases its prediction accuracy.

## ACKNOWLEDGMENT AND FUNDING

This research was funded by the Deanship of Scientific Research at Princess Nourah bint Abdulrahman University through the Fast-track Research Funding Program.

## REFERENCES

- [1] G. Cacciapaglia, C. Cot, & F. Sannino, "Multiwave pandemic dynamics explained: how to tame the next wave of infectious diseases," *Sci. Rep.*, vol. 11, 2021.
- [2] W. T Harvey et al. "SARS-CoV-2 variants, spike mutations and immune escape," *Nat. Rev. Microbiol.*, vol. 19, pp. 409–424, 2021.
- [3] A. Sheikh, J. McMenamin, B. Taylor, & C. Robertson, "SARS-CoV-2 Delta VOC in Scotland: demographics, risk of hospital admission, and vaccine effectiveness," *Lancet.*, vol. 397, pp. 2461–2462, 2021.
- [4] Worldometer, "Coronavirus disease (COVID-19) outbreak." World Health Organization, Europe.
- [5] E. Dong, H. Du & L. Gardner, "An interactive web-based dashboard to track COVID-19 in real time," *Lancet. Infect. Dis.*, vol. 20, pp. 533–534, 2020.
- [6] M. Wolkeewitz & L. Puljak, "Methodological challenges of analysing COVID-19 data during the pandemic," *BMC Med. Res. Methodol.*, vol. 20, pp. 1–4, 2020.
- [7] G. Shinde et al. "Forecasting Models for Coronavirus Disease (COVID-19): A Survey of the State-of-the-Art," *SN Comput. Sci.*, vol. 14, issue 1, pp. 1–15, 2020.
- [8] ak and control in Henan province caused by the output population from Wuhan," *medRxiv*, 2020. doi:10.1101/2020.05.03.20089193.
- [9] N. Sansa, "The Correlation between COVID-19 Confirmed and Recovered Cases in China: Simple Regression Linear Model Evidence," *SSRN Electron. J.*, 2020. doi:10.2139/SSRN.3556549.
- [10] D. Alboaneen, B. Pranggono, D. Alshammari, N. Alqahtani, & R. Alyaffer, "Predicting the Epidemiological Outbreak of the Coronavirus Disease 2019 (COVID-19) in Saudi Arabia," *Int. J. Environ. Res. Public Health.*, vol 17, pp. 1–10, 2020.
- [11] W. Kermack, & A. McKendrick, "Contributions to the mathematical theory of epidemics," *Bull. Math. Biol.*, vol. 53, pp. 33–55, 1991.
- [12] G. Chowell, L. Simonsen, C. Viboud, & Y. Kuang, "Is West Africa Approaching a Catastrophic Phase or is the 2014 Ebola Epidemic Slowing Down? Different Models Yield Different Answers for Liberia," *PLoS Curr.* 6, 2014.
- [13] V. Chaurasia, & S. Pal, "Application of machine learning time series analysis for prediction COVID-19 pandemic," *Res. Biomed. Eng.*, pp. 1–13, 2020.
- [14] B. S. Frey, & H. Weck, "Estimating the Shadow Economy: A "Naïve" Approach," *Oxf. Econ. Pap.*, vol. 35, pp. 23–44, 1983.
- [15] A. K. Dubey, S. Narang, A. Kumar, S. Sasubilli, & V. Garcia-Diaz, "Performance estimation of machine learning algorithms in the factor analysis of COVID-19 dataset," *Comput. Mater. Contin.*, vol. 66, pp. 1921–1936, 2020.
- [16] Kaliappan et al. "Performance Evaluation of Regression Models for the Prediction of the COVID-19 Reproduction Rate," *Front. Public Heal.*, vol. 1319, 2021.
- [17] B. Yahaya, L. Muhammad, N. Abdulganiyyu, F. Ishaq, & Y. Atomsa, "An Improved C4.5 Algorithm using Hospital Rule for Large Dataset," *Indian J. Sci. Technol.*, vol. 11, pp. 1–5, 2017.
- [18] B. S. Everitt, S. Landau, M. Leese, and D. Stahl, "Miscellaneous clustering methods," *Cluster analysis*, pp. 215–255, 2011.
- [19] M. Islam, H. Iqbal, M. Haque, & M. Hasan, "Prediction of breast cancer using support vector machine and K-Nearest neighbors," *Proc. 5th IEEE Reg. 10 Humanit. Technol. Conf.*, pp. 226–229, 2018.
- [20] L. Muhammad, M. Islam, S. Usman, & S. Ayon, "Predictive Data Mining Models for Novel Coronavirus (COVID-19) Infected Patients' Recovery," *SN Comput. Sci.*, vol. 1, 2020.
- [21] H. Mahmoud, Parametric versus Semi and Nonparametric Regression Models. *Int. J. Stat. Probab.*, vol. 10, 2019.
- [22] Z. Yao, & W. Ruzzo, "A Regression-based K nearest neighbor algorithm for gene function prediction from heterogeneous data," *BMC Bioinforma.*, vol. 71, issue 7, pp. 1–11, 2006.
- [23] N. Ali, D. Neagu, & P. "Trundle. Evaluation of k-nearest neighbour classifier performance for heterogeneous data sets," *SN Appl. Sci.*, vol. 112, issue 1, pp. 1–15, 2019.
- [24] N. Parveen, S. Zaidi & M. Danish, "Support vector regression model for predicting the sorption capacity of lead (II)," *Perspect. Sci.*, vol. 8, pp. 629–631, 2016.
- [25] T. Hofmann, B. Schölkopf, & A. "Smola, Kernel methods in machine learning," vol. 36, pp. 1171–1220, 2008.
- [26] S. Uddin, A. Khan, M. Hossain, & M. Moni, "Comparing different supervised machine learning algorithms for disease prediction," *BMC Med. Informatics Decis. Mak.*, vol. 191, issue 19, pp. 1–16, 2019.
- [27] L. Breslow, & A. Leonard, W. David, "Simplifying decision trees: A survey," *Knowl. Eng. Rev.*, vol. 12, pp. 1–40, 1997.
- [28] S. Boslaugh, "The Pearson Correlation Coefficient," in *Statistics in a Nutshell*, 2nd Edition, O'Reilly Media, Inc., pp. 80–92, 2012.
- [29] J. Fan, "Nonparametric Models," in *Nonlinear Time Series*, New York: Springer, pp. 313–403, 2008.
- [30] J. Fan, "Nonparametric Density Estimation," in *Nonlinear Time Series*, Springer New York, pp. 193–214, 2008. doi: 10.1007/978-0-387-69395-8\_5.
- [31] J. Fan, *Nonlinear Time Series - Nonparametric and Parametric Methods*. Springer New York.
- [32] A. Gonçalves, E. Orton, J. Boon, & M. Salman, "Linear, logarithmic, and polynomial models of M-mode echocardiographic measurements in dogs," *Am. J. Vet. Res.*, vol. 63, pp. 994–999, 2002.
- [33] B. Wang, W. Shi, & Z. Miao, Comparative "Analysis for Robust Penalized Spline Smoothing Methods," *Math. Probl. Eng.*, 2014.
- [34] K. Ravindra, P. Rattan, S. Mor, & A. Aggarwal, "Generalized additive models: Building evidence of air pollution, climate change and human health," *Environ. Int.*, vol. 132, 2019.

# Comparison of Machine Learning Algorithms for Sentiment Classification on Fake News Detection

Yuzy Mahmud, Noor Sakinah Shaeali, Sofianita Mutalib  
Faculty of Computer and Mathematical Sciences, Universiti Teknologi MARA  
40450, Shah Alam, Selangor, Malaysia

**Abstract**—With the wide usage of World Wide Web (WWW) and social media platforms, fake news could become rampant among the users. They tend to create and share the news without knowing the authenticity of it. This would become the most critical issues among the societies due to the dissemination of false information. In that regard, fake news needs to be detected as early as possible to avoid negative influences on people who may rely on such information while making important decisions. The aim of this paper is to develop an automation of sentiment classifier model that could help individuals, or readers to understand the sentiment of the fake news immediately. The Cross-Industry Standard Process for Data Mining (CRISP-DM) process model has been applied for the research methodology. The dataset on fake news detection were collected from Kaggle website. The dataset was trained, tested, and validated with cross-validation and sampling methods. Then, comparison model performance using four machine learning algorithms which are Naïve Bayes, Logistic Regression, Support Vector Machine and Random Forest was constructed to investigate which algorithms has the most efficiency towards sentiment text classification performance. A comparison between 1000 and 2500 instances from the fake news dataset was analyzed using 200 and 500 tokens. The result showed that Random Forest (RF) achieved the highest accuracy compared to other machine learning algorithms.

**Keywords**—Data mining; fake news; sentiment classification; supervised machine learning; text mining

## I. INTRODUCTION

Fake news is now viewed as one of the greatest threats to democracy, journalism, and freedom of expression. Fake news is typically produced by people, the so-called “fakesters”, who generate an article with fake content often injected to an original real and trusted news content [1]. Although fake or satirical news can be less deceptive, intentional readers may still be deceived. Satirical news may deliberately establish a false expectation in the minds of readers through traditional meanings of dissatisfaction, taken as a face value. The untruthfulness is badly dissimulated and demand to be known [2]. According to Parikh and Atrey [3], researchers around the world have been very involved in the issue of fake news detection. Their studies have been carried out on the impact of fake news and how people react to it by viewing the title of the story, and cover image of the story. These factors might convince the readers about the content in the story or in news is realistic. Thus, the headline and image should be given more attention and take a step back and analyze the story or news after reading it so that readers might not believe the news fast enough. The fake news issues have become more popular after

the Presidential election of U.S. which makes many researchers trying to find out better solutions for machine learning classification [4].

Sentiment analysis study has taken a long time. Sentiment analysis in science and development has been the main problem of today’s world. As the number of users on social networking websites increases daily, enormous quantities of data are produced in text, audio, video, and images. Sentiment analysis as messages or posts must be carried out to decide if the sentiment is positive, negative, or neutral. Many automated classifiers are introduced to identify the text in the basic phrases, but new informal terms are applied to the current environment in the minimal spheres, which implies everything in the social realm [5].

This research focuses on filling the research gap between the machine learning algorithm and fake news challenges and assessments. Therefore, the research aims to perform research for automated prediction on fake news detection and investigate the performance of the machine learning technique to predict the fake news using text classification of the data. Manual analysis of the textual review can be frustrated and tedious. Some of data contains a lot of textual unrelated and unimportant message and this would be some challenges to define the best text representation for the textual classification.

In this research work, the textual classification and prediction can help an organization, a group of teams, or the other people to understand and expose more to the efficiently and effectively of fake news detection. Despite that, the automated natural language processing concept will be proposed and implemented that can be adaptive by the business or some organization to handle the hugely massive fake news textual data that show the genuinely comes from the truth sources. The remainder of this work is structured as follows: Section 2 presents the literature review. Section 3 explains the methodology of the research. Section 4 describes the result and discussions, and Section 5 explains the conclusion and future work that can be made to improve the research.

## II. LITERATURE REVIEW

Sentiment analysis or opinion mining, as it is often called, is indeed one of the computational studies that discuss the analysis of opinion-oriented natural languages [6, 7]. These opinion-oriented work comprises, along with other aspects, gender disparities, emotion, and attitude detection, ranks, evaluations of significance, textual perspective, description of source documents, and descriptive opinion [8]. The sentiment

analysis puts together several fields of research, such as natural language processing, data mining and text mining. The purpose is to use artificial intelligence tools in the activities, and to simplify and develop their goods and services which are becoming extremely essential for the enterprises. The goal is to discover views of people articulated in the written language (text) in sentiment analysis or opinion mining [9].

Machine learning techniques are particularly effective for classifying sentiments in positive, negative, or neutral types for classified document [10]. Training and testing datasets are needed in machine learning techniques. A testing data collection is used to study the documents and to verify the accuracy of the evaluation dataset. To classify and evaluate the performance of fake news data, some machine learning techniques were utilized and modelled. Based on the literature findings, there are four common classification machine learning models that have been used in many research to build the model which are Support Vector Machine, Naïve Bayes, Logistic Regression and Random Forest classifier [e.g: 11, 12, 13].

Few studies on comparing the machine learning classification algorithms on fake news have been conducted. For example, Hasan, et al. [11] has performed lexicon-based sentiment analysis (W-WSD, SentiWordNet and TextBlob) with two machine learning algorithms, Naïve Bayes and Support Vector Machine. The finding shows that W-WSD has a better result when analyzing the Tweets. Another research was by Aphiwongsophon and Chongstitvatana [12] who have conducted the experiments using Naïve Bayes, Neural Network and Support Vector Machine classification algorithms to detect fake news. The result shows that Naïve Bayes has the accuracy of 96.08%, and Neural Network and SVM provide the accuracy of 99.09%. Next, Hiramath and Deshpande [13] proposed fake news detection system based on classification using Logistic Regression, Naïve Bayes, Support Vector Machine, Random Forest, and Deep Neural Network for detecting fake news. The result shows that deep neural network is more crucial in detecting the fake news.

### III. RESEARCH METHODOLOGY

This research is conducted using CRISP-DM methodology. CRISP-DM is a modelling process which provides a data mining framework that could be used in technology and industry sectors to improve cost-effectiveness, reliability, repeatability, and speed for large data mining projects [14]. Fig. 1 shows the six phases of CRISP-DM methodology namely business understanding, data understanding, data preparation, modelling, evaluation, and deployment. The explanation of each phase will be explained in the next subsections.

#### A. Phase 1: Business Understanding

Business understanding is the first place of this research area. In this phase, the main area that will be examined is issues that are related with fake or real news and the representation of text and the lexicon-based method [15] to preprocess the textual data that are consider the point and significant phase in this text mining project. The initial business understanding phases emphasis on understanding the

business objective from business point of view, then changing over this knowledge into a research question, and after that create a research plan to accomplish the research objectives. This phase involves two activities. The first activity focuses on delivering research title, problem statement, research objectives, and research significance. While the second activity focuses on delivering the literature review to understand how previous scholars conduct the research in this area, for example what techniques have been used, what are the research findings, and what are the limitation of their research.

#### B. Phase 2: Data Understanding

This phase requires the researchers to obtain the required data and transformed it into a format that could be mined using data mining tools. Two activities are involved in this phase. The first activity is conducting data gathering. In this study, we used dataset from Kaggle website. However, this dataset might occur data incompleteness and data redundancy. Hence, several alternatives need to be applied to solve the problems, such as replace with alternative data source, gather new data, or narrow down the research scope. For this research, the dataset of Fake News Prediction consists of 12999 instances news with 20 attributes included the news title, authors, and others in year 2016 when the US President Election was happened. The second activity is to verify the quality of data. Up to this phase, data has been examined and studied, hence, it is crucial to confirm whether the data is good enough to support the objective of this research. Any missing value or error need to be identified and come out with the lists of action that can be taken to overcome this issue.

#### C. Phase 3: Data Preparation

Data preparation refers to preprocess the dataset for the modelling phase. This activity needs to perform multiple times to ensure the quality of the data. Fig. 2 illustrates the five stages of data preparation process which consists of data selection, data cleaning, data construction, data integration and data formatting. However, for this text mining research, the process is slightly different from the data mining process where some of the stages will happen in the middle of the modelling phases and not before. This is the flexibility of adapting CRISP-DM framework for textual mining research.

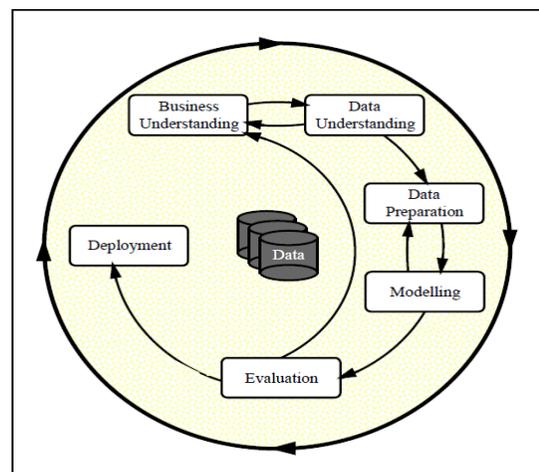


Fig. 1. Life Cycle of CRISP-DM [14].

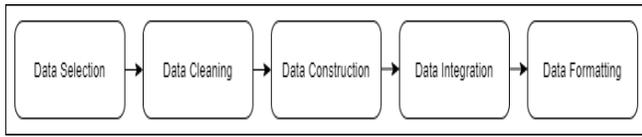


Fig. 2. Data Preparation Process.

#### D. Phase 4: Textual Data Labelling

Before the sentiment text classification performance can be compared, the model of the sentiment text classification must be constructed first. Fig. 3 shows the work flows of textual representation process.

The process starts with preprocessing the raw text data from the Fake News Dataset. Then, the data is transformed into a tokens and tags formation in Data Selection, which has been filtered and cleaned. When the data is ready, the preprocessed text will be sent to the sentiment analysis to label the sentiment from the review text data. Hu and Liu [16] sentiment analysis widget is based on the lexicon has been chosen for these activities. Unlike Vader method [17], Liu Hu method is simpler, which generate a single output of sentiment integer. However, the sentiment integer label is not represented as sentiment classification. The comparison result between the use of Liu Hu and Vader methods will be shown later in the results and discussions section. Therefore, the unsupervised label integer sentiment needs to classify using the hierarchical clustering technique. The purpose of this technique is to cluster integer sentiment that has close relations to classify into three groups of sentiment classification. Thus, the negative integer sentiment label will cluster under the negative values, the positive sentiment label will cluster under the positive values and the neutral sentiment label will cluster between -1 and 1 values.

#### E. Phase 5: Modelling

Orange data mining toolkit has been used in this phase to show the relationships between data in an understandable figure. The modelling method in this study is divided into three tasks, which consist of textual representation using a sentiment rating model, a content comparative model, and a predictive model. The process flow of architecture design in this research is shown in Fig. 4. The cleaned dataset derived from this phase was fed into the Designing Test task. There is one process occurred here, which is training process. To train the models, four machine learning algorithms are selected namely Naïve Bayes, Logistic Regression, Support Vector Machine and Random Forest. The selection of a best classification model is based on the highest coefficient accuracy result. The prediction model will use the same dataset during the model building phase. This is to produce the best classification model in predicting the fake news dataset.

A predictive model will be developed during this process. The Orange data mining prediction model is transparent and simple. Fig. 5 shows the prediction model process workflow. The prediction analysis uses the same data sets for classification model as the data set. The model is therefore nearly similar to the one for the performance analysis, in which the beginning component before the word bag is the same. The data sampler module is then used to separate the datasets into training and test results. The method of sampling is the one-on-

10-fold testing of the selected fold. One-fold will select 2000 instances from 6525 instances of datasets of input. The data sample serves as the test data and connects to the prediction module. In the meantime, the rest of the data acts as training data and connects to the learning algorithms.

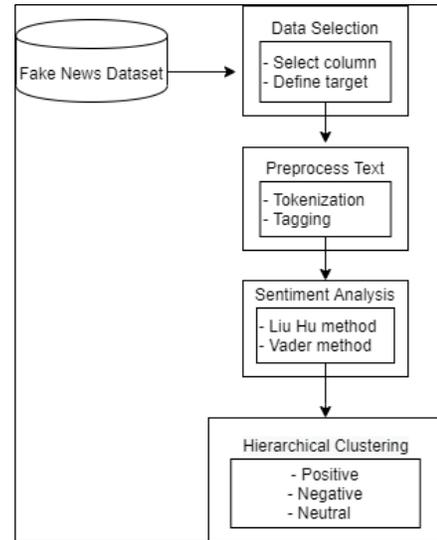


Fig. 3. Textual Representation Process Workflow.

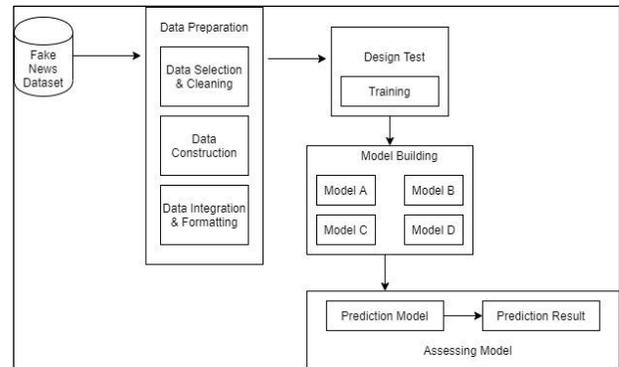


Fig. 4. The Process Flow of Architecture Design .

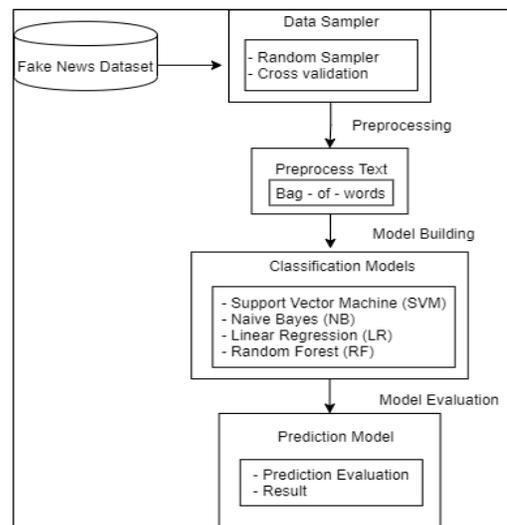


Fig. 5. Prediction Model Process Workflow.

Then, performance of each model is compared for sentiment classification. The process begins with the Data Sampler where the random sampler and ten-fold cross-validation will be done in this process using the same dataset. Then, the preprocess text activity and bag-of-words activity is combined to produce the clean data. For classification models, four accessible machine learning algorithms in the literature [18] has been determining to assess the performance of machine learning on sentiment classification. The selected machine learning algorithms are Support Vector Machine, Naive Bayes, Logistic Regression, and Random Forest. Each of classification model was developed through the training and testing process, following the supervised method. For that training and testing process, both the cross-validation approach was applied with 10 folds and hold out method through random data sampler, with 66% of dataset as training set and 34% of dataset as testing set.

#### F. Phase 5: Evaluation

In the evaluation phase, the performance of the predictive model is evaluated. The model is assessed in terms of precision, accuracy, recall and value of F1 classification. Error rates are used by supervised classification tasks to assess the consistency of data mining process. The dataset is also measured by the difference in the value of fixed data and the most common tokens for determining whether the data set size may affect the machine performance. If the process is failed, it is necessary to identify any possible reasons why the model did not satisfy the requirement. The data mining process also need to check thoroughly if there is existing additional process of iterations that can be made. The evaluation on the results from the comparison of the classification algorithms is performed on the dataset. In comparison, the assessment of datasets involves 10 cross validation directories and 10 random samples containing 60 per cent training results. This is an important experiment to determine how well the model can predict based on the data sets of training. There are two categories of performance measure that comprises of accuracy measures, as in (1) and error measures, as in (2). These performance measures will be discussed in the results and findings section.

$$\text{accuracy} = \frac{TP+TN}{TP+TN+FP+FN} \quad (1)$$

$$\text{error rate} = \frac{FP+FN}{TP+TN+FP+FN} \quad (2)$$

#### G. Phase 6: Deployment

Deployment is the final phase of the CRISP-DM approach. This phase requires all the process involves in this research are documented properly. Every part of the experimental results and comparative textual analysis from findings of this research are discusses and presents.

### IV. RESULT AND DISCUSSION

This section discusses the results and findings of the applied classification methods that had been chosen. It also provides the analysis on the trained and testing results based on

ten folds cross-validation and sampling methods of 66% training set and 34% testing set. The first experiment is performed to determine the label of each record in the Kaggle fake new dataset. This is a crucial process for textual classification using supervised method. The second experiment is focused on evaluating the performance of machine learning algorithms, which are Naïve Bayes, Logistic Regression, Support Vector Machine and Random Forest, for textual classification problems in the fake news data set. The third experiment is to compare the four machine learning algorithms with top frequent tokens. To compare the quality of the machine learning algorithms, the researchers used different performance measures such as accuracy score, precision, recall, and F-Score.

#### A. Experiment 1: Labelling of Textual Data using Lexicon Scores

Textual representation model experiment is more likely to a sentiment classification model where it has been conducted to prove the effective way to automated sentiment analysis through textual representation. Initially, the textual data and type of data is selected using select columns and corpus. Then, the raw data will be sent to preprocess text module which need to go through several stages to prepare the data for the sentiment analysis process. The text preprocessed activities generate 673862 based on the tokenization and uni-gram with bi-grams technique. Among all the token generated, 45183 types were identified as unique tokens. All the generated tokens will be feed into sentiment analysis widget to predict and label the sentiment on each news text. The sentiment classification labelling is conducted using lexicon-based dictionary approach by Liu Hu and Vader [16, 17] which produces the sentiment value. The sample of two lexicon-based sentiment is shown in Table I. Based on the sample of bias type, the first news text sentiment is bias with a negative value of sentiment. The second news text sentiment is also bias but with a positive value of sentiment.

The next process is to group the sentiment values to represent textual labels. Hierarchical clustering has used with distances to produce ten clusters contains positive sentiment values, negative sentiment values and lastly neutral sentiment values. A result of hierarchical clustering with Top-N = 10 selections for the three textual representation models for (a) Liu Hu [16] and (b) Vader [17] methods using ‘ward’ as the linkage between the attributes and 10 levels of pruning were compared. The 10 Top-N was chosen for this experiment because of the sentiment values show the random and mixture values of sentiments, so to make the next process easier, and an “Edit Domain” widget is used to group the 10-clusters into the three categories which is positive, negative, and neutral groups. Fig. 6 shows how the 10 Top-N cluster was categorized and labelled into three clusters group of positive, negative, and neutral sentiment according to sentiment values produced in hierarchical clustering chart in Fig. 7 (Liu Hu method) and Fig. 8 (Vader method).

TABLE I. SAMPLE OF LEXICON-BASED SENTIMENT

News Text	Type	Sentiment
Print They should pay all the back all the money plus interest. The entire family and everyone who came in with them need to be deported asap. Why did it take two years to bust them? Here we go again ...another group stealing from the government and taxpayers!	Bias	-1.961
Share on Facebook You've got to hand it to this guy for such an ingenious, yet simple design. The how-to example in the video below is made from approximately 12 feet of copper tubing plus a few fittings (the stainless steel tube option is shown too). Follow the instructions in the video below to learn how to build it yourself. If a torch isn't something you have in your tool kit you can find "push on" fittings from a hardware store that you won't need to solder.	Bias	1.786
Today Dr. Duke and Dr. Slattery talked about Hillary's clear acts of treason against the United States by providing massive shipments of weapons to Saudi Arabia at a time that she knew they were providing support to ISIS. Dr. Duke, if elected to the Senate, would be in a position to expose Hillary and push for her impeachment should she win (steal) the election. BLOOD ON THE TRAITOR'S HANDS!	Hate	0.784
Today Dr. Duke discussed the state of his campaign, including television commercials that he was preparing. He will be in a televised debate with the other leading candidates, which should be critical in putting him in the run off. Pastor Mark Dankof took over the show at the break. He took calls from listeners. One call asked about Jesus's warning about the Synagogue of Satan. Pastor Dankof ended the show with a passionate warning about the risk of World War III should Hillary be elections. This is another great show that you won't want to miss.	Hate	-1.370
COLUMBUS, OH (AP) — History was made today in Columbus, Ohio when more than 3 million Amish poured into the city to see the American Amish Brotherhood (AAB), an organization which acts as an informal governing body for the Amish community, endorse Donald Trump for president. That number represents a significant portion of the total Amish population, which the United States Census Bureau says numbers more than 20 million men and women nationwide all pledging their vote to Trump for President.	Fake	0.796
64 SHARE President Obama has signed an Executive Order declaring an investigation into the election results and plans for a revote on December 19th. (AP Photo / Dennis System)	Fake	0.385

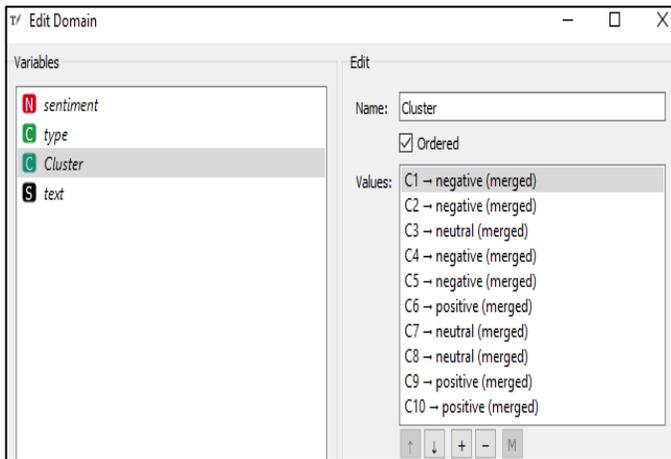
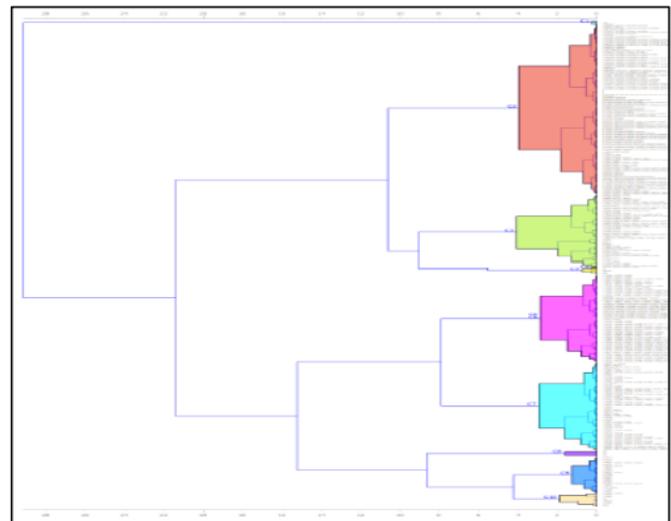


Fig. 6. Edit Domain Widget Process.

The comparison results of hierarchical clustering between Liu Hu [16] and Vader [17] methods does not show a lot of differences, but from other perception, Liu Hu method shows the most useful information that needed in this experiment as it uses lexicon-based sentiment analysis to classify each data in the dataset. Liu Hu method is easier because it shows the result of the sentiment directly and the values of sentiment for each cluster using the 'edit domain' widget. While for Vader method, the result from the hierarchical clustering shows a 'pos', 'neg', 'neu' and 'compound' values. The result from Vader method makes this experiment confusing because there is too much value of sentiment with the compound values that we define it was not useful for this experiment. So, for the next experiment Liu Hu's method will be chosen.

By referring to the text reviews in Table I for the bias texts, the negative and positive value sentiments are due to hierarchical clusters of Ward linkage combine with Euclidean on distances widget. The probability of correcting the precise opinion would evaluate the distance between two points in the line and then measure the number of squared differences within

each of the clusters. This means that most of the result is close to the average neutral sentiment. The findings of the output sentiment can be acknowledged therefore by analyzing the dispersal plot between the output sentiment and the text types ranking scale.



title	type	text	Cluster	sentiment
1	bias	Print They shou...	positive	-1.961
2	bias	Why Did Attorn...	positive	-1.488
3	bias	Red State: Fox ...	positive	-1.460
4	bias	Email Kayla Mu...	negative	0.000
5	bias	Email HEALTH...	positive	-0.804
6	bias	Print Hillary go...	neutral	-5.490
7	bias	BREAKING! NY...	positive	-1.446
8	bias	BREAKING! NY...	neutral	-3.319
9	bias	Limbaugh said ...	positive	-1.224
10	bias	Email These pe...	positive	-1.316

Fig. 7. Hierarchical Clustering and Sample of Data Sentiment Values using Liu Hu Method.

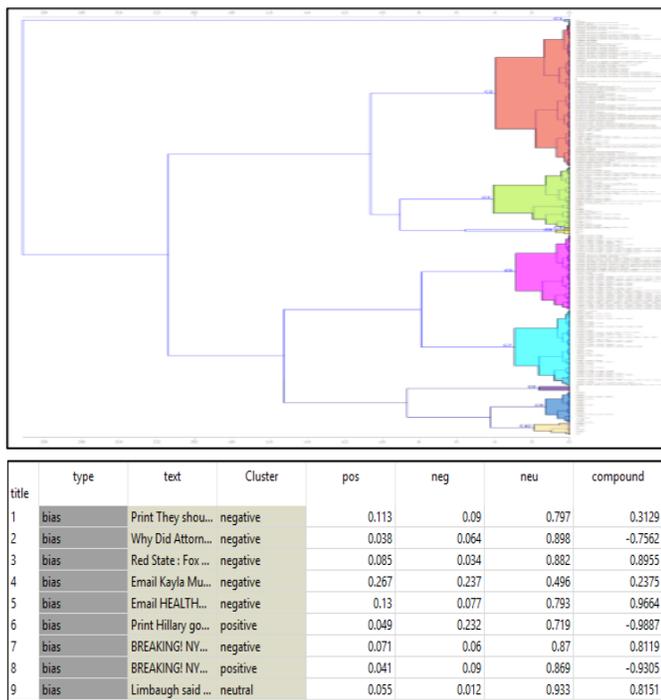


Fig. 8. Hierarchical Clustering and Sample of Data Sentiment Values using Vader Method.

**B. Experiment 2: Classification Model Construction**

In the evaluation of prediction models, the same dataset was used to compare the output sentiment result of the automated sentiment classification based on the lexicon-based approach in Experiment 1, and the result of the prediction model using LR supervised machine learning in Experiment 3. The only different in dataset for Experiment 2 is the dataset will be split into two subsets of data using ‘data sampler’ widget for the training dataset and the testing dataset. Based on the confusion matrix for prediction model in Fig. 9, negative prediction on sentiment text classification is 100%, which shows that the accuracy is perfect. However, the percentage results for this dataset are likely to change after inserting more data. The highest value of misclassified is through neutral sentiment, which is 5.1%. However, the misclassified sentiment cannot assume as wrongly predicted. For example, in Table II, it shows the differences value of misclassified for Naïve Bayes is quite high but for correctly prediction, Naïve Bayes provides the highest accuracy among the other classifiers. Based on the situation, the researchers conclude that by using machine learning algorithms, the automated sentiment text classification can be improved.

	negative	positive	neutral	Σ
Actual negative	100.0 %	0.0 %	1.4 %	366
Actual positive	0.0 %	100.0 %	3.7 %	83
Actual neutral	0.0 %	0.0 %	94.9 %	801
Σ	354	52	844	1250

Fig. 9. Sample of Confusion Matrix of Prediction Model.

TABLE II. DATA AND PREDICTION USING MACHINE LEARNING CLASSIFIERS

Classifier	Support Vector Machine (SVM)	Random Forest (RF)	Naïve Bayes (NB)	Logistic Regression (LR)
Correctly Classified	99.8%	99.9%	84.0%	96.7%
Correctly prediction	99.6%	99.3%	99.7%	92.8%
Misclassified	12.0%	8.4%	56.4%	7.4%

**C. Experiment 3: Comparison Performance Model with Top Frequent Tokens**

The third experiment was conducted to compare four machine learning strategies for sentiment text classification with selected terms. The models are developed using a bag of words and four supervised machine learning technology, which includes Support Vector Machine, Naïve Bayes, Logistic Regression and Random Forest. The news text will be pre-processed by text and sent to bag-of-words to count the number of words occurring in the news text. Then two setups for experiments using four machine learning techniques of supervision are carried out. To assess the efficiency of this machine learning, four main efficiency indicators (KPI) will be evaluated which are classification accuracy, F-1 Score, Precision and Recall.

Table III shows the machine learning classification accuracy based on fixed proportion data and the number of tokens that are most common, as the first set up. The effect based on the number of tokens can be seen by comparing Set A for 1000 instances with 250 most frequent token, Set B for 1000 instances with 500 most frequent token, Set C for 2500 instances with 250 most frequent token and Set D for 2500 instances with 500 most frequent token.

TABLE III. CLASSIFICATION ACCURACY BASED ON SIZE DATA AND THE AMOUNT OF TOKENS

Label	Classifier	SVM	NB	LR	RF
Set A	50% proportion of data (1000 instances) with 250 most frequent tokens	96.2%	87.6%	94.9%	<b>98.7%</b>
Set B	50% proportion of data (1000 instances) with 500 most frequent tokens	<b>99.4%</b>	86.3%	93.4%	97.8%
Set C	50% proportion of data (2500 instances) with 250 most frequent tokens	55.6%	48.9%	45.1%	<b>58.4%</b>
Set D	50% proportion of data (2500 instances) with 500 most frequent tokens	49.2%	35.8%	54.6%	<b>60.2%</b>

The results show that the amount of the most frequent tokens (Set B and Set D) does not affect the classification accuracy, while the lowest number of tokens show a higher classification accuracy (Set A and Set C). By contrast, the effect based on the size of proportion data can be seen by comparing Set A with Set C and Set B with Set D. The

different of classification accuracy for comparing these set is quite high. Thus, this can conclude that the size of proportion data is affecting the classification accuracy but not heavy. One unanticipated finding was that all the classification accuracy of A is higher when the size proportion of data is bigger for Set A with Random Forest accuracy 98.7% except Set B for Naive Bayes, Set C for Logistic Regression and Set D for Naive Bayes. Surprisingly, Support Vector Machine has the highest achievable classification accuracy of 99.4% with a variable of high proportion data and high frequent token in Set B. However, with 2500 instances for 250 and 500 most frequent tokens in Set C and Set D show that the classification accuracy for all four methods was unsatisfied, whereby the classification accuracy for Set C shows that Random Forest with highest accuracy of 58.4% and the highest accuracy for Set D is 60.2% for Random Forest. In conclusion, variable Set B shows the best option for creating classification accuracy with the highest result and can be considered to adopt for the next experiment.

In the second set up of experiment, the machine learning performance were evaluated based on the sampling approach, which are ten folds cross-validation and ten repeat train or test random sampling with 60% training set size. The same data for the four KPIs will be analyzed in these experiments to studies the performance of a machine learning technique for textual sentiment classification. Later, the confusion matrix will be applied to observe the proportion between the actual and predicted class. With the confusion matrix, a misclassified instance can use to review the textual data in detail to discover the reason behind it. Table IV and Table V show the KPI of machine learning algorithms for textual sentiment classification using 1000 instances and 2500 instances. The results for show that the highest classification accuracy is 98.5% for 1000 instances and 99.9% for 2500 instances using Random Forest algorithm. By comparing between sampling type, the different of KPI for all algorithms are not much except for Naïve Bayes algorithm. All algorithms have slightly higher KPI result for using ten folds cross-validation sampling except for Naïve Bayes, which KPI result is better on ten folds cross-validation. As the conclusion from this experiment, both

sampling approaches give almost the same value of classification accuracy results and do not contribute to classification performance.

For further analysis, the confusion matrix in Fig. 10 and Fig. 11 shows the comparison of the proportion of the predicted sentiment on the text datasets with 1000 instances and 2500 instances. The results show that most predicted correctly is positive sentiment of fake news for 1000 instances is 82.1%, while for 2500 instances is 98.8% of positive sentiment for fake news. However, neutral sentiment for fake news in Fig. 10 archived 100% accuracy, while Fig. 11 shows the highest accuracy of neutral sentiment is 99.7%. In contrast, negative sentiment for fake news in both result shows lower accuracy compared to the rest. In conclusion, the bigger proportion of data to be tested, the bigger accuracy can be classified and evaluated, compare to the small proportion of data that predicted as positive, negative, and neutral sentiment.

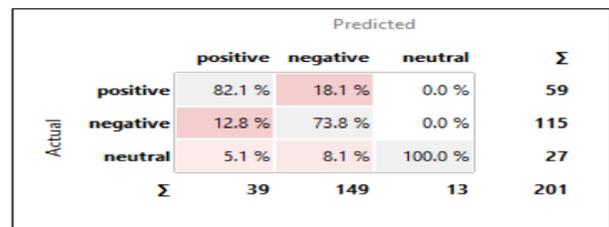


Fig. 10. Confusion Matrix of Predicted Sentiment using 1000 Instances.

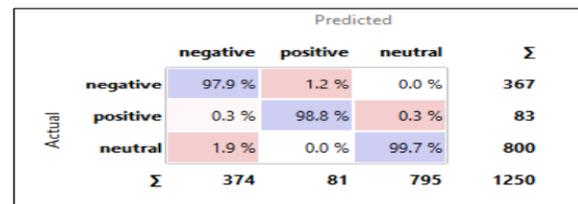


Fig. 11. Confusion Matrix of Predicted Sentiment using 2500 Instances.

TABLE IV. KPI OF MACHINE LEARNING ALGORITHMS FOR TEXTUAL SENTIMENT CLASSIFICATION USING 1000 INSTANCES

Machine Learning Algorithms	10-folds cross validation				10 repeat train/test random sampling with 60% training set size			
	CA	Precision	Recall	F1	CA	Precision	Recall	F1
Logistic Regression (LR)	94.5%	94.9%	95.4%	94.3%	93.1%	93.4%	93.1%	92.8%
Support Vector Machine (SVM)	96.0%	96.2%	96.0%	96.0%	97.5%	99.7%	97.5%	97.5%
Naïve Bayes (NB)	84.5%	87.6%	84.5%	84.9%	84.1%	86.3%	84.1%	84.7%
Random Forest (RF)	98.5%	98.5%	98.5%	98.5%	97.8%	97.8%	97.8%	97.8%

TABLE V. KPI OF MACHINE LEARNING ALGORITHMS FOR TEXTUAL SENTIMENT CLASSIFICATION USING 2500 INSTANCES

ML Algorithms	10-folds cross validation				10 repeat train/test random sampling with 60% training set size			
	CA	Precision	Recall	F1	CA	Precision	Recall	F1
Logistic Regression (LR)	96.6%	96.7%	96.6%	96.3%	95.7%	96.0%	95.7%	95.3%
Support Vector Machine (SVM)	99.1%	99.1%	99.1%	99.1%	99.4%	99.8%	99.8%	99.8%
Naïve Bayes (NB)	89.0%	84.0%	89.0%	86.0%	88.9%	83.9%	88.9%	84.7%
Random Forest (RF)	99.9%	99.9%	99.9%	99.9%	99.8%	99.8%	99.8%	99.8%

## V. CONCLUSION AND RECOMMENDATION

The study includes the comparison of four classification algorithms to evaluate the performance of classification accuracy in sentiment text classification. The evaluation process includes several aspects such as the size of data, amount of token, and test sampling approach. A 1000 instances dataset and 2500 instances dataset with different values of 250 and 500 most frequent tokens were applied in this experiment. The four classification algorithms used in this experiment are Support Vector Machine, Naïve Bayes, Random Forest and Logistic Regression. By that, a model was evaluated to measure the accurateness and the exactness of the model to make a prediction on a new dataset. Prior to the model evaluation, the model was able to predict all the fake news correctly, which makes the model reliable and trustworthy to be used to predict the fake news detection status.

However, there are some limitations in this research that need to be highlighted. Firstly, Orange toolkits have some technological weakness and limitation when managing massive databases. This work will therefore process randomly 1,000 fake news and 2500 fake news from the initial data sets out 12999 total of fake news during US Presidential Election in 2016. Secondly, this research focuses on the Fake News Detection dataset, which focused on a single objective. The research can be applied to another dataset such as from twitter or social media to mine the knowledge from the text deeper to understand its sentiment. Lastly, in the case of model validation using a cross-validation and/or an individual validation method, Orange Toolkits provide the facilities but cannot save the model and need to rebuild the model each time for the next data set.

For some future work, there is another feature and word representation approach that can be used for text mining project. Nevertheless, in this research there is only focuses on bag-of-words feature approach. There is a possibility that another feature approach can increase classification accuracy performance. Based on literary research, the sentiment analysis may be carried out with the modification of lexicon-based dictionary using a specific language. For more study, an automatic sentiment analysis multi-classification is also can be done for future work.

## ACKNOWLEDGMENT

The authors would like to thank the Faculty of Computer and Mathematical Sciences and Research Management Center Universiti Teknologi MARA, Shah Alam, Selangor for supporting this research.

## REFERENCES

[1] R. K. Nielsen and L. Graves. "'News you don't believe': Audience perspectives on fake news." Reuters Institute (accessed 30 September, 2021).

[2] N. M. N. Mathivanan, N. A. M. Ghani, R. M. Janor, and Ieee, "Analysis of K-Means Clustering Algorithm: A Case Study Using Large Scale E-Commerce Products," presented at the 2019 IEEE Conference on Big Data and Analytics (ICBDA), 2019.

[3] S. B. Parikh and P. K. Atrey, "Media-Rich Fake News Detection: A Survey," in 2018 IEEE Conference on Multimedia Information Processing and Retrieval (MIPR), 10-12 April 2018 2018, pp. 436-441, doi: 10.1109/MIPR.2018.00093.

[4] T. Abdullah Ali, E. M. Mahir, S. Akhter, and M. R. Huq, "Detecting Fake News using Machine Learning and Deep Learning Algorithms," in 2019 7th International Conference on Smart Computing & Communications (ICSCC), 28-30 June 2019 2019, pp. 1-5, doi: 10.1109/ICSCC.2019.8843612.

[5] A. Shelar and C.-Y. Huang, "Sentiment analysis of twitter data," in 2018 International Conference on Computational Science and Computational Intelligence (CSCI), Las Vegas, NV, USA, 2018: IEEE, doi: 10.1109/CSCI.2018.00251.

[6] M. Puteh, N. Isa, S. Puteh, N. A. Redzuan, and A. M. Korsunsky, "Sentiment Mining of Malay Newspaper (SAMNews) Using Artificial Immune System," presented at the World Congress on Engineering - WCE 2013, Vol III, 2013.

[7] N. A. S. Abdullah and N. I. A. Rusli, "Multilingual Sentiment Analysis: A Systematic Literature Review," PERTANIKAJOURNAL OF SCIENCE AND TECHNOLOGY, vol. 29, no. 1, pp. 445-470, JAN 2021, doi: 10.47836/pjst.29.1.25.

[8] A. Kumar and T. M. Sebastian, "Sentiment Analysis: A Perspective on its Past, Present and Future," International Journal of Intelligent Systems and Applications, vol. 4, no. 10, pp. 1-14, 2012, doi: 10.5815/ijisa.2012.10.01.

[9] M. Farhadloo and E. Rolland, "Fundamentals of Sentiment Analysis and Its Applications," in Sentiment Analysis and Ontology Engineering, vol. 639: Springer, Cham, 2016.

[10] N. N. Yusof, A. Mohamed, and S. Abdul-Rahman, "Reviewing Classification Approaches in Sentiment Analysis," in 1st International Conference on Soft Computing in Data Science (SCDS), Putrajaya, MALAYSIA, Sep 02-03 2015, vol. 545, in Communications in Computer and Information Science, 2015, pp. 43-53, doi: 10.1007/978-981-287-936-3\_5. [Online].

[11] A. Hasan, S. Moin, A. Karim, and S. Shamshirband, "Machine Learning-Based Sentiment Analysis for Twitter Accounts," Mathematical and Computational Application, vol. 23, no. 1, 2018, doi: https://doi.org/10.3390/mca23010011.

[12] S. Aphiwongsophon and P. Chongstitvatana, "Detecting Fake News with Machine Learning Method," in 2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON), 18-21 July 2018 2018, pp. 528-531, doi: 10.1109/ECTICon.2018.8620051.

[13] C. K. Hiramath and G. C. Deshpande, "Fake News Detection Using Deep Learning Techniques," in 2019 1st International Conference on Advances in Information Technology (ICAIT), 25-27 July 2019 2019, pp. 411-415, doi: 10.1109/ICAIT47043.2019.8987258.

[14] R. Wirth and J. Hipp, "CRISP-DM: Towards a standard process model for data mining," Proceedings of the 4th International Conference on the Practical Applications of Knowledge Discovery and Data Mining, 01/01 2000.

[15] S. B. bin Rodzman et al., "Experiment with Lexicon Based Techniques on Domain-Specific Malay Document Sentiment Analysis," presented at the 2019 IEEE 9TH Symposium on Computer Applications & Industrial Electronics (ISCAIE), 2019.

[16] M. Hu and B. Liu, "Mining opinion features in customer reviews," in AAAI'04: Proceedings of the 19th national conference on Artificial intelligence, San Jose California 25 - 29 July 2004: AAAI Press.

[17] C. Hutto and E. Gilbert, "VADER: A Parsimonious Rule-Based Model for Sentiment Analysis of Social Media Text," in Proceedings of the International AAAI Conference on Web and Social Media, 2014, vol. 8, no. 1, pp. 216-225.

[18] W. Wang and K. Siau, "Artificial intelligence, machine learning, automation, robotics, future of work and future of humanity: A review and research agenda," Journal of Database Management, vol. 30, no. 1, pp. 61-79, 2019, doi: 10.4018/JDM.2019010104.

# Performance Analysis of IoT-based Healthcare Heterogeneous Delay-sensitive Multi-Server Priority Queuing System

Barbara Kabwiga Asingwire<sup>1</sup>, Alexander Ngenzi<sup>2</sup>, Louis Sibomana<sup>3</sup>, Charles Kabiri<sup>4</sup>

African Centre of Excellence in Internet of Things, College of Science and Technology, University of Rwanda<sup>1</sup>

Department of Computer Engineering, Busitema University, Uganda<sup>1</sup>

African Centre of Excellence in Internet of Things, College of Science and Technology, University of Rwanda<sup>2,4</sup>

African Centre of Excellence in Internet of Things, College of Science and Technology<sup>3</sup>

University of Rwanda and National Council for Science and Technology, Rwanda<sup>3</sup>

**Abstract**—Previous studies have considered scheduling schemes for Internet of Things (IoT)-based healthcare systems like First Come First Served (FCFS), and Shortest Job First (SJF). However, these scheduling schemes have limitations that range from large requests starving short requests, process starvation that results in long time to complete if short processes are continuously added, and performing poorly under overloaded conditions. To address the mentioned challenges, this paper proposes an analytical model of a prioritized scheme that provides service differentiation in terms of delay sensitive packets receiving service before delay tolerant packets and also in terms of packet size with the short packets being serviced before large packets. The numerical results obtained from the derived models show that the prioritized scheme offers better performance than FCFS and SJF scheduling schemes for both short and large packets, except the shortest short packets that perform better under SJF than the prioritized scheme in terms of mean slowdown metric. It is also observed that the prioritized scheme performs better than FCFS and SJF for all considered large packets and the difference in performance is more pronounced for the shortest large packets. It is further observed that reduction in packet thresholds leads to decrease in mean slowdown and the decrease is more pronounced for the short packets with larger sizes and large packets with shorter sizes.

**Keywords**—Delay tolerant; delay sensitive; internet of things; mean slowdown; prioritized scheme

## I. INTRODUCTION

The recent advances in technologies have led to the emergence of Internet of Things (IoT) [1], [2] that interconnects everything around us, including sensors, devices and systems and also supports a range of applications. IoT has been applied in several domains including but not limited to remote health monitoring [3]. IoT-enabled remote health monitoring systems have huge advantages over traditional health monitoring systems and are likely to improve the future of healthcare monitoring and emergency management.

In remote health monitoring, the IoT-based physical monitoring devices need to transmit collected data in real time, with low latency and in a highly reliable way so as to ensure accurate monitoring of patients. This is because healthcare systems are highly time-sensitive and require minimal delay.

Specifically, it is required that medical emergencies are given precedence in reporting over other regular services [4]. Further to this, transmission services for medical signals should be classified based on the different signal requirements. Besides, low latency is important for healthcare environments such that in cases of emergencies timely notification allows the medical personnel responsible to respond accordingly [5],[6].

The traditional computing server scheduling schemes are not ripe enough to provide services to IoT based healthcare services due to the heterogeneity of IoT applications and traffic which require different levels of service guarantees [7].

Healthcare IoTs may tolerate delays ranging from milliseconds to microseconds [8], [9]. Increase in the data size leads to increase in delay for the healthcare IoT applications and for time-sensitive applications the delay may vary from milliseconds to minutes [8], [10], and this worsens the performance of real time healthcare IoTs [11], [12].

While, scheduling traffic in healthcare systems, the following issues need to be addressed [13]:

1) *Emergent medical situations* should be given precedence in reporting than those with regular importance. This is because excessive delays in the transmission of emergent medical situations may deteriorate health services to patients. To address this issue, this study prioritizes delay sensitive packets over delay tolerant packets.

2) *Transmission services* for non-emergent medical situations should be differentiated by their heterogeneous delay sensitivities with regards to different application purposes. Applying absolute priority rule can maintain the transmission priorities among different medical levels, but may lead to tremendously large waiting delays for “less important” packets and yet the “less important” medical packets are also critical components of patients’ health profiles. To address this issue, service differentiation is implemented, in this study, to differentiate the traffic based on the delay sensitivity of the traffic and also based on the size of each packet, with the short packets being serviced before large packets in order to improve on the number of requests served per unit time.

3) *Healthcare IoT* devices generate huge volumes of healthcare data which results in high data traffic that causes network congestion and high latency [18]. By servicing short packets before the large packets, the number of packets served will increase hence reducing the congestion.

Recent developments within the research community provide numerous scheduling schemes for IoT-based healthcare systems namely: First Come First Served (FCFS) [19], Shortest Job First (SJF) [24], [25], preemptive resume service priority [20]. Unfortunately, these schemes have limitations that range from large requests starving short requests [19], process starvation that results in a long time to complete if short processes are continuously added [24], to high priority requests starving lower priority requests [6].

To address the above limitations, this study formulates an analytical framework for the performance evaluation of IoT-based healthcare heterogeneous delay-sensitive multi-server priority queuing system based on the formulated packet transmission scheduling.

The contribution of this paper is two-fold. Firstly, the study developed models of mean slowdown for the prioritized scheduling scheme for IoT-based healthcare monitoring systems. Secondly, the performance of the proposed models is evaluated against the FCFS and SJF scheduling schemes. The rest of the paper is organized as follows: Section II is related work. The analytical models are presented in Section III, while Section IV presents the performance evaluation, discussions are presented in Section V, conclusion in Section VI and future work is presented in Section VII.

## II. RELATED WORK

First-Come-First-Served (FCFS) scheduling scheme applied in [19] is the simplest scheduling policy where requests are served according to their order of arrival. As a non-preemptive scheduling discipline, once a request has a server, it runs to completion. One of the major drawbacks of FCFS scheme is that the emergent healthcare packets are completely starved of service and this increases the average waiting time of emergent healthcare packets which may result into serious issues in healthcare including death.

Therefore, scheduling techniques that provide fairness to all competing packets is required in the allocation of resources to prevent starvation of some packets.

Preemptive resume service priority introduced in [20] is a scheduling scheme where incoming traffic are prioritized into normal and emergency traffic, where normal traffic has low priority and emergency traffic has high priority. This scheduling is based on preemptive priority mechanism where a higher priority traffic is serviced before a low priority traffic but each category of traffic is served in a FCFS order. A lower priority traffic is preempted on arrival of emergent traffic and the lower priority traffic could be dropped if the buffer is full so as not to cause data loss or delay of sensitive traffic. However, the weakness of preemptive resume service priority is that when high priority rate exhibits high arrival rate, the low priority traffic is starved. Hence, there is need to place a threshold on the amount of high priority traffic to be serviced

during high arrival rate of high priority traffic so as not to starve the low priority traffic.

A priority-aware truthful mechanism for scheduling delay constrained medical packet transmissions in IoT-based healthcare networks is proposed in [13]. The study considered multiclass health packets from the biosensors arriving randomly at each gateway and their delay-constrained transmission requests are immediately reported to the base station. The base station schedules the transmissions by including the priority and the delay constraints of medical packet transmissions. However, the limitation of this scheme is that; the absolute prioritized transmission used naturally results in a non-preemptive priority queueing, where under high arrival rates of higher priority medical packets, the lower priority medical packets are starved. In addition, the servers (channels) are taken to be homogeneous implying same characteristics, which in reality is not the case being that different channels have different characteristic and can be modeled as heterogeneous servers.

In [22], a dynamic scheduling of beyond-WBAN medical packet transmissions is modeled by  $M/G/K$  queues with a Poisson packet arrival, generally distributed service (transmission) time and priority disciplines. The system consists of a gateway, a number of heterogeneous biosensors worn on different parts of the human body and the Base Station (BS). The BS serves the packets in a priority order with emergent medical packets being given a higher priority over those with regular importance. In scheduling, some channels are completely reserved for emergent medical packets and the balance of the channels are reserved for non-emergent channels. However, when channels are completely partitioned for each packet class, the use of the un-utilized channels of one class of packets cannot be used by other classes of users and therefore the capacity is wasted.

T. Aladwani [23] proposed to use fog computing between sensors and cloud computing to reduce the amount of data that is transported between the cloud and the sensors. In addition, the authors improved task scheduling algorithm by making the main factor in giving priority to tasks their importance regardless of their length. The authors proposed a new method of scheduling called Tasks Classification and Virtual Machines Categorization (TCVC) based on tasks importance. Tasks that are received by IoT are classified based on their importance into three classes: high importance, medium importance, and low importance tasks based on the patient's health status. In scheduling, critical tasks take high importance, important tasks take medium importance, and general tasks take low importance. The limitation of this scheme is matching the virtual machine's capability to the important of tasks, and also under high arrival rate of higher priority tasks, the lower priority tasks are starved of service.

SJF scheduling policy has been used in scheduling tasks in healthcare systems, for example, an innovative IoT based remote healthcare monitoring system by using Free RTOS with priority scheduling based on SJF is proposed in [24]. The proposed system provides vital health information and live video of a patient who is located in a rural area. A framework that utilizes the 5G network's low-latency, high bandwidth

functionality to detect COVID-19 using chest X-ray or CT scan images, and to develop a mass surveillance system to monitor social distancing, mask wearing, and body temperature using the SJF policy is proposed in [25]. The weakness of the SJF scheduling algorithm is that it gives priority to tasks based only on their length. This leads to unfairness, as the large tasks must be waiting in the tasks list until the smallest tasks finish execution even if it is important.

In summary, the limitations of the existing studies include; lack of a fair scheduling scheme that prioritizes traffic in the system without penalizing other classes of traffic, lack of scheme that caters for the dynamic changes in the periods, starvation of emergent healthcare packets, and lack of optimized frameworks and algorithms in allocation of system resources.

In contrast to the existing work reported in the literature, this study proposes an analytical model that will aid in studying and analyzing performance of healthcare monitoring systems considering different packet sizes and packet thresholds.

### III. SYSTEM MODEL

The healthcare monitoring system consists of heterogeneous healthcare monitoring data packets from different independent sensors mounted on the body to monitor different health situations. In the considered system model as shown in Fig. 1, the heterogeneous data packets generated by the different sensors arrive randomly to the network gateway following a Poisson process, the Poisson distribution has been found to approximate well the arrival patterns of healthcare data packets [26], [27].

Fig. 1 shows the queue system model with healthcare data packets generated from different sensor nodes mounted on the body.

The gateway is required to immediately declare a transmission packet along with the corresponding packet priority based on the time sensitivity of the packets, this is done at classifier 1, where requests are classified into delay sensitive and delay tolerant based on their delay requirements, for example EEG/ECG/EMG has delay requirement of less than 250ms, Glucose monitoring less than 20ms, Blood pressure less than 750ms, Endoscope imaging less than 500ms [13]. Examples of delay tolerant traffic include access to a patient’s Electronic Health Records; home tele-monitoring, medication dispenser data, etc. [14].

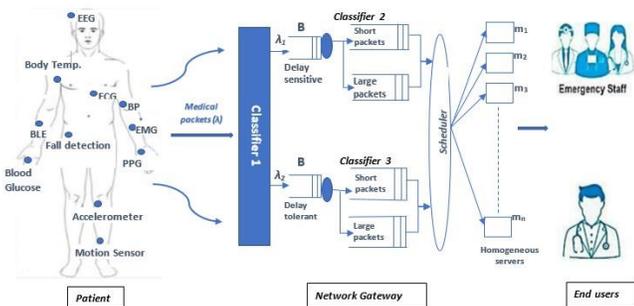


Fig. 1. Queue System Model.

A major requirement in scheduling transmissions of multiclass healthcare packets with different criticality is the priority awareness [28]. For each queue of the delay sensitive or delay tolerant classes, packets are queued in the buffers assumed to be infinite. For each of the delay sensitive and delay tolerant classes, the data packets are further classified as short or large based a threshold. Short packets are chosen for the next execution before the large packets, the idea being to reduce the average waiting time for other packets awaiting execution. After classifying the packets by their sizes, the packets are forwarded to the scheduler which allocates the packets to the different servers. This scheduling scheme considers shared servers for each priority class. Considering the diversities in terms of packet sizes, the transmission time of healthcare packets can be represented by a generic random variable, that is, follows the general service distribution [13]. In particular, the service rate of packets will follow the exponential distribution [21]. The probability density function of an exponential distribution is given as [13]:

$$f(x) = \mu e^{-\mu x}, x \geq 0, \mu \geq 0 \tag{1}$$

where  $\mu$  is the service rate and  $x$  is the size of the packet. The proposed policy is a delay sensitive non-preemptive size-based scheduling policy where packets are classified as delay sensitive or delay tolerant at the first priority level and also on their sizes, namely  $(x_s)$  and large  $(x_l)$ . For each delay sensitive or delay tolerant classes, short packets are served before large packets. Within each class, packets are served in a FCFS order using multiple servers. The system model can be represented as a multi-server queue. For each queue of the delay sensitive or delay tolerant classes, packets are queued in the buffers assumed to be infinite. The queue model can be formulated under the following assumptions:

The arrival rate follows the Poisson process with parameter  $\lambda_i, i = 1, 2$ , where  $\lambda_1$  is the arrival rate of delay sensitive packets and  $\lambda_2$  is the arrival rate of delay tolerant packets.

The service times of each server is independent and identically distributed exponential random variable with

parameter  $\mu_i, i = 1, 2$ , where  $\mu_1$  is the service rate of delay sensitive packets and  $\mu_2$  is the service rate of delay tolerant packets.

There are  $m$  servers through which the service is provided.

The capacity of each server is finite,  $N$ .

The above system can be represented as an  $M/M/m/N$  queue system, where the first  $M$  represents random arrivals of packets following the Poisson process, the second  $M$  represents exponentially distributed service time, with  $m$  servers each of finite capacity  $N$ .

#### A. Mathematical Background

Denote the probability density function of a packet of size  $x$  as  $f(x)$  defined in equation 1. The cumulative distribution function is then given as:  $F(x) = \int_0^x f(t)dx$ .

Using a naive definition of packet size based on threshold  $x_t$  which may be dynamic, all packets that have sizes less than or equal to  $x_t$  are said to be short, whereas packets that are larger than  $x_t$  are said to be large.

The load due to packets with sizes less than or equal to  $x_t$  is given as  $\rho_{x_t} = \lambda \int_0^{x_t} tf(t)dt = \frac{\lambda}{\mu}(1 - e^{-\mu x_t}) - x_t e^{-\mu x_t}$  [15], where  $\mu$  is the service rate of packets, while the load due to packets with sizes greater than  $x_t$  is given as.

$$\rho_{x_l} = \lambda \int_{x_t}^{\infty} tf(t)dt = \lambda e^{-\mu x_t} \left( x_t + \frac{1}{\mu} \right)$$

The steady state equations of the  $M/M/m/N$  queue model are derived as follows:

The probability that there are packets in the system is given as [17]:

$$P_n = \begin{cases} \frac{\rho^n}{n!} P_0, & 1 \leq n \leq m \\ \frac{\rho^n}{m!} \left( \frac{\rho}{m} \right)^{n-m} P_0, & m < n \leq N-1 \end{cases} \quad (2)$$

where  $P_0$  is the probability that the system is empty and is given by;

$$P_0 = \left[ \sum_{n=0}^m \frac{\rho^n}{n!} + \sum_{n=m+1}^N \frac{\rho^n}{m!} \left( \frac{\rho}{m} \right)^{n-m} \right]^{-1} \quad (3)$$

The expected waiting time in the queue can be deduced as

$$W_q = \frac{1}{\lambda} \sum_{n=m}^N (n-m) P_n \quad (4)$$

Hence,

$$W_q = \sum_{n=m}^N (n-m) \frac{\rho^n}{\lambda m!} \left( \frac{\rho}{m} \right)^{n-m} P_0 \quad (5)$$

We next define the expressions for the mean response time under FCFS and SJF, which will be used to compare with the prioritized scheduling scheme. An arriving packet to the FCFS queue has to wait for all packets it finds in the queue upon arrival. The mean response time of a packet of size  $x_s$  in an  $M/G/m/FCFS$  system is given as [15].

$$T^{FCFS}(x_s) = x_s + W^{FCFS}(x_s) \quad (6)$$

where  $W^{FCFS}(x_s) = \frac{\overline{\lambda x_s^2}}{2(1-\rho_{x_s})}$  and  $\rho_{x_s} = \frac{\lambda}{m\mu}$

Under SJF, the shortest packet in the queue is given priority. Therefore, at every instant, the next packet to be serviced is the smallest one in the queue. A packet of size  $x_s$  is then delayed by packets in the system that is less or equal than its size. The mean response time of the packet of size  $x_s$  under SJF is given as [15].

$$T^{SJF}(x_s) = x_s + W^{SJF}(x_s) \quad (7)$$

where  $W^{SJF}(x_s) = \frac{\overline{\lambda x_s^2}}{2(1-\rho_{x_s})^2}$  and  $\rho_{x_s} = \frac{\lambda}{m\mu}$ ,  $m$  being the number of servers.

### B. Model for Delay Sensitive Packets

Consider a tagged packet arriving to a delay sensitive queue, two scenarios arise, the first scenario is when the tagged

packet finds in the queue short delay sensitive packets being serviced, including at least one delay sensitive large packet, the second scenario includes the tagged packet arriving to a delay sensitive queue with only short packets. We consider scenario one where at least one delay sensitive large packet is found in service.

Assuming the tagged delay sensitive short packet, its service will be delayed by all delay sensitive short packets it finds in the queue and the remaining service of the large packets it finds in the servers when it arrived. The mean response time for the delay sensitive short packet of size  $x_s$  is given as [15]:

$$T(x_{ts}) = x_{ts} + W(x_{ts}) + W_r(x_{ts}) \quad (8)$$

where

$$W(x_{ts}) = \sum_{n=m}^N (n-m) \frac{\rho_{x_{ts}}^n}{\lambda_1 n!} \left( \frac{\rho_{x_{ts}}}{m} \right)^{n-m} P_0^{x_{ts}} \quad (9)$$

and

$$P_0^{x_{ts}} = \left[ \sum_{n=0}^m \frac{\rho_{x_{ts}}^n}{n!} + \sum_{n=m+1}^N \frac{\rho_{x_{ts}}^n}{m!} \left( \frac{\rho_{x_{ts}}}{m} \right)^{n-m} \right]^{-1} \quad (10)$$

$$\rho_{x_{ts}} = \lambda_1 \int_0^{x_{ts}} tf(t)dt$$

$$W_r(x_{ts}) = \sum_{n=m}^N (n-m) \frac{\rho_{x_{ts}}^n}{\lambda_1 n!} P_0^{x_{ts}} \quad (11)$$

Where

$$P_0^{x_{ts}} = \left[ \sum_{n=0}^m \frac{\rho_{x_{ts}}^n}{n!} + \sum_{n=m+1}^N \frac{\rho_{x_{ts}}^n}{m!} \left( \frac{\rho_{x_{ts}}}{m} \right)^{n-m} \right]^{-1} \quad (12)$$

$$\text{and } \rho_{x_{ts}} = \lambda_1 \int_{x_{ts}}^{\infty} tf(t)dt$$

On the other hand, the delay sensitive large packet is delayed by all delay sensitive short packets found in the queue plus all delay sensitive large packets found in the queue, and the mean service time of the large packets the tagged large packet finds in the servers when it arrived. In addition, all delay sensitive short packets that arrive after the tagged large packet is in the queue will be served before the tagged large packet. The mean response time for the delay sensitive large packet of size  $x_l$  is given as:

$$T(x_{ls}) = x_{ls} + 2W(x_{ts}) + W(x_{ls}) + W_r(x_{ls}) \quad (13)$$

The term  $2W(x_{ts})$  is the contribution from delay sensitive short packets found in the queue and the delay due to the delay sensitive short packets that arrive after the tagged large packet is in the queue,  $W(x_{ts})$  and  $W_r(x_{ls})$  are as given in equations 9 and 11 respectively and.

$$W(x_{ls}) = \sum_{n=m}^N (n-m) \frac{\rho_{x_{ls}}^n}{\lambda_1 n!} \left( \frac{\rho_{x_{ls}}}{m} \right)^{n-m} P_0^{x_{ls}} \quad (14)$$

where,

$$P_0^{x_{ls}} = \left[ \sum_{n=0}^m \frac{\rho_{x_{ls}}^n}{n!} + \sum_{n=m+1}^N \frac{\rho_{x_{ls}}^n}{m!} \left( \frac{\rho_{x_{ls}}}{m} \right)^{n-m} \right]^{-1} \quad (15)$$

### C. Model for Delay Tolerant Packets

Consider a tagged packet arriving to a delay tolerant queue. In case the tagged packet is a short delay tolerant packet its service will be delayed by all delay sensitive short packets, all delay sensitive large packets and all delay tolerant short packets found in the queue. In addition, the short delay tolerant packet will be delayed by all delay sensitive short and large packets that arrive after the tagged delay sensitive short packet is in the queue will be served before the tagged delay tolerant short packet is serviced. The mean response time for the delay tolerant short packet of size  $x_{sd}$  is given as:

$$T(x_{sd}) = x_{sd} + 2W(x_{ts}) + 2W(x_{ls}) + W(x_{td}) \quad (16)$$

where,

$$W(x_{td}) = \sum_{n=m}^N (n-m) \frac{\rho_{x_{td}}^n}{\lambda_2 n!} \left(\frac{\rho_{x_{td}}}{m}\right)^{n-m} P_o^{x_{td}} \quad (17)$$

and

$$P_o^{x_{td}} = \left[ \sum_{n=0}^m \frac{\rho_{x_{td}}^n}{n!} + \sum_{n=m+1}^N \frac{\rho_{x_{td}}^n}{m!} \left(\frac{\rho_{x_{td}}}{m}\right)^{n-m} \right]^{-1} \quad (18)$$

$$\rho_{x_{td}} = \lambda_2 \int_0^{x_{td}} tf(t) dt$$

The term  $2W(x_{ts})$  is as explained for equation 13.

For the case of the tagged large delay tolerant packet its service will be delayed by all delay sensitive short packets, all delay sensitive large packets, all delay tolerant short packets and all delay tolerant large packets found in the queue. In addition, the tagged large delay tolerant packet will be delayed by short and large delay sensitive packets that arrive after the tagged delay tolerant large packet is in the queue will be served before the tagged delay tolerant large packet. The mean response time for the delay tolerant large packet of size  $x_{ld}$  is given as:

$$T(x_{ld}) = x_{ld} + 2W(x_{ts}) + 2W(x_{ls}) + W(x_{ld}) \quad (19)$$

where

$$W(x_{ld}) = \sum_{n=m}^N (n-m) \frac{\rho_{x_{ld}}^n}{\lambda_2 n!} \left(\frac{\rho_{x_{ld}}}{m}\right)^{n-m} P_o^{x_{ld}} \quad (20)$$

and

$$P_o^{x_{ld}} = \left[ \sum_{n=0}^m \frac{\rho_{x_{ld}}^n}{n!} + \sum_{n=m+1}^N \frac{\rho_{x_{ld}}^n}{m!} \left(\frac{\rho_{x_{ld}}}{m}\right)^{n-m} \right]^{-1} \quad (21)$$

$$\text{and } \rho_{x_{ld}} = \lambda_2 \int_{x_{td}}^{\infty} tf(t) dt$$

The term  $2W(x_{ts})$  is the contribution from delay sensitive short packets found in the queue and the delay due to the delay sensitive short packets that arrive after the tagged large packet is in the queue,  $2W(x_{ls})$  is the contribution from delay sensitive large packets and delay sensitive large packets that arrive after the tagged delay tolerant large packet is in the queue.

In the next section, we present the performance evaluation of the derived models in terms of mean slowdown.

## IV. PERFORMANCE EVALUATION

In order to evaluate the performance of the proposed IoT-based healthcare monitoring system, the derived models are used to plot graphs using MATLAB and in particular Simulink package was used [16]. Simulink provides a graphical editor, customizable block libraries, and solvers for modeling and simulating dynamic systems. It is integrated with MATLAB, enabling one to incorporate MATLAB algorithms into models and exporting simulation results to MATLAB for further analysis.

The performance of the proposed system is evaluated using mean slowdown as the performance metrics. Mean slowdown is the normalized response time, i.e., the ratio of the response time of a packet to the size of that packet. Unlike mean response time which tends to be representative of the performance of just a few big packets since they count the most in the mean because their response times tend to be highest [32], slowdown is a useful metric to analyze fairness of a scheduling scheme.

The paper investigates how the prioritized scheduling (PS) scheme performs compared to the FCFS and SJF scheduling schemes for short and large packets. The effect of key parameters such as packet sizes on mean slowdown is investigated.

### A. Model Parameters

Table I shows the hypothetical parameters used in the analysis which is consistent with parameters used in literature [29], [30]. The packet arrival rate and service rate follow Poisson distribution [15].

TABLE I. IMPLEMENTATION PARAMETERS

Parameter	Value
Number of servers, $m$	10 [29]
The maximum number of health data packets in the queue $N$	150 [30]
Packets arrival rate $\lambda$	6.549 packets/second [31]
Packets service rate $\mu$	8.8 packets/second [31]
The average packet size $x_r$	100 Kb [13]
Threshold size of the packet size $x_{ts}$	75 Kb [13]

### B. Evaluation of the mean Slowdown with Packet Sizes for Delay Sensitive Packets

This section presents the performance of the packets in terms of mean slowdown while varying packet sizes for delay sensitive packets.

Fig. 2 shows the mean slowdown of delay sensitive short packets under FCFS, SJF, and PS schemes where short packets are packets with sizes less or equal to  $x_s = 75Kb$ . It is also observed that some shorter packets experience lower mean slowdown under SJF than under the PS scheme. The situation is however very different as the sizes of packets increase, the PS scheme performs better than FCFS and SJF by offering lower mean slowdown. It is shown that the difference in performance between the PS scheme and SJF and FCFS is more pronounced as the packet sizes increase for short packets. It can be observed that in all cases, the FCFS scheme performs

worse than SJF and PS scheme for all packet sizes for short packets. We can also see from Fig. 2 that the PS scheme performs much more closely with FCFS and SJF for small packet sizes for short packets.

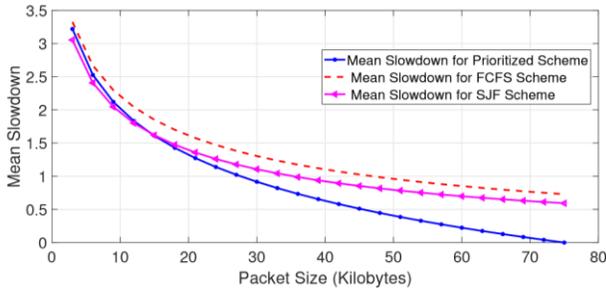


Fig. 2. Mean Slowdown for Delay Sensitive Short Packets under PS, SJF and FCFS Schemes.

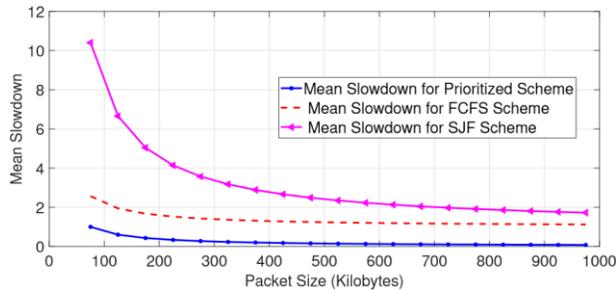


Fig. 3. Mean Slowdown for Delay Sensitive Large Packets under PS, SJF and FCFS Schemes.

Fig. 3 shows the mean slowdown of delay sensitive large packets under FCFS, SJF, and PS schemes where large packets are packets with sizes greater than  $x_s = 75$  bytes. It can be observed from the figure that the PS scheme performs better than FCFS and SJF scheduling policies regardless of the packet size for large packets. In turn, FCFS also performs better than the SJF scheme for all large packet sizes considered. This is because under FCFS, there is a mix of short and large packets resulting into lower mean slowdown, whereas under SJF, large packets are serviced last and will always experience higher mean slowdown. The difference in performance is much more pronounced for shorter packet sizes, however as the packet sizes increase, the performance becomes closer as the mean slowdown values are closer.

### C. Evaluation of the Mean Slowdown with Packet Sizes for Delay Tolerant Packets

This section presents the performance of the packets in terms of mean slowdown for the PS scheme in comparison with the FCFS and SJF scheduling schemes for delay tolerant packets.

Fig. 4 shows results of PS scheme in comparison with FCFS and SJF scheduling schemes for delay tolerant short packets. It can be seen that the SJF scheme performs better than the PS scheme for shorter packet sizes, this is because delay tolerant short packets are delayed by delay sensitive large packets which is not the case under SJF where there are only short packets, however as the packet sizes increase, the PS scheme performs better than SJF by offering lower mean slowdown. Similar to Fig. 2, it can be observed that in all

cases, the FCFS scheme performs worse than SJF and PS scheme for all packet sizes for short packets. It is observed that the difference in performance between the PS scheme, SJF and FCFS is more pronounced as the packet sizes increase for short packets. In general, the PS scheme performs better than SJF and FCFS as the packet sizes increase for short packets.

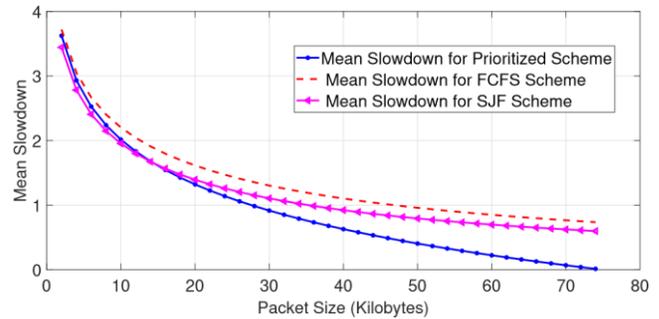


Fig. 4. Mean Slowdown for Delay Tolerant Short Packets under Prioritized, SJF and FCFS Schemes.

Fig. 5 shows results of PS scheme in comparison with FCFS and SJF scheduling schemes for delay tolerant large packets. It is observed that for the considered packet sizes, the PS scheme performs better than FCFS and SJF schemes by offering lower mean slowdown; the FCFS in turn is observed to offer lower mean slowdown than SJF scheme. It is further observed that the difference in mean slowdown is higher for shorter packet sizes and closer when the packet sizes increase. The performance between PS, FCFS and SJF schemes differ specifically for shorter packets where SJF performs worse than FCFS which in turn performs worse than the PS scheme.

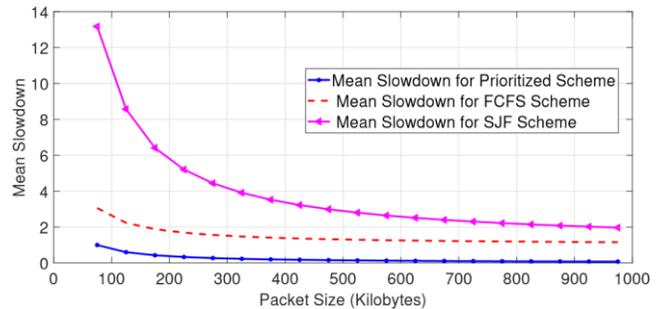


Fig. 5. Mean Slowdown for Delay Tolerant Large Packets under Prioritized, SJF and FCFS Schemes.

### D. Evaluation of the Effect of Packet Threshold on Mean Slowdown for the PS Scheme for Delay Sensitive Packets

This section presents the performance of the packets in terms of mean slowdown for the PS scheduling scheme for different thresholds for delay sensitive packets. In doing this, the effect of the variation of the packet threshold in terms of size is investigated.

The results of the effect of varying the packet threshold on the mean slowdown for delay sensitive short packets are shown in Fig. 6. It can be observed that the decrease in the packet threshold leads to a reduction in the mean slowdown of delay sensitive short packets. The reduction in mean slowdown is observed to be more pronounced as the packet sizes increase, however for smaller packet sizes, the packet threshold has very

little effect. When the packet thresholds are reduced, it means the number of shorter packets are reduced hence the reduction in the mean slowdown.

Fig. 7 shows the variation of mean slowdown for delay sensitive large packets under the PS scheme for different packet thresholds. It can be observed that the decrease in the packet threshold reduces the mean slowdown of delay sensitive large packets. The reduction in mean slowdown is observed to be more pronounced for large packets with smaller sizes, however as the sizes of the delay sensitive packets increase, the packet threshold has very little effect. When the packet thresholds are reduced, the large packets with shorter sizes experience a more reduced mean slowdown due to the reason presented in Fig. 6.

#### E. Evaluation of the Effect of Packet Threshold on Mean Slowdown for the PS Scheme for Delay Tolerant Packets

This section presents the performance of the packets in terms of mean slowdown for PS scheduling scheme for different packet thresholds for delay tolerant packets as shown in Fig. 8 and 9.

Fig. 8 shows the variation of mean slowdown for delay tolerant short packets under the PS scheme for different packet thresholds. It can be observed that when the packet thresholds are reduced, the mean slowdown of delay tolerant short packets is reduced. The reduction in mean slowdown is observed to be more pronounced as the packet sizes increase, however for smaller packet sizes, the packet threshold has minimal effect and this is similar to the observation noted for delay sensitive short packets in Fig. 6. When the packet thresholds are reduced, the number of shorter packets is reduced hence the reduction in the mean slowdown.

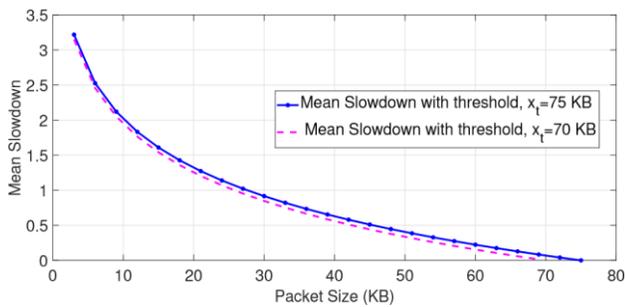


Fig. 6. Mean Slowdown for Delay Sensitive Short Packets under Prioritized Scheme for different Thresholds.

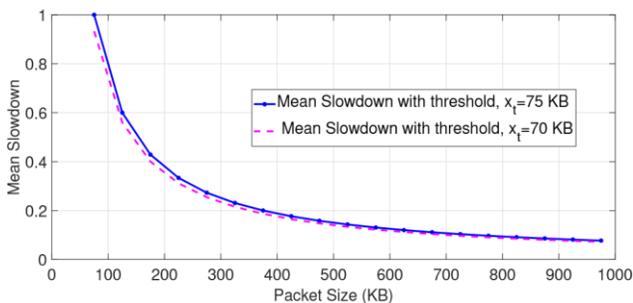


Fig. 7. Mean Slowdown for Delay Sensitive Large Packets under PS Scheme for different Thresholds.

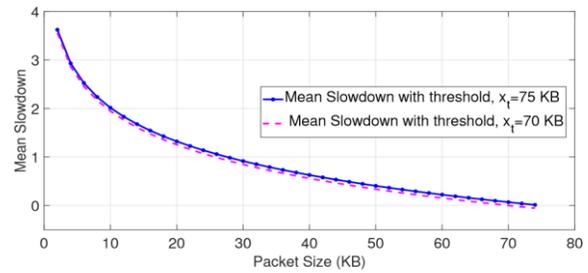


Fig. 8. Mean Slowdown for Delay Tolerant Short Packets under PS Scheme for different Thresholds.

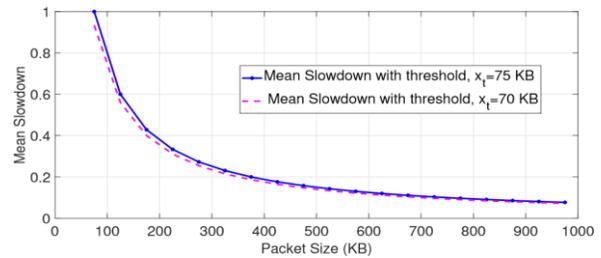


Fig. 9. Mean Slowdown for Delay Tolerant Large Packets under PS Scheme for different Thresholds.

Fig. 9 shows the variation of mean slowdown for delay tolerant large packets under the PS scheme for different packet thresholds. It can be observed that the decrease in the packet threshold reduces the mean slowdown of delay tolerant large packets. The reduction in mean slowdown is noted to be more pronounced for large packets with smaller sizes, however as the sizes of the delay tolerant packets increase, and the packet threshold has minimal effect on the mean slowdown. When the packet thresholds are reduced, the large packets with shorter sizes experience a more reduced mean slowdown due to increased number of large packets with shorter packet sizes.

## V. DISCUSSION

This study developed analytical models of mean slowdown for the PS scheme where incoming packets are prioritized based on the delay requirement and size of the packets and serviced using multiple servers. The effect of varying packet sizes on the mean slowdown under the PS is investigated in comparison with the FCFS and SJF scheduling policies. Results from the derived models show that the largest short packets perform better under the PS scheme than under the SJF and FCFS schemes. Similar observation has been noted by SWAP policy which also favors short packets to the expense of delaying large ones within the queue [15]. On the other hand, all large packets perform better under the PS scheme compared to the FCFS and SJF schemes. By giving priority to short packets under the PS scheme, more packets are served and hence large packets do not have to wait for so long for service. Large packets perform worse under FCFS scheme because their services are interrupted by large packets whose sizes may be larger. Similar explanations hold for the SJF scheme where large packets remain in the queue for a long time and may even lead to starvation.

## VI. CONCLUSION

The PS scheduling scheme has been modeled and evaluated for varying packet sizes and thresholds. The numerical results

obtained from the derived models show the PS scheme generally reduces the mean slow down for most of the packet sizes considered. The comparison of the PS scheme with FCFS and SJF show that the PS scheme is superior in reducing the mean slowdown except for the few shortest short packets under SJF. The performance difference is more pronounced for the large packets with shorter sizes. It is also observed that short packets which are much shorter perform better under SJF than under the Prioritized scheme, however as the packet sizes increase, the PS scheme offers better performance than FCFS and SJF. It is further observed that when the packet threshold is reduced, the mean slowdown packets are reduced and the reduction is more pronounced for the short packets with larger sizes and large packets with shorter sizes.

## VII. FUTURE WORK

In this paper, numerical results for the PS scheduling scheme using multiple homogeneous servers are presented. In the future, it will be interesting to investigate the effect of using heterogeneous servers on the performance, and also the effect of varying arrival and service rates.

### REFERENCES

- [1] Ala, M. Guizani, M. Mohammad and M. Aledhari, "Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications," *IEEE Communications Surveys & Tutorials*, vol. 17, no. 4, pp. 2347-2376, 2015.
- [2] H. Zhang, J. Li, B. Wen, Y. Xun and J. Liu, "Connecting intelligent," *IEEE Internet of Things*, vol. 5, no. 4, p. 1550-1560, June 2018.
- [3] H. Bhatia, S. N. Panda and D. Nagpa, "Internet of Things and its Applications in Healthcare-A Survey," in 8th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions), Noida, India, 2020.
- [4] C. Yi and Jun Cai, "Transmission Management of Delay-Sensitive Medical Packets in Beyond Wireless Body Area Networks: A Queueing Game Approach," *IEEE Transactions on Mobile Computing*, vol. 17, no. 9, pp. 2209 - 2222, 15 January 2018.
- [5] E. Gomes, M.A.R. Dantas and P. Plentz, "A Real-Time Fog Computing Approach for Healthcare Environment," Springer, pp. 85-95, 2019.
- [6] C. Yi and J. Cai, "A priority-aware truthful mechanism for supporting multi-class delay-sensitive medical packet transmissions in e-health networks," *IEEE Trans. Mobile Computing*, vol. 16, no. 9, pp. 2422-2435, September 2017.
- [7] N. Nasser, L. Karim and T. Taleb, "Dynamic multilevel priority packet scheduling scheme for wireless sensor network," *IEEE Transaction on Wireless Communication*, vol. 12, no. 4, p. 1448-1459, 2013.
- [8] A. M. Rahmani, T. N. Gia, B. Negash, A. Anzanpour, I. Azimi, M. Jiang and P. Liljeberg, "Exploiting smart e-Health gateways at the edge of healthcare Internet-of-Things: A fog computing approach," *Future Generation Computer Systems*, vol. 78, no. 2, pp. 641-658, 2018.
- [9] S.C. Hung, D. Liau, S-Y. Lien and K-C. Chen, "Low latency communication for Internet of Things," in *IEEE/CIC International Conference on Communications in China*, 2015.
- [10] T.N Gia, M. Jiang, A-M Rahmani and T. Westerlund, "Fog computing in healthcare internet of things: A case study on ecg feature extraction," in *IEEE International Conference on Computer and Information Technology*, 2015.
- [11] G. Lee, W. Saad W and M. Bennis, "An Online Optimization Framework for Distributed Fog Network Formation With Minimal Latency," *IEEE Transactions on Wireless Communications*, vol. 18, no. 4, pp. 2244-2258, 2019.
- [12] H. Gupta, D. A. Vahid Dastjerdi, S.K. Ghosh and R. Buyya, "iFogSim: A toolkit for modeling and simulation of resource management techniques in the Internet of Things, Edge and Fog computing environments," *Journal of Software: Practice and Experience*, vol. 47, no. 9, pp. 1275-1296, 2017.
- [13] Y. Changyan and J. Cai, "A Truthful Mechanism for Scheduling Delay-Constrained Wireless Transmissions in IoT-Based Healthcare Networks," *IEEE Transactions on Wireless Communications*, vol. 18, no. 2, pp. 912 - 925, December 2018.
- [14] K. Park, J. Park and J. Lee, "An IoT System for Remote Monitoring of Patients at Home", *Journal of Applied Sciences*, March 2017.
- [15] I. A. Rai and M. Okopa, "Modeling and evaluation of swap scheduling policy under varying job size distributions", *The Tenth International Conference on Networks, IARIA*, pp. 115-120, 2011.
- [16] D. K. Chaturvedi, "Modeling and Simulation of Systems Using Matlab and Simulink," CRC Press, 2010.
- [17] P. J. Smith, A. Firag, P. A. Dmochowski, and Mansoor Shafi, "Analysis of the M/M/N/N Queue with Two Types of Arrival Process: Applications to Future Mobile Radio Systems", *Journal of Applied Mathematics*, 2012.
- [18] S. Shukil, M. F. F. Hassan, M. K. Khan, L. T. Jung and A. Awang, "An analytical model to minimize the latency in healthcare internet-of-things in fog computing environment," *PLoS ONE*, vol. 14, no. 11, pp. 1-31, 2019.
- [19] S. El Kadhali and K. Salah, "Performance Modeling and Analysis of IoT-enabled Healthcare Monitoring Systems," *The Institute of Engineering and Technology (IET) Journals*, pp. 1-12, 18 September 2018.
- [20] I. Awan, M. Younas and W. Naveed, "Modelling QoS in IoT Applications," in *International Conference on Network-Based Information Systems*, 2014.
- [21] C. Yi and J. Cai, "A Truthful Mechanism for Scheduling Delay-Constrained Wireless Transmissions in IoT-Based Healthcare Networks," *IEEE*, pp. 1-14, 2018.
- [22] Y. Changyan and J. Cai, "Transmission Management of Delay-Sensitive Medical Packets in Beyond Wireless Body Area Networks: A Queueing Game Approach," *IEEE Transactions on Mobile Computing*, vol. 17, no. 9, pp. 2209 - 2222, January 2018.
- [23] T. Aladwani, "Scheduling IoT Healthcare Tasks in Fog Computing Based on Their Importance," *Procedia Computer Science*, vol. 163, pp. 560-569, 2019.
- [24] M. A. Deepika, N. K. Sudhama, "Internet Connected e-Healthcare System with Live Video Monitoring using LWIP Stack and SJF Priority Scheduling," *International Journal of Recent Technology and Engineering*, vol. 8, 2019.
- [25] M. Shamim Hossain; Ghulam Muhammad; Nadra Guizani, "Explainable AI and Mass Surveillance System-Based Healthcare Framework to Combat COVID-19 Like Pandemics," *IEEE Network*, vol. 34, no. 4, July/August, 2020.
- [26] D. Niyato, E. Hossain and S. Camorlinga, "Remote patient monitoring service using heterogeneous wireless access networks: architecture and optimization," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, pp. 412-423, 2009.
- [27] H. Su and X. Zhang, "Battery-dynamics driven TDMA MAC protocols for wireless body-area monitoring networks in healthcare applications," *IEEE Journal on Selected Areas in Communications*, vol. 27, no. 4, p. 424-434, 2009.
- [28] S. Rashwand and J. Mistic, "Two-tier WBAN/WLAN Healthcare Networks: Priority Considerations," in *IEEE/GLOBECOM*, 2012.
- [29] K. Salah and S. El Kadhali, "Performance Modeling and Analysis of IoT-enabled Healthcare Monitoring Systems,"
- [30] K. Salah and S. El Kadhali, "Performance Modeling and Analysis of Hypoexponential Network Servers", *Journal of Telecommunications System*, vol. 65, no. 4, pp. 717-728, 2017.
- [31] C. Majumdar, M. Lopez-Benitez, and S.N. Merchant, "Experimental Evaluation of the Poisson Process of Real Sensor Data Traffic in the Internet of Things," in *Proc. 6th IEEE Annual Consumer Communications & Networking Conference*, Jan. 2019, pp. 1-7.
- [32] M. Okopa, D. Turatsinze, T. Bulega and J. Wampande, "Revenue Maximization Based on Slowdown in Cloud Computing Environments" *Australasian Journal of Computer Science*, vol 4, pp. 1-16, 2017.

# A Survey on Sentiment Analysis Approaches in e-Commerce

Thilageswari a/p Sinnasamy, Nilam Nur Amir Sjaif  
Razak Faculty of Technology and Informatics  
Universiti Teknologi Malaysia  
Kuala Lumpur, Malaysia

**Abstract**—Sentiment analysis represents the process of judging customers' behavior expression and feeling as either positive, negative or neutral. Hence, a tangle of different approaches for sentiment analysis is being used, reflecting analysis of unstructured customers' reviews dataset to guide and generate insightful and helpful information. The aim of this paper is to highlight research design of sentiment analysis and choice of methodological by other researchers in E-Commerce customers' reviews to guide future development. This paper presents a study of sentiment analysis approaches, process challenges and trends to give researchers a review and survey in existing literature. Next, this study will discuss on feature extraction and classification method of sentiment analysis of customers' reviews to have an exhaustive view of their methods. The knowledge on challenges of sentiment analysis underpins to clarify future directions.

**Keywords**—Sentiment analysis; e-Commerce; feature extraction; classification; customers' reviews

## I. INTRODUCTION

Since COVID-19 is a pandemic globally and causing companies to not be able to operate normally due to locked-down with business operators to doing e-Commerce to survive [1]. e-Commerce is a safe way for consumers who make purchases for essentials and non-essentials goods and services online while staying home during the lock-down phase. E-Commerce is made possible via different online platforms. Online platform is known as e-commerce or Electronic commerce which is online transaction business used in buying and selling products through internet [2] [3]. Examples of e-Commerce are Shopee, Lazada, Zalora and eBay. These are world famous platforms selling goods, necessary products or services over the internet. However, people are doubtful of buying products from online platforms [4]. According to USA survey, there are 81% internet users who are buying products from online platform [5]. These customers express their feedback on their purchased items or services by writing reviews online at the comments section. Hence, reading other customers' feedback, comments or reviews is important to understand more about the products or services. Customers' reviews also known as Word of mouth (WOM) [3] [6] help other customers or clients to understand about the products, services and retailers. The more convincing the reviews are, the more confident the potential customers or clients will feel toward the products or services and be convinced to select and purchase them. Though customers' reviews are vital to effective customers' decision to make the right choices, the

increasing number of reviews will require a potential customer to spend more time and effort to go through each review thus affecting the decision making process to be quite tedious as the potential customer has to read each review and analyze the product or service involved before making the final decision [1] [2]. Thus, to assist customers to improve making purchase decisions, many reviews analysis methods are employed to extract useful information for customers. Sentiment analysis helps to identify and analyze customers' or clients' sentiments in their text reviews to extract and present specific information necessary to make better purchase decisions on products or services in E-Commerce. This paper contributes survey analysis results by other researchers on sentiment analysis methods future development.

The paper is organized as follows: after this introduction, level of sentiment analysis, method for identification and basic requirement of sentiment analysis is discussed in Section 2. Section 3 outlines sentiment analysis process presented with supporting examples. Section 4 reviews studies on related works from other researchers in different backgrounds and E-Commerce customers' reviews using sentiment analysis. Section 5 discusses comparative analysis table of sentiment analysis with different methods in e-Commerce. Section 6 present discussion on comparative analysis table. Finally in Section 6, the paper ends with conclusions and acknowledgements.

## II. SENTIMENT ANALYSIS LEVEL

Nowadays, the huge number of reviews requires efficient method for analyzing [4]. Customers and retailers reading thousands of reviews manually take plenty of time to classify the reviews in e-commerce using sentiment analysis method. The volume of reviews stored like mountain which requires some effective classifier to identify valuable information from text. Sentiment analysis or opinion mining is useful to extract customer's behavior by analyzing and exploring customer's reviews in E-commerce [7] [8] [9]. Customers express their emotions by writing subjective judgement about the products in E-commerce [40]. Sentiment analysis also helps to categorize the unstructured text as positive, negative and neutral whereby summarizes judgement by customers in order to understand other customer's expression and strength better about product and retailer [7] [10] [11]. Unstructured sentiments refer to detailed opinion by customer about the product [8]. Some information is explicit and others are implicit features. There are three levels of sentiment analysis:

Document-level Sentiment Analysis (DSA), Sentence-level Sentiment Analysis (SSA) and Aspect-level Sentiment Analysis (ASA).

#### A. Document-Level Sentiment Analysis (DSA)

A document talk about negative or positive sentiment is called DSA. It is extracting sentiments from whole document [8] [12] [13]. The scenario has applied the sentiment analysis of air purifier based on coarse-grained reviews whereby the researcher presented neural network model to identify semantics of sentences classification [14].

#### B. Sentence-Level Sentiment Analysis (SSA)

SSA means sentiment expressed in sentences which decide whether negative or positive. Whereby it is simple sentiment analysis for extracting sentiments or customer's experiences from sentences [8] [12] [13]. At sentence level, the researchers present phrase recursive autoencoder (PRAE) model to identify sentiment in sentences for analysis of coarse-grained reviews [14]. However, according to [14] document and sentences level sentiment analysis unable to fine-grained features from the words.

#### C. Aspect-Level Sentiment Analysis (ASA)

ASA is opinion that classifies by identifying entities and their properties by classification and extraction [13] [15]. Whereby, it is interested on opinion words only from the reviews such as "Love the Amazon show", it is clearly mentioned using the word love [12]. The aspect 'love' from the text is important feature extraction phase that needed for sentiment analysis method. At aspect level classification, researcher presents hybrid model for the analysis of fine-grained product's features [14]. It also expressed out sentiment polarity for further prediction process [16].

### III. SENTIMENT ANALYSIS PROCESS

Fig. 1 shows process flow of sentiment analysis where by divided three main stages: product feature extraction, sentiment classification and ranking alternative products [2].

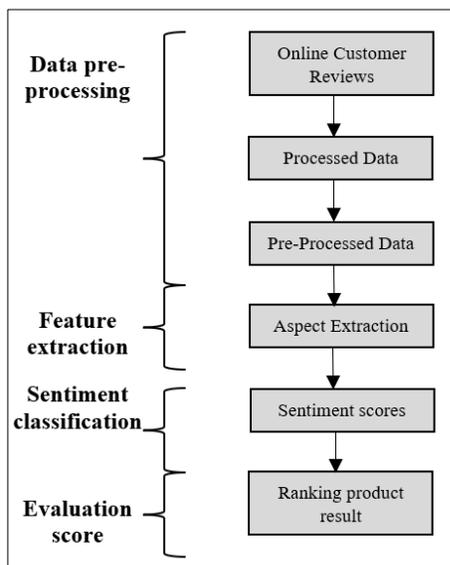


Fig. 1. Sentiment Analysis Process Flow [2] [4] [15].

#### A. Preprocessed Texts

As first step, data cleaning exhibit to clean unnecessary reviews from selected dataset [17] [18]. Data preprocessing perform to remove all missing values, remove stop words, tokenization, unwanted symbols, digits and URL tags [31]. Tokenization helps divide sentences into words, phrase or symbol and remove all stop words such as 'the', 'is', 'are' and 'a' [9]. The words required to convert to lower case as preparation for next step.

#### B. Feature Extraction

Aspect extraction from unstructured data helps extract all relevant information from dataset, reduces or removes irrelevant features of data for sentiment classification whereby the method is known as feature extraction [2] [19]. Feature extraction also helps extract implicit information from reviews other than explicit opinion to give more effective and better performance. There are few methods used for feature extraction :- frequent pattern mining with association rule mining, term document matrix (TDM), parts-of-speech (POS) tagging, Maximum entropy (ME), N-gram and lexicon [2] [8] [10] [16]. Those methods have advantages and disadvantages while applying for extract features in reviews. Frequent pattern mining is itemset, subsequence or substructures which helps find sequence database [20]. Apriori algorithm with association rules is one of the approach is in many fields. Other than that, according to U.A.Chauhan with other researchers has implemented Part-of-speech to find differences between noun, adjective, verb and adverb [5]. By extracting the term, in sentences reveals the hidden story and emotions of customers to be classified positive or negative. Furthermore, TDM is implemented to compute frequency of each word using method like bag of words and term frequency-inverse document frequency (TF-IDF) [5] [21] [22] [23]. TF-IDF helps to calculate number of times the word occurs and focuses on the importance term. By extracting most frequent words, researchers can ignore words with least scores. Some implement N-gram features for extracting the features as unigram (One word), bigram (2 words) and trigram (3 words) whereby N represent number of words [22] [24]. Based on researchers, unigrams features commit to increase accuracy result in classification method. N-grams helps to avoid semantic scores, the score calculation creates domain independent sentiment dictionary and computes to eliminate human annotators. These are some options by researchers for extract features from dataset before classifying the sentiment into positive, negative or neutral.

#### C. Sentiment Classification

Sentiment refers to feeling, emotions or responses of an individual by words for expressing human behavior and character [11] [25]. Hence, in this area explicit and implicit features that extract and identify hidden sentiment in measurable format. Whereby there are few methods to polarize the aspect in review theoretically: lexicon and machine learning classifier [2] [11] [13]. There are dictionary-based and corpus-based approaches for lexicon based such as Senti, HowNet, and Wordnet [8]. It is WorldNet dictionary which is stored with polarity positive, negative and neutral. Whereby automatically it is able to score the words in documents by

counting number of positive and negative words in review [21]. If the review has more positive words than negative words, it is polarized as positive reviews. Some machine learning classifier for supervised learning are Naïve Bayes, Support vector machines (SVM), Maximum Entropy and Random forest [2] [9] [10] [26] [27] [31]. Fig. 2 shows summary overall sentiment classification based machine learning and lexicon approaches. Supervised learning required training labeled data to process output result based on input data [21], whereas unsupervised learning requires unlabeled training data to identify pattern of data output. Many researches used Naïve Bayes and SVM machine learning method for sentiment classification [15] [21].

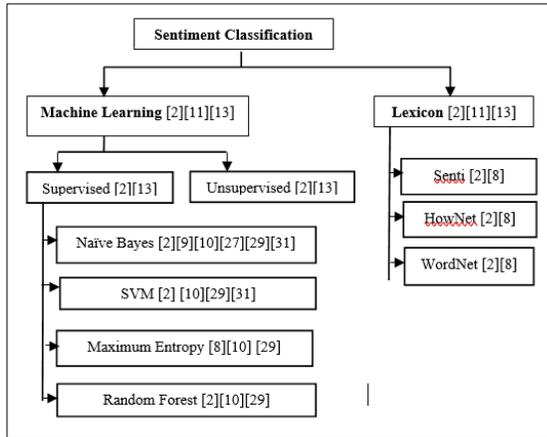


Fig. 2. Sentiment Classification Methods [2] [8] [9] [10] [11] [13] [26] [27] [31].

#### D. Evaluation Score

Based on feature extraction and sentiment classification on online reviews is rank the result using statical method [2]. The overall evaluation result is very important to judge subjective online reviews for customers. The result can predict or measure with mean squared error (MSA), confusion matrix, accuracy, precision, recall and F1-score [9] [15] [28] [29].

Equation of precision is presented as true positive (high quality reviews) divide by true positive (high positive reviews) + false positive (low quality reviews) [5] [18] [29].

$$\text{Precision} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Positive}} \quad (1)$$

Recall represented as true positive (high quality reviews) divide by true positive (high quality reviews) + False negative (low quality reviews) [5] [18] [29].

$$\text{Recall} = \frac{\text{True Positive}}{\text{True Positive} + \text{False Negative}} \quad (2)$$

F-score is calculated based on recall and precision as) [5] [18] [29]:-

$$F_{\text{Score}} = \frac{2 * \text{Precision} * \text{Recall}}{\text{Precision} + \text{Recall}} \quad (3)$$

Mean absolute error (MAE) and Root Mean Square Error (RMSE) measure the closeness between fitted line to the data points [18] [29] [30].

$$\text{MAE} = \frac{1}{n} \sum_{i=1}^n |d_i - d_i^{\wedge}| \quad (4)$$

Confusion matrix helps to show data difference between two classes [29]. Here, example of confusion matrix sketch with values True positive (TP), False positive (FP), False negative (FN) and True Negative (TN) as refer Fig. 3 [9] [15] [31].

TP: The output where correctly predicts the positive class.

FN: The output where incorrectly predicts the negative class whereby mislabeled as negative.

FP: The output incorrectly predicts the positive class whereby mislabeled as positive.

TN: The output where correctly predicts the negative class.

		ACTUAL VALUES	
		Positive	Negative
PREDICTED VALUES	Positive	TP	FP
	Negative	FN	TN

Fig. 3. Confusion Matrix for Amazon Dataset [9] [15] [31].

#### IV. RELATED WORK

This section presents related studies of sentiment analysis on customer's reviews which conducted by researchers on E-Commerce and different background of studies.

##### A. Previous Work from Different Background

Sentiment analysis is applied in different background of study. In Indonesia, Twitter status analyze with sentiment analysis method using SentiWordNet [32]. The emotion in tweet describes sentiment of user in Indonesian language whereby each sentences can polarize to positive, negative and neutral. Researcher used SentiWordNet which contains set of words score between 0 (negative) to 1(positive). After scoring of sentiment, final result identified by sentiment classification method by calculating accuracy positive score 0.77, neutral score 0.60, negative score 0.78 and average score is 0.74. Hence, emotions that express in words transform to meaning information. Other than that, sentiment analysis is also applied to extract Arabic opinions from text which is collected from twitter posts. In this research, Machine learning (ML) and Lexicon based (LB) approach with respect sentiment orientation is applied. The data collected and query using Tweepy Application Programming Interface (API) whereby positive and negative tweets are selected. N-gram features applied to divide the letter as Unigram (one word), bigram (two words) or trigram (three words). ML classifiers such as Naïve Bayes (NB), BNB, Multinomial NB (MNB), Maximum Entropy (ME), Support Vector Machine (SVM), Logistic Regression (LR), Stochastic Gradient Decent (SGD), RR, Adaptive Boosting (Ada-boost) and PA. To evaluate the performance of classifier accuracy, precision, recall and F-score is used. Based on final result, single fold SVM 99.31 with unigram feature shows highest accuracy and 10 fold PA 99.96% with unigram feature shows highest accuracy. The

classifier helps to extract and discover the polarity of the given tweet. On other hand, movies' reviews and score in Rotten Tomatoes website predict with sentiment analysis method [33]. In this research, lexical based approach and supervised machine learning approach were used to predict sentiment polarity in movies' reviews. This researcher also has polarized the sentiment in review using SentiWordNet whereby it classified into two classes rotten (negative) and fresh (positive). The result evaluate by comparing proposed method and baseline method by calculating average precision, recall and F measure whereby proposed method shows highest result 0.97. Hence, it is able to show better judgement on movies' reviews from rotten tomatoes website.

### B. Theory of Sentiments Analysis in E-Commerce

This section discussed previous work related sentiment analysis in customers' reviews e-commerce. Amazon dataset on product's reviews has been selected by few writers for sentiment analysis. Sentiment analysis of unstructured data in Amazon dataset helps to measure and evaluate information in sentiment in reviews using natural language processing techniques [4] [7] [34]. Sentiment analysis was implemented for analysis of e-commerce product reviews to categorize negative and positive comments and visualize it in charts [4]. The model is developed with unigram and bigram and evaluate with classifier such as linear support vector machine,

Multinomial Naïve Bayes, Stochastic Gradient, Random Forest, Logistic regression and Decision tree by product category cellphone, musical and electronics [4] [27]. The result measure using accuracy, precision, recall and F-measure whereby linear support machine shows highest accuracy 93.57 better results compared to other papers. Text mining techniques Apriori and Term Frequency-Inverse Document Frequency (TF-IDF) were applied for identifying text features in proper way [23] [34].

### V. COMPARATIVE ANALYSIS

Table I shows implementation of sentiment analysis on review by some researchers based on Amazon dataset. The table presents many research and different sentiment analysis approaches toward resolving problems in e-commerce customers' reviews. Process of identifying sentiment from unstructured dataset provides different results as different methods are applied. The challenging part of sentiment analysis is to discover what customers like and dislike as written expression [15] [27]. The researchers used sentiment analysis method for identifying sentiment scores in online reviews and overall result as presented in Table I. Different researchers have conducted different approaches for feature extraction and sentiment classification, hence, some future improvement in method application is needed to attain greater accuracy.

TABLE I. RELATED STUDIES BASED ON FEATURE EXTRACTION IN SENTIMENT ANALYSIS

Paper Title	Year	Dataset	Feature Extraction	Sentiment classification	Result
Amazon Reviews business analytics with sentiment analysis [35]	2016	Review of Cellphone & accessories	N/A	MNB	Accuracy:- 72.95%
				SVM	Accuracy:- 80.11%
Comparison of classification techniques for Feature Oriented Sentiment Analysis of Product Review Data [27]	2016	Amazon fine foods:-214 reviews [36]	POS tagging, Bigram	Naïve Bayes	Accuracy:- 74.76% Precision:- 79.54% Recall:-75.89% F-Measure:- 73.75%
				SVM	Accuracy:- 82.85% Precision:- 84.45% Recall:-82.13% F-Measure:- 82.38%
				Maximum Entropy	Accuracy:- 79.04% Precision:- 81.75% Recall:-79.99% F-Measure:- 78.59%
Sentiment Analysis on Large Scale Amazon Product Reviews [4]	2018	Review of cellphone & accessories :- 21600 reviews [37]	TF-IDF	Linear support vector machine	Accuracy:- 93.57%
		Review of electronics:- 24352 reviews [37]			Accuracy:- 93.52%
		Reviews of music instruments :- 2548 reviews [37]			Accuracy:- 94.02%
Sentiment classification on Amazon reviews using machine learning approaches [21]	2018	Amazon dataset :- 252000 reviews from snap dataset	Bag of words model	Naïve Bayes	Accuracy:- 92.72%
				SVM	Accuracy:- 93.20%
Classification of Amazon Book Reviews Based on Sentiment Analysis [23]	2018	Amazon Book reviews [38]	TF-IDF	Random Forest	Accuracy:- 90.15%
Aspect-Level Sentiment Analysis on E-Commerce Data [13]	2018	Customer reviews from Amazon products	Apriori algorithm	Naïve Bayes	Accuracy:- 90.423%
				SVM	Accuracy :- 83.423%
Machine learning based aspect level sentiment analysis for Amazon products [15]	2020	Amazon Products :- [39]	N/A	SVM classifier (RBF Kernel, BP-ALSA)	Accuracy:- 97%
A comprehensive analysis of adverb types for mining user sentiments on amazon product reviews [5]	2020	Amazon DVD musical product :- .Net Crawler, 9555 reviews	POS Tagging (Constituent Likelihood Automatic Word-tagging System (CLAWS))	Hybrid approaches	Precision :- 0.89, Recall:- 0.84, F-Measure:-0.86

## VI. DISCUSSION

The survey table presents comparison result for years from 2016 till 2020 in sentiment analysis E-Commerce from various categories of Amazon dataset. Based on Table I, most of the method in sentiment analysis implement feature extraction and sentiment classification in their process flow for get better accuracy results. Many researchers have implemented text mining method for extract most frequent information from dataset like TF-IDF and Apriori algorithm. Machine learning supervised method is used in most of the papers for classification of information. The experimental results from frequent pattern mining and supervised machine learning methods are able to provide more than 90% accuracy result. For future investigation, lexicon method and result analysis needed for compare accuracy result with machine learning method in sentiment analysis of customers' reviews.

## VII. CONCLUSION

In this paper, we have presented methodology of sentiment analysis and approaches based on previous studies in E-commerce. Research studies results are to address customer satisfaction on online shopping platform based on other's reviews. Data analysis approach presents statical result for predicting and building strong confidence among customers who purchase product from online. Most researches have looked into many approaches and challenges, toward judging customers' behavior as discussed in different methods. The approaches are further applied in other field like Airline, Tourism, Hotel industry, hospitality and others. Sentiment analysis methodology and interpretation using analytic tools perform accurate result to customers. Hence, there are many challenges and ongoing more research in this area have to be discussed and improved to produce more efficient and reliable sentiment analysis approaches.

## ACKNOWLEDGMENT

The authors would like to thank Ministry of Higher Education (MOHE) and Universiti Teknologi Malaysia (UTM) for their educational and financial support. This work is conducted at Razak Faculty of Technology and Informatics, under Cyber Physical Systems Research Group and funded by MOHE (FRGS: R.K130000.7856.5F026) and (UTM GUP: Q.K130000.2538.18H42).

## REFERENCES

- [1] L. T. T. Tran, "Managing the effectiveness of e-commerce platforms in a pandemic Lobel," sciencedirect, pp. 0969-6989, 2021.
- [2] F. P. Zhi, G. M. Li and Y. Liu, "Processes and methods of information fusion for ranking products based on online reviews: An overview," Science Direct, pp. 87-97, 2020.
- [3] S. Sanyala and M. Wamique Hisamb, "Factors Affecting Customer Satisfaction with Ecommerce Websites – An Omani Perspective," IEEE, pp. 232-236, 2019.
- [4] T. Ul Haque, N. Nawal Saber and F. Muhammad Shah, "Sentiment Analysis on Large Scale Amazon Product Reviews," IEEE, pp. 1-7, 2018.
- [5] U. A. Chauhan, M. T. Afzal, A. Shahid, M. Abdar, M. E. Basiri and X. Zhou, "A comprehensive analysis of adverb types for mining user sentiments on amazon product reviews," Springer, p. 1811–1829, 2020.
- [6] S. Al-Natour and O. Turetken Ted, "A comparative assessment of sentiment analysis and star ratings for consumer reviews," ScienceDirect, pp. 0268-4012, 2020.
- [7] A. S. Rathor, A. Agarwal and P. Dimri, "Comparative Study of Machine Learning Approaches for Amazon Reviews," ScienceDirect, pp. 1552-1561, 2018.
- [8] D. M. El-Din Mohamed and Hussein, "A survey on sentiment analysis challenges," ScienceDirect, pp. 330-338, 2018.
- [9] P. Kencana Sari, A. Alamsyah and S. Wibowo, "Measuring e-Commerce service quality from online customer review using sentiment analysis," IOP Publishing, pp. 1-7, 2018.
- [10] T. Quyyam and D. H. Ghous, "Sentiment Analysis of Amazon Customer Product Reviews: A Review," ijsred, pp. 564-595, 2021.
- [11] A. Ligthart, C. Catal and B. Tekinerdogan, "Systematic reviews in sentiment analysis: a tertiary study," Springer, pp. 1-57, 2021.
- [12] M. Tubishat, N. Idris and M. Abushariah, "Explicit aspects extraction in sentiment analysis using optimal rules combination," ScienceDirect, pp. 448-480, 2021.
- [13] M. B. Satuluri Vanaja, "Aspect-Level Sentiment Analysis on E-Commerce Data," IEEE, pp. 1275-1279, 2018.
- [14] Jing Zhang, Aijia Zhang, Dian Liu and Yiwen Bian, "Customer preferences extraction for air purifiers based on fine-grained sentiment analysis ofonline reviews," ScienceDirect, pp. 1-15, 2021.
- [15] N. Nandal, R. Tanwar and J. Pruthi, "Machine learning based aspect level sentiment analysis for Amazon products," Springer, p. 601–607, 2020.
- [16] M. Ahmed, Qun Chen and Zhanhui Li, "Constructing domain-dependent sentiment dictionary for sentiment analysis," Springer, pp. 14719-14732, 2020.
- [17] M. Aman Ullah, S. Maliha Marium, S. Ara Begum and N. Saha Dipa, "An algorithm and method for sentiment analysis using the text and emoticon," ScienceDirect, pp. 357-360, 2020.
- [18] A. Angelpreethi and D. S. BrittoRameshKumar, "An Enhanced Architecture for Feature Based Opinion Mining from Product Reviews," IEEE, pp. 89-92, 2017.
- [19] G. Anand babu and B. Srinivasu, "A Conceptual Based Approach in Text Mining: Techniques and Applications," IJITEE, pp. 2278-3075, 2019.
- [20] Jiawei Han, Dong Xin, Hong Cheng and Xifeng Yan, "Frequent Pattern Mining: Current Status and Future Directions," ResearchGate, pp. 1-33, 2019.
- [21] S. Paknejad, "Sentiment classification on Amazon reviews using machine learning approaches," KYH Computer Science and Communication, pp. 1-23, 2018.
- [22] R. Ahuja, A. Chug, S. Kohli, S. Gupta and P. Ahuja, "The Impact of Features Extraction on the Sentiment Analysis," ScienceDirect, pp. 341-348, 2019.
- [23] K. S. Srujan, S. S. Nikhil, H. Raghav Rao, K. Karthik, B. S. Harish and H. M. Keerthi Kumar, "Classification of Amazon Book Reviews Based on Sentiment Analysis," Springer, pp. 1-12, 2018.
- [24] A. Dey, M. Jenamani and J. J.Thakkar, "Senti-N-Gram : An n -gram lexicon for sentiment analysis," ScienceDirect, pp. 92-105, 2018.
- [25] K. Chakraborty and A. Alla Hassanien, "Sentiment Analysis on a Set of Movie Reviews Using Deep Learning Techniques," Science Direct, pp. 1-14, 2019.
- [26] K. Ashok Kumar, C. Jagadeesh, P. Kshirsagar and S. M. Marve, "Sentiment Analysis of Amazon Product Reviews using Machine Learning," Reseach gate, pp. 5245-5254, 2020.
- [27] C. Pujari, A. and N. P. Shetty, "Comparison of classification techniques for Feature Oriented Sentiment Analysis of Product Review Data," ResearchGate, pp. 1-9, 2016.
- [28] X. Dou, "Online Purchase Behavior Prediction and Analysis Using Ensemble Learning," IEEE, pp. 532-536, 2020.
- [29] S. Saumya, J. Prakash Singh, A. Mohammed Baabdullah, N. P. Rana and Y. k. Dwivedi, "Ranking Online Consumer Reviews," ResearchGate, pp. 1-39, 2019.

- [30] Jicheng Li and Xinyue Huang, "Target customer selection method based on data mining in big data environment," IEEE, pp. 286-289, 2017.
- [31] D. Shailendra Narayan Singh and Twinkle Sarraf, "Sentiment Analysis of a Product based on User Reviews using Random Forests Algorithm," IEEE, pp. 112-116, 2020.
- [32] N. Maulidiah Elfajr and R. Sarno, "Sentiment Analysis using Weighted Emoticons and SentiWordNet for Indonesian Language," IEEE, pp. 234-238, 2018.
- [33] Suhariyanto, Ari Firmanto and Riyanarto Sarno, "Prediction of Movie Sentiment based on Reviews and Score on Rotten Tomatoes using SentiWordnet," IEEE, pp. 202-206, 2018.
- [34] A. L. Robert Ireland, "Application of data analytics for product design: Sentiment analysis of online product reviews," ScienceDirect, p. 128-144, 2018.
- [35] E. M. Soledad and Y.-F. W. , "Amazon Reviews, business analytics with sentiment analysis," ResearchGate, 2016.
- [36] Krevl and J. Leskovec, "SNAP Datasets," June 2014. [Online]. Available: <http://snap.stanford.edu/data>.
- [37] McAuley, Ruining He and Julian, "Ups and downs: Modeling the visual evolution of fashion trends with one- class collaborative filtering.," Feb 2016. [Online]. Available: <https://arxiv.org/abs/1602.01585>.
- [38] ZhiLiu, "UCI:- Machine Learning Repository," 11 06 2011. [Online]. Available:<https://archive.ics.uci.edu/ml/datasets/Amazon+book+reviews>.
- [39] R.Mitchell, "Web scraping with python: collecting more data from the modern web," April 2018. [Online]. Available: <https://www.oreilly.com/library/view/web-scraping-with/9781491985564/>.
- [40] A. Alamoodi, B. Zaidan, A. Zaidan, O. Albahri, K. Mohammed, R. Malik, E. Almahdi, M. Chyad, Z. Tareq, A. Albahri, H. Hameed and M. Alaa, "Sentiment analysis and its applications in fighting COVID-19 and infectious diseases: A systematic review," ScienceDirect, pp. 2-13, 2020.

# Assessment Framework for Defining the Maturity of Information Technology within Enterprise Risk Management (ERM)

Rokhman Fauzi, Muharman Lubis

Department of Information System, Telkom University, Bandung, Indonesia

**Abstract**—The process of reviewing, assessing and improving the organization's IT risk management requires some basic information summarized in a process maturity profile. In general, IT risk management standards or frameworks do not include a mechanism for assessing the maturity level of process implementations. This study was conducted to develop a framework, which can be applied to assess the maturity level of IT risk management under ISO / IEC 27005. A standards-based management system implementation can be represented as a model cycle of planning, implementation, validation and also action plan. The proposed evaluation framework consists of templates, methods, and working papers. Therefore, the template focus on the evaluation areas, which are planning, execution, validation, and execution, then evaluation area details (8 domains, 35 subdomains, 82 items), and evaluation metrics and criteria. Meanwhile, a working paper has been created to assist in conducting the evaluation. Actually, by using this evaluation framework, it can provide a representation of the maturity level from the entire process in managing IT risk, based on the provisions of ISO/IEC 27005. This framework complements the existing model with the representation of (1) providing a single-cycle planning, establishment, validation, and execution, (2) evaluation tools, (3) more comprehensive data collection methods, and (4) priority list of elements to be reformed and/or improved.

**Keywords**—Risk management; assessment framework; maturity level; PDCA cycles; ISO/IEC 27005

## I. INTRODUCTION

In the process of forecasting, minimizing, monitoring, and controlling the likelihood or impact of unfortunate events, also in maximizing the realization of opportunities; organizations utilize enterprise risk management (ERM) frameworks in particular to manage every potential loss, problem or damage towards company. This framework needs to provide a structured process that integrates risk management activities into the systems development life cycle (SDLC) or agile management project to enable risk managers in making the informed decisions. In general, this process should involve determining the accuracy of risk decisions and the possible accepted risks. On the other hand, good prescriptions for making risk decisions include a mixture of objective data, pass or fail test results, mitigation measures, qualitative analysis, subjective data, and a healthy bit of intuition [1]. In actual, a description of the enterprise's risk management maturity level should provide the benefit of identifying the actual strengths and weaknesses of risk management in the enterprise. Then get

measurement results that will help organization to increase its maturity level and ladder. It also integrates organizational risk management documents to enhance its contribution to be more effective organizational governance and to improve the quality of risk management and risk mitigation processes. Thus, the company's leadership must define expectations for the company's risk management programs on how to measure them, especially the security assessment stage of the risk management framework. Asking the right questions is important for auditors to discover how risk management software works and the true state of program integration. Moreover, audit teams need to focus and concentrate on a more in-depth review of a broader set of systems and integrity testing.

Each year, the public sector provides indicators and metrics to support government compliance and reporting requirements. Some of these many metrics include the number of systems that company operates in their viability to execute and risk of acceptability. Therefore, the accuracy in measuring the effectiveness of risk management programs depends on whether safety controls are regularly tested as well retested, and whether there is a record of test results related to five primary sources of risk namely production, marketing, financial, legal and human [2]. Risk is a necessary part of doing business and in a world where massive amounts of data are processed at an ever-increasing rate, identifying and mitigating risks is a challenge for any company. Actually, little wonder that many contracts and insurance policies require strong evidence of good risk management practices [3]. In addition, it is imperative that the framework provides guidance for companies to integrate risk-based decision-making into organizational governance, planning, management, reporting, policies, values and culture. It is an open principles-based system that allows organizations to apply standard principles in their context.

Every International Standard Organization (ISO) are reviewed every five years and revised as needed. This allows them to remain a useful and relevant tool in the market. Therefore, in this case, the study focuses on old versions and emphasize about ownership that many organizations face obstacles and barriers directly to further modernizing technology and infrastructure, while at the same time needing the guidance to be as simple as possible so the older versions provide benefit in term of contextual more compare to the latest version developed. In particular, this framework helps provide the basis for a comprehensive risk management

methodology for assessing and improving program risk management practices. The risk management framework can be applied to all stages of the system development life cycle, including acquisition, development and operations. In addition, the framework can be used to guide the management of various types of risks, including acquisition program risks, software development risks, operational risks, and information security risks [4]. In short, risks are of paramount importance to organizations that need to identify, assess, manage and the process to report many types of risks for the company is extremely important to improve external and internal decision-making. Interestingly, risks can be viewed as threats or called as a negative event to the organization. Managing risk in this context means using management techniques to reduce the likelihood and impact of adverse events without incurring excessive costs. On the other hand, risk also can be defined as uncertainty as the danger related to the distribution of all possible outcomes, positive and negative. Thus, managing risk means minimizing the difference between expected and actual results. Finally, risk can be described contextually as an opportunity that can be viewed as a source of business opportunities [5], [6]. Thus, it is recommended to utilize the popular and older version of ISO/IEC 27005 with the modified version to bring simplification to the organization that have been used in certain period of time without the burden in the transition process or adopting the new method regularly every five year while at same time creating flexibility and improvement to the business process as a whole, which, this study want to offer the ERM template.

## II. LITERATURE REVIEW

Processes in risk management besides functioning to reduce negative impacts can also be used to identify and optimizing the positive and potential aspect of the organization. Meanwhile, ISO/IEC Guide 73 defines risk as a combination of an opportunity (likelihood) and its impact (implication). Information Technology (IT) Risk is a business risk related to the use, ownership, operation, involvement, influence, and application of IT in a company [7], [8]. It is also defined as something that is wrong with IT and has a negative impact on business [9], [10]. The types of risks that affect and/or become a direct result of IT activities have a broad scope. In short, risks can be grouped into several categories that help providing an overview of the organization's risk profile. The IT risk portfolio is one approach in identifying and grouping IT risks, which can be grouped into 7 (seven) categories, namely: projects, continuity of IT services, information assets, service providers, applications, infrastructure, and strategic matters [11], [12]. The IT risk portfolio provides an overview of things that should be the main concern of the organization in managing the risks associated with IT, which Symantec [13] classifies IT risk into 4 categories, namely: security risk, availability risk, performance risk, and compliance risk. In addition, the common threads that serve as for the various IT risk rating models are confidentiality, integrity, and availability [14].

In general, PDCA (Plan, Do, Check, Act) is included in an endless cycle of risk management where all executed and implemented solutions can be seen as indicators of further improvement activities. This knowledge is used as a basis and

fundamental organizational resource that provides an ongoing competitive advantage in a relevant and dynamic environment and market by identifying gap between strategic planning and potential knowledge [12]. National Institute of Standards and Technology [15] defines IT Risk Management as a process that allows IT managers to balance operational and economic costs from the protection of IT and benefit from such protection. This definition compromises between classical definitions in business and definitions in the context of the organization's IT operations. Risk management also must be carried out continuously and have sustainability to be developed in order to overcome the risks of the organization at present and in the future. Thus, every manager and staff must understand their roles and responsibilities in risk management. In addition, risk management must also be integrated with organizational culture through policies and programs led directly by senior management [16]. In fact, IT Risk Management is the foundation of the implementation of the Information Security Management System [17]. ISO/IEC 27001 stipulates that the controls implemented within the scope, limits, and context of the Information Security Management System (ISMS) must be risk-based. The PDCA has been engaged as an impressive and essential tool for quality and continuous improvement with both simple and powerful to implement the strategy and policy in the organization. The application of the PDCA cycle has been found more effective than adopting "the right first time" approach. By using of the PDCA cycle means continuously looking for better methods of improvement and enhancement [18].

Implementing a risk management process is not always easy, and some organizations give up without achieving the desired results. This may be due to the inability to implement the risk management process in a consistent and predictable manner in the long term. On the other hand, a maturity model is a tool that represents the pathway to an increasingly structured and systematic way of doing business, usually involving people, organizations, and processes. Over the past few years, these tools have become very popular, using models of maturity in many areas, such as data management, information security, and project management. In a maturity model, the evolutionary path is described through separate stages. To reach the next level, the organization must achieve the objectives of the required level and all previous levels [19], [20]. To enable the measurement of maturity levels and identify gaps between current levels and follow-up to enable planning efforts; priorities and objectives should be formulated to achieve proposed goals. It allows the assessment process run smoothly and building the achievement compliance. Ultimately, this approach provides organizations with an understanding of strengths, weaknesses, and opportunities that can support audits, benchmarks, and progress assessments against goals, strategic decisions, and project portfolio management [21], [22].

The difference between organizations whose systems are more or less mature is not only related to the results of the indicators used, but also to the fact that dominantly mature organizations measure differently using various indicators when compared to immature organizations. The concept of maturity is related to one or more of the elements identified as

being related but the concept of function is only appropriate for each of these elements [23], [24]. It appears very important for non-financial companies to promote and discuss on how to implement and manage risk management efforts. One of the key issues is how to effectively evaluate the quality of a company's risk management performance. The most important factor is the growth of a consistent risk culture and the independence of the board of director in determining the decision for integration process within the organization [25], [26], [27]. Therefore, it is also important to understand the role of individual, institutional and environmental within the organization as the primary prerequisites for improvement in raising awareness of the strategies used in each business process within the framework of a particular project or service [28].

### III. FRAMEWORK DESIGN

This study was conducted using several phases: literature review, framework design, and case studies (see Fig. 1). The evaluation framework, on the other hand, consists of evaluation forms, methods, and a worksheet of descriptive structure (see Fig. 3). Evaluation forms are a key component of this framework, which this model consists of 8 domains, 35 subdomains, and 4 evaluation domains (PDCA) detailing 82 items with the detail area is a set of provisions of the ISO / IEC 27005 standard. The domains are taken from the main blocks in the standard process model. Meanwhile, subdomains and elements refer to clauses of the standard in each domain. Interestingly, the presence of a Chief Risk Officer (CRO) does not clarify the level of support and leadership from the CEO and the Board of Directors in relation to the creation and distribution of risk information throughout the organization, which dedicated to mitigate and manage major risks [29], [30]. Most importantly, create a portfolio of company risks and opportunity events: finance, strategy, compliance, operations, and reputation can influence the achievement of strategic goals.

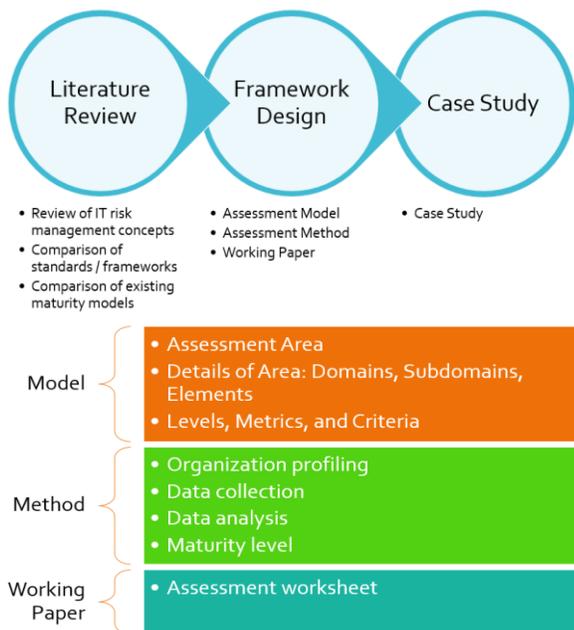


Fig. 1. Methodology and Assessment Framework.

### IV. ASSESSMENT AREA

In fact, this study divided the process into five groups related to the plan in implementing ERM: full implementation, partial execution, implementation planning process, feasibility study or evaluation, and level of ERM implementation. On the other hand, traditional risk management approaches utilize segmented methods to face different risks across different organizations. In contrast, ERM is a relatively new paradigm that enhances a company's ability to predict the set of risks it faces [31], [32], [33]. ERM is a top-down approach that includes identifying, assessing and addressing strategic, operational and financial risks to achieve the following four objectives: (1) high-level strategic objectives aligned with the corporate mission, (2) effective and efficient use of resources, (3) reliability of reporting, and (4) compliance - enforcement of legal and regulatory compliance [34]. As can be seen in Fig. 2, the process is started and ended with context establishment to risk identification, estimation and evaluation, the once again context become the consideration to determine risk treatment as well risk acceptance.

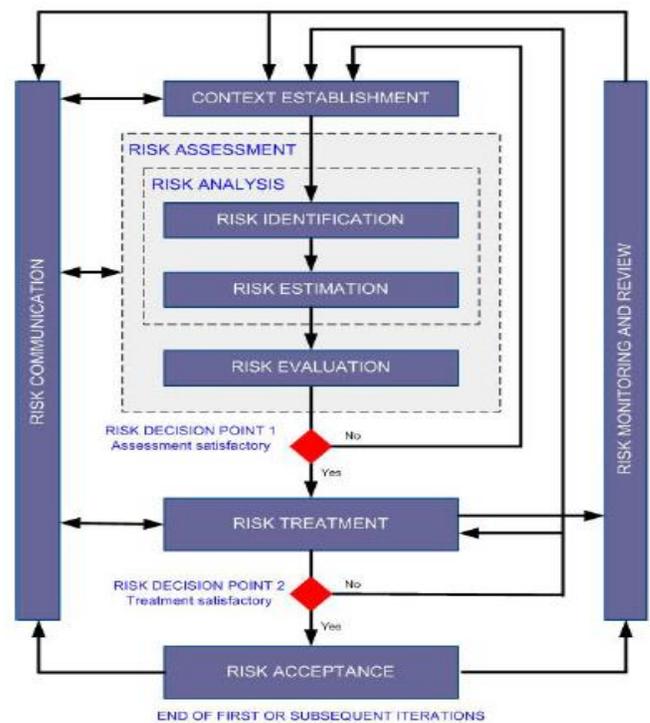


Fig. 2. Process Model of ISO/IEC 270005.

The main purpose of placing this evaluation form is to provide a structured description of the improvement stages of the PDCA cycle process. The following table defines levels using the Business Risk Management Maturity Model and the Business Process Maturity Model. Providing metrics is essential because the lack of process measurement affects the determination of performance levels and further disrupts the organization's business and activity improvement processes. Measurements are an approach of the evaluation process and organizational performance, and in this model the standard is defined as a metric of the elements score level and a list of conditions that indicate the determination of requirements. In

addition, referring to the standard paragraph, each domain is divided into several subdomains and elements. The result was 35 subdomains and 82 items (Table I). In addition, PDCA code elements are assigned to classify needs based on several specifications to increase the sustainability of the activity process (Table II).

TABLE I. SUBDOMAINS AND ELEMENTS

Domains	Number of subdomains	Number of elements
Context Establishment	6	16
Risk Communication	4	13
Risk Identification	5	15
Risk Estimation	4	6
Risk Evaluation	3	4
Risk Treatment	7	7
Risk Acceptance	2	2
Risk Monitoring and Review	4	19
	35	82

TABLE II. MAPPING OF AREA: PLAN, DO, CHECK AND ACT

Area	Code of elements
PLAN	1.1.1, 1.2.1, 1.3.1, 1.4.1, 1.4.2, 1.4.3, 1.4.4, 1.4.5, 1.4.6, 1.4.7, 1.4.8, 1.4.9, 1.4.10, 1.4.11, 1.5.1, 1.6.1
	2.1.1, 2.2.2, 2.3.1, 2.3.2, 2.3.3, 2.3.7, 2.3.8, 2.3.9
	3.1.1, 3.1.2, 3.1.3, 3.1.4, 3.2.1, 3.2.2, 3.2.3, 3.3.1, 3.3.2, 3.4.1, 3.4.2, 3.4.3, 3.5.1, 3.5.2, 3.5.3
	4.1.1, 4.1.2, 4.2.1, 4.2.2, 4.3.1, 4.4.1
	5.1.1, 5.2.1, 5.2.2, 5.3.1
	6.1.1, 6.2.1, 6.7.1
	7.1.1, 7.1.2
DO	2.4.1
	6.3.1, 6.4.1, 6.5.1
CHECK	2.2.1, 2.3.5
	6.6.1
	8.1.1, 8.1.2, 8.1.3, 8.1.4, 8.1.5, 8.1.6, 8.1.7, 8.2.1
ACT	2.3.4, 2.3.6
	8.3.1, 8.3.2, 8.3.3, 8.3.4, 8.3.5, 8.3.6, 8.3.7, 8.3.8, 8.3.9, 8.4.1, 8.4.2

The life cycle of an innovation project is a series of interrelated processes and stages of novelty. Innovation projects generally include the following life cycle rule with well-defined stages: innovation development, production readiness, market entry, growth, maturity, recovery, or decline. In order to maintain the competitiveness of innovation projects at all stages, it is necessary to develop and implement specific type of innovations (incremental, responsive, disruptive or radical) that are included in the portfolio of innovation projects and which are implemented in a specific order with different levels of innovation content and research intensity [35]. Entirety was used then to map the component into each Assessment Area, in which each element is also mapped into

them respectively (Fig. 3-7). The level and criteria should be defined to set the indicators that can be looked at and matching for the purpose of improvement in the process (Table III). Meanwhile, the metrics is also essential to simplify the process maturity to be recognized in every type of risk domain respectively (Table IV). Risks are localized in implementing innovation projects in the process of analyzing and modeling a set of innovations. Choosing the best combination of risk management techniques as part of a particular innovation project requires assessing a range of factors, such as the complexity and specificity of innovation activities and the level of profitability of the innovation at a given time. Time periods, insurance service costs, likelihood of risk, size and quality, predictability of risk, legal limits and provisions, and project implementation phases are several aspects that become primary considerations [36].

TABLE III. LEVEL AND CRITERIA

Level	Criteria
Level 5	Organizational focus is the ongoing improvement process. The whole process was in accordance with the reference standard.
Level 4	Organizational focus is the evaluation and optimization of existing resources. Much of the process followed a reference standard.
Level 3	Organizational focus is to build a standard managerial processes to achieve organizational goals. A small part of the process followed the reference standard.
Level 2	Organizational focus is to build managerial foundation in every program or project. Some processes are standardized, without a reference standard.
Level 1	No specific targets. Achievement of the organization depends on the competence and hard work of a handful of personnel. There is no standard process.

TABLE IV. METRIC COMPONENTS

Domain	M1	M2	M3	M4	M5	M6
Context Establishment	P	P	P	P		
Risk Communication	P		P	P		P
Risk Identification	P		P	P	P	P
Risk Estimation	P		P	P	P	P
Risk Evaluation	P		P	P	P	P
Risk Treatment	P		P	P	P	P
Risk Acceptance	P		P	P		
Risk Monitoring and Review	P		P	P	P	P

\*P: Primary related; metric component used in the domain assessment

Metrics and Assessment Criteria are determined per domain because each has its input, process and output characteristics. In this case, it used various assessments namely [M1] policy, plans and procedures, [M2] goals and success measurements, [M3] roles and responsibilities, [M4] communications, [M5] skills and trainings, as well as [M6] tools. Furthermore, the metric components used in the domain context of establishment; the assessment are [M1], [M2], [M3] and [M4] communications. On the other hand, the metric components used in the domain of risk communication; the assessment are [M1], [M3], [M4] and [M6]. Nonetheless, the

metric components used in the domain risk identification; the assessment are [M1], [M3], [M4], [M5] and [M6]. Then, the metric components used in the domain of risk estimation; the assessment are [M1], [M3], [M4], [M5] and [M6].

The ERM template can be seen in Table V is designed for use as a self-assessment for the tool to be effective; it must be conducted in such a way that the process is as objective as possible to avoid bias or group thinking. From experience using the model, the self-evaluation discussion includes the following important considerations such as project duration and role responsibility. According to the government comments, it could take hours to a day or more, depending on the amount of preparation before the group discussion and the level of detail of the discussion itself take place. Ideally, there should be a diverse group of employees responsible for managing ERM involved in the self-assessment across the ranks. Thus, caring must be taken to ensure that the

conversation is open and transparent, which people should be encouraged to express their opinions. It may be helpful to ask someone outside of the management chain to manage ERM to facilitate discussion. That person should read specific note and understand on how to handle the self-evaluation of the form [37]. In addition to facilitating discussions, a person should be able to challenge the opinions of the self-assessment group, including looking for supporting evidence as needed. The metric components used in the domain risk evaluation, the assessment are [M1], [M3], [M4], [M5] and [M6]. Meanwhile, the metric components used in the domain risk treatment; the assessment are [M1], [M3], [M4], [M5] and [M6]. Nevertheless, the metric components used in the domain risk acceptance; the assessment are [M1], [M3] and [M4]. At last, the metric components used in the domain risk monitoring and review; the assessments are [M1], [M3], [M4], [M5] and [M6]. All of them can be seen in Table VI, respectively based on each separated criteria level.

TABLE V. LEVELS, METRICS AND CRITERIA FOR DOMAIN CONTEXT ESTABLISHMENT, RISK COMMUNICATION, RISK IDENTIFICATION AND RISK ESTIMATION

Level	Criteria	Criteria	Criteria	Criteria
Domain	Context Establishment	Risk Communication	Risk Identification	Risk Estimation
Level 5	All items in this clause already exist in the Policy, Planning and/or Procedure documents. Defining goals and measures of success is clearly given. All roles and responsibilities are clearly described and there is no overlap. Socialization is carried out on all stakeholders.	Senior management and all stakeholders understand and care about key aspects of IT risk management; IT risk is part of the main consideration of decision making. All roles and responsibilities are clearly described and there is no overlap. There are procedures for all forms of risk communication needed. There are communication aids that support normal and emergency conditions.	Risk identification activities are regulated in Policies, Planning and/or Procedures. Risk identification details are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk identification involves all parties involved. Implementing risk identification is an internal team of organizations (who have received special training) and experts from outside the organization. Risk identification is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk estimation activities are regulated in Policies, Planning and/or Procedures. Details of risk estimates are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk estimates involve all parties involved. The executor of risk estimation is the internal team of the organization (who has received special training) and experts from outside the organization. Risk estimates are carried out with tools that are in accordance with the Standards and conditions of the Organization.
Level 4	All items in this clause already exist in the Policy, Planning and/or Procedure documents. Defining goals and measures of success is clearly given. All roles and responsibilities are clearly described and there is no overlap. The socialization was carried out for some stakeholders.	Senior management and all stakeholders understand and care for key aspects of IT risk management. All roles and responsibilities are clearly described and there is no overlap. There are procedures for all forms of risk communication needed. There are communication aids that support normal and emergency conditions.	Risk identification activities are regulated in Policies, Planning and/or Procedures. Risk identification details are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk identification involves all parties involved. Implementers of risk identification are internal organization teams (who have received special training) or experts from outside the organization. Risk identification is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk estimation activities are regulated in Policies, Planning and/or Procedures. Details of risk estimates are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk estimates involve all parties involved. Implementers of risk estimation are internal organization teams (who have received special training) or experts from outside the organization. Risk estimates are carried out with tools that are in accordance with the Standards and conditions of the Organization.
Level 3	All items in this clause already exist in the Policy, Planning and/or Procedure documents. Defining goals and measures of success is clearly given. All roles and responsibilities are clearly described, but	IT and Management staff related to IT understand and care for key aspects of IT risk management. All roles and responsibilities are clearly described, but there are still overlaps. There are procedures for some form of risk communication that is needed.	Risk identification activities are regulated in Policies, Planning and/or Procedures. Risk identification details are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are still overlaps. Risk identification involves all parties involved. Implementers of risk identification are	Risk estimation activities are regulated in Policies, Planning and/or Procedures. Details of risk estimates are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are overlaps. Risk estimates involve all parties involved. The executor of risk estimation is an

	there are still overlaps.	There are communication aids that support normal conditions.	internal organization teams (who have not received special training) or experts from outside the organization. Risk identification is carried out with tools that are in accordance with the Standards and conditions of the Organization.	internal team of organizations (who have not received special training) or experts from outside the organization. Risk estimates are carried out with tools that are in accordance with the Standards and conditions of the Organization.
Level 2	Some items in this clause already exist in the Policy, Planning and/or Procedure documents. Defining goals and measures of success is not clearly stated. All roles and responsibilities have been described, but are still unclear and there are overlaps.	IT and Management staff related to IT understand and care for key aspects of IT risk management. All roles and responsibilities are described, but still unclear and there are overlaps. There is no procedure; risk communication is carried out informally.	Risk identification activities are regulated in Policies, Planning and/or Procedures. Risk identification details are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk identification does not involve all parties involved. Implementing risk identification is an internal team of organizations (who have not received special training)	Risk estimation activities are regulated in Policies, Planning and/or Procedures. Details of risk estimates are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk estimates do not involve all parties involved. Implementing risk estimates is an internal team of organizations (who have not received special training)
Level 1	This clause does not yet exist in the Policy, Planning and/or Procedure document. Defining goals and measures of success is not clear.	There is still IT staff who do not understand and care for the key aspects of IT risk management.	Risk identification activities are not regulated in Policies, Planning and/or Procedures. Risk identification does not involve all parties involved. Implementing risk identification is an internal team of organizations (who have not received special training).	Risk estimation activities are not regulated in Policies, Planning and/or Procedures. Risk estimates do not involve all parties involved. Implementing risk estimates is an internal team of organizations (who have not received special training).

TABLE VI. LEVELS, METRICS AND CRITERIA FOR DOMAIN RISK EVALUATION, RISK TREATMENT, RISK ACCEPTANCE AND RISK MONITORING & REVIEW

Level	Criteria	Criteria	Criteria	Criteria
Domain	Risk Evaluation	Risk Treatment	Risk Acceptance	Risk Monitoring and Review
Level 5	Risk evaluation activities are regulated in Policies, Planning and/or Procedures. Details of risk evaluation are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap by involving all parties involved. Risk evaluation implementers are internal organizational teams (who have received special training) and experts from outside the organization. Risk evaluation is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk handling activities are regulated in Policies, Planning and / or Procedures. Risk handling details are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk management involves all parties involved. Risk management executors are internal organization teams (who have received special training) and experts from outside the organization. ERM is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk acceptance activities are regulated in Policies, Planning and/or Procedures. Roles and responsibilities are clearly defined. Acceptance of risk in accordance with all risk acceptance criteria. Justification, communication and monitoring of risk acceptance are carried out in accordance with the clause in the Standard	Monitoring and risk checking activities are regulated in Policies, Planning and / or Procedures. Details of monitoring and risk checking are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk monitoring and inspection involves all parties involved. Implementers of risk monitoring and inspection are internal organization teams (who have received special training) and experts from outside the organization. Risk monitoring and inspection is carried out with tools that are in accordance with the Organization's Standards and conditions.
Level 4	Risk evaluation activities are regulated in Policies, Planning and/or Procedures. Details of risk evaluation are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk evaluation involves all parties involved. Risk evaluation implementers are internal organization teams (who have received special training) or experts from outside the organization. Risk evaluation is carried out with tools that are in accordance with the	Risk handling activities are regulated in Policies, Planning and/or Procedures. Risk handling details are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk management involves all parties involved. Risk management executors are internal organization teams (who have received special training) or experts from outside the organization. Risk management is carried out with tools that are in accordance with the	Risk acceptance activities are regulated in Policies, Planning and / or Procedures. Roles and responsibilities are clearly defined. Acceptance of risk is in accordance with some risk acceptance criteria. Justification, communication and monitoring are carried out on the entire list of risk acceptance that does not meet the criteria.	Monitoring and risk checking activities are regulated in Policies, Planning and / or Procedures. Details of monitoring and risk checking are in accordance with all clauses in the Standard. All roles and responsibilities are clearly described and there is no overlap. Risk monitoring and inspection involves all parties involved. Implementers of monitoring and risk checking are internal organization teams (who have received special training) or experts from outside the organization. Risk monitoring and inspection is carried out with tools that are in accordance with the Organization's Standards and conditions.

	Standards and conditions of the Organization.	Standards and conditions of the Organization		
Level 3	Risk evaluation activities are regulated in Policies, Planning and/or Procedures. Details of risk evaluation are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are overlaps. Risk evaluation involves all parties involved. The risk evaluation implementer is an internal team of organizations (who have not received special training) or experts from outside the organization. Risk evaluation is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk handling activities are regulated in Policies, Planning and/or Procedures. Risk handling details are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are still overlaps. Risk management involves all parties involved. Risk management implementers are internal organization teams (who have not received special training) or experts from outside the organization. Risk management is carried out with tools that are in accordance with the Standards and conditions of the Organization.	Risk acceptance activities are regulated in Policies, Planning and/or Procedures. Roles and responsibilities are clearly defined. Acceptance of risk is in accordance with some risk acceptance criteria. Justification, communication and monitoring are carried out on part of the risk acceptance list that does not meet the criteria.	Monitoring and risk checking activities are regulated in Policies, Planning and / or Procedures. Details of monitoring and risk checking are in accordance with some clauses in the Standard. All roles and responsibilities are clearly described, but there are overlaps. Risk monitoring and inspection involves all parties involved. Implementers of monitoring and risk checking are internal organization teams (who have not received special training) or experts from outside the organization. Risk monitoring and inspection is carried out with tools that are in accordance with the Organization's Standards and conditions.
Level 2	Risk evaluation activities are regulated in Policies, Planning and/or Procedures. Details of risk evaluation are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk evaluation does not involve all parties involved. Risk evaluation implementers are internal organization teams (who have not received special training)	Risk handling activities are regulated in Policies, Planning and/or Procedures. Risk handling details are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk management does not involve all parties involved. Risk management executors are internal organization teams (who have not received special training)	Risk acceptance activities are regulated in Policies, Planning and / or Procedures. Roles and responsibilities are not clearly defined.	Monitoring and risk checking activities are regulated in Policies, Planning and / or Procedures. Details of monitoring and risk checking are in accordance with some clauses in the Standard. All roles and responsibilities are described, but still unclear and there are overlaps. Risk monitoring and inspection do not involve all parties involved. Implementers of risk monitoring and inspection are internal organizational teams (who have not received special training)
Level 1	Risk evaluation activities are not regulated in Policies, Planning and/or Procedures. Risk evaluation does not involve all parties involved. The risk evaluator is an internal team of organizations (who have not received special training).	Risk handling activities are not regulated in the Policy, Planning and/or Procedure. Risk management does not involve all parties involved. Risk management implementers are internal organization teams (who have not received special training).	Risk acceptance activities are not regulated in the Policy, Planning and / or Procedure.	Monitoring and risk checking activities are not regulated in Policies, Planning and / or Procedures. Risk monitoring and inspection do not involve all parties involved. Implementers of risk monitoring and inspection are internal organization teams (who have not received special training).

In general, the framework evaluation process consists of four steps, starting with the definition of an organizational profile, the collection and analysis of data, and finally the maturity profile of the presentation. In the early stages of defining an organization's profile, it helps determine the most suitable data collection method for targeted application. The next step is data collection, which the methods are: (1) Document analysis, (2) Interview, (3) Questionnaire, or (4) Material review [19, 20]. Methods (1) and (2) are the two main data collection methods for obtaining evidence. Methods (3) and (4) are necessary when the organization is highly complex and high risks are expected in the IT arena. The resulting data is processed into a worksheet that contains the results of data evaluation, data manipulation and data processing in the basic form as shown graphically in the Fig. 3.

$$\text{Maturity Level} = (\sum \text{Area Score}) \times 1.25 \quad (1)$$

$$\text{Area Score} = (\sum \text{Actual Score}) / (\text{Maximum Score})$$

$$\text{Maximum Score} = (\sum \text{Elements}) \times 5$$

The result at this phase is related to the maturity of the PDCA cycle. These values also indicate the plane position (1-5) and its properties. In addition to the PDCA cycle maturity model, data processing can also explain the status of each component in each region. These results form the basis of the merit assessment of each component. The final step is to prepare a PDCA cycle maturity profile for the organization. This profile consists of at least: (1) Maturity model, (2) Maturity evaluation of each component, (3) Evaluation of conclusions and recommendations.

AREA	ID	DOMAIN	ID	SUBDOMAIN	ID	ELEMENT	ID	CRITERIA					EVIDENCE	ACTUAL SCORE
								1	2	3	4	5		
PLAN														
DO														
CHECK														
ACT														
												SCORE		
												MAXIMUM SCORE		
												AREA SCORE		

Fig. 3. Working Paper.

V. CASE STUDY

The organization's overview involves services with offices in multiple cities with more than 1000 employees, information technology (IT) helps supporting basic business and IT departments with the employees at around 30 to 60 people. The data was collected using interviews and document analysis, which is obtained through storage process using the analytical methods described in the previous section. The interview was conducted with an IT risk manager with the material used was the material described in the worksheet and clarified with the reference document for evaluation. The analysis performed on the referenced document was directly related to IT risk management as they are complementary methods. A list of included documents can be stated such as MRTI/20xx policy, MRTI/20xx appendix policy, asset registration software, hardware asset registration, movable property registration, asset data or information record. The evaluation results consist of (a) PDCA cycle maturity, (2) maturity evaluation of each component, and (3) conclusions and recommendations. Organizational policies are forward-looking policies, based on strong evidence of what the organization can achieve, and that promote a consistent approach to health and safety at all levels of the organization. Therefore, organizational leaders promote a consistent approach to health and safety and setting the transition or transmitting the clear directives that shape daily activities. It also works continuously at all levels of the organization, promotes the values, ethics and culture needed to achieve the goals of the organization, and transforms the leadership style for the entire organization rather than transactional [38]. The result for case study can be seen in Table VII for the maturity assessment.

ERM should be viewed as an evolutionary process within an organization. This is often considered a compliance driven exercise that is achieved, documented and presented while it is doubtful at certain situation whether much value can be extracted from this type of effort [39]. Solving cost and skill problems in the evaluation process also motivates the organization to provide correct answers, and to show robust results in all real-world ways [40]. Aligning the IT investments with ever-changing business goals and priorities remains a major challenge for IT managers. Despite management's efforts to improve project success, an unacceptable number of IT initiatives cannot reach specific goals and target, or simply do not reach the objective in full. There is no end to the various factors that can contribute to the failure of the project. As a result, IT organizations have invested significantly in improving output predictability, productivity, and quality. Techniques such as estimation, risk assessment, process management, delivery management, and project management improve project implementation, but they cannot address the more important issues of investment selection and improving IT performance [41].

As can be seen in Fig. 4 to 7, each code of element and heatmap are distributed to plan, do, check and act realm. The resulting heat map can also be used to inform senior management, audit committees and councils of risk assessment. By having iterative design and management methods used in the business, it can support for continuous control and improvement of processes and products. Basically,

the two frameworks in this study cannot be compared with the difference in maturity model for reference. However, the framework proposed in this study includes several aspects that may complement the missing aspects of the current model such as the representation, measurement, method, and presentation of evaluation results as the conclusion. It is important to keep the results anonymous in certain timeframe to ensure that community or governments are not influenced by the use of the maturity model due to concerns about outside perceptions, and its primary purpose as a self-assessment tool to inform the future strategies as well as to promote the attempt to assess the process quality within the organization [37]. Historically, organizations have sought to improve project visibility by compiling schedules, budgets, progress, and spending information from detail-oriented project management tools or enterprise risk management systems.

TABLE VII. MATURITY PROFILE OF IT RISK MANAGEMENT PROCESS

AREA	AREA SCORE
PLAN	0.65926
DO	0.45
CHECK	0.52727
ACT	0.6
MATURITY OF THE PDCA CYCLE	2.79566



Fig. 4. Case Study: Area PLAN Evaluation.

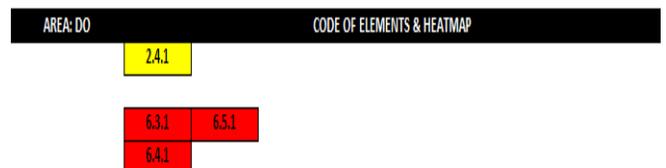


Fig. 5. Case Study: Area DO Evaluation.

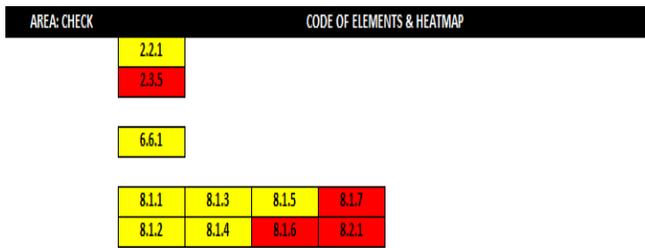


Fig. 6. Case Study: Area CHECK Evaluation.



Fig. 7. Case Study: Area ACT Evaluation.

To be successful, all projects must be planned in detail and updated in a consistent and reliable manner. This is a rare case, and the resulting collected data is often inaccurate, outdated and misleading [41]. It should be noted that PDCA cycle in IT Risk Management (ISO/IEC 27005) could not be separated from the company's overall risk management [42]. In addition, clients and organizations often misunderstand responsibilities and rights in business functions, processes, and levels. Thus, it is necessary for professionals to think about how to formulate the rules governing the collection and distribution of information; also, information system specifications and requirements for developers and administrators. Therefore, to improve the effectiveness of stakeholder interactions and communication, many related factors such as human beings, environment, culture, language, literacy, and organization have to be taken into account [43], [44], [45]. Interestingly, by leveraging the creativity and entrepreneurial spirit of employees and managers, it should depend on the ability of the organization to create favorable conditions for potential entrepreneurial to emerge in the proper way that align with context and trend within the environment [46], [47], [48]. In the end, the most effective risk functions have gained strategic influence within the organization and are empowered to invest in the overall development of task and role responsibilities [49], [50].

## VI. CONCLUSION

The unexpected framework recommends establishing the appropriate alignment between the ERM design parameters called ERM Mix or Modified with contingent variables in order to achieve organizational effectiveness. These type of ERM includes specific roles for risk identification processes, frequency of risk meetings, risk tools, risk functions, then, contingent variables as the types of risks that refer to preventable organizational and industry variables, parameters, strategy or external domain. Finally, it must also be understood that it is impractical to expect an ERM process to develop into this mature state in a relatively short period of time. Interestingly, it can be implemented shortly if the organization want to concentrate or focusing in assessing certain aspects only such as risk treatment and risk acceptance by utilizing

context establishment. Several sample companies have integrated ERM software for some time and the process still ongoing especially to improve the quality. On the other hand, the ERM process should continually update existing risk inventories and reviewing probability and impact assessments to ensure that significant and potentially catastrophic risks are not overlooked. To ensure that this ERM approach becomes dominant within the company, both the Board of Directors and the CEO explicitly agree on the ERM efforts, and elements of the mature ERM process described by the framework reported with the ERM staff as it is also essential to have sufficient resources available to fully achieve the implementation. As this modified framework has been used in case study, it is expected to be evaluated further in different context and perspective of diverse case study to strengthen and advance the proposed framework.

## REFERENCES

- [1] L. Dubsky. Assessing Security Controls: Keystone of the Risk Management Framework. *ISACA Journal* 6, 2016.
- [2] L. Grane, G. Gantz, S. Isaacs, D. Jose and R. Sharp. *Introduction to Risk Management: Understanding Agricultural Risk*. 2<sup>nd</sup> Edition, Extension Risk Management Education and Risk Management Agency, 2013.
- [3] ISO. *Risk Management ISO 31000*. International Organization for Standardization, February 2018.
- [4] C.J. Alberts and A.J. Dorofee. *Risk Management Framework*. Software Engineering Institute, Technical Report, August 2010.
- [5] J. Harvey. *Introduction to managing risk. Topic Gateway series no. 28*. The Chartered Institute of Management Accountant, 2007.
- [6] P.M. Collier and S. Agyei-Ampomah. *Management accounting: risk and control strategy*. Oxford: Elsevier. (CIMA Official Study System), 2006.
- [7] ITGI. *IG Measurement Tools*. Information Technology Governance Institute, 2005.
- [8] ITGI. *Information Risks: Whose Business Are They?* IT Governance Institute, 2005.
- [9] ITGI. *COBIT 4.0/COBIT 4.1*. Information Technology Governance Institute, 2005/2007.
- [10] ITGI. *Enterprise Risk: Identify, Govern and Manage IT Risk*. The Risk IT Framework Exposure Draft. 2009.
- [11] M. Jagusiak-Kocik. PDCA Cycle as a Part of Continuous Improvement in the Production Company – A Case Study. *Production Engineering Archives* 14, pp. 19-22, 2017.
- [12] E. Jordan and L. Silcock. *Beating IT Risks*. John Wiley & Sons, England., 2005.
- [13] Symantec. *IT Risk Management Report Volume 2*. White Paper 2008.
- [14] T. Abram. The Hidden Values of IT Risk Management. *ISACA Journal*, 2, 2009.
- [15] NIST. *Risk Management Guide for Information Technology Systems – Recommendations of the NIST*. SP 800-30, USA, 2002.
- [16] AIRMIC - ALARM - IRM. *Risk Management Standard*. 2002.
- [17] ISO/IEC. 27001:2005 – 27002:2005 – 27005:2008.
- [18] M. Sokovic, D. Pavletic, K.K. Pipan. Quality Improvement Methodologies – PDCA Cycle, RADAR Matrix, DMAIC and DFSS. *Journal of Achievement in Materials and Manufacturing Engineering*, vol. 43(1), pp. 476-483, 2010.
- [19] D. Proenca, J. Estevens, R. Vieira and J. Borbinha. Risk Management: A Maturity Model Based on ISO 31000. *IEEE 19<sup>th</sup> Conf. on Business Informatics* 2017.
- [20] D. Proenca, R. Vieira and J. Borbinha. *A Maturity Model for Information Governance*. In book: Research and Advanced Technology for Digital Libraries. Springer International Publishing, September 2016.
- [21] D. Proenca and J. Borbinha. Maturity Assessment of TOGAF ADM using Enterprise Architecture Model Analysis and Description Logics. In book: Advances in Enterprise Engineering XIII, 2020.

- [22] D. Proenca and J. Borbinha. Maturity Models for Information Systems – A State of the Art. *Procedia Computer Science* 100, 1042-1049, 2016.
- [23] T. Cooke-Davies and A. Arzymanowc. The maturity of project management in different industries: An investigation into variations between project management models. *International Journal of Project Management*, Vol. 21, No 6, pp. 471-478. 2003.
- [24] M. Koshgoftar and O. Osman. Comparison between maturity models. *2nd IEEE International Conference on Computer Science and Information Technology*, Vol. 5, pp. 297-301. 2009.
- [25] M. Wiczorek-Kosmala. Risk Management Practices from Risk Maturity Models Perspective. *J. for East European Management Studies* 19(2), 133-159, 2014.
- [26] H.Y. Ching and T.M. Colombo. Enterprise Risk Management Good Practices and Proposal of Conceptual Framework. *J. of Management Research* 6(6/3), 69-85, 2015.
- [27] E. Kerraous. A literature review of the factors that influence the adoption of an Enterprise Risk Management's process. *Revue Internationale des Sciences de Gestion* 6(3/1), 774-798, 2020.
- [28] A.R. Ahlan, M. Lubis, A.R. Lubis. Information Security Awareness at the Knowledge-based Institution: Its Antecedents and Measures. *Procedia Computer Science*. 72: 361-373, 2015.
- [29] Y. Aleisa. Factors affecting implementation of enterprise risk management: an exploratory study among Saudi organizations. *J. of Economics, Business and Management* 6(1), 2018.
- [30] A. Mikes and R. S. Kaplan. Towards a contingency theory of enterprise risk. *Working Paper* 13-063, Harvard Business School, 2014.
- [31] S. Soltanzadeh, S.Z.A. Rasid, N. Golshan, F. Quoquab and R. Basiruddin. Enterprise Risk Management Practices Among Malaysian Firms. *Procedia – Social and Behavioral Sciences* 164, 2015.
- [32] A.P. Liebenberg, and R.E. Hoyt. The determinants of enterprise risk management: Evidence from the appointment of chief risk officers. *Risk Management and Insurance Review*, 6(1), 37-52, 2003.
- [33] M.S. Beasley, R. Clune and D.R. Hermanson. Enterprise risk management: An empirical analysis of factors associated with the extent of implementation. *Journal of Accounting and Public Policy*, 24(6), 521-531, 2005.
- [34] M.M. Harner. *Barriers to effective risk management*. Seton Hall L. Rev., 40, 1323, 2010.
- [35] M. Aleksandrova, N. Sergeeva, L. Zakharova, E. Okolelova and M. Shibaeva. Formation of a portfolio of innovation projects based on management of their life cycle parameters. *MATEC Web of Conf.* 265(80-1), 07033, 2019.
- [36] S.M.S. Danish, M. Ahmadi, M.S.S. Danish, P. Mandal, A. Yona and T. Senjyu. A Coherent Strategy for Peak Load Shaving using Energy Storage Systems. *Journal of Energy Storage* 32, 101823, 2020.
- [37] OECD. *Enterprise Risk Management Maturity Model*. Forum on Tax Administration, Model Series, 2021.
- [38] N. Anderson. Risk Management Maturity Model. *White Paper*, Strategic Risk and Competence Team, 2017.
- [39] CGMA. How to evaluate enterprise risk management maturity: case study. *White Paper*, 2012.
- [40] B. Monda and M. Giorgino. An Enterprise Risk Management Maturity Model. *Munich Personal RePEc Archive* 45421, 2013.
- [41] J. Miller. *A proven project portfolio management process*. Project Management Institute Annual Seminars & Symposium, 2002.
- [42] R. Fauzi, S.H. Supangkat and M. Lubis. *The PDCA Cycle of ISO/IEC 27005:2008 Maturity Assessment Framework*. In book: User Science and Engineering, Springer, 2018.
- [43] Rosmaini, E., Kusumasari, T.F., Lubis, M., Lubis, A.R.: Insights to develop privacy policy for organization in Indonesia. *J. Phys.: Conf. Ser.* 978(1), 012042, 2018.
- [44] M. Lubis and A.H. Azizah. *Towards Achieving the Efficiency in Zakat Management System: Interaction Design for Optimization in Indonesia*. In book: User Science and Engineering, Springer, 2018.
- [45] G. Elia and A. Margherita. Assessing the maturity of crowventuring for corporate entrepreneurship. *Business Horizons* 61(2), 271-283, 2018.
- [46] M. Sokovic, D. Pavletic, K.K. Pipan. Quality Improvement Methodologies – PDCA Cycle, RADAR Matrix, DMAIC and DFSS. *Journal of Achievement in Materials and Manufacturing Engineering*, vol. 43(1), pp. 476-483, 2010.
- [47] The IACCM. Organizational Maturity in Business Risk Management. RM Working Group, 2003.
- [48] R. Fauzi, S.H. Supangkat and M. Lubis. The PDCA Cycle of ISO/IEC 27005:2008 Maturity Assessment Framework. *Communications in Computer and Information Science*, 2018.
- [49] T. Abram. The Hidden Values of IT Risk Management. *ISACA Journal*, 2, 2009.
- [50] A.R. Ahlan, M. Lubis, A.R. Lubis. Information Security Awareness at the Knowledge-based Institution: Its Antecedents and Measures. *Procedia Computer Science*. 72: 361-373, 2015.

# Using Eye Tracking Approach in Analyzing Social Network Site Area of Interest for Consumers' Decision Making in Social Commerce

Suaini Binti Sura<sup>1</sup>, Nona M. Nistah<sup>2</sup>, Sungwon Lee<sup>3</sup>, Daimler Benz Alebaba<sup>4</sup>

Faculty of Computing and Informatics, Universiti Malaysia Sabah, Sabah, Malaysia<sup>1,2,4</sup>  
Department of Convergence Software, Kyungmin University, Gyeonggi-do, South Korea<sup>3</sup>

**Abstract**—The growing popularity of social network site (SNS) in social commerce (s-commerce) has intensified interest in understanding consumers decision making based on the SNS seller generated content (SGC) and user generated content (UGC). This study examines consumers' decision making while doing online shopping by analyzing both SNS's seller-user generated content on SNS utilizing eye tracking approach. Based on eye tracking experimental with 50 participants, gaze map in term of fixation time were collected and analyzed to measure the order of identified Area of interest (AOI) by which consumer viewed and heat map to measure the consumer intensity when looking at the identified AOIs. The results identify that SCG is most important AOI compare to UGC and that product image and description receive the greatest attention from consumers when making decision. Furthermore, seller information serves as a key entry point for SNS-based commerce based on fixation time. The analysis result shows that there is no significant influence of AOIs order based on consumers' viewed on the intensity which consumers look at the AOIs. The comparison between Facebook and Instagram reveals some substantial differences in mean between AOIs based on fixation time and intensity. The findings suggest several AOIs should be addressed and emphasized for sellers and companies who interested in utilizing SNS for their s-commerce strategy.

**Keywords**—Eye tracking; SNS-based commerce; seller generated content; user generated content; social commerce

## I. INTRODUCTION

The emergence of social media has facilitated the new way of conducting online commerce, whereby rather than doing commerce (sell and buy), it allows users to socialize and build virtual community to generate better information in order to support their decision on commerce activities [1, 2]. This new way of conducting online commerce is known as social commerce (s-commerce). In other words, s-commerce refers to any commerce activities conducted through web 2.0 tools and social media in consumers' online shopping process includes the interaction between business with their customers (B2C), and customer with other customers (C2C) [2]. The concept of interaction and socialization among s-commerce's consumers empowers the e-WOM creates user generated data (UGC), another source of information required both business and consumer in doing their social commerce decision [2, 3, 4].

Social network site (SNS) (i.e. Facebook, and Instagram) is the most popular platform among social media user. Initially

SNS was created to build virtual network communities so that user can communicate and share experience, idea, information and common interest as in real-life connection [5]. The increase users of SNS, has boosted the use of SNS as s-commerce platform. In the context of s-commerce, SNSs a widely support both B2C and C2C commerce model. For B2C, a company creates it's an own SNS account or page to promote and sell their products or services and usually it is linked to company's website. Company has also taken an opportunity to join SNS marketplace and commerce or retail group. As for C2C, SNS marketplace and group (based on common interest) is the best choice to sell and promote the products and services. This kind of SNS is assisting consumer by offering seller or marketer or produce generated content (SGC) such as product or service and seller information, consumer experience and other s-commerce constructs generated from e-WOM based on reviews, ratings, likes, shares, comments and recommendations [5, 6, 7]. The widely use of SNS for online commerce can be seen through the report by [8] claiming that, in case of Malaysia, 26 million Internet users access to SNS and 41% of Malaysian use SNS as source of new brand discovery and inspiration for their purchases decision. Therefore in this study, we refer SNS based-commerce as the use of SNS platform for online commerce activities in order to support s-commerce activities.

The increase use of SNS as s-commerce platform has motivated researchers to investigate this phenomenon, particularly the SNS consumers' behavior toward s-commerce decision. Understanding customers' behavior is essential for both business and customer. SNS as source for commercial information and social exchange enrich consumer s-commerce decision that lead to higher positive perception of the consumers to the SNS, products and services, resulting increase in volumes of sales, customer loyalty and decreased costs [6, 9]. In another words, it helps business to plan its s-commerce strategy as well as marketing strategy [1, 9].

Previous studies indicated the website consumers' behavior is not only affected by the content itself but also the design of website, and position on screen is a critical, particularly in influencing consumer decision-making [7, 9, 10]. In studying of consumers' behavior related to website design and position on screen, eye tracking is one of the methods used by researchers. Eye tracking tool is used to collect the fixation data based on consumers' gaze on certain area known of area of interest (AOI) [11, 12]. Eye-tracking technique is always

---

This work was supported by Universiti Malaysia Sabah (SLB0160)

used because researchers believe what a person looking at indicates that a person currently is thinking about or attending to and it leads to purchase decision [13, 14]. Thus, investigating purchase decision related to website design gain mass attentions from researchers. For example, Hwang & Lee [15], Chae & Lee [16], Huddleston et al.[17], Maslowska et al [18], and Cortins et al. [19] conducted eye tracking study on AOIs of SGC e-commerce website. Huang & Kuo [20], Wang et al. [21] and Pavani et al [22] conducted eye tracking study on information presentation, navigation and complexity level and task of e-commerce website. Menon et al. [23], Mikalef et al. [24, 25] and Kumar et al. [26] conducted eye tracking study on the s-commerce context. All studies showed the significant finding of eye-tracking data associate with consumers' purchase decision.

In the context of s-commerce website, the design and position highlight two main components: SGC and UGC from e-WOM among consumers, and these explain the main difference between e-commerce and s-commerce. S-commerce focuses on support of social connection during commerce activity, meanwhile e-commerce focuses on product information and features by seller, and personalized shopping experience [6].The emergence of Web 2.0 technology has triggered the evolution of s-commerce platforms and each platform has its own unique function and design to support s-commerce. For instant, SNS mainly known for its' social connection, with more unstructured data sources, limited design for information space and features in facilitating s-commerce activities, is difference from s-commerce website which is primarily created for the aim business goal, therefore has less unstructured data source and more business features (i.e. shopping cart, ordering) [3, 6].

Despite of significant finding of eye-tracking study related to consumers' purchase decision in the context of e-commerce, there are limited study using eye-tracking approach in the context s-commerce particularly the SNS platform. To date, limited studies related to s-commerce can be found especially on SNS platform. In addition, majority of studies gave most focus on UGC components and less on SGC components as well as the combination of the components. Given 1) the increase popularity of eye tracking method in research related to decision making, 2) the limited amount of empirical researches that has employed eye tracking to examine SNS consumer decision making especially examining both SGC and UGC, and 3) the differences between s-commerce website and SNS, have motivated us to conduct this study. Our purpose of conducting this study is to investigate s-commerce consumers' decision making by analyzing SNS (i.e., Facebook and Instagram) AOIs using eye tracking approach, so that we could propose the most important AOI for SNS based-commerce which has ability to affect consumers' decision making. Therefore, we pose these research questions:

- What are the most important AOI for SNS-based commerce based on gaze maps and heat maps?
- Is there any difference on how SNS consumers perceived AOIs based on the gaze maps and heat maps?
- Is there any different of gaze maps and heat maps between Facebook and Instagram?

In this study, we divide the Facebook and Instagram page to targeted AOIs by considering the SNS layout. We used gaze map of fixation time to investigate the order by which SNS consumers viewed the AOIs and heat map to investigate the intensity of SNS consumers look at the each AOI [11, 12].

This rest of the paper is organized as follows: Section 2 discusses background and related literature on s-commerce decision and the use of eye-tracking in analyzing SNS. Section 3 details the research methodological design. Section 4 presents the results. Section 5 discusses the finding and implication of the finding on theory and practice. Last, Section 6 is conclusion emphasizes the purpose of the research and explains the limitation and recommendation of further study.

## II. BACKGROUND AND RELATED LITERATURE

### A. S-commerce Decision

S-commerce refers to commerce activities conducted using the social media platform that support social interaction activities and formation of UGC through consumers participations in the buying and selling products or services in online environment settings [4, 10]. Thus, social platform supports reviews, ratings, online communities and recommendations) about the products/services enhance the s-commerce [7]. The increase popularity of social media usage in s-commerce has attracted many researchers to discover how the social platform shaping the consumer behavior due to the fact understanding consumer behavior particularly, consumer decision making in s-commerce is important for planning a new marketing strategy as well as revise the existing strategy, so that it is oriented to particular market audience directly increase the sale [9]. The five stages model of consumer decision making highlights purchase decision is one of the important process and it is commonly accepted and the decision is not only supported by the content offered by the seller but also UGC formation by customers participation [10, 27].

In the s-commerce, seller quality and product quality play important role in determining consumer purchase decision quality, and product type can moderate almost all the association [28]. Social constructs consist of forum and communities, reviews and rating, and recommendations, which are the source of UGC were found out have significant influence on consumers' purchase decision making [28, 29]. In addition, SNS platform influences consumers' decision making in s-commerce [27]. Huang and Benyoucef [10] investigated the effect of social commerce design factors on the consumer decision and claimed that website or webpage design has considerable effect on consumer behavior. Specifically, web design includes the layout and content are significantly influence consumer purchase decision. Nevertheless, for SNS, the essence of the content design is its UGC [23, 26]. These contents are organized in specific area in SNS page and eye tracking approach always used in order to examine the area [11, 12] because eye tracking is one of the process tracking method to determine consumer decision making due to the fact eye movement and gaze can reflect human thought in decision making [20,21].

### B. Eye Tracking and SNS based- commerce AOI

In recent years, eye tracking approach is widely used in website design studies. Eye tracking used to observe consumer cognitive process to investigate how specific visual features in webpage influence the eye gaze and movement which directly indicate that a person is currently thinking or attending to can lead to a better understand of decision making process [13, 18]. This suggest eye movement and gaze patterns are consistent with pattern predict by the decision adopted [12, 20]. Researchers have adopted eye-tracking approach to examine website design because of the two advantages. First, compare to other approaches particularly, questionnaire and interview, eye tracking eliminates the subjectivity of self-reporting data. Second, eye tracking capability captures user reaction to webpage and show the page part that captured most user attentions [21].

In process tracking study, eye movements capture the gaze maps and heat maps which are composed of fixation and saccades [11, 12, 30]. Gaze maps capture sequence of fixation in term of fixation i) duration which captures the duration of AOIs looked at, ii) frequency which measures how many time AOIs visited, and iii) time which tells the order by which users viewed the AOIs [12, 30]. However, heat maps measure the intensity of people look at the objects recognized as fixation intensities telling us the attention key point of website design [11, 31]. In the context of web design study, webpage grouped in to regions called AOI in various ways depend on website and research purpose. AOIs are categorized based on certain area (e.g., top, middle or bottom) or specific elements (e.g., logo, picture, description) [11, 20]. Eye-tracking tool is used in collecting fixation data based on the AOIs to measure user interest [12, 13]. In the s-commerce context, especially SNS-based commerce, AOIs specific elements are divided into two main parts, SGC consist areas which information provided by the seller, and UGC consist areas which information provided and supported by SNS-based commerce consumers [24, 25].

Eye-tracking studies in the e-commerce context focusing on SGC have shown SGC areas received significant higher attention. The higher level attention on SGC areas associate with human brand has significant influence with perceived purchase decision [16]. Based on fixation count, more attention on product image and description indicate consumers more likely to buy [17]. Based on Cortinas [19], heat maps data showed that product area consist of product name, image, price is likely grab more attention from consumers. For s-commerce platform, some eye tracking studies have investigated the consumer purchase decision based on both SGC and UGC AOIs have been conducted and yielded significant finding. The study found out that UGC areas moderate the effect fixation for SCG area based on fixation duration [15]. Nevertheless, fixation duration and heat maps showed that both UGC and SCG especially, image and description captures more consumers' attention. [18, 24], and fixation duration confirmed that consumer spend more attention to positive review [25]. However, lack studies have been undertaken through SNS-based commerce. Menon et al [23] and Kumar [26] have conducted eye tracking study by examining targeted area of Facebook but solely focusing on SGC AOIs. The results indicated fixation duration higher on price placement near

image [23] and heat maps showed the placement of the image of human face gets more consumers' intensity and attention [26].

From these literatures, we can conclude examining both SGC and UGC AOI using eye-tracking offered researchers a new unique insight to understand consumer's decision making. However, existing studies have not fully explored the impact both SGC and UGC on consumers' decision making in the context SNS-based commerce. Most studies either using eye tracking to analyze SGC or UGC areas. Thus, we took an opportunity to utilize eye tracking approach in examine both SCG and UGC area in the context SNS-based commerce. Our main challenge is to choose the measurement for our eye tracking assessment. Despite fixation duration has been used widely as a measurement, we used fixation time to capture the order by which users viewed the AOIs because we believe the visual hierarchies are important guide for consumer to find the entry point to the SNS page [11, 12]. Furthermore, longer duration fixation doesn't mean always positive attention, it may cause of confusion, for example consumers need time to digest the information that difficult to understand [11,30]. In addition we used heat maps to measure consumer intensity toward AOIs because it is efficiently more effective for web design [11,31].

## III. RESEARCH METHOD

### A. Subject and Design

50 participants consisted of staffs and students of Universiti Malaysia Sabah Labuan International Campus (UMSLIC) participated in the lab experiment. The participants were divided into two groups: Facebook and Instagram (25 participants for each group). The respondents' range was in age from 24 – 36 years old. All of the respondents have experience using SNS for online shopping. The selection of UMSLIC students and staffs as a sample is related to the research material whereby the material for the research is based on the existing Facebook page “Jualan Borong Barang Terpakai UMSKAL 2012” as SNS-based commerce platform. The main purpose of this page is to facilitate selling and buying of second hand product targeting UMSLIC community. For this research, a new Facebook and Instagram page as stimuli were created based on the existing page and calibrated it with eye-tracking device. Fixation time and intensity data were collected for further analysis.

### B. Material

The experimental design was based on two simulated SNS: Facebook and Instagram. To retain the nature looking of the existing SNS and the degree of realism, the primary traits and components are kept by retaining the seven AOIs' locations. The AOIs were divided into two main parts. The first part, SGC, consists of Seller profile and product information. Seller profile, which is AOI reflected the seller information, includes the SNS seller's account photo, profile, and name. By clicking the seller's photo and name, the SNS consumers are linked to the seller's SNS page. Product information comprises four AOIs: the product name, image, price, and description. The second part, UGC includes two AOIs, Likes and Comments, which allow the SNS consumers to express their thought and

feeling about the product or services. The arrangement of the AOIs follows the layout provided by the SNS itself. We included only three products from the same category for each SNS to limit time spent on the assignment and prejudice in product selection. The product was chosen based on the most popular searches in the existing SNS, which are printers and stationeries. As a result, we designated a printer for Facebook and stationery for Instagram.

### C. Procedure and Task

The study was conducted within two days, 50 UMSLIC staffs and students were participated in the lab experiment. The first day was for Facebook group consisted with 25 participants and the second day was for Instagram participant with 25 participants. Two days were required in conducting this experiment due to the size of computer lab. The experiment was conducted following three phases:

1) *Phase 1* – Respondents were needed to complete a basic questionnaire in order to obtain demographic information, online purchasing experience, and familiarity with SNS for online shopping. We give the respondent 5 minutes to complete the task.

2) *Phase 2* – Experiment execution: Respondents were briefed on the experiment prior to its execution. Respondents were informed that their browsing activity is recorded. Respondents were given 5 minutes to browse the SNS page without any intervention from the researcher. In this task, respondents were required to browse to search the product that they intended to buy.

3) *Phase 3* – Post-test questioning. Following the experiment, a basic interview was conducted to capture the respondent's answer to the product they intended to purchase.

### D. Method and Measurement

The experiment allowed the researcher to obtain eye tracking data. The data were based on gaze maps in term of fixation time and heat maps. For the analysis, the gaze maps and heat maps within the selected AOIs were counted in, therefore fixation outside AOIs treated as outliers [19]. The heat maps in term of fixation intensity were represented using the color. The dark color represented the highest level of fixation and light color represented the lowest level of fixation [21]. For analysis purpose, the heat maps color was coded to 5 scales from the scale 1 represented by the blue light color means the lowest level of fixation to scale 5 represented dark red representing the highest level degree of fixation.

Fixation time was used to measure the AOI order based on consumers' viewed. The fixation sequence was ordered from 1 to 7, with 1 being the AOI that the consumers viewed at first and 7 representing the AOIs that the consumers viewed at last. Descriptive statistic was used to analyze the fixation intensity and fixation time. The Independent Sample T-Test was used to compare the differences in mean of the fixation time and fixation intensity between Facebook and Instagram. The SPSS v21 programme was used to analyze the data.

## IV. RESULT

The eye tracking data from 44 participants were used for further data analysis, with 6 participants' eye-tracking data being omitted due to calibration issues. As a result, the total number of participants was 24 for Facebook and 20 for Instagram. The findings were organized in accordance with the research questions.

RQ1: What is the most important AOI for SNS-based commerce based on gaze maps and heat maps?

Table I and Table II present the descriptive statistic mean and standard deviation of heat maps and gaze maps fixation time. Table I, descriptive statistic mean and standard deviation measure the intensity of consumer look at the AOIs meaning that the highest number of mean implies the AOI receives the most intensity from the consumers and the lower number of mean implies the AOI receives the less intensity from the consumers. Therefor heat maps results indicate product image (Mean=4.59, SD =0.726) received most intensity, product description (Mean 3.18, SD= 1.514) received acceptable intensity, and both likes (Mean = 1.77, SD = .985) and comments (Mean = 1.77, SD = .459) received less intensity.

As shown in Table II, the descriptive statistic mean and standard deviation represent the fixation time, which measures the order of AOIs viewed by the consumers, beginning with the AOI viewed first and ending with the AOI viewed last. The AOI viewed first by the consumer is indicated by the lowest number of means, while the AOI viewed last by the consumer is shown by the largest number of means. Therefore the results indicate seller profile (Mean=1.59, SD =1.317) is the AOI the consumers viewed first and comments (Mean=6.55, SD= 1.130) is the AOI the consumers viewed last.

RQ2: Is there any difference on how SNS consumers perceived AOIs based on the gaze maps and heat maps?

TABLE I. HEAT MAP (FIXATION INTENSITY) ON AOIS RESULT

AOI	Mean	Std. Deviation
Seller profile	2.41	1.436
Product name	2.68	1.410
Product price	2.43	1.437
Product image	4.59	0.724
Product description	3.28	1.514
Like	1.77	0.985
Comment	1.77	0.459

TABLE II. GAZE MAP (FIXATION TIME) ON AOIS RESULT

AOI	Mean	Std. Deviation
Seller profile	1.59	1.317
Product name	3.30	1.193
Product price	4.05	1.099
Product image	3.16	1.817
Product description	4.91	1.309
Like	4.50	1.798
Comment	6.55	1.130

V. DISCUSSION

Table III shows the ranking of AOI from most important to least important for both heat maps and gaze maps (fixation time). It implies a significant difference in how SNS consumers perceive the seller profile. Based on heat maps, consumers regard the seller profile as a less important AOI (rank = 5), yet in the fixation time, the seller profiles (rank = 1) is the first AOI viewed by consumers, indicating that it is the most important AOI. The same is true for comments, which both the heat maps and the fixation time suggest as the less important AOIs.

We further investigated the relationship between gaze maps (fixation time) and heat maps, whether the order of viewed AOIs by consumers has an influence on the intensity which they look at the AOIs. Thus, result in Table IV, the regression coefficient results ( $\beta = -0.163$ ,  $t = -1.075$ ,  $p > 0.05$ ) show there is no significant influence of the gaze maps (fixation time) (AOI rank – viewed by consumer) on heat maps (the intensity of consumer look at AOIs).

RQ3: Is there any different of gaze maps fixation time and heat maps between Facebook and Instagram?

T-Test for equality of mean is used to compare the differences in gaze maps (fixation time) and heat maps between Facebook and Instagram. Based on heat maps data, Table V shows the differences between Facebook and Instagram. The results show there are significant difference on fixation intensity between Facebook and Instagram for product name ( $t = -4.581$ ,  $p < 0.001$ ), product price ( $t = -9.334$ ,  $p < 0.001$ ) product image ( $t = 10.870$ ,  $p < 0.001$ ), product description ( $t = -8.452$ ,  $p < 0.001$ ) and likes ( $t = 9.314$ ,  $p < 0.001$ ). But there is no significant difference for seller profile ( $t = -0.726$ ,  $p > 0.05$ ) and comments ( $t = -1.792$ ,  $p > 0.05$ ).

Table VI presents how Facebook and Instagram differ in terms of gaze maps (fixation time). The findings demonstrate that there is a substantial variation in the order in which SNS consumers viewed AOI on Facebook and Instagram for product description ( $t = 4.926$ ,  $p < 0.001$ ), but there is no statistically significant difference for others AOIs.

TABLE III. AOI RANK MOST CRUCIAL TO LESS CRUCIAL

AOI	Rank	
	Heat map	Gaze map (Fixation time)
Seller profile	5	1
Product name	3	3
Product price	4	4
Product image	1	2
Product description	2	6
Likes	6	5
Comments	6	7

TABLE IV. AOI RANK MOST CRUCIAL TO LESS CRUCIAL

AOI	Heat map		
	$\beta$	t	Sig.
Gaze map (Fixation time)	-.164	-1.075	.289

The findings reveal that SGC areas, particularly product image and description attracted greater attention from SNS-based commerce consumers as compare to UGC area in making purchase decision. This result is in accordance with the previous studies finding, largely have confirmed that SCG in term of product information namely, product name, image, price and description have significant influence on consumer decision making [16, 17, 19]. The most significant aspects of product information are the product image and description, which have the capacity to increase consumers’ trust and confident in the product [7, 17]. The results from gaze maps (fixation time) indicate that SCG of seller information is the first area visited by the consumers. We believe this result is related to SNS (i.e., Facebook and Instagram) page design specifically, the layout, in which seller information, including seller photo, profile, and name, is displayed at the top of the post. According to Huang and Benyoucef [10] website design is one of the consumers purchase decision determinants. However, the heat maps results show that seller information is the least important area among SCG, meaning that consumers place more emphasis on product information during the product search and purchasing process.

Although previous studies [24, 25] have argued SNS consumers give more focus and attention to UGC areas in making purchase decision, but it contradicts with our findings. This phenomenon can be explained based on (1) the role of UGC itself. In this study, SNS UGC comprises of likes and comments, which are considered as supplementary information that the seller does not supply. SNS consumers prioritize product information; but, if they are dissatisfied or uncertain with the information provided by the seller, or if they require extra clarification, they search it form of likes and comments as claimed by Hwang & Lee [15] and Maslowska et al. [18] UGC supports and moderates the product information for consumer conducting their decision making. (2) Limitation of SNS page design. SNS page design is different from s-commerce webpage. More social constructs for UGC to promote selling and buying activities can be found on s-commerce websites. S-commerce websites typically include rating and product recommendations features and these features are not available on SNS. Although the likes feature is accessible in SNS, it does not imply purchasing when compared to the rating function, which is generated after the purchase done.

TABLE V. T-TEST EQUALITY OF MEAN RESULT FOR HEAT MAP

AOI	t	df	Sig. (2-tailed)	Mean difference	Std. Error difference
Seller profile	0.726	40.41224.586	0.472	.292	0.402
Product name	4.581	30.662	0.000	1.367	0.273
Product price	9.334	31.66	0.000	1.750	0.187
Product Image	10.870	27.660	0.000	3.042	0.280
Product description	8.452	24.266	0.000	2.000	0.237
Likes	9.318	29.229	0.000	2.842	0.305
Comments	1.792		0.080	0.558	0.312

TABLE VI. T-TEST EQUALITY OF MEAN RESULT FOR GAZE MAP

AOI	t	df	Sig. (2-tailed)	Mean difference	Std. Error difference
Seller profile	0.038	41.718	0.969	0.017	0.429
Product name	1.016	41.949	0.316	0.425	0.419
Product price	0.350	41.679	0.728	1.50	0.429
Product Image	0.957	36.200	0.345	2.00	0.209
Product description	4.926	41.996	0.000	1.800	0.362
Likes	0.475	41.753	0.637	1.142	0.298
Comments	0.828	41.971	.0413	0.308	0.373

We analyzed whether the order of consumers viewed AOIs has significant effect on the intensity of consumer look at the AOIs. Our findings show that there is no significant effect of the order in which consumers viewed AOIs on the intensity with which they looked at the AOIs, suggesting that consumers' attention on SNS AOIs stems from their own context related to purchasing decision. Purchasing decision making is usually more linked to the material's content and the information consolidation of the products or services [19].

The results of the comparison between Facebook and Instagram show that there are some significant difference in mean on the intensity with which consumers look at product information namely, product name, price, image and description, and likes. We argue that the differences in the goals and features served by each SNS, as well as the manner in which sellers utilize the both SNS to provide information, are the main contributors to this findings. Facebook is mainly used to associate with individuals and brands, helping in enhancing brand by leveraging eWom [32]; however Instagram mainly used to share picture, video or other kind of media, and for each media usually followed by story [32]. Additionally, fixation time results which used to measure the order of AOIs indicate the significant different solely for product description. We believe that the differences in the layout of both SNS's webpages contribute to these findings. On Facebook, the product description displays first, followed by the product image, but it is other way round for Instagram.

The results of this study have important implications for both theory and practices. From a theoretical standpoint, most prior research in s-commerce [15, 23, 24, 25, and 26] adopted eye tracking approached to investigate consumers' decision making in utilization of both SGC and UGC. Despite of significant results of those studies, lack of research was undertaken through SNS platform in particularly examining the UGC components. Therefore, this study attempted to fill this gap by extending Mikalef et al [24] with adaption of SGC and UGC through SNS platform. Our findings pinpoint SGC receives more attention from consumers compare to UGC during performing their decision making. Surprisingly, it contradicts the purpose of the SNS which is promoting sociability, indicating while doing online shopping consumers generally focus on their goal which is to purchase. In addition, UGC which is most important to determine consumers' decision making in s-commerce does not in line with our findings. Thus, our study provides the enrichment to existing literature concerning consumers' decision making in s-commerce by highlighting both SGC and UGC in a new related setting called SNS-based commerce. From our findings, we

argue (1) the difference of s-commerce platform contributes to different features of UGC and indirectly viewed and perceived differently by consumers and (2) UGC plays a role as supportive, additional or alternative information will be referred by consumers if they unsatisfied or uncertain with product information provided by seller. Further study is needed to acquire better understanding of this occurrence.

From a practical viewpoint, the important of our findings generates insights for who are interested to utilize SNS-based commerce as individual sellers or as a company for s-commerce strategy. The results reveal product information especially image and description, grab the most of consumers' intensity and attention, indicating product image as key point of the SNS page. It suggests seller and company should focus on how to present their product image and description in order to grab consumers' attention. Company and seller should utilize any method or technique to highlight the product image. Providing additional support to highlight product image include zoom function, close-up or use of human (model) has proven to attract consumers' attention [16, 33]. The way in which product descriptions are presented should be emphasized so that they are able to attract consumers' attention; failure to do so will result in consumers diverting their attention to gain additional or alternative information from other sources such as product reviews, which is quite risky and may cause consumers to refrain from making purchases. Therefore, seller and company should provide detail information about the product because it has been proven from previous research asserted the good quality of product description means consumers more likely to buy. [17,18, 25] Although UGC (i.e., likes and comments) component is less important, it is not insignificant. Seller and company should continually monitor and response wisely. Furthermore, seller information is discovered as a critical key entry point for both Facebook and Instagram. As a result, clear and exact seller information is required in order to obtain consumer trust and confidence [17].

## VI. CONCLUSION

In summary, we present a study to investigate s-commerce consumers' decision making by analyzing SNS (i.e., Facebook and Instagram) AOIs using eye tracking approach. We used gaze maps (fixation time) to measure the order by which consumers viewed the AOIs and heat maps (fixation intensity) to measure the intensity of people look at the AOIs. In addition, we compared consumer decision-making on Facebook and Instagram based on gaze maps and heat maps data. The findings revealed that both fixation time and intensity suggest that the most important AOI for consumers during their decision making process is product image and the least important is comments. Our investigation showed that the gaze maps (fixation time) (the rank of AOI viewed by the consumer) has no significant effect on heat maps (the intensity of consumer look at AOIs). Furthermore, a comparison of Facebook and Instagram revealed there is significant difference in consumers' intensity on SCG of product information and UGC of like, as well as a significant difference in gaze maps (fixation time) on product description.

The first limitation is the generalizability of the research mainly sample respondents and SNS applications. The sample

responders consist only UMSLIC students and staffs, age between 22- 34 years old, do not overall picture the SNS user population particularly Malaysia. Therefore the future research, with more samples represents SNS-based commerce consumers population must be adopted to obtain better understanding on subject matters. Because of the popularity of these applications in Malaysia, this study focused mostly on Facebook and Instagram; however, with the advancement of technology and globalization, certain SNS, such as Tiktok and Pinterest, have begun to gain awareness. Each SNS has its own set of primary function criteria. Therefore, in future research, adopting this research to examine the AOIs of the identified SNS to highlight its' function and criteria. Second, current study focuses on gaze maps (fixation time) and heat maps. In the future study, the use of fixation count, frequency and duration will be needed to measure the degree of attention and focus on AOIs. Thus, comparison study can be conducted to provide deep understanding of SNS consumers' attention. Third, for each SNS, we placed three products in the same category, with the goal of making it easier for consumer to search within a limited time frame. However, this is not really represent the real setting of SNS consists more products from variety categories. For the future research, we explicitly recommend different products from different categories should be included to obtain deep understanding on how SNS user make decision based on product and category differentiation. Despite its limitation, we believe this study is still beneficial for company, business organization, and individuals who are interested in utilizing SNS as one of their s-commerce marketing strategies. For other researchers, this study offers fundamental understanding of consumers' attention on SNS page in context s-commerce as a foundation for future research in this field.

#### ACKNOWLEDGMENT

We acknowledge financial support for this research from the Universiti Malaysia Sabah: SLB0160.

#### REFERENCES

- [1] C. Wang and P. Zhang, The evolution of social commerce: the people, management, technology: and information dimensions. *Communications of the Association for Information Systems*, 2012, 31, 1-23.
- [2] X Lin, Li, Y. Li, & X. Wang, Social commerce research: Definition, research themes and the trends. *International Journal of Information Management*, 2017, 37(3), 190-201.
- [3] Q. Yan, S. Wu, L. Wang, P. Wu, H. Chen and G. Wei, E-WOM from e-commerce websites and social media: Which will consumers adopt?, *Electronic Commerce Research and Applications*, 2016, 17, 62-57.
- [4] Y. Wang and C. Yu, Social interaction-based consumer decision-making model in social commerce: The role of word of mouth and observational learning. *International Journal of Information Management*, 2017, 37(3), 179-189.
- [5] Z. Sheikh, L. Yezheng, T. Islam Z. Hamead & I.U. Khan, Impact of social commerce constructs and social support on social commerce intentions, *Information Technology & People*, 2019, 32(1), 68 – 93.
- [6] H. Han, H. Xu, & H. Chen, Social commerce: A systematic review and data synthesis. *Electronic Commerce Research and Applications*, 2018, 30, 38-50.
- [7] N. Hanjli, Social commerce constructs and consumer's intention to buy, *International Journal of Information Management*, 2015, 35, 183-191.
- [8] Kemp, Digital 2020: Global digital yearbook. Access from [wearesocial.com/special-reports/digital-in-2020](https://wearesocial.com/special-reports/digital-in-2020), 2020.
- [9] E. Mazurova, Exploratory analysis of the factors affecting consumer choice in e-commerce: Conjoint analysis, *Journal of Information Systems Engineering & Management*, 2017, 2(2), 12.
- [10] Z. Huang and M. Benyoucef, The effects of social commerce design on consumer purchase decision-making: An empirical study, *Electronic Commerce Research and Applications*, 2017, 25, 40-58.
- [11] S. Djamasbi, Eye tracking and web experience, *AIS Transaction on Human Computer Interaction*, 2014, 6(2), 37-54
- [12] B. T. Carter & S. G. Luke. Best practices in eye tracking research. *International Journal of Psychophysiology*, 2020, 155, 49-62.
- [13] S.F. Yang and H.H Lin, Effects of attribute framing varying with the elaboration in online shopping: An eye-tracking approach. In 2014 47th Hawaii International Conference on System Sciences, 2014, 3083-3092.
- [14] T. Friedrich, S. Schlauderer, and S. Overhage, The impact of social commerce feature richness on website stickiness through cognitive and affective factors: An experimental study, *Electronic Commerce Research and Applications*, 2019, 36, 100861.
- [15] Y.M. Hwang and K.C. Lee, How does Consumers' Emotion Affect Visual Attention Patterns in Online Shopping Environments? – Emphasis on Eye-Tracking Approach, *Recent Advance on Finance Science and Management*, 2015, 51-55.
- [16] S.W. Chae and K.C. Lee, Exploring the effect of the human brand on consumers' decision quality in online shopping: An eye-tracking approach, *Online Information Review*, 2013. 37(1), 83-100.
- [17] P. Huddleston, B.K. Behe, S. Minahan, and R. T. Fernandez, Seeking attention: an eye tracking study of in-store merchandise displays. *International Journal of Retail & Distribution Management*, 2015. 43(6), 561-574.
- [18] E. Maslowska, C.M. Segijn, K.A. Vakeel and V. Viswanathan, How consumers attend to online reviews: an eye-tracking and network analysis approach, *International Journal of Advertising*, 2020, 39:2, 282-306.
- [19] M. Cortinas, R. Cabeza, R. Chocarro, A. Villanueva, Attention to online channels across the path to purchase: An eye-tracking study, *Electronic Commerce Research and Applications*, 2019, 36, 100864.
- [20] Y.F. Huang and F.Y. Kuo, An eye - tracking investigation of internet consumers' decision deliberateness. *Internet Research*, 2011, 21(5), 541-561.
- [21] Q. Wang, S. Yang, M. Liu, Z. Cao and Q. Ma, An eye-tracking study of website complexity from cognitive load perspective, *Decision Support Systems*, 2014, 62, 1-10.
- [22] M. L. Pavani, A. B. Prakash, M.S. Koushik, J. Amudha, and C. Jyotsna, Navigation through eye-tracking for human-computer interface, *Information and Communication Technology for Intelligent Systems*, 2019, pp. 575-586.
- [23] R. V. Menon, V. Sigurdsson, N.M. Larsen, A. Fagerström, and G. R. Foxall, Consumer attention to price in social commerce: Eye tracking patterns in retail clothing. *Journal of Business Research*, 2016, 69(11), 5008-5013.
- [24] P. Mikalef, K. Sharma, I.O. Pappas, and M. N. Giannakos, Online reviews or marketer information? An eye-tracking study on social commerce consumers. In *Conference on e-Business, e-Services and e-Society*, 2017, 388-399.
- [25] P. Mikalef, K., Sharma, I.O. Pappas, and M. Giannakos. Seeking information on social commerce: An examination of the impact of user- and marketer-generated content through an eye-tracking study. *Information Systems Frontiers*, 2020, 1-14.
- [26] N. Kumar, V. Maheshwari, and J. Kumar, A comparative study of user experience in online social media branding web pages using eye tracker. In 2016 international conference on advances in human machine interaction (HMI), 2016, 1-6.
- [27] H. A. H Hettiarachchi, C. N. Wickramasinghe, and S. Ranathunga, The influence of social commerce on consumer decisions. *The International Technology Management Review*, 2018, 7(1), 47-58.
- [28] A. Chen, Y. Lu, and S. Gupta, Enhancing the decision quality through learning from the social commerce components. *Journal of Global Information Management (JGIM)*, 2017, 25(1), 66-91.

- [29] R. Shekhar and U.P. Jaidev, Antecedents of online purchase intention in the context of social commerce. *International Journal of Applied Management Science*, 2020, 12(1), 68-95.
- [30] P. Bera, P. Soffer & J. Parsons. Using eye tracking to expose cognitive processes in understanding conceptual models. *MIS Quarterly*, 2019, 43(4), 1105-1126.
- [31] T. Blascheck, K. Kurzhals, M. Raschke, M. Burch, D. Weiskopf & T. Ertl. Visualization of eye tracking data: A taxonomy and survey. In *Computer Graphics Forum*, 2017, 36(8),260-284.
- [32] D. Belanche, I. Cenjor, and A. Pérez-Rueda, Instagram Stories versus Facebook Wall: an advertising effectiveness analysis. *Spanish Journal of Marketing-ESIC*. 2019, 23(1), 69 – 93.
- [33] R. Boardman and H. McCormick, The impact of product presentation on decision-making and purchasing. *Qualitative Market Research: An International Journal*. 2019, 22(33), 365-380.

# Chatbot Design for a Healthy Life to Celiac Patients: A Study According to a New Behavior Change Model

Eythar Alghamdi<sup>1</sup>, Reem Alnanih<sup>2</sup>

Computer Sciences Department, Faculty of Computing and Information Technology<sup>1,2</sup>  
King Abdulaziz University, Jeddah, Saudi Arabia<sup>1,2</sup>  
University of Bisha, Bisha, Saudi Arabia<sup>1</sup>

**Abstract**—There is an absolute need for technology in our daily life that makes people busy with their smartphones all day long. In the healthcare field, mobile apps have been widely used for the treatment of many diseases. Most of these apps were designed without considering health behavior change models. Celiac disease is a significant public health problem worldwide. In Saudi Arabia, the incidence of celiac disease is 1.5%. Celiac patients have a natural demand for resources to facilitate care and research; however, they have not received much attention in the field of healthcare apps. This study introduced a new health behavior change model based on the existing common models and adapted it to the use of technology for the changing behavior of celiac patients towards healthy suitable food. As proof of concept, the new model was applied to the WhatsApp chatbot for patients with celiac disease. To test the impact of the chatbot, 60 Saudi celiac patients participated in three steps. First, they completed a pre-test questionnaire. Then, the participants were divided into two groups: the control group, which was left without any intervention, and the test group, who used the chatbot for 90 days. Finally, all participants completed the post-test questionnaire. The results confirmed a significant statistical difference between both groups, and the test group improved their healthy life in terms of eating habits, reduced celiac symptoms, and commitment to the treatment plan.

**Keywords**—Celiac disease; health behavior changes models; healthcare apps; user-centered design; experiment test; WhatsApp chatbot

## I. INTRODUCTION

There is an absolute need for technology in daily life. Everyone is dependent on technology to the point that we cannot stay without it; starting from communicating with others and ending monitoring of health. One of the most popular technologies worldwide is mobile, and the number of people around the world who use mobile in 2021 is 5.27 billion users, accounting for 66.85% of the total global population, every one of them spends an average of 145 minutes daily online [1][2]. In addition, statistics show that mobile users in the United State rely on their mobile devices to make decisions about many things, such as making decisions about purchasing a product, choosing a place to live, or choosing daily activities [3].

In the healthcare field, mobile apps have been used widely for many diseases, such as atrial fibrillation and diabetes. It has

also been used to control or change unhealthy behaviors, such as smoking and alcohol drinking [4-7]. Most healthcare apps aim to monitor patients' behaviors and follow their improvement [8]. On one hand, most of these apps were designed without considering the health behavior change models such as the health belief model (HBM), theory of planned behavior (TPB), diffusion of innovation theory (DOI), social norms theory (SNT), and transtheoretical model (TTM) [8]. This cast doubts their effectiveness in controlling user behavior or changing it [9]. On the other hand, a few apps are based on one of the health behavior change models, but some studies have proven that they are ineffective in avoiding relapse and because there are many flaws in these models [9].

Health apps depend on the user to enter most of the data, and if the user does not commit to using them daily by entering the required data, it may become useless. A study has proven that the more apps on the mobile device, the less the user uses them [10]. This means that if a mobile user has 20 apps on his mobile device, he uses approximately 8-10 of them actually. In addition, some statistics showed that mobile users use social networks more than other apps, spend half of the mobile use time on it, and they use it daily and for extended hours.

A social network service is an online platform that people use to build social relations with other people by sharing their interests. WhatsApp is the most used social network globally, with 1.5 billion monthly active users [10]. WhatsApp allows the user to communicate with other users using writing messages, voice notes, voice calls, and video calls through simple encrypted interfaces. WhatsApp also supports the conversational system, which is a computer system intended to converse with a human in a manner similar to a human using writing, speaking, or gesturing. The conversational system actions are based on user inputs using both short-and long-term user knowledge [11]. The chatbot is a conversational system supported by WhatsApp. Chatbots have been widely used in customer service. In the field of health, chatbots are used on a small scale to spread health information, deny rumors, and correct false information [12, 13].

Celiac disease is a significant public health problem worldwide. It is an autoimmune enteropathy resulting from the interplay between environmental and genetic factors, which is affected by eating gluten-containing grains [14]. The current worldwide prevalence of celiac disease is between 0.7% and

1.4%, and it affects women more than men and children more than adults [15]. In Saudi Arabia, the incidence of celiac disease in adults and children is 1.5%, which is at least twice the average prevalence rate in Europe and North America [16, 17]. Although it is a high rate, there is a study that confirmed that the incidence of celiac disease in Saudi Arabia is higher than 1.5% and reaches 2.7% [18]. However, celiac patients have not received much attention in the field of healthcare apps; rather, they rely heavily on nutrition apps, and only 5% of specialists use social networks, websites, and nutrition apps to educate celiac patients [19, 20]. In contrast, celiac patients have a natural demand for web-based resources to facilitate care and research, especially on mobile devices [21].

Therefore, this paper aims to take the benefit of user experience toward using social media but, instead of taking this user experience randomly, we take it based on a scientific model. All this is motivated by the human sense to improve the life quality of celiac patients since the potential benefits of the proposed solution are painless and easy life for them. This paper focuses on the problem from two perspectives, as follows:

- The user's perspective: The user uses many apps in order to change his/her health behavior, but a large number of apps on the mobile cause him to become distracted, which makes him gradually tend to quit using those apps. In addition, healthcare apps built based on one of the common health behaviors change models are negatively affected by their limitations. Therefore, it would be better to design a model that avoids the limitations of common models and benefits from the apps that the user already uses to change behavior.
- Developer's perspective: The developer wants to develop an app that achieves widespread and supports the sustainability of continuous use by users, especially if its target changes behavior. It has been noticed that social networks are the most used mobile apps. Therefore, it would be better to use social networks to change healthy behaviors rather than developing a new mobile app.

In this paper, the authors proposed a new health behavior change model that can be adapted to the technology. The proposed model is based on common health behavior change models in terms of the defined criteria of objectives for using each one, method of implementation, duration of implementation, advantages, and disadvantages. As a proof of concept, the proposed model was applied to the chatbot through WhatsApp. The chatbot is designed for celiac patients as a scope of the research, and gamification is used as an engagement boost tool. This study's main contributions are the new health behavior change model and the benefit of social media in behavior change. The implications of these contributions are to the creation of a health behavior change model that avoids the shortcomings of existing models. Also, taking advantage of the long hours that users spend using social media.

The proposed design was empirically tested with 60 celiac patients divided into two groups for three months (90 days)

based on a study that proved that celiac patients' condition could improve from one month to six months [22, 23].

The rest of the paper is organized as follows: The second section contains the literature review, and the third section provides the data collection and analysis. The fourth section explains the proposed model, and the fifth section shows the prototyping and design phases. The sixth section presents the details of the experimental design, the seventh section discusses the results, and the eighth section concludes the paper.

## II. LITERATURE REVIEW

This section divides the literature review into several subsections in terms of the health behaviors change models, their applications in the healthcare field, mobile health apps, WhatsApp and chatbot, and the methods used to collect and analyze the data.

### A. Health Behavior Change Models

Social and behavioral sciences researchers have invented different models to change people's behavior in the health field. The most common models are the HBM, TPB, DOI, TTM, and SNT [24-28].

Although these models have some advantages, they have many disadvantages: for example, HBM works only with a fatal disease [24], TPB is based on motivation and ability [25], DOI works better with the adoption of behaviors rather than cessation or prevention of behaviors [26], SNT focuses only on social influences and their impact on an individual's behavior [28], while TTM operates on the assumption that taking years to change behaviors [27]. In addition, many of these models do not consider the maintenance of behavior, but rather focus on initiating behavior.

### B. Health Behavior Change Models Applications

To the best of our knowledge, no studies have explored the impact of the application of health behavior change models on celiac patients. One study [29] found that TPB was used to measure celiac patients' beliefs about a gluten-free diet. However, it did not measure the effect of TPB on patients with celiac disease in terms of health behavior change.

The authors in [30-33] used HBM in their studies. The authors in [30] targeted the asymptomatic hyperuricemia patients, but measured 5 of HBM constructs only, the follow-up was short, and participants were from one community. The authors in [31] targeted the obesity patients, but the sample was small because of the low response rate and data collection was from a single campus. The authors in [32] targeted the gestational diabetes patients, but there was a lack of related works on which the study relied, and they used self-reporting. The authors in [33] targeted the smokers, but gathering information was by self-reporting, the study relied on people's ability to remember past behaviors accurately, which cannot be trusted, and due to some legal, ethical, and social reasons in the study community, it is not possible to trust that the answers obtained were accurate.

The authors in [34-36] used TPB in their studies. The authors in [34] targeted the smokers, but the implementation

was in the tobacco belt, which may affect the reactions of the participants, and the study measured the smoking behaviors before the campaign only, it did not measure it after the campaign. The authors in [35] targeted the type two diabetes patients, but the study did not take the patient's diversity into account and the social desirability bias might affect the accuracy of the data. The authors in [36] targeted the cervical cancer patients, but the study did not employ an experimental design to establish the causal effect relations among variables.

The authors in [37-38] used DOI in their studies. The authors in [37] targeted the smokers, but the implementation relied mainly on community awareness in a community that accepts smoking and there was no monitor of participants to ensure adherence. Authors in [38] targeted the maternal and neonatal health, but the health systems problems, Infrastructure problems, and cultural constraints affected the study result.

The authors in [39-41] used TTM in their studies. The authors in [39] targeted the smokers, but the study did not use the blood tests to measure nicotine before and after the experiment, the study did not include all TTM stages, the sample was small, and the follow-up was short. Authors in [40] targeted the cardiovascular patients, but the intervention was based on individuals' readiness for behavioral changes, and it had not part in making them ready, and the post-test was not applied. Authors in [41] targeted the obesity patients, but gender was not considered as a mediating variable, and there was the sample loss during the study.

Finally, the authors in [42-44] used SNT in their studies. The authors in [42] targeted the smokers, but the study linked social norms and the use of tobacco products with a temporal relationship, which in turn changes and therefore it is not possible to establish the relationships between them. Authors in [43] targeted the type two diabetes patients, but there was a lack of real behavioral measurements, which limits the

generalization of these results. Authors in [44] targeted the people who eat junk food, but the follow-up was very short.

From our review and analysis of the methodologies that were used in previous studies, the aim of each model and the most appropriate case for its use became clear. Also, the shortcomings of each model were discovered. Table I describes the proposed new model compared to the other common models in terms of a set of criteria such as the number of processes, the healthcare domain, problem-solving issues, applying the technology, using social networks, taking advantage of social influences, and the ability of the model to work with behavior adoption, behavior prevention, and behavior maintenance.

C. Healthcare Mobile Apps

Based on the studies published in the field of health apps, it was noticed that many of those apps work based on one or more of the health behavior change models in order to track behavior [8]. The authors in [4] used SNT in their app and targeted the atrial Fibrillation disease patients, but a very small sample used the app (only 2 patients). Authors in [5] used TTM in their app and targeted the Type two diabetes patients, but it was limited to patients with high motivation to use a mobile app for self-management. Authors in [7] used SNT in their app and targeted the alcohol drinkers, but the sample was from rural and urban without consider the digital divide between them. Authors in [45] used TPB in their app and targeted the hospitalized smokers, but the sample size was relatively small, and the follow-up was short. Authors in [46] used DOI in their app and targeted the gestational diabetes mellitus patients, but the number of interviews was limited. Authors in [47] used TTM in their app and targeted the children with diabetes, but the app did not include all TTM stages.

TABLE I. THE COMPARISON CRITERIA BETWEEN MODELS

Model	Process	Problem	Healthcare Domain	Technology	Social Networks	Social Influences	Behavior Adoption	Behavior Prevention	Behavior Maintenance
HBM	Six constructs	Diabetes, Hyperuricemia, Obesity Smoking.	√	√	√	X	√	√	X
TPB	Six constructs	Cancer, Diabetes, Smoking.	√	X	X	X	√	X	X
DOI	Five categories	Maternal & Neonatal health, Smoking.	√	X	X	X	√	X	X
TTM	Six stages	Cardiovascular, Obesity, Smoking.	√	X	X	X	√	√	√
SNT	Six phases	Diabetes, junk food eating, Smoking.	√	X	X	√	√	X	X
The new model	Four stages	Celiac, Chronic disease.	√	√	√	√	√	√	√

#### D. WhatsApp and Chatbot

WhatsApp is the most widely used social and communication app globally. User engagement owing to its features, such as free calls and messages, the user interfaces are simple, easy to use, and messaging encryption [10]. The chatbot is a conversational agent that interacts with users using natural language [48]. Chatbot inhabits platforms such as Facebook, Messenger, WhatsApp, Telegram, iMessage, and even websites. Users communicate with a chatbot via the chat interface, such as talking to a real person, chatbot interprets, and processes the user's words and provides an instant answer.

Different chatbots have been developed using text communication, and they have been used in various domains such as customer service, education, and website help [48]. Chatbots have been used in the healthcare field for many reasons, like:

- Change behavior as in food consumption chatbot [11] on Facebook Messenger and smoking cessation chatbot [49] on Telegram.
- Sharing health information as in COVID-19 chatbot [12] on WhatsApp and Saudi health ministry chatbot [13] on Telegram.
- Monitoring Patients as in chronic conditions' teenagers chatbot [50] by Text Message.

As a summary for this section, the common existing models for health behavior change have critical limitations that effect of their applications negatively. Therefore, this paper intends build a new model to avoid those limitations. Also, it's notice that the use of social media to change health behavior is an idea that was previously applied, but not applied to change the behavior of patients with chronic diseases. Therefore, this paper intends to take advantages and use social media to change behavior of chronic diseases patients.

### III. DATA COLLECTIONS AND ANALYSIS

Three different collection methods were used in this study: 1) Interview with celiac expert users. 2) Questionnaire distributed to patients with celiac disease. 3) Studying exciting changing behavior models in the literature review. The reason is to collect the information data from different angles and draw a complete picture of the existing problem. The following subsections describe each method and their results.

#### A. Existing Health Behavior Models

Five common existing health behavior models were explored, examined, and analyzed. The existing health behavior models were HBM, TPB, TTM, DOI, and SNT. The goal was to determine the similarity, differences, necessary stages, and unnecessary stages to build a new health behavior change model that is compatible with the needs of patients with celiac disease. To analyze the five-existing model, three steps were followed:

- 1) Finding similarities between the three models (HBM, TPB, TTM).
- 2) Dispense with unnecessary stages in the three models (HBM, TPB, and TTM).

3) SNT and DOI were added to the three models (HBM, TPB, and TTM).

#### B. Interviews

Interviews were conducted with celiac experts to find out the following:

- The most common celiac symptoms.
- The most common treatment plan for celiac.
- The difficulties that celiac patients face in treatment plan commitment.

The celiac experts were divided into four categories as follows:

- Group 1: A patient diagnose with celiac four years ago or more.
- Group 2: A patient's parent who was diagnosed with celiac four years ago or more.
- Group 3: A dietitian who has supervised the diet of celiac patients for four years or more.
- Group 4: A gastroenterologist who has treated celiac patients for four years or more.

The reason of chosen four years or more as a criterion are:

- 1) The period required to change behavior.
- 2) The period required for a person to become an expert in a field.

It has been proven that any behavior can be changed within 18 days and not more than 254 days (less than a year) [51, 52]. It has also been proven that a person can become an expert in a field by practicing for not less than 10,000 hours [53], which can be considered as 3.9 years if the practice is daily, as in the case of chronic diseases, for 7 hours.

Ten questions were designed and prepared for the interviews. Before the interviews were conducted, a pilot test was conducted with an expert to test the suitability of the questions. The expert is a female celiac patient since 2015 and lives in Madinah, Saudi Arabia. She helps new patients adhere to their treatment plan by providing educational lectures about celiac and how to cope with it. After expert-approval, the interviews were conducted by phone, due to the social distancing measures that were imposed in the summer of 2020–the time of the interviews conducted- due to the spread of COVID-19. The interviews were conducted with four celiac patients, two celiac patients' parents, two dietitians, and three gastroenterology consultants. 54.5% of the interviewees were females, 45.5% were males. 36.4% of the interviewees had Ph.D. degree, 27.3% had bachelor's degree, 18.2% had master's degree, 9.1% had degree less than a bachelor's degree, and 9.1% prefer not to answer the question. 100% of the interviewees believed that the best treatment way for celiac is Gluten-free diet. The celiac symptoms -based on the interviewees' opinions- were stomachache, bloating, diarrhea, nausea, headache, and fatigue. 100% of the interviewees confirmed that the patients never experience the same symptoms after commit the treatment way. Difficulties that the

patients meet -based on the interviewees' opinions- were lack of alternatives, the need to sessions with a dietitian, and lack of support groups.

### C. Questionnaire

The questionnaire was distributed among different celiac patients' communities targeting the celiac patients and their relatives to answer the following questions:

- How are patients ranked as the most common physical and psychological symptoms based on the fastest appearance when they eat gluten?
- How are patients ranked as the most common physical and psychological symptoms based on the fastest disappearance when they stop eating gluten?
- What are the patients' preferences regarding the use of technology?

A total of 137 responses were received. The questionnaire was divided into five sections, and each section contained several questions. Before the questionnaire was distributed, an expert tested content validity and face validity. Many comments were received and considered before being distributed.

For reliability, one week after the questionnaire was administered. Sixty-nine participants agreed to retake the questionnaire (50.36% of the total participants). The questions' results were tested by finding the correlation between the results of the first time the questionnaire was submitted and the results of the second time. The overall correlation was 0.9749042904, which indicates a very high positive correlation.

When finding the correlation for each question separately, the results ranged between 0.7967715443 and 1, which made the correlation moderate, and reliability was acceptable. The above results proved the following:

- 83.8% of patients are female.
- 87.6% of patients are Saudi.
- 46% of the patients are 29 years old or less.
- 83.2% of the patients lived in three regions: Riyadh (34.3%), Makkah (29.2%), and Eastern (19.7%) regions.
- 75.18 of the patients lived in six cities: Riyadh (30.7%), Jeddah (22.63%), Madinah (8.03%), Dammam (5.11%), Dhahran (5.11%), and Makkah (3.6%).
- When patients eat gluten, they suffer from stomachache, bloating, diarrhea, nausea, headache, and fatigue.
- When patients suffer from eating gluten symptoms, they feel a desire to isolate themselves, worry that symptoms get worse, fear of what others think about them, that they are a burden to others, shame about their illness, depression, and the desire to cry.
- 67.9% of patients think that having a health application will benefit them.

- All patients can read Arabic.
- 82.5% of patients prefer WhatsApp over any other social media apps.
- Patients want the mobile application to provide alternative products, gluten-free recipes, medical and psychological follow-up, gluten-free diet suggestions, and periodic reports.

## IV. PROPOSED MODEL

To build a new health behavior change model, the focus has been on, in the first hand, the users and their needs, and, in the second hand, the software development life cycle. Therefore, user-centered design (UCD) has been used as a model that focuses on the users' needs and the waterfall model as a software development life cycle model. In the following subsection, details about the proposed model and its phases, phase duration, and phase quiz.

### A. The Chronic Diseases Extended Model

Since the new model extends from five old models, it was decided to name the new model "The Chronic-Disease Extended Model," or "CDEM" in short form. This section provides an overview of CDEM and its phases.

The CDEM involves progress through a series of phases, but progression occurs in a nonlinear fashion. This means that patients can progress from the earlier phase to later ones, regress from the later phase to the earlier one, and recycle through the phases from the last phase to the first one. As shown in Fig. 1, the model consists of the following four phases.

- Phase 1: Preparedness: the phase in which the patient knows what to feel about the disease.
- Phase 2: Readiness: the phase where the patient is ready to deal with the disease.
- Phase 3: Confidence: the phase in which the patient can find solutions for every barrier that faces.
- Phase 4: Continuance: The phase where the patient commits to the treatment plan.

Every phase has its own actions that help reach the phase goal. In addition, a patient is assigned to one of the phases based on his answers on the phase quiz, which is conducted every two weeks.



Fig. 1. Chatbot Processes.

TABLE II. THE PHASES AND THE WAY TO PROGRESS THROUGH THEM

The phase level	Phase character	Progressing status
<b>Preparedness</b>	Person knows what to feel about his disease and be conscious of the need for innovation.	Motivation to start treatment
<b>Readiness</b>	Person feels the seriousness of leaving the disease untreated and knowing treatment ways.	deciding to change behavior
<b>Confidence</b>	Person believes that social norms approve the new behavior and starting the new behavior.	feeling confident in the ability to perform a behavior.
<b>Continuance</b>	Person's perception of the obstacles to performing the behavior and knowing the factors that facilitate the performance of a behavior.	-

Table II presents the phases and ways of progressing through them. The first column in the table shows the phases' level, the second column shows the patient attributes in the different phases, and the last column shows the attribute that makes the patient ready to move to the next phase.

**B. Phases Duration**

Each phase differs from another in its goals and actions, and each patient differs from the other in his personality and needs. Therefore, it is difficult to predict how long each patient needs at each phase because of the large number of variables. This model suggests that the duration of each phase is a minimum of two weeks and a maximum of three months, based on the duration average of the five models that have been studied. To determine if the patient is ready to move to the next stage, a test called the phase quiz.

**C. Phases Quiz**

A phase quiz was developed based on the TTM instrument. The TTM instrument was created by Prochaska and DiClemente and validated in different intervention studies, which have focused on multiple health problems. Furthermore, phase quizzes develop based on the short version of the instrument, and its validation has been proven [54]. The reason for this choice is that the short version contains only one question, and the patient never feels bored when he takes the test every two weeks. The phase quiz consists of one question with four clauses that detriment whether patients stay, progress, or regress in the phases based on the sentence the patient's choice. Table III presents the question, its clauses, and action when choosing every clause.

TABLE III. PHASE QUIZ QUESTION AND ITS CLAUSES

Question	Clauses	The action when choosing the clause
Did you do the habit that was recommended to stay away from it in the last two weeks?	Yes, and I feel no bad about it.	The patient is in phase 1: <b>Preparedness</b>
	Yes, but I regret it.	The patient is in phase 2: <b>Readiness</b>
	No, But I still face some obstacles with no solutions.	The patient is in phase 3: <b>Confidence</b>
	No, and I totally committed to the treatment plan.	The patient is in phase 4: <b>Continuance</b>

**V. PROTOTYPING AND DESIGNING**

For proof of concept, the proposed model was applied to the chatbot. This section presents the chatbot analysis and chatbot design.

**A. Chatbot Analyzing**

To analyze the chatbot, the flowchart diagram as shown in Fig. 2 starts with a welcome message that explains the chatbot's goal and how to interact with it. Then, the pre-processing step, which is a pre-questionnaire to collect demographic information about the participants and their health behaviors and eating habits. After that, the processing includes the phase quiz to determine each participant's phase and interact with them with different actions based on their phase.

For example, in some phases, participants learn about celiac and its complications; in other phases, participants can find a place to order a gluten-free meal. The participants took the quiz phases every two weeks to reassign them to a suitable phase. Finally, after the experiment period was completed, the participants took post-processing, which is a post-questionnaire to collect information about their health behaviors and eating habits.

**B. Chatbot Design**

This section presents the chatbot prototype, tool used for development, pilot test feedback, and final chatbot design layout.

1) *Chatbot prototype*: To ensure the correctness of the information provided by the chatbot, information about celiac was collected from the website of the Saudi Ministry of Health. The chatbot prototype was designed using a chatbot design tool called "Botsociety".

2) *Deployment service provider*: To deploy the chatbot on WhatsApp, based on WhatsApp policy, it is necessary to deal with a licensed company. A search was conducted to identify different licensed companies that work as chatbot deployment service providers. The "Widebot" platform was used for chatbot design after strict comparison between five different companies based on the target customers, supporting WhatsApp, supporting Arabic, having an AI engine, and supporting natural language processing (NLP). For AI, "Widebot" uses its own classifier that combination between exact matching, fuzzy matching, and Naive Bayes classifier. For NLP, "Widebot" uses BERT model.

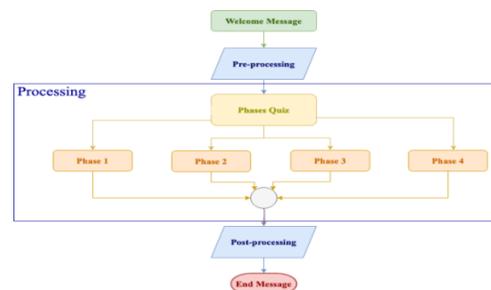


Fig. 2. The Chatbot Flowchart.

## VI. EXPERIMENT

This section presents the details of the experimental design, including, participants, materials and testing procedure.

### A. The Participants

The experiment was conducted on 60 Saudi participants diagnosed with celiac disease. Sixty participants were recruited through online virtual communities of celiac patients in Saudi Arabia. Many patients expressed their desire to participate in the experiment (137 patients). Only 60 participants met the experimental criteria. The criteria were:

- The participants lived in Jeddah. Jeddah city was chosen because it can suggest places that provide gluten-free meals only in Jeddah.
- Participants read and wrote Arabic fluently. Arabic was chosen because Arabic is the language of the chatbot.
- The participant approves to participate in the experiment and commits to it until the experiment ends by signing the consent form.

The 60 celiac patients who participated in the study experiment were split randomly into two groups: the control group and the test group. The control group was left without any intervention, which means that the proposed chatbot was not used, while the test group used the proposed chatbot.

### B. The Materials

An empirical study was planned and executed through three steps to determine whether the new model helps patients improve their health and adhere to the treatment plan. In addition, determining whether the idea of benefiting from the user experience of WhatsApp may be beneficial in the health field. The three steps are:

- Step 1: Pre-test questionnaire to collect the participants' data on eating habits, celiac symptoms, and treatment plan commitment.
- Step 2: Formal test to collect the data attributes during the test and record it in the log-in form to evaluate the participants interacting with the chatbot and their time of use.
- Step 3: Post-test questionnaire to collect the participants' data about eating habits, celiac symptoms, and treatment plan commitment to evaluate the participants' experience in using the proposed design as a tool to improve their health.

### C. Testing Procedure

The participants in the test group only used the proposed chatbot for three months (90 days) since the improvement in celiac patient health could show in a week to 6 months [22, 23]. The experiment was conducted from December 20, 2020, to March 19, 2021. During this process, the researcher observed the WhatsApp conversations with the participants and collected the data daily. The "Widebot" platform is dedicated for collecting the data. This allows the observer to read the conversations and extract data from them. It also gives him an analysis of the chatbot performance and the users' use of it.

## VII. RESULTS AND DISCUSSION

This section analyzes the pre-test and post-test questionnaire results.

### A. Pre-Test Result

First, the control and test groups answered the pre-test questionnaire on December 19, 2020, and the test group started using the proposed chatbot on December 21, 2020. The pre-test questionnaire consisted of the following four questions:

- 1) When was the last symptoms date?
- 2) Do you face difficulties in finding gluten-free products?
- 3) Do you face difficulties committing to the treatment plan?
- 4) Did you eat any food that contains gluten in the last two weeks? (Phase quiz)

From the result, it was noticed that 6.67% of the participants in the control group and 6.67% of the participants in the test group felt celiac symptoms last time on the same day they answered the pre-questionnaire. In addition, 30% of the participants in the control group and 30% of the participants in the test group always had difficulty finding gluten-free products. Additionally, 20% of the participants in the control group and 16.67% of the participants in the test group always had difficulties committing to the treatment plan. Finally, 30% of the participants in the control group and 30% of the participants in the test group were in phase one, based on the CDEM.

### B. Formal Test

The test group started to use the chatbot only. This step provided a clear picture of the number of chatbot times of use, the chatbot features that user tend to use, and the participants' progress in the CDEM phases. Analyzing the result of this step is useful in improving the chatbot for future research and does not affect the outcome of the experiment.

### C. Post-Test Result

After the experiment was completed, both groups of participants answered the post-test questionnaire on March 20, 2021. The post-test consists of the following four questions:

- 1) When was the last symptoms date?
- 2) Do you face difficulties in finding gluten-free products?
- 3) Do you face difficulties committing to the treatment plan?
- 4) Did you eat any food that contains gluten in the last two weeks? (Phase quiz)

From the result, it was noticed that 0.33% of the participants in the control group felt celiac symptoms last time on the same day they answered the post-questionnaire, but none of the participants in the test group felt celiac symptoms on the same day. In addition, 20% of the participants in the control group always had difficulties finding gluten-free products, but only 0.33% of the participants in the test group always had difficulties finding gluten-free products. Additionally, 6.67% of the participants in the control group

never had difficulties committing to the treatment plan, but 46.67% of the participants in the test group never had difficulties committing to the treatment plan. Finally, 26.67% of the participants in the control group were in phase one based on the CDEM, while none of them were in phase four. However, none of the participants in the test group were in phase one, while 43.33% of them were in phase four.

In general, and based on the previous comparison, it is clear that the status of participants in the control group, who were left without any intervention, did not improve; on the contrary, it regressed in many cases. However, the status of the participants in the test group, who used the proposed chatbot, improved, except concerning difficulty committing to the treatment plan.

**D. Discussion**

This section discusses the results statistically to reach the results of this study. The first two subsections compare the results of the two groups in the pre-test and post-test by finding the correlation, and ANOVA test.

1) *Correlation between the two groups:* After obtaining the results, Pearson’s correlation analysis between the two groups’ results for each question was applied, as it is the most used measure of correlation to show the degree of the linear relationship between variables. Table IV presents the results.

As Table IV shows the correlations between the two groups’ answers on the pre-test four questions were large positive correlations between 0.88 and 0.99. The correlations between the two groups’ answers to the post-test questions were as follows:

- Medium positive correlation in one out of four questions, equal to 0.76,
- Medium negative correlation in two out four questions between -0.73 and -0.60,
- No correlation in one out of four questions, equal to -0.06.

This means that the two groups were close in their answers in the pre-test. Still, after the test group participants conducted the experiment, the answers differed greatly, which made some correlation results appear negative, which can be said that the intervention applied to the test group (the experiment) affected the results of the group. Therefore, this intervention can help to reach the goal of changing health behaviors using social media.

However, the "no correlation" result for the second question, which was related to facing difficulties in finding gluten-free products, in the post-test was noticed. This result can be attributed to the fact that the 60 participants were reached through some virtual celiac patient communities, in which patients share experiences about gluten-free products, including the free-gluten products’ companies, and where those products are available. Therefore, it may be difficult to establish a relationship between the status of the participants in the two groups regarding this question.

2) *ANOVA Test between the two groups:* An ANOVA test was applied to determine which hypotheses are listed below:

- H0: There is no difference between the behavior of the Celiac patients before and after using the Chatbot based behavior change.
- H1: There is a difference between the behavior of the Celiac patients before and after using the Chatbot based behavior change:

The ANOVA test finds the p-value, a value that determines whether a significant statistical difference exists between the groups.

Table V shows the ANOVA test results of the pre-test for the groups, while Table VI shows the ANOVA test results of the post-test for the groups.

A P-value < 0.05, indicating a significant statistical difference between the groups. In the two tables above, the P-value for the pre-test was 0.77, which is more than 0.05, which means there is no significant statistical difference, but the P-value for the post-test was 0.0, which means there is a statistically significant difference between the groups. Therefore, we can confirm that the proposed chatbot helped celiac patients improve their eating habits.

TABLE IV. THE PRE-TEST AND POST-TEST CORRELATION BETWEEN THE CONTROL GROUP AND TEST GROUP

The list of questions	Pre-test correlation	Post-test correlation
When was the last symptoms date?	0.96	0.76
Do you face difficulties in finding gluten-free products?	0.88	-0.06
Do you face difficulties committing to the treatment plan?	0.98	-0.73
Did you eat any food that contains gluten in the last two weeks? (Phase quiz)	0.99	-0.60

TABLE V. ANOVA TEST RESULT OF THE PRE-TEST FOR THE CONTROL GROUP AND TEST GROUP

Source of Variation	Sum of Squares	Degrees of Freedom	Mean Square	F-statistic value	P-value
Between Groups	0.06666666667	1	0.06666666667	0.08618127786	0.7701371105
Within Groups	44.866666667	58	0.7735632184		
Total	44.933333333	59			

TABLE VI. ANOVA TEST RESULT OF THE POST-TEST FOR THE CONTROL GROUP AND TEST GROUP

Source of Variation	Sum of Squares	Degrees of Freedom	Mean Square	F-statistic value	P-value
Between Groups	28.03333333	1	28.033333333	50.61574074	0.000000003250293
Within Groups	28.8	52	0.5538461538		
Total	56.83333333	53			

It can be generalized that the chatbot intervention based on the proposed model had a positive effect on the results of the test group compared to the control group that did not use the chatbot, in terms of eating habits, finding alternatives, and progressing in the phases of the new model. However, patients still have difficulties committing to the treatment plan, which may be caused by the difficulty of the treatment plan itself, which includes stopping eating many of the common meals consumed in daily life and social occasions. Also, the reason for the decrease in chatbot usage rate from month to month may be due to the fact that the communication with the chatbot is by using writing, which allows reading the messages again and again that makes the user benefit from the chatbot message history without making a new chat with the chatbot.

### VIII. CONCLUSION

This study built a new health behavior change model based on the common existing models. Then, it used that model to design and test a chatbot for celiac patients in order to find out the answers to the research questions: Does the proposed behavior-changing model-based design of WhatsApp chatbot help celiac patients improve their eating habits?

In order to do that, the data were collected using three methods: studying the most common health behavior change models (HBM, TPB, DOI, TTM, and SNT), interviews with patients, their parents, dietitians, and gastroenterologists, and questionnaires for celiac patients and their relatives. Using these data, the new model was built (called CDEM) and adapted for use in technology. As a proof of concept, the CDEM was applied to WhatsApp chatbot for patients with celiac disease.

Two groups participated in the experiment: the control group and the test group. The control group was left without any intervention, whereas the test group used the chatbot. The results showed improvement in the eating habits of patients with celiac disease after using the chatbot in the test group compared to the control group. Therefore, it can be said that the proposed behavior-changing model-based design of WhatsApp chatbot can help celiac patients improve their eating habits.

This study faced many challenges because the timing of this study coincided during the Covid-19 pandemic, which led to limited communication with the target group, as well as limiting the pre-test and post-test to electronic tests. The study was conducted in the Kingdom of Saudi Arabia and on a Saudi sample from Jeddah only. The same study may provide different results with a different demographic sample or a diverse demographic group.

Our future direction is to conduct more experiments on the CDEM and use it in different social networks, since the experiment was applied in WhatsApp only. In the future work, the authors will study another social network apps' ability to change behavior, as we believe that some apps will give better results than others in achieving the goal. Also, may be carried out on other categories of society to improve the quality of life for sustainability factors.

### REFERENCES

[1] S. Kemp, "Digital 2021 global overview", We are Social, 2021.

[2] K. Okeleke and S. Suardi, "The mobile economy 2021", GSMA Intelligence, Jun 2021.

[3] A. Smith and D. Page, "US smartphone use in 2015," 2015.

[4] M. Peleg et al., "Ideating mobile health behavioral support for compliance to therapy for patients with chronic disease: a case study of Atrial Fibrillation management," *Journal of Medical Systems*, vol. 42, no. 11, p. 234, 2018/10/13 2018, doi: 10.1007/s10916-018-1077-4.

[5] D. Y. P. Chao, T. M. Y. Lin, and W.-Y. Ma, "enhanced self-efficacy and behavioral changes among patients with diabetes: cloud-based mobile health platform and mobile app service," *JMIR Diabetes*, vol. 4, no. 2, p. e11017, 2019/05/10 2019, doi: 10.2196/11017.

[6] K. Regmi, N. Kassim, N. Ahmad, and N. Tuah, "Effectiveness of mobile apps for smoking cessation:  $\alpha$  review," *Tob. Prev. Cessation*, vol. 3, 04/12 2017, doi: 10.18332/tpc/70088.

[7] D. M. Kazemi, B. Borsari, M. J. Levine, K. A. Lamberson, and B. Dooley, "REMIT: Development of a mHealth theory-based intervention to decrease heavy episodic drinking among college students," *Addiction Research & Theory*, vol. 26, no. 5, pp. 377-385, 2018/09/03 2018, doi: 10.1080/16066359.2017.1420783.

[8] D. J. Dute, W. J. E. Bemelmans, and J. Breda, "using mobile apps to promote a healthy lifestyle among adolescents and students: a review of the theoretical basis and lessons learned," *JMIR mHealth uHealth*, vol. 4, no. 2, p. e39, 2016/05/05 2016, doi: 10.2196/mhealth.3559.

[9] S. R. Paige, J. M. Alber, M. L. Stelfefon, and J. L. Krieger, "Missing the mark for patient engagement: mHealth literacy strategies and behavior change processes in smoking cessation apps," *Patient Education and Counseling*, vol. 101, no. 5, pp. 951-955, 2018/05/01/ 2018, doi: <https://doi.org/10.1016/j.pcc.2017.11.006>.

[10] A. Annie, "The state of mobile.," 2019.

[11] J. Åberg, "Chatbots as a mean to motivate behavior change : how to inspire pro-environmental attitude with chatbot interfaces," Independent thesis Advanced level (degree of Master (Two Years)) Student thesis, 2017. [Online]. Available: <http://urn.kb.se/resolve?urn=urn:nbn:se:umu:diva-135835>.

[12] WhatsApp. "Coronavirus - WHO health alert launch " WhatsApp.com. <https://www.whatsapp.com/coronavirus/who/> (accessed 11 April, 2020).

[13] Telegram. "Coronavirus news and verified channels." Telegram.com. <https://telegram.org/blog/coronavirus> (accessed 19 April), 2020).

[14] E. Lionetti and C. Catassi, "New clues in celiac disease epidemiology, pathogenesis, clinical manifestations, and treatment," *International Reviews of Immunology*, vol. 30, no. 4, pp. 219-231, 2011/07/29 2011, doi: 10.3109/08830185.2011.602443.

[15] P. Singh et al., "Global prevalence of Celiac disease: systematic review and meta-analysis," *Clinical Gastroenterology and Hepatology*, vol. 16, no. 6, pp. 823-836.e2, 2018/06/01/ 2018, doi: <https://doi.org/10.1016/j.cgh.2017.06.037>.

[16] Y. M. Khayyat, "Serologic markers of gluten sensitivity in a healthy population from the western region of Saudi Arabia," (in eng), *Saudi J Gastroenterol*, vol. 18, no. 1, pp. 23-25, Jan-Feb 2012, doi: 10.4103/1319-3767.91733.

[17] A. Al-Hussaini et al., "Mass screening for celiac disease among school-aged children: toward exploring celiac iceberg in Saudi Arabia," *Journal of Pediatric Gastroenterology and Nutrition*, vol. 65, no. 6, 2017. [Online]. Available: [https://journals.lww.com/jpgn/Fulltext/2017/12000/Mass\\_Screening\\_for\\_Celiac\\_Disease\\_Among.12.aspx](https://journals.lww.com/jpgn/Fulltext/2017/12000/Mass_Screening_for_Celiac_Disease_Among.12.aspx).

[18] M. A. Safi, "Prevalence of Celiac disease in Saudi Arabia: meta-analysis," *Global Vaccines and Immunology*, vol. 3, 01/01 2018, doi: 10.15761/GVI.1000134.

[19] J. L. Nagel, "Survey of registered dietitians' proficiency of Celiac disease and use of Twitter, Facebook, Smart Phone app, and internet for Celiac Disease management," ed: North Dakota State University, 2014.

[20] A. J. Dowd, C. Jackson, K. T. Y. Tang, D. Nielsen, D. H. Clarkin, and S. N. Culos-Reed, "MyHealthyGut: development of a theory-based self-regulatory app to effectively manage celiac disease," (in eng), *Mhealth*, vol. 4, p. 19, 2018, doi: 10.21037/mhealth.2018.05.05.

[21] K. Park, M. Harris, N. Khavari, and C. Khosla, "Rationale for using social media to collect patient-reported outcomes in patients with Celiac

- Disease," (in eng), *J Gastrointest Dig Syst*, vol. 4, no. 1, p. 166, 2014, doi: 10.4172/2161-069X.1000166.
- [22] A. M. H. Alshebani and Z. S. Abdalhamza, "The role of celiac disease antibodies in the follow up of patient on gluten free diet " *Revista Latinoamericana de Hipertension*, vol. 13 6, pp. 561-566, <sup>[1]</sup><sub>SEP</sub>, 2018.
- [23] G. Midhagen et al., "Antibody levels in adult patients with coeliac disease during gluten-free diet: a rapid initial decrease of clinical importance," *Journal of Internal Medicine*, vol. 256, no. 6, pp. 519-524, 2004, doi: 10.1111/j.1365-2796.2004.01406.x.
- [24] I. M. Rosenstock, V. J. Strecher, and M. H. Becker, "Social learning theory and the health belief model," *Health Education Quarterly*, vol. 15, no. 2, pp. 175-183, 1988/06/01 1988, doi: 10.1177/109019818801500203.
- [25] M. Conner, "Theory of planned behavior," *Handbook of Sport Psychology*, p. 3, 2020.
- [26] G. Silverberg, G. Dosi, and L. Orsenigo, "Innovation, diversity and diffusion: a self-organisation model," *The Economic Journal*, vol. 98, no. 393, pp. 1032-1054, 1988, doi: 10.2307/2233718.
- [27] The transtheoretical model: Applications to exercise. (1994). Human Kinetics Publishers, Champaign, IL, England.
- [28] H. W. Perkins and A. D. Berkowitz, "perceiving the community norms of alcohol use among students: some research implications for campus alcohol education programming\*," *International Journal of the Addictions*, vol. 21, no. 9-10, pp. 961-976, 1986/01/01 1986, doi: 10.3109/10826088609077249.
- [29] K. Sainsbury and B. Mullan, "Measuring beliefs about gluten free diet adherence in adult coeliac disease using the theory of planned Behavior," *Appetite*, vol. 56, no. 2, pp. 476-483, 2011/04/01/ 2011, doi: <https://doi.org/10.1016/j.appet.2011.01.026>.
- [30] C. Shao, J. Wang, J. Liu, F. Tian, and H. Li, "Effect of a Health Belief Model-based education program on patients' belief, physical activity, and serum uric acid: a randomized controlled trial," (in eng), *Patient Prefer Adherence*, vol. 12, pp. 1239-1245, 2018, doi: 10.2147/PPA.S166523.
- [31] L. H. McArthur, A. Riggs, F. Uribe, and T. J. Spaulding, "Health Belief Model offers opportunities for designing weight management interventions for college students," *Journal of Nutrition Education and Behavior*, vol. 50, no. 5, pp. 485-493, 2018/05/01/ 2018, doi: <https://doi.org/10.1016/j.jneb.2017.09.010>.
- [32] B. Mohebbi, A. Tol, R. Sadeghi, S. F. Mohtarami, and A. Shamshiri, "Self-management intervention program based on the Health Belief Model (HBM) among women with Gestational Diabetes Mellitus: a quazi-experimental study," (in eng), *Arch Iran Med*, vol. 22, no. 4, pp. 168-173, Apr 1 2019.
- [33] A. K. Jeihooni, S. F. Dindarloo, and P. A. Harsini, "Effectiveness of Health Belief Model on oral cancer prevention in smoker men," *Journal of Cancer Education*, vol. 34, no. 5, pp. 920-927, 2019/10/01 2019, doi: 10.1007/s13187-018-1396-7.
- [34] R. A. Record, N. G. Harrington, D. W. Helme, and M. W. Savage, "Using the Theory of Planned behavior to guide focus group development of messages aimed at increasing compliance with a tobacco-free policy," (in eng), *Am J Health Promot*, vol. 32, no. 1, pp. 143-152, Jan 2018, doi: 10.1177/0890117116687467.
- [35] İ. Dilekler, C. Doğulu, and Ö. Bozo, "A test of theory of planned behavior in type II diabetes adherence: The leading role of perceived behavioral control," *Current Psychology*, 2019/05/27 2019, doi: 10.1007/s12144-019-00309-7.
- [36] F. Abamecha, A. Tena, and G. Kiros, "Psychographic predictors of intention to use cervical cancer screening services among women attending maternal and child health services in Southern Ethiopia: the theory of planned behavior (TPB) perspective," *BMC Public Health*, vol. 19, no. 1, p. 434, 2019/04/25 2019, doi: 10.1186/s12889-019-6745-x.
- [37] H. Trisnowati, D. Kusuma, A. Ahsan, D. E. Kurniasih, and R. S. Padmawati, "Smoke-free home initiative in Bantul, Indonesia: Development and preliminary evaluation," (in eng), *Tob Prev Cessat*, vol. 5, pp. 40-40, 2019, doi: 10.18332/tpc/113357.
- [38] L. Paina et al., "Applying the model of diffusion of innovations to understand facilitators for the implementation of maternal and neonatal health programmes in rural Uganda," *Globalization and health*, vol. 15, no. 1, p. 38, 2019, doi: 10.1186/s12992-019-0483-9.
- [39] A. Koyun and K. Eroglu, "The effect of transtheoretical model-based individual counseling, training, and a 6-month follow-up on smoking cessation in adult women: A randomized controlled trial," *TURKISH JOURNAL OF MEDICAL SCIENCES*, vol. 46, pp. 105-111, 01/05 2016, doi: 10.3906/sag-1407-100.
- [40] E. Shakiba et al., "Efficacy of transtheoretical model on preventive nutritional behaviors of cardiovascular diseases: a randomized controlled trial," *J-Mazand-Univ-Med-Sci*, vol. 28, no. 163, pp. 24-37, 2018. [Online]. Available: <http://jmums.mazums.ac.ir/article-1-10713-en.html>.
- [41] R. d. M. Boff, M. A. Dornelles, A. M. P. Feoli, A. d. S. Gustavo, and M. d. S. Oliveira, "Transtheoretical model for change in obese adolescents: MERC randomized clinical trial," *Journal of Health Psychology*, p. 1359105318793189, 2018, doi: 10.1177/1359105318793189.
- [42] M. Cooper, M. Creamer, C. Ly, B. Crook, M. Harrell, and C. Perry, "Social norms, perceptions and dual/poly tobacco use among texas youth," *American journal of health behavior*, vol. 40, pp. 761-770, 01/11 2016, doi: 10.5993/AJHB.40.6.8.
- [43] P. Pansu, V. Fointiat, L. Lima, C. Blatier, P. Flore, and N. Vuillerme, "Changing behaviors: using norms to promote physical activity for type 2 diabetes patients," *European Review of Applied Psychology*, vol. 69, no. 2, pp. 59-64, 2019/03/01/ 2019, doi: <https://doi.org/10.1016/j.erap.2019.03.001>.
- [44] S. Higgs, J. Liu, E. I. M. Collins, and J. M. Thomas, "Using social norms to encourage healthier eating," *Nutrition Bulletin*, vol. 44, no. 1, pp. 43-52, 2019/03/01 2019, doi: 10.1111/mbu.12371.
- [45] J. Finkelstein and E. M. Cha, "Using a mobile app to promote smoking cessation in hospitalized patients," *JMIR mHealth uHealth*, vol. 4, no. 2, p. e59, 2016/05/06 2016, doi: 10.2196/mhealth.5149.
- [46] C. Khalil, "Understanding the adoption and diffusion of a telemonitoring solution in gestational diabetes mellitus: qualitative study," *JMIR Diabetes*, vol. 4, no. 4, p. e13661, 2019/11/28 2019, doi: 10.2196/13661.
- [47] N. Alsaleh and R. Alnanih, "Gamification-based behavioral change in children with diabetes mellitus," *Procedia Computer Science*, vol. 170, pp. 442-449, 2020/01/01/ 2020, doi: <https://doi.org/10.1016/j.procs.2020.03.087>.
- [48] H.-y. Shum, X.-d. He, and D. Li, "From Eliza to Xiaoice: challenges and opportunities with social chatbots," *Frontiers of Information Technology & Electronic Engineering*, vol. 19, no. 1, pp. 10-26, 2018/01/01 2018, doi: 10.1631/FITEE.1700826.
- [49] F. Dubosson, R. Schaer, R. Savioz, and M. Schumacher, "Going beyond the relapse peak on social network smoking cessation programmes: ChatBot opportunities," *Swiss Medical Informatics*, 09/20 2017, doi: 10.4414/smi.33.00397.
- [50] J. Beaudry, A. Consigli, C. Clark, and K. J. Robinson, "Getting ready for adult healthcare: designing a chatbot to coach adolescents with special health needs through the transitions of care," *Journal of Pediatric Nursing*, vol. 49, pp. 85-91, 2019/11/01/ 2019, doi: <https://doi.org/10.1016/j.pedn.2019.09.004>.
- [51] P. Lally, C. H. M. van Jaarsveld, H. W. W. Potts, and J. Wardle, "How are habits formed: modelling habit formation in the real world," *European Journal of Social Psychology*, vol. 40, no. 6, pp. 998-1009, 2010, doi: 10.1002/ejsp.674.
- [52] M. Maltz, *New Psycho-Cybernetics*. Penguin, 2002.
- [53] M. Gladwell, *Outliers: the story of success*. Audio-Tech Business Book Summaries, 2017.
- [54] S. Terrell, and D. Miranda, *The Transtheoretical Model (TTM)*, the. *Health Care Financing Review* 2001, 23(1), p.87.

# Design of Optimal Control of DFIG-based Wind Turbine System through Linear Quadratic Regulator

Ines Zgarni, Lilia ElAmraoui

Research Laboratory Smart Electricity & ICT, SE&ICT Lab., LR18ES44  
National School of Engineers of Carthage  
University of Carthage, Tunisia

**Abstract**—This paper is devoted to implement an optimal control approach applying Linear Quadratic Regulator (LQR) to control a DFIG based Wind Turbine. The main goal of proposed LQR Controller is to achieve the active and reactive power and the DC-link voltage control of DFIG system in order to extract the maximum power from the wind turbine. In fact, the linearized state-space model of studied system in the d-q rotating reference frame is established. However, the overall system is controlled using MPPT strategy. The simulation results are obtained with Sim-Power-System and Simulink of MATLAB in terms of steady-state values, Peak amplitude, settling time and rise-time. Finally, the eigenvalue analysis and the simulation results are rated to ensure studied system robustness and stability, and the effectiveness of the control strategy.

**Keywords**—Wind turbine system; doubly fed induction generator; DFIG; optimal control; linear quadratic regulator; LQR

## I. INTRODUCTION

The main renewable energy sources are Hydro Energy, Wind Energy (onshore or offshore), Solar Energy (PV or thermal), Biomass, Geothermal Energy, Wave Energy, Tidal Energy, and other alternative sources [1].

In 2020, according to IRENA (International Renewable Energy Agency), the share of renewable energy of global electricity production reached 36.6% which 9.58% produced by Wind energy [2][3].

Nowadays, due to the importance that takes the energy, which is at the core of all economic activity, the massive integration of wind turbine systems on power grids has created an effervescence in the world of scientific research, thus making it possible to improve the performance of wind turbines in terms of efficiency, reduced overall costs and maximum extraction energy [4].

In fact, many research works have been established studying the development of new design and control approaches for wind power system.

The most common combination for wind turbines is that with variable speed (with wide range of operation) and based on Doubly Fed Induction Generator (DFIG) which offers 10-15% higher wind energy capture and holds flexible control [5].

In the literature, Vector control is generally applied to control active and reactive powers of DFIG [6]. Even if, over the last three decades, the PI controller is the most successful controllers mostly in the 1st order SISO model of DFIG.

Nevertheless, facing variation of DFIG's parameters (MIMO system), PI becomes vulnerable. [7].

This research work stands out an LQR regulator, as a feedforward controller, using a linearized state-space model of the DFIG wind turbine. This approach reaches zero error between the desired magnitudes and the measured ones for the active and reactive powers and the DC-link voltage within a considerable time delay.

This paper is structured as follows. Section II presents related works. Section III describes the equivalent circuit of wind turbine based on DFIG and the modeling of the wind turbine, the DFIG, the grid side filter and the DC-link in d-q rotating reference frame. Section IV presents the linearized system around a point of equilibrium. In Section V, an LQR control strategy for studied system is discussed. Section VI is devoted to the implementation by creating a block diagram by MATLAB Simulink. Section VII details the simulation of studied system and the obtained results. Section VIII concludes the paper. Finally, Section IX details system parameters.

## II. LITERATURE REVIEW

In recent years, many works have been established on linear control of DFIG Based wind energy conversion system.

A direct control power output for DFIG wind turbine using LQR regulator for rotor side and grid side converters is evoked and discussed in [8].

A LQR Robust static state tracking control, described in [9], is designed to ensure tracking of the active and reactive power of the WECS over the wind speed range employing a polytopic LPV DFIG model.

In [10] they opted to use two control loops; from the reference power, the outer loop determines the reference rotor current and the interloop regulates the rotor current according to the outer loop output using LQR.

In this respect, in this paper, LQR Controller approach is proposed to improve the stability and robustness of the linearized DFIG system.

## III. DFIG-WIND TURBINE SYSTEM MODELING

The aim of this section is to present the Overall system which explains the configuration of the doubly fed induction generator (DFIG) wind turbine.

At first sight, Gearbox establishes the connection between wind generator (DFIG) and wind turbine [11]. Then, the stator is directly connected to the grid, whereas the rotor is connected to the grid via back-to-back converter (RSC and GSC) [12].

Rotor-side-Converter (RSC) represents a rectifier which transforms AC currents and voltages delivered by the rotor into DC currents and voltages, thus allowing a decoupled control of the active and reactive powers [13].

However, GSC stands for a PWM controlled inverter that recuperates DC current and voltage at the output of RSC to generate a three phase AC current and voltage system with the same frequency as the grid given that the variation of the speed of the rotor according to the speed of the wind generates a current with variable frequency.

This configuration allows variable speed operation of wind turbines [14].

Fig. 1 shows general configuration of Wind Turbine system based on DFIG. At the beginning, each part is modeled separately.

### A. The Model of Wind Turbine

Given that the static characteristics of a wind turbine rotor are derived from the relationships between the total wind power and the mechanical power of the wind turbine.

Some parameters of the variable speed wind turbine are taken into consideration in order to modeling DFIG.

In this study, turbine angular speed is considered equal to generator angular speed. Thus, system analysis and modeling have been done as a one-mass.

In Addition, the pitch angle controller dynamics is not taken into consideration on account of the fact that its slower response compared to the electrical control dynamics. Then, differential equation 1 reveals the rotation equation.

$$\frac{d\omega_r}{dt} = \frac{1}{2H} T_m - \frac{1}{2H} T_e \quad (1)$$

Where,  $\omega_r$  : Generator angular speed; H: total equivalent inertia (the equivalent inertia reduced to the shaft);  $T_m$ : Mechanical torque and  $T_e$ : Electromagnetic torque.

The mechanical power captured by the WT is described as follows: [16]

$$P_m(t) = \frac{1}{2} \rho_{air} \pi R^2 C_p(\lambda, \beta) V_w^3(t) \quad (2)$$

Where  $\rho_{air}$  identifies the air density, R is the blade radius,  $C_p$  denotes Power coefficient, and  $V_w$  represents the wind speed.

The power coefficient  $C_p$  depends essentially on two parameters which are  $\beta$  (Pitch angle of the blade) and  $\lambda$  (Tip speed ratio).

$\lambda$  is defined by the following expression: [17]

$$\lambda = \frac{R\omega_r}{V_w} \quad (3)$$

Thus, the curve describing the Power coefficient  $C_p$  as a function of the Tip speed ratio  $\lambda$  by taking a fixed value of pitch angle of the blades  $\beta$  is given by Fig. 2.

As shown in Fig. 2,  $C_p$  has a maximum point to a specific value of  $\lambda$  equal to  $\lambda_{opt}$ .

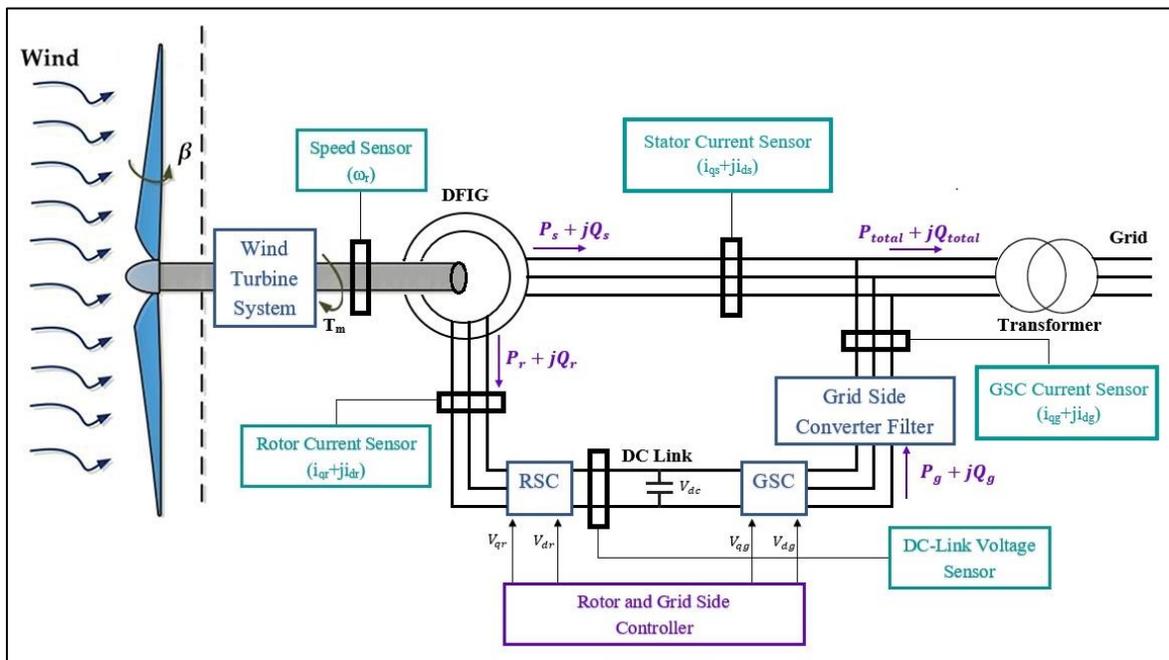


Fig. 1. General Configuration of Wind Turbine System based on DFIG. [15].

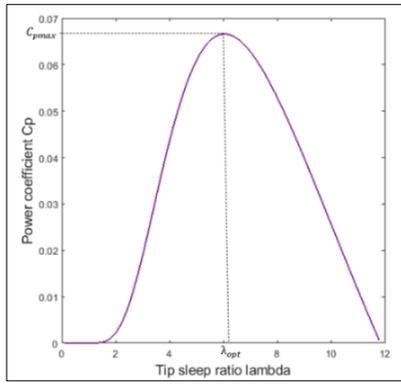


Fig. 2. Power Coefficient as a Function of the Tip Sleep Ratio.

Therefore, the expression of maximum mechanical power  $P_{max}$  is determined by equation 4. [18].

$$P_{max}(t) = \frac{1}{2} \rho_{air} \pi R^2 C_{pmax} V_w^3(t) \quad (4)$$

Furthermore, the range of the optimal power control for WT is obtained when:  $\omega_r \in [\omega_{rmin}, \omega_{rated}]$  and  $V_w \in [V_{wmin}, V_{wrated}]$ .

The control system for wind turbines is generally operates according to the technique of MPPT (Maximum Power Point Tracking). Then, the equation 5 represents the turbine power and the mechanical torque [19], [20].

$$P_{MPPT} = K_{opt} \omega_r^3 \text{ and } T_m = K_{opt} \omega_r^2 \quad (5)$$

$$\text{With: } K_{opt} = \frac{1}{2} \rho \pi R^5 \frac{C_{pmax}}{\lambda_{opt}^3} \quad [21]$$

In fact, the electromagnetic torque is obtained by making the ratio of air gap power to the DFIG mechanical speed. it is then written in the form:

$$T_e = L_m i_{qs} i_{dr} - L_m i_{ds} i_{qr} \quad (6)$$

To sum up, the rate of change of the generator angular speed is obtained from equations 1, 5 and 6.

$$\frac{d\omega_r}{dt} = \frac{K_{opt}}{2H} \omega_r^2 - \frac{L_m}{2H} i_{qs} i_{dr} + \frac{L_m}{2H} i_{ds} i_{qr} \quad (7)$$

### B. DFIG Model

The DFIG is described in the dq frame as follows: the equations describing DFIG in dq frame are as follows: [22]

$$V_{ds} = -R_s i_{ds} - \omega_s \Psi_{qs} - \frac{1}{\omega_B} \frac{d(\psi_{ds})}{dt} \quad (8)$$

$$V_{qs} = -R_s i_{qs} + \omega_s \Psi_{ds} - \frac{1}{\omega_B} \frac{d(\psi_{qs})}{dt} \quad (9)$$

$$V_{dr} = -R_r i_{dr} - (\omega_s - \omega_r) \Psi_{qr} - \frac{1}{\omega_B} \frac{d(\psi_{dr})}{dt} \quad (10)$$

$$V_{qr} = -R_r i_{qr} + (\omega_s - \omega_r) \Psi_{dr} - \frac{1}{\omega_B} \frac{d(\psi_{qr})}{dt} \quad (11)$$

With:

$$\psi_{ds} = L_{ss} i_{ds} + L_m i_{dr} \quad (12)$$

$$\psi_{qs} = L_{ss} i_{qs} + L_m i_{qr} \quad (13)$$

$$\psi_{dr} = L_m i_{ds} + L_{rr} i_{dr} \quad (14)$$

$$\psi_{qr} = L_m i_{qs} + L_{rr} i_{qr} \quad (15)$$

And

$$L_{ss} = L_s + L_m \quad (16)$$

$$L_{rr} = L_r + L_m \quad (17)$$

Where  $(V_{ds}, V_{qs})$  and  $(V_{dr}, V_{qr})$  represents stator and rotor voltages in dq frame, respectively;  $(i_{ds}, i_{qs})$  and  $(i_{dr}, i_{qr})$  denotes stator and rotor currents in dq frame, respectively;  $(\psi_{ds}, \psi_{qs})$  and  $(\psi_{dr}, \psi_{qr})$  identifies stator and rotor flux in dq frame, respectively;  $L_{ss}$  and  $L_{rr}$  stands for stator and rotor self-inductance, respectively;  $(L_s, R_s)$  represents stator leakage inductance and resistance;  $(L_r, R_r)$  represents rotor leakage inductance and resistance;  $L_m$  is an abbreviation for mutual inductance; at last,  $\omega_s$  identifies synchronous angular speed.

Moreover, the base speed is taken equal to  $\omega_B = 2\pi f$  with  $f = 50$  Hz which represents nominal frequency. [23]

The rotor slip is determined as follows:

$$s = 1 - \frac{\omega_r}{\omega_s} \quad (18)$$

Section 8.1 includes all constant parameters of studied system.

From the equations 8 to 17, the rate change of rotor and stator current in dq frame is established [24].

$$\begin{aligned} \frac{di_{qs}}{dt} = & \left( \frac{\omega_B R_s L_{rr}}{L_m^2 - L_{ss} L_{rr}} \right) i_{qs} + \left( \frac{\omega_B}{L_m^2 - L_{ss} L_{rr}} \right) [(\omega_s - \omega_r) L_m^2 - \\ & \omega_s L_{ss} L_{rr}] i_{ds} - \left( \frac{\omega_B R_r L_m}{L_m^2 - L_{ss} L_{rr}} \right) i_{qr} + \left( \frac{\omega_B}{L_m^2 - L_{ss} L_{rr}} \right) [(\omega_s - \\ & \omega_r) L_m L_{rr} - \omega_s L_m L_{rr}] i_{dr} - \left( \frac{\omega_B L_m}{L_m^2 - L_{ss} L_{rr}} \right) V_{qr} + \\ & \left( \frac{\omega_B L_{rr}}{L_m^2 - L_{ss} L_{rr}} \right) V_{qs} \end{aligned} \quad (19)$$

$$\begin{aligned} \frac{di_{ds}}{dt} = & \left( \frac{\omega_B}{L_m^2 - L_{ss} L_{rr}} \right) [\omega_s L_{ss} L_{rr} - (\omega_s - \omega_r) L_m^2] i_{qs} + \\ & \left( \frac{\omega_B R_s L_{rr}}{L_m^2 - L_{ss} L_{rr}} \right) i_{ds} - \left( \frac{\omega_B R_r L_m}{L_m^2 - L_{ss} L_{rr}} \right) i_{dr} + \\ & \left( \frac{\omega_B}{L_m^2 - L_{ss} L_{rr}} \right) [\omega_s L_m L_{rr} - (\omega_s - \omega_r) L_m L_{rr}] i_{qr} - \\ & \left( \frac{\omega_B L_m}{L_m^2 - L_{ss} L_{rr}} \right) V_{dr} + \left( \frac{\omega_B L_{rr}}{L_m^2 - L_{ss} L_{rr}} \right) V_{ds} \end{aligned} \quad (20)$$

$$\begin{aligned} \frac{di_{qr}}{dt} = & - \left( \frac{\omega_B R_s L_m}{L_m^2 - L_{ss} L_{rr}} \right) i_{qs} + \left( \frac{\omega_B}{L_m^2 - L_{ss} L_{rr}} \right) [\omega_s L_m L_{ss} - \\ & (\omega_s - \omega_r) L_m L_{ss}] i_{ds} + \left( \frac{\omega_B R_r L_{ss}}{L_m^2 - L_{ss} L_{rr}} \right) i_{qr} + \\ & \left( \frac{\omega_B}{L_m^2 - L_{ss} L_{rr}} \right) [\omega_s L_m^2 - (\omega_s - \omega_r) L_{ss} L_{rr}] i_{dr} + \\ & \left( \frac{\omega_B L_{ss}}{L_m^2 - L_{ss} L_{rr}} \right) V_{qr} + \left( \frac{\omega_B L_m}{L_m^2 - L_{ss} L_{rr}} \right) V_{qs} \end{aligned} \quad (21)$$

$$\begin{aligned} \frac{di_{dr}}{dt} = & \left( \frac{\omega_B}{L_m^2 - L_{ss} L_{rr}} \right) [(\omega_s - \omega_r) L_m L_{ss} - \omega_s L_m L_{ss}] i_{qs} - \\ & \left( \frac{\omega_B R_s L_m}{L_m^2 - L_{ss} L_{rr}} \right) i_{ds} + \left( \frac{\omega_B R_r L_{ss}}{L_m^2 - L_{ss} L_{rr}} \right) i_{dr} + \left( \frac{\omega_B}{L_m^2 - L_{ss} L_{rr}} \right) [(\omega_s - \\ & \omega_r) L_{ss} L_{rr} - \omega_s L_m^2] i_{qr} + \left( \frac{\omega_B L_{ss}}{L_m^2 - L_{ss} L_{rr}} \right) V_{dr} - \\ & \left( \frac{\omega_B L_m}{L_m^2 - L_{ss} L_{rr}} \right) V_{ds} \end{aligned} \quad (22)$$

### C. The Model of the Grid-side Filter

As it is known that the GSC serves to stabilize DC voltage by supervising the power transition in the grid, whereas the GSC filter is employed to minimize the system harmonics as well as to adjust the phase and amplitude of the voltage in the output of the GSC [25].

The circuit corresponding to the GSC Filter is given by Fig. 3.

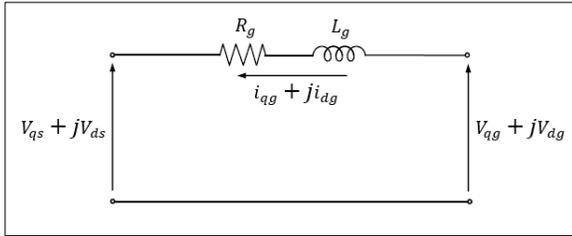


Fig. 3. GSC Filter Equivalent Circuit.

Where  $R_g$  and  $L_g$  identifies the resistance and the inductance of the Grid side filter, respectively, and  $(i_{dg}, i_{qg})$  and  $(V_{dg}, V_{qg})$  stands for the GSC current and voltage components, respectively. [26].

Furthermore, the GSC current are given as follows:

$$\frac{di_{qg}}{dt} = -\frac{\omega_B R_g}{L_g} i_{qg} + \omega_B \omega_s i_{dg} + \frac{\omega_B}{L_g} V_{qg} - \frac{\omega_B}{L_g} V_{qs} \quad (23)$$

$$\frac{di_{dg}}{dt} = -\omega_B \omega_s i_{qg} - \frac{\omega_B R_g}{L_g} i_{dg} + \frac{\omega_B}{L_g} V_{dg} - \frac{\omega_B}{L_g} V_{ds} \quad (24)$$

### D. The Model of DC-Link

The two converters of the wind energy conversion system (RSC and GSC) are interconnected via a DC-link capacitor which allows energy storage.

Acting as a reactive power source, the rotor-side magnetizing current is supplied by DC-link. Otherwise, the control of the stator-side power factor can be established.

In this study, supposing that the losses of the converter are neglected, the active power of DC-link  $P_{DC}$  is determinate as follows:

$$P_{DC} = P_r - P_g \quad (25)$$

Where  $P_g$  and  $P_r$  identifies the active power at the RSC and GSC AC terminal, respectively.

It is also written in this form:

$$P_{DC} = V_{DC} i_{DC} = V_{DC} C_{DC} \frac{dV_{DC}}{dt} \quad (26)$$

Where  $V_{DC}$  and  $i_{DC}$  are the voltage across DC-link capacitor and the current flowing through the capacitor, respectively.

The derivative of  $V_{DC}$  is, thus, obtained as a function of  $P_g$  and  $P_r$ .

$$\frac{dV_{DC}}{dt} = \frac{1}{C_{DC} V_{DC}} (P_r - P_g) \quad (27)$$

Moreover, by calculating the apparent power, the stator active power  $P_s$  represents real part of equation 28. As for the stator reactive power  $Q_s$ , it denotes the imaginary part.

$$P_s + jQ_s = V_{dqs} i_{dqs}^* = (V_{qs} + jV_{ds})(i_{qs} + ji_{ds})^* \quad (28)$$

Accordingly, the expressions of  $P_s$  and  $Q_s$  are given by equations 29 and 30. [27].

$$P_s = [V_{qs} i_{qs} + V_{ds} i_{ds}] \quad (29)$$

$$Q_s = [V_{ds} i_{qs} - V_{qs} i_{ds}] \quad (30)$$

Based on the same principle, the rotor active and reactive powers can be obtained as follows: [28].

$$P_r = [V_{qr} i_{qr} + V_{dr} i_{dr}] \quad (31)$$

$$Q_r = [V_{dr} i_{qr} - V_{qr} i_{dr}] \quad (32)$$

Similarly, the active and reactive power, on the Grid-side converter, is given by equations 33 and 34.

$$P_g = [V_{qg} i_{qg} + V_{dg} i_{dg}] \quad (33)$$

$$Q_g = [V_{dg} i_{qg} - V_{qg} i_{dg}] \quad (34)$$

Then, by exploiting the equations 27 to 34, the expression of  $\frac{dV_{DC}}{dt}$  becomes as follows:

$$\frac{dV_{DC}}{dt} = \frac{1}{C_{DC} V_{DC}} (V_{qr} i_{qr} + V_{dr} i_{dr} - V_{qg} i_{qg} - V_{dg} i_{dg}) \quad (35)$$

## IV. STUDIED SYSTEM LINEARIZATION

The dynamic characteristics of the studied system will be analyzed by studying the different linearization techniques and eigenvalues.

The modeling of the whole of the studied system comprising DFIG, GSC filter, and the subsystem of drive train is obtained by combining the models of the above-mentioned subsystems.

The small-signal model is established revealing linearization around operating point:

$$(i_{qs0}, i_{ds0}, i_{qr0}, i_{dr0}, i_{qg0}, i_{dg0}, \omega_{r0}, V_{DC0})$$

Moreover, q axis of the machine is set in such a way that it coincides with stator voltage  $V_s$ . Consequently, the total voltage corresponds to q-axis stator voltage ( $V_s = V_{qs}$ ) and d-axis stator voltage is taken zero ( $V_{ds} = 0$ ).

The generalized equations are written as follows: [29]

$$\dot{x} = f(x, y) \quad (36)$$

$$y = g(x, y) \quad (37)$$

Vectors  $x$ ,  $y$  and  $u$  represent the state vector, the output vector, and the control vector respectively.  $f$  and  $g$  denote nonlinear functions.

The equations of the state-space are as follows: [30]

$$\Delta \dot{x} = A \Delta x + B \Delta u \quad (38)$$

$$\Delta y = C \Delta x + D \Delta u \quad (39)$$

With  $\Delta$  stands for the deviation. Thus, the deviations of the state, input and output variables are given by equations 40, 41, and 42.

$$\Delta x = [\Delta i_{qs} \ \Delta i_{ds} \ \Delta i_{qr} \ \Delta i_{dr} \ \Delta i_{qg} \ \Delta i_{dg} \ \Delta \omega_r \ \Delta V_{DC}]^T \quad (40)$$

$$\Delta u = [\Delta V_{qr} \ \Delta V_{dr} \ \Delta V_{qg} \ \Delta V_{dg}]^T \quad (41)$$

$$\Delta y = [\Delta P_s \ \Delta Q_s \ \Delta P_r \ \Delta Q_r \ \Delta P_g \ \Delta Q_g \ \Delta V_{DC}]^T \quad (42)$$

The matrices A, B, C and D which stand for respectively the state matrix, the control matrix, output matrix and feedforward matrix are computed and shown in equations 43, 46.

$$A = \begin{bmatrix} A_{11} & A_{12} & A_{13} & A_{14} & A_{15} & A_{16} & A_{17} & A_{18} \\ A_{21} & A_{22} & A_{23} & A_{24} & A_{25} & A_{26} & A_{27} & A_{28} \\ A_{31} & A_{32} & A_{33} & A_{34} & A_{35} & A_{36} & A_{37} & A_{38} \\ A_{41} & A_{42} & A_{43} & A_{44} & A_{45} & A_{46} & A_{47} & A_{48} \\ A_{51} & A_{52} & A_{53} & A_{54} & A_{55} & A_{56} & A_{57} & A_{58} \\ A_{61} & A_{62} & A_{63} & A_{64} & A_{65} & A_{66} & A_{67} & A_{68} \\ A_{71} & A_{72} & A_{73} & A_{74} & A_{75} & A_{76} & A_{77} & A_{78} \\ A_{81} & A_{82} & A_{83} & A_{84} & A_{85} & A_{86} & A_{87} & A_{88} \end{bmatrix} \quad (43)$$

All the elements of matrix A are given in section 8.2.

$$B = \begin{bmatrix} \frac{-\omega B L_m}{L_m^2 - L_{SS} L_{rr}} & 0 & 0 & 0 \\ 0 & \frac{-\omega B L_m}{L_m^2 - L_{SS} L_{rr}} & 0 & 0 \\ \frac{\omega B L_{SS}}{L_m^2 - L_{SS} L_{rr}} & 0 & 0 & 0 \\ 0 & \frac{\omega B L_{SS}}{L_m^2 - L_{SS} L_{rr}} & 0 & 0 \\ 0 & 0 & \frac{\omega B}{L_g} & 0 \\ 0 & 0 & 0 & \frac{\omega B}{L_g} \\ 0 & 0 & 0 & 0 \\ \frac{i_{qr0}}{C_{DC} V_{DC0}} & \frac{i_{dr0}}{C_{DC} V_{DC0}} & \frac{-i_{qg0}}{C_{DC} V_{DC0}} & \frac{-i_{dg0}}{C_{DC} V_{DC0}} \end{bmatrix} \quad (44)$$

$$C = \begin{bmatrix} V_{qs0} & V_{ds0} & 0 & 0 & 0 & 0 & 0 & 0 \\ V_{ds0} & -V_{qs0} & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & V_{qr0} & V_{dr0} & 0 & 0 & 0 & 0 \\ 0 & 0 & V_{dr0} & -V_{qr0} & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & V_{qg0} & V_{dg0} & 0 & 0 \\ 0 & 0 & 0 & 0 & V_{dg0} & -V_{qg0} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix} \quad (45)$$

$$D = \begin{bmatrix} 0 & 0 & 0 & 0 & i_{qs0} & i_{ds0} \\ 0 & 0 & 0 & 0 & -i_{ds0} & i_{qs0} \\ i_{qr0} & i_{dr0} & 0 & 0 & 0 & 0 \\ -i_{dr0} & i_{qr0} & 0 & 0 & 0 & 0 \\ 0 & 0 & i_{qg0} & i_{dg0} & 0 & 0 \\ 0 & 0 & -i_{dg0} & i_{qg0} & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{bmatrix} \quad (46)$$

### V. LQR CONTROLLER DESIGN

Modeling the small signal is set in order to apply the control law:  $u = -K_{LQR}x$ . The control law is determined by minimizing the LQR cost function given by equation 47. [31].

$$J = \int_0^{\infty} (x^T Q x + u^T R u) dt \quad (47)$$

Where Q ( $8 \times 8$ ) and R ( $4 \times 4$ ) denotes the state and control weighting matrices. They are symmetric and square.

Besides, in this study, Q and R are chosen as identity matrices.

As a result of the theory of linear control, matrix gain  $K_{LQR}$  is obtained as follows:

$$K_{LQR} = R^{-1} B^T P \quad (48)$$

Where P (positive-definite matrix) is spotted by solving the following continuous Riccati equation: [32].

$$A^T P + P A - P B R^{-1} B^T P + Q = 0 \quad (49)$$

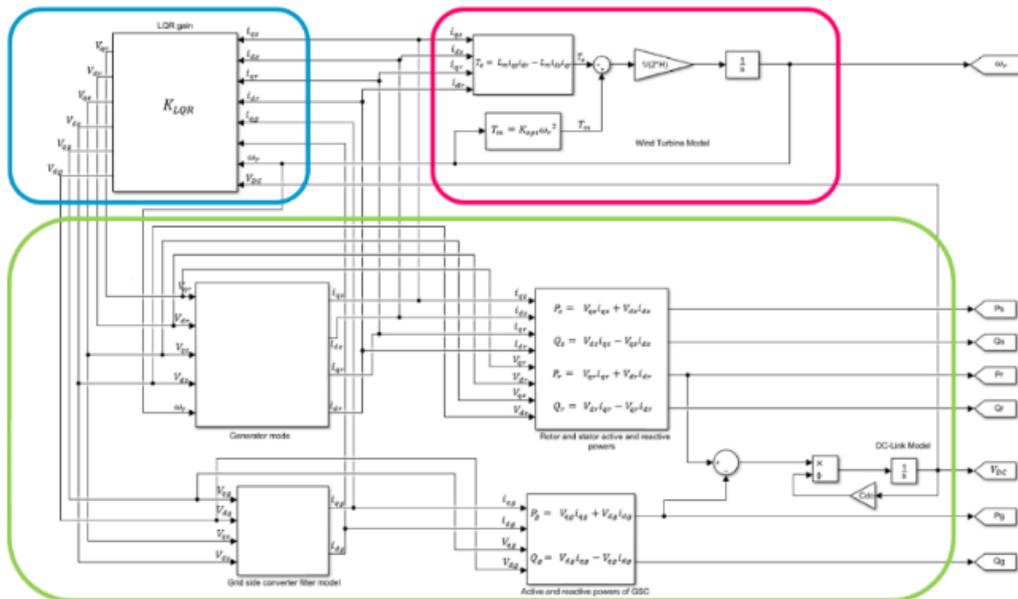


Fig. 4. Block Diagram of Studied System Simulation.

In fact,  $K_{LQR}$  is determined by ensuring the stability of the system. The checks carried out are as follows:

The controllability of (A, B) and the observability of (Q, A),

$(A - BK_{LQR})$  which represents the closed-loop system must be asymptotically stable, that is, accomplished by checking the matrix eigenvalues that they must have a negative real part.

The step response of studied system is detailed in Section 5 after identifying the feedback LQR gain  $K_{LQR}$  which is detailed in Section 8.3.

Given that the cost function J represent the integral summing of the control effort  $J_u$  and the criterion of performance  $J_x$  illustrated by equations 50 and 51.

$$J_u = (V_{qr})^2 + (V_{dr})^2 + (V_{qg})^2 + (V_{dg})^2 \quad (50)$$

$$J_x = (i_{qs})^2 + (i_{ds})^2 + (i_{qr})^2 + (i_{dr})^2 + (i_{qg})^2 + (i_{dg})^2 + (\omega_r)^2 + (V_{DC})^2 \quad (51)$$

### VI. IMPLEMENTATION OF STUDIED SYSTEM

The Fig. 4 shows the block diagram of studied system simulation, which is accomplished using Simulink of MATLAB, the help of Sim power System and the built-in LQR function of MATLAB.

According to Fig. 4, the overall operational diagram of studied system is described as follows: the blue box presents the proposed LQR controller algorithm, the pink box indicates the wind turbine model, and the green box encompasses the DFIG model, the GSC Filter model and the DC-Link model.

### VII. SIMULATION AND RESULTS

The studied system's response as achieved using previously detailed and discussed control algorithm, are described in this section.

The DFIG's overall characteristics and the location of the poles have been obtained in such a way that ensures the stability of the system.

Table I illustrate the DFIG's eigenvalues without and with proposed controller.

Without controller, the positive real part was identified for one eigenvalue that is providing the instability of the initial system. As shown in Table I, in case of proposed controller, all eigenvalues dispose negative real part.

TABLE I. DFIG'S EIGENVALUES WITHOUT AND WITH PROPOSED CONTROLLER

Without LQR controller	With LQR Controller
$-16.2 \pm 313.5i$	$-13963.6 \pm 314i$
-4.8	$-4429 \pm 94.25i$
$-14.4 \pm 120i$	$-1.4 + 314i$
$-167.5 \pm 314i$	-9.2
+0.00000071	-1.3

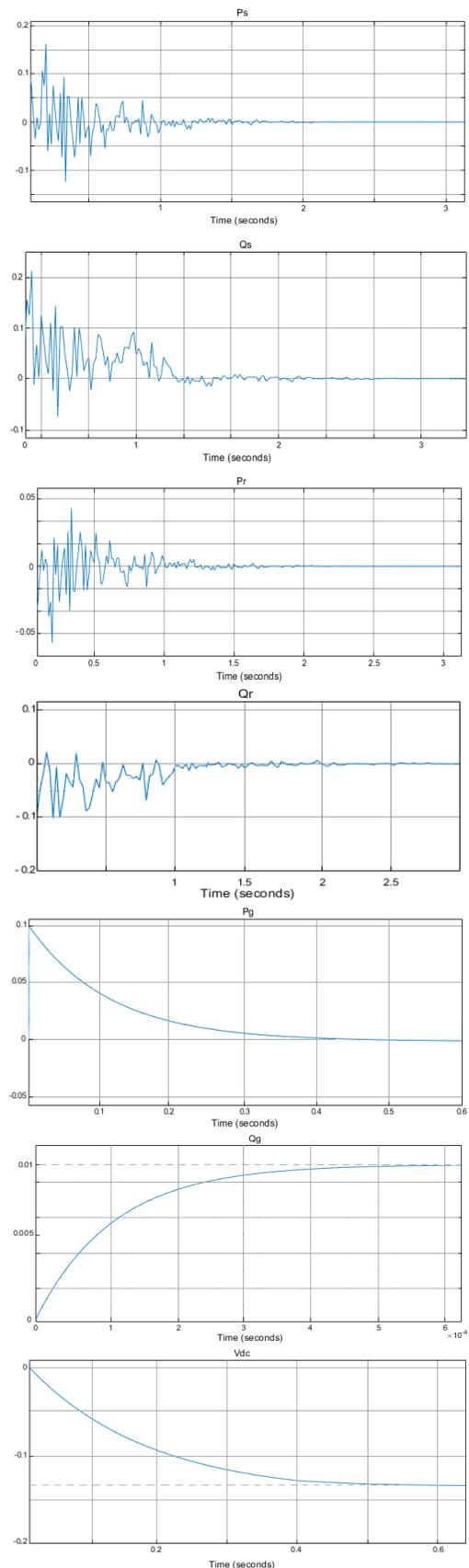


Fig. 5. Output Variables Errors with Proposed Control Approach.

From the simulation, the active and reactive powers, the DC-Link voltage, and the generator angular speed have been determined.

To sum up, the following specifications of time-domain, given by Table II, have been obtained from Fig. 5.

TABLE II. (A) SPECIFICATIONS OF TIME-DOMAIN

Output variables	$P_s$	$Q_s$	$P_r$	$Q_r$
Peak-value	-0.161pu	0.218pu	-0.186pu	-0.102pu
Rise-time	7.39e-04s	0.001 s	1.1e-04 s	1.6e-04 s
Settling time	2.37s	2.77 s	0.112 s	2.77 s
Steady-state-value	-0.078pu	0.0193pu	-0.021pu	0.004 pu

(B) SPECIFICATIONS OF TIME-DOMAIN

Output variables	$P_g$	$Q_g$	$V_{DC}$
Peak-value	0.09 pu	0.01 pu	-0.131 pu
Rise-time	0.403 s	2.19e-04 s	0.238 s
Settling time	0.576 s	0.54e-04 s	0.52 s
Steady-state-value	-0.002 pu	0.01 pu	-0.131 pu

Previously, the simulation results described are satisfactory in terms of Peak-value, rise-time and settling time.

Given that the evaluation of optimization problems without constraints is a primary objective of an LQR controller.

However, the proposed controller ensures a systematic computation of the state feedback gain matrix as well as a regulation of all the states to zero which is validated by the values of steady-state found for the active and reactive powers and the DC-Link voltage.

### VIII. CONCLUSION

In this paper, the design, and the implementation of LQR controller as a feedforward controller employing a linearized state-space model of the DFIG wind turbine in the rotating dq reference frames, is achieved in order to control the active and reactive powers and the DC-link voltage.

Further, the choice of the weighting matrices R and Q is focused on the investigation of a satisfactory response of the simulation.

According to the simulation results, with proposed controller, errors between the actual and desired values converged to zero and the response of the system shows good performance.

Finally, given that the LQR criterion can be perceived as a compromise between performance (described by the state weighting matrix Q) and consumption (denoted by the control weighting matrix R), the choice of the matrices R and Q (other than identity matrices) will be investigated in the forthcoming studies. Furthermore, comfortable stability margins will be determined to guarantee the robustness of the control.

### IX. SYSTEM PARAMETERS

Simulations are obtained with a 7.5kW generator connected to a 220V/50Hz grid.

#### A. Parameters of Studied System and Steady State

The machine and steady-state parameters are illustrated in Table III.

TABLE III. PARAMETERS OF STUDIED SYSTEM AND STEADY STATE

Parameter	Designation	Value
$\omega_B$	Base speed	314.16 rad/s
$\omega_s$	Synchronous angular speed	1 pu
s	Rotor slip	-0.03
$R_s$	Stator resistance	0.005 pu
$R_r$	Rotor resistance	0.0055 pu
H	Total inertia (Wind turbine + generator)	3.5s
$L_m$	Mutual inductance	2.25 pu
$L_{ss}$	Stator self-inductance	2.2725 pu
$L_{rr}$	Rotor self-inductance	2.2839 pu
$L_g$	GSC filter inductance	0.0225 pu
$R_g$	GSC filter resistance	0.012 pu
$X_t$	Transmission line resistance and reactance	0.0225 pu
$k_{opt}$	Constant corresponding to the maximum power coefficient	0.5787
$C_{dc}$	DC-link capacitor	0.0001 pu
$V_{dc0}$	Initial DC-link voltage	1200 V
$P_{total}$	Total active power	1 pu
$V_s$	Stator voltage	1 pu
$V_r$	Rotor voltage	$V_s/n$ pu
$V_B$	Slack bus voltage	1 pu
n	Stator to rotor turns ratio	1.5
$i_{qs0}$	Initial stator currents in dq frame	0.9999
$i_{ds0}$		-0.0563
$i_{qr0}$	Initial rotor currents in dq frame	1.437e-04
$i_{dr0}$		0.0675
$i_{qg0}$	Initial GSC currents in dq frame	1.437e-04
$i_{dg0}$		0.0675
$\omega_{r0}$	Initial generator angular speed	1.03
$V_{qr0}$	Initial rotor voltages in dq frame	0.6667
$V_{dr0}$		0
$V_{qs0}$	Initial stator voltages in dq frame	1
$V_{ds0}$		0
$V_{qg0}$	Initial voltages at the GSC terminal in dq frame	1.00000172
$V_{dg0}$		0.0008

B. Elements of Matrix A

$$A_{11} = \frac{\omega_B R_s L_{rr}}{L_m^2 - L_{ss} L_{rr}}; A_{12} = \frac{\omega_B((\omega_s - \omega_{r0})L_m^2 - \omega_s L_{ss} L_{rr})}{L_m^2 - L_{ss} L_{rr}};$$

$$A_{13} = \frac{-\omega_B R_r L_m}{L_m^2 - L_{ss} L_{rr}}; A_{14} = \frac{\omega_B((\omega_s - \omega_{r0})L_m L_{rr} - \omega_s L_m L_{rr})}{L_m^2 - L_{ss} L_{rr}}$$

$$A_{15} = A_{16} = A_{18} = 0; A_{17} = \left(\frac{-\omega_B L_m^2 i_{dso}}{L_m^2 - L_{ss} L_{rr}}\right) - \left(\frac{\omega_B L_m L_{rr} i_{dro}}{L_m^2 - L_{ss} L_{rr}}\right);$$

$$A_{21} = -A_{12}; A_{22} = A_{11}; A_{23} = -A_{14};$$

$$A_{24} = A_{13}; A_{25} = A_{26} = A_{28} = 0;$$

$$A_{27} = \left(\frac{\omega_B L_m^2 i_{qso}}{L_m^2 - L_{ss} L_{rr}}\right) + \left(\frac{\omega_B L_m L_{rr} i_{qro}}{L_m^2 - L_{ss} L_{rr}}\right); A_{31} = \frac{-\omega_B R_s L_m}{L_m^2 - L_{ss} L_{rr}};$$

$$A_{32} = \frac{\omega_B(\omega_s L_m L_{ss} - (\omega_s - \omega_{r0})L_m L_{ss})}{L_m^2 - L_{ss} L_{rr}}; A_{33} = \frac{\omega_B R_r L_{ss}}{L_m^2 - L_{ss} L_{rr}};$$

$$A_{34} = \frac{\omega_B(\omega_s L_m^2 - (\omega_s - \omega_{r0})L_{ss} L_{rr})}{L_m^2 - L_{ss} L_{rr}};$$

$$A_{35} = A_{36} = A_{38} = 0; A_{37} = \left(\frac{\omega_B L_m L_{ss} i_{dso}}{L_m^2 - L_{ss} L_{rr}}\right) + \left(\frac{\omega_B L_{ss} L_{rr} i_{dro}}{L_m^2 - L_{ss} L_{rr}}\right);$$

$$A_{41} = -A_{32}; A_{42} = A_{31}; A_{43} = \frac{\omega_B((\omega_s - \omega_{r0})L_{ss} L_{rr} - \omega_s L_m^2)}{L_m^2 - L_{ss} L_{rr}};$$

$$A_{44} = A_{33}; A_{45} = A_{46} = A_{48} = 0;$$

$$A_{47} = \left(\frac{-\omega_B L_m L_{ss} i_{qso}}{L_m^2 - L_{ss} L_{rr}}\right) + \left(\frac{-\omega_B L_{ss} L_{rr} i_{qro}}{L_m^2 - L_{ss} L_{rr}}\right);$$

$$A_{51} = A_{52} = A_{53} = A_{54} = A_{57} = A_{58} = 0; A_{55} = \frac{-\omega_B R_g}{L_g};$$

$$A_{56} = \omega_B \omega_s; A_{61} = A_{62} = A_{63} = A_{64} = A_{67} = A_{68} = 0;$$

$$A_{65} = -A_{56}; A_{66} = A_{55};$$

$$A_{71} = \frac{-L_m i_{dro}}{2H}; A_{72} = \frac{L_m i_{qro}}{2H}; A_{73} = \frac{L_m i_{dso}}{2H}; A_{74} = \frac{-L_m i_{qso}}{2H};$$

$$A_{75} = A_{76} = A_{78} = 0; A_{77} = \frac{\omega_{r0} K_{opt}}{H};$$

$$A_{81} = A_{82} = A_{87} = 0; A_{83} = \frac{V_{qro}}{C_{DC} V_{DC0}}; A_{84} = \frac{V_{dro}}{C_{DC} V_{DC0}};$$

$$A_{85} = \frac{-V_{qgo}}{C_{DC} V_{DC0}}; A_{86} = \frac{-V_{dgo}}{C_{DC} V_{DC0}};$$

$$A_{86} = \frac{V_{dro} i_{dro} + V_{qro} i_{qro} - V_{dgo} i_{dgo} - V_{qgo} i_{qgo}}{C_{DC} V_{DC}^2}$$

C. Numerical Values of LQR Controller Gain

$$K_{LQR} = \begin{bmatrix} -3.9908 & 4.8113 & -5.3490 & 4.7635 & 0.0002 & -0.0000 & -0.0390 & -0.4281 \\ -4.8137 & -3.9730 & -4.7661 & -5.3307 & -0.0000 & 0.0000 & 0.6911 & 0.0166 \\ -0.0019 & 0.0370 & 0.0031 & 0.0366 & 0.9890 & -0.0000 & -0.1458 & -0.9035 \\ -0.0000 & 0.0010 & 0.0002 & 0.0010 & 0.0000 & 0.9880 & -0.0036 & -0.0219 \end{bmatrix}$$

REFERENCES

[1] N. A. Randriantsoa, A. H. Fakra, M. P. Ranjaranimaro, M. N. M. Rachdi, J. C. Gatina, "New Management Algorithms for Smart Electricity Network: Designing and Working Principles", Progress in Advanced Computing and Intelligent Engineering, pp. 671-682, 2021.

[2] M. P. Pablo-Romero, A. Sanchez-Braza, A. Galyan, "Renewable energy use for electricity generation in transition economies: Evolution, targets and promotion policies", Renewable and Sustainable Energy Reviews, vol.138, 110481, 2021.

[3] IRENA. Renewable capacity statistics 2021. Abu Dhabi: International Renewable Energy Agency; 2021.

[4] <https://www.irena.org/publications/2021/March/Renewable-Capacity-Statistics-2021>.

[5] A. Chehouri, R. Younes, A. Ilinca, J. Perron, "Review of performance optimization techniques applied to wind turbines", Applied Energy, vol. 142, pp. 361-388, 2015.

[6] R. Kumar, K. Raahemifar, A. S. Fung, "A critical review of vertical axis wind turbines for urban applications", Renewable and Sustainable Energy Reviews, vol. 89, pp. 281-291, 2018.

[7] D. Zouheyr, L. Baghli, A. Boumediene, "Real-Time Emulation of a Grid-connected Wind Energy Conversion System Based Double Fed Induction Generator Configuration under Random Operating Modes", European Journal of Electrical Engineering, vol. 23, pp. 207-219, 2021.

[8] K. Kim, H.-G. Kim, Y. Song, and I. Paek, "Design and Simulation of an LQR-PI Control Algorithm for Medium Wind Turbine", Energies, vol. 12, 2248, 2019.

[9] D. Chung Phan, T. H. Trinh, "Application of linear quadratic regulator to control directly power for DFIG wind turbine". Journal of Electrical systems, vol. 15-1, pp. 42-52, 2019.

[10] S. Salhi, S. Salhi, "LQR Robust control for active and reactive power tracking of a DFIG based WECS", International Journal of Advanced Computer Science and Applications, vol. 10-1, pp. 565-579, 2019.

[11] R. Bhusan, K. Chatterjee, "Mathematical modeling and control of DFIG-based wind energy system by using optimized linear quadratic regulator weight matrices". International Transaction on Electrical energy system, e. 2416, 2017.

[12] B. Subudhi, P. S. Ogeti, "Optimal preview stator voltage-oriented control of DFIG WECS", the institution of Engineering and technology, vol. 12, pp. 1004-1013, 2018.

[13] E. Chetouani, Y. Errami, A. Obbadi, S. Sahnoun, "Optimal tuning of PI controllers using adaptive particle swarm optimization for doubly-fed induction generator connected to the grid during a voltage dip", Bulletin of Electrical Engineering and Informatics, vol. 10-5, pp. 2367-2376, 2021.

[14] Y.-K. Wu, W.-H. Yang, "Different control strategies on the rotor side converter in DFIG-based wind turbines", 3rd International Conference on Power and Energy Systems Engineering, vol. 8-12, pp. 551-555, Japon, 2016.

[15] D. Xu, F. Blaabjerg, W. Chen, N. Zhu, "Advanced control of doubly fed induction generator for wind power systems", John Wiley & Sons, pp. 85-95, 2018.

[16] V. Yaramasu, B. Wu, "Model predictive control of wind energy conversion systems", John Wiley & Sons, pp. 405-406, 2017.

[17] S. B. Abul Kashem, M. E. H. Chowdhury, A. Khandakar, A. Jubaer, A. Azad, S. Nushrat, "Wind Power Integration with Smart Grid and Storage System: Prospects and Limitations", International Journal of Advanced Computer Science and Applications, vol. 11-5, pp. 552-569, 2020.

[18] E. Chetouani, A. Obbadi, S. Sahnoun, "Backstepping and indirect vector control for rotor side converter of doubly fed-induction generator with maximum power point tracking", Chapter, Digital Technologies and Applications, pp. 1711-1723, 2021.

[19] D.-C. Phan, S. Yamamoto, "Maximum Energy Output of a DFIG Wind Turbine Using an Improved MPPT-Curve Method", Energies, vol. 8, pp. 11718 - 11736, 2015.

[20] D. Ounnas, M. Ramdani, S. Chenikher, T. Bouktir, "A fuzzy tracking control design strategy for wind energy conversion system", International conference on Renewable Energy Research and Applications, Italy, 2015.

[21] T. Ghennam, "Supervision of a wind farm for its integration into the management of an electrical network, Contribution of multi-level converters to the adjustment of wind turbines based on doubly fed induction machine", Doctoral thesis, Central School of Lille, pp. 66-68, 2011.

[22] A. Hammami, I. Saidi, D. Soudani, "Comparative Study of PMSG Controllers for Variable Wind Turbine Power Optimization", International Journal of Advanced Computer Science and Applications, vol. 9-8, pp. 239-246, 2018.

[23] B. Q. V. Ngo, P. Rodriguez-Ayerbe, S. Oluar, "Model Predictive Direct Power Control for doubly fed induction generator based wind turbines with three-level neutral-point clamped inverter", 42nd Annual Conference of the IEEE Industrial Electronics Society, Italy, 2016.

- [24] A. J. Laafou, A. A. Madi, A. Addaim, A. Intidam, "Dynamic modeling and improved control of a grid-connected DFIG used in wind energy conversion systems", *Mathematical Problems in Engineering*, 2020.
- [25] F. Blaabjerg, D. M. Ionel, "Renewable Energy Devices and Systems with Simulations in MATLAB and ANSYS", CRC Press, pp.213-221, 2017.
- [26] J. Hu, Y. Huang, D. Wang, H. Yuan, X. Yuan, "Modeling of grid-connected DFIG-based wind turbines for DC-link voltage stability analysis", *IEEE Transactions on sustainable energy*, vol. 6, pp. 1325-1336, 2015.
- [27] G. Abad, "Power Electronics and Electric Drives for Traction Applications", John Wiley & Sons, pp. 162-176, 2017.
- [28] N. Gurung, R. Bhattarai, S. Kamalasan, "Optimal linear-quadratic-integral controller design for doubly-fed induction generator", *IEEE Power & Energy Society General Meeting*, 2017.
- [29] K. S. Islam, W. Shen, A. Mahmud, M. A. Chowdhury, J. Zhang, "Stability enhancement of DFIG wind turbine using LQR pitch control overrated wind speed", *IEEE 11th Conference on Industrial Electronics and Applications*, 2016.
- [30] B. Mehta, P. Bhatt, V Pandya, "Small signal stability enhancement of DFIG based wind power system using optimized controllers' parameters", *International Journal of Electrical Power and Energy Systems*, vol. 70, pp. 70-82, 2015.
- [31] H. Oktay Erkol, "Linear Quadratic Regulator Design for position control of an inverted pendulum by grey wolf optimizer", *International Journal of Advanced Computer Science and Applications*, vol. 9, pp. 13-16, 2018.
- [32] R. Bhushan, K. Chatterjee, R. Shanka, "Comparison between GA-based LQR and Conventional LQR Control Method of DFIG Wind Energy System", *3rd International Conference on Recent Advances in Information Technology*, 2016.
- [33] I.Zgarni, L. El Amraoui, "Study of optimal control applied to a Doubly Fed Induction Generator attached to wind turbine system", *6th IEEE International Energy Conference*, pp. 511-514, 2020.

# Mask RCNN with RESNET50 for Dental Filling Detection

S Aparna<sup>1</sup>, Kireet Muppavaram<sup>2</sup>, Chaitanya C V Ramayanam<sup>3</sup>, K Satya Sai Ramani<sup>4</sup>

Department of Computer Science Engineering, GITAM School of Technology, Hyderabad, Telangana, India<sup>1</sup>

Department of Computer Science Engineering, JNTUH College of Engineering, Hyderabad, Telangana, India<sup>2</sup>

Student, Department of Computer Science Engineering, GITAM School of Technology, Hyderabad, Telangana, India<sup>3,4</sup>

**Abstract**—Teeth are very important for humans to eat food. However, teeth do get damaged for several reasons, like poor maintenance. Damaged teeth can cause severe pain and make it difficult to eat food. To safeguard the tooth from minor damages, an inert material is used to close the gap between the live part of the teeth or sometimes even the nerve and enamel. Although, long-time ignorance can increase the damage and inevitably result in root canal or tooth replacement. In the case of root canal, the gap between nerve and enamel is filled with an inert material. To check if the filling has been done properly, an X-ray is taken and verify. As technology is developing, robots are being introduced into many fields. In the medical field, there are instances where robots do surgery. For dental treatment, as an X-ray is taken to determine the filing, this work introduces a model to analyze the X-ray taken and estimate the level of filing done. The model is constructed using Mask RCNN with ResNet50 architecture. A dataset of different kinds of filings is taken and trained using the model. This model can be used to enable machines to perform dental operations as it works on pixel-level classification.

**Keywords**—Dental x-rays; deep learning; mask RCNN; RESNET50

## I. INTRODUCTION

Humans need food to survive. For eating food, teeth are essential and healthy teeth indicate healthy life. As medical sciences have advanced, dental research and learning also have advanced. People of the present generation have the most common issues related to teeth. As teeth are one of the most important parts of the body, which does most of the work helping in grinding the food consumed and supporting the digestive system, they need to be safeguarded from damage [28]. Not taking proper care of teeth may lead to some issues like cavities, swelling of gums, broken teeth, etc. When an issue arises, there are dentists who can attend the issue, and different problems need a different kind of treatment. Many issues may arise in teeth, and multiple solutions might be there to cure them. This project focuses on the external material that a dentist uses to fill, do the treatment, or close the gaps in teeth. This work mainly focuses on three things, namely “Endodontic”, “Restoration” and “Implant” [9], [13]. “Endodontic” refers to the stick-like tools that a dentist generally uses to clean the inner part of teeth. “Restoration” refers to the filing that a dentist does on some break, some cavities, and then caps that are used after a root canal. “Implant” is a screw-like structure used to provide rigidity and structure to the teeth. Many studies were also conducted

regarding identification of human using dental X-rays [7], [14], [16]. The aim of their work was to identify teeth as a unique bio metric system [21], [22], [23]. Their studies help this work by providing ways in which the uniqueness of teeth was identified by using computer vision.

This work aims at helping dentists identify the objects in a dental radiograph. This work benefits dentists, but it also helps common people read their own dental radiograph and understand the treatment being done [1], [2], [3], [4], [5]. The model focuses on detecting the filings in dental x-rays, which have been generalized to three classes. Assuming a case of many cases arising, there will be many x-rays taken to identify the teeth damage. Automating the detection helps reduce time and improve efficiency [6],[8].

Also, as robotics is being advanced and are brought into different fields, the medical field has also conducted experiments. There are works demonstrating robots doing and assisting in surgeries. In the future dental operations can also be automated, and robots can perform minor operations. By identifying objects at pixel level, this work can help robots in real-time identification of objects in radiographs. The models trained in this work use the concept of transfer learning where “COCO” (Common Objects in Context) dataset trained weights are imported, and the new dataset updates those weights for results [9]. A Mask RCNN (regional convolutional neural network) model is used with RESNET50 (residual neural network) as its backbone architecture.

The dataset for this project has been collected from different dental clinics in Hyderabad, Telangana, India. The dataset consists of several dental radiographs in “JPG” format containing RGBA (red, green, blue, alpha) channels. The images were processed and converted to RGB (red, green, blue) format with fixed dimensions of 416\*416. Then the images were annotated using the “Labelme” tool with three classes. After annotations, the model was trained with 100 images, 250 images, 500 images, 750 images, 1000 images, and 1755 images to see the improvement in results as the dataset size increases [27].

In this work, the medical radiographs are collected, which is the dataset required, annotated the images obtained. Then trained a MASK RCNN model with RESNET50 architecture with increasing dataset sizes, epochs in two variants. Also, the model is tested with increasing validation sets and considering the average as the final result.

## II. LITERATURE REVIEW

Chen H, et al, (2019) [6], have taken a dataset of 1250 dental X-ray films of periapical view and have trained a Faster RCNN model. They have done some post-processing to reduce the complexity of data for faster training of the model. Also, they suggest a filtering algorithm to delete overlapping boxes detected by their model. They have computed their results using IoU (Intersection over Union) score to calculate average recall. However, their work is limited to bounding boxes only which cannot be used for treatment with precision. The current work strives to improve the detection at pixel level to enable computer understand the exact position and region of treatment.

Jie Yang, et al, (2018) [27], have used a small dataset of 196 dental radiographs. They have said in their work that dental radiographs are important for clinical diagnosis and treatment. They have taken two classes for the condition of teeth. A CNN (convolutional neural network) model was constructed, and the F1 score was the measure of evaluation. Although, the author demonstrates results with a small dataset the accuracy is not satisfactory in terms of real time treatment. Taking the model into consideration, the current work intends to obtain the results which are more accurate and required for real time operations.

Kim J, et al, (2019) [19], have used a huge dataset of 12,179 panoramic dental radiographs to train a deep convolutional neural network. They have suggested a different measuring system where they have considered an increasing validation set count and finally computed the average F1 score. The mechanism to calculate results proposed by the author is unique. As such a similar way of validation system is implemented to summarize the end results of the current work.

## III. PROPOSED MODEL

As shown in Fig. 1, the project has four steps:

- Data Collection and processing
- Data Annotations
- Model Training
- Testing

In this work, data is collected, i.e., dental periapical view radiographs from different dental clinics in Hyderabad, Telangana, India [10]. After the collecting step, the data is processed, as shown by Chen H, et al, (2019) [6]. The dimensionality of images has to be reduced for less computational complexity, and also resizing images is a must for a model to accept them as training input. Then proceed to the data annotations step, where annotations are done for required objects in an image. An image can contain more than one object. After the annotations are done, the corresponding files are passed to the model for training. The model is trained with certain parameters and is passed to the testing stage. The IoU threshold in the testing phase is set to 50% and AP50 (average precision) score is obtained.



Fig. 1. Proposed Model Workflow.

### A. Data Collection

In this work, 1000 dental radiographs of periapical view have been collected from different dental clinics in Hyderabad, Telangana, India. The dental radiographs collected are images of “JPG” format with four channels RGBA. The images are processed by resizing to 416x416 dimensions to reduce the dimensional complexity. Also, the alpha channel is being eliminated, i.e., the images are converted from RGBA to RGB data. The images have a total of three classes: “endodontic”, “restoration” and “implant”.

### B. Data Annotations

The images collected have to be annotated. Annotation indicates creating a mask around the desired object for the algorithm to identify and train on. Image annotations are done using “Labelme” tool. “Labelme” tool, as shown in Fig 2, is an open-source manual annotation creator. It provides us with the “create polygons option” that is used to create a mask around desired objects. A single image can have more than one desired object and of different class. A json file is generated containing the mask coordinates and the class identity name for every image annotated.

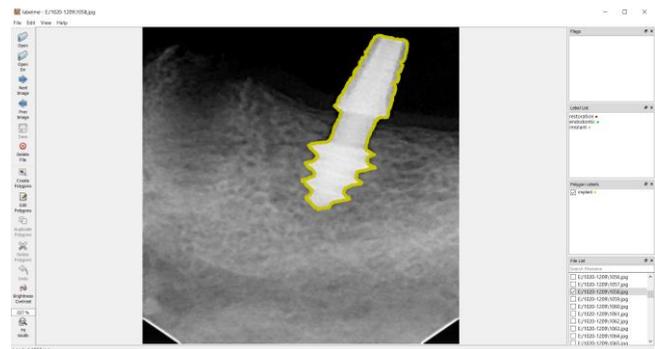


Fig. 2. Labelme Tool Interface.

### C. Model Training

After the annotations have been completed, combine all the json files to a single json file for the model to train on. A python script is used for the conversion. All the images along its corresponding json file are uploaded into google drive. The main model used to train is Mask RCNN which is capable of instance segmentation [11], [15]. The model was trained with base learning rate of 0.002, with 600 epochs and 10 images per batch. The model weights are the “COCO” instance model weights which are updated through transfer learning [24], [25].

## IV. MODELS

### A. Mask RCNN

Mask RCNN is a deep neural built to process instance segmentation i.e., it can identify objects at pixel level. Mask RCNN does both object detection and instance segmentation. As the work is aimed at identifying objects in real time at pixel level, the algorithm implemented is Mask RCNN. Mask RCNN has two stages of training. Initially, region proposals are generated where objects might be present in an input image. Now, in the second stage, these proposals are used to predict the object class and construct a bounding box around the object detected. The bounding box is refined and a mask is generated

at pixel level for the proposal in the first stage. Both these stages are connected to the backbone architecture.

The backbone architecture used in this project is “RESNET50” [17], [18]. A backbone architecture is a feature pyramid network-style deep neural network. “RESNET50” architecture is a bottom-up pathway that extracts features from the input raw images. Fig. 3 shows the architecture of Mask RCNN algorithm.

In the first stage, use a region proposal network to propose the regions where objects are expected. Now a feature map is generated through the proposals to bind the features to their locations in raw images. Now, use anchors, a set of boxes with predefined locations that are scaled with respect to the images. Use anchors of different size to bind the different levels of feature map, the region proposal network uses these anchors to Fig out the region of the feature map that should get an object and what dimension the bounding box should be. Convolution, down sampling and up sampling of feature map would retain the relative positions of objects in the original image.

In the second stage, take another neural network that takes proposed regions as input which is generated by the region proposal network in stage one [26]. The pixel level classification is done by fully connected network (FCN) as shown in Fig. 4. These proposals are now taken by a new neural network and assigned to several specific areas of a feature map level. These areas are scanned and object classes are generated with bounding boxes and masks. The main trick used here is the “ROI align” (Region of interest) used to locate the relevant areas of the feature map. A branch of “ROI align” is used to generate masks at pixel level for an image.

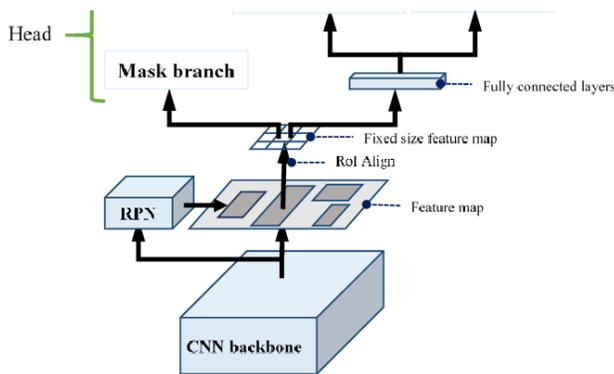


Fig. 3. Mask RCNN Architecture.

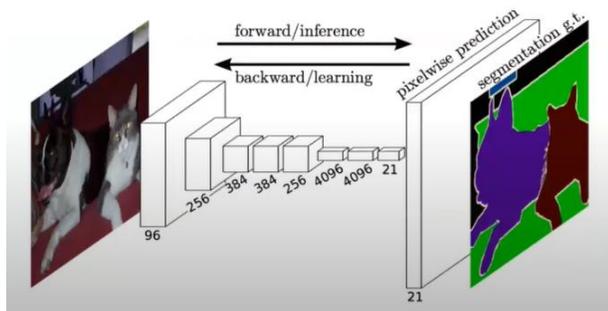


Fig. 4. FCN Showing Pixel Level Classification.

In “Faster RCNN” it uses “ROI pooling” for the case quantization where the bounding box dimensions become the desired dimensions [12]. In case of “ROI align” there is no necessity for quantization for data pooling [6]. As shown in Fig. 5 the dimensionality has to be changed in mapping or pooling process requiring the use of bilinear interpolation.

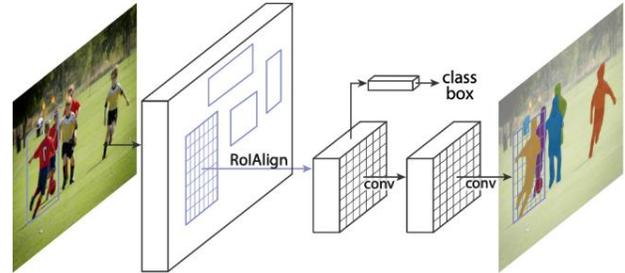


Fig. 5. ROI Align in RESNET50 Architecture.

### B. RESNET50

Resnet50 algorithm was made with the aim of solving vanishing gradient problem [20]. Vanishing gradient problem is a case in neural networks where the loss when sent back to update weights of the nodes, the differential value calculated becomes so small that the weights no longer get updated. In such a case the loss of the model does not decrease and the model is not capable of learning anymore. In case of RESNET models the input and processed input are both sent to the next stage of layers and the same happens when loss is propagated through the model. This concept is known as “skip connection”.

If ‘x’ is the input and f(x) is the function output. As neural networks are good function approximators, they should be capable to identify a function where the output becomes input itself.

$$f(x) = x \tag{1}$$

Assuming this if the input of the first layer of model is bypassed to be the output of the last layer of the model, the network should be able to predict the function it was learning before with the input added to it.

$$f(x) + x = h(x) \tag{2}$$

With RESNET one can pass the gradients through skip connections to the next layers of a model and from end layers to initial layers. Resnet50 deals with 48 convolutional layers along with 1 “MaxPool” and 1 “Average Pool”. It all starts with a convolutional layer with kernel size 7\*7\*3 with dimension of 64 and then stride 2. Then “MaxPooling” is done where for each feature map the maximum number is extracted to reduce the dimension of the image, which also reduces noise and then enter into the main Resnet layers in which they perform the convolutions with kernel size of 3\*3\*3 with the dimension set of 64, 128, 256 and 512. For every 2 convolutional blocks the skip connection takes place where the input and output value doesn’t change.

The dimension changes with stride 2 during the skip connection, like from 64 to 128 then dimension change causes

problem at that particular time. In any case one convolutional block is added to the skip connection process for dimension change to take place without mismatch and errors. After all the RESNET layers are traversed, “Average pooling” is done where the average value is taken from a particular feature map and gives the output. This helps in smoothening of the image but this method cannot be used for sharp images. Fig. 6 showcases the concept of “skip connection”.



Fig. 6. RESNET Model Skip Connection.

After that, the obtained feature map is flattened and then passed to an artificial neural network. The process continues where certain weights are assigned with the inputs and sent to the successive layers, known as forward propagation. Loss is calculated at the output layer which is back propagated to the previous layers to update weights for improving the model. Fig. 7 shows a demonstration of RESNET50 architecture.

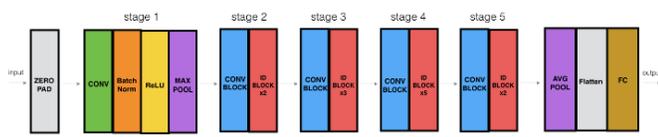


Fig. 7. RESNET50 Architecture.

### V. RESULTS

The results for the instance segmentation problems are measured using the average precision scores. For measuring any classification object, preliminarily calculate “True Positive” (TP), “True Negative” (TN), “False Positive” (FP) and “False Negative” (FN). In instance segmentation, calculate them by using Intersection over Union (IoU) score as shown in Fig. 8. As a mask is being generated around the objects in the input image and have the ground truth of the object, try to find the area of intersection of the two masks and calculate the area union of the two masks. These values are divided to get Intersection over Union score.

The Intersection over Union score is now used as along with a threshold where if the IoU score is greater than threshold then it is considered as “True Positive” and if the IoU score is less than threshold then it is considered as “False Positive”. If an object is not being recognized, it is a “False Negative” and a wrong classification is considered “False Positive”. Fig. 9 is a sample of area covered by bounding boxes and ground truth to calculate IoU score for classification.

Using these values, the precision values are calculated. Precision is the measure of true positive detections.

$$Precision = \frac{TP}{TP+FP} \tag{3}$$

$$IoU = \frac{\text{area of overlap}}{\text{area of union}} = \frac{\text{area of intersection}}{\text{area of union}}$$

Fig. 8. Intersection over Union Calculation.

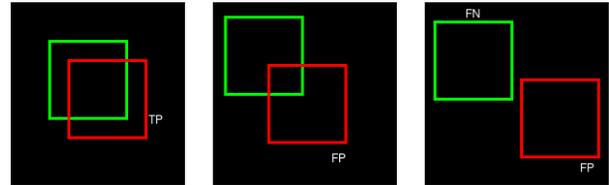


Fig. 9. IoU Score Classification.

In evaluations, 50% threshold is being considered. AP50 means the average precision at 50% IoU threshold.

The dataset has been split into parts of increasing order to observe the change in results as the dataset used for training is being improved. Taking the data sizes of 100, 250, 500, 750 and 1000 into consideration and testing over validations sets of 20, 50, 100, 150 and 200 [27], [29]. After calculating the results, the average value was calculated and was considered the final AP50 score. Starting with dataset of 100 the results obtained for bounding boxes are: 55.963, 54.636, 54.12, 46.881, 63.141 and for mask segmentation are: 58.186, 51.193, 51.649, 37.723, 56.268 respectively as shown in Fig. 10. The dataset was trained for 600 epochs as the loss was minimum and stable at that point.

Moving on to the dataset with 250 images; the results for bounding box AP50 scores are: 59.571, 55.252, 54.14, 51.654, 55.503 and for mask segmentation are: 59.571, 50.282, 49.546, 40.736, 46.59 as shown in Fig. 11. The dataset was trained for 600 epochs as well.

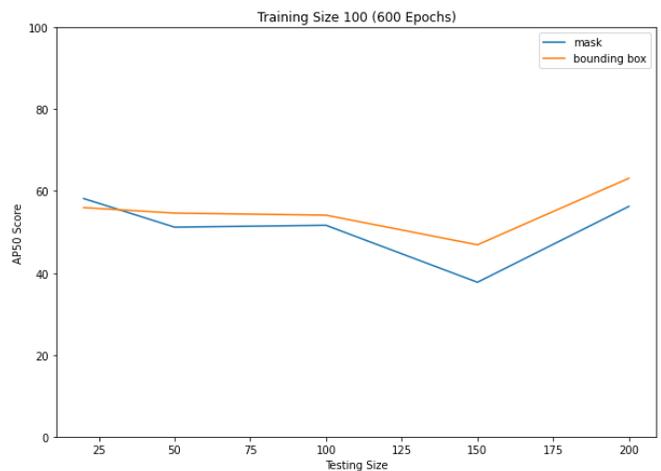


Fig. 10. AP50 Scores Obtained for Dataset of 100 Images.

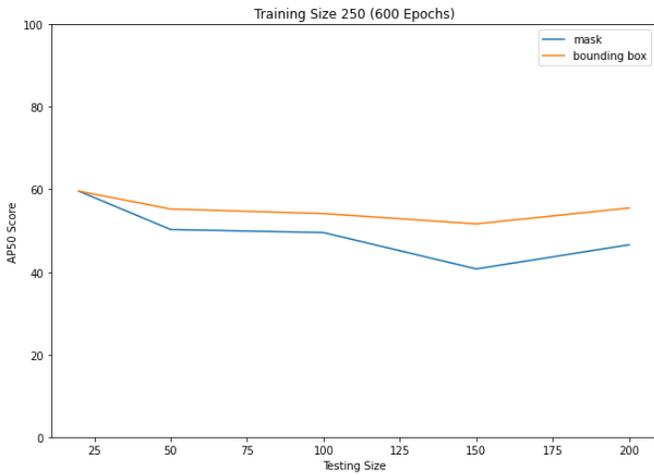


Fig. 11. AP50 Scores Obtained for Dataset of 250 Images.

Moving on to the dataset with 500 images; the results for bounding box AP50 scores are: 75.596, 71.929, 76.32, 60.471, 76.283 and for mask segmentation are: 69.166, 64.899, 72.075, 47.209, 66.472 as shown in Fig. 12. The dataset was trained for 600 epochs as well.

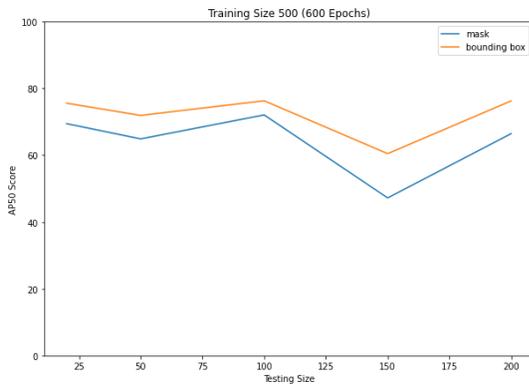


Fig. 12. AP50 Scores Obtained for Dataset of 500 Images.

Moving on to the dataset with 750 images; the results for bounding box AP50 scores are: 83.168, 81.3, 79.203, 68.126, 80.022 and for mask segmentation are: 85.269, 78.019, 75.605, 57.17, 71.194 as shown in Fig. 13. The dataset was trained for 600 epochs as well.



Fig. 13. AP50 Scores Obtained for Dataset of 750 Images.

Finally, the dataset with 1000 images; the results for bounding box AP50 scores are: 84.334, 82.489, 78.091, 84.083, 83.28 and for mask segmentation are: 86.883, 76.708, 75.186, 72.115, 76.029 as shown in Fig. 14. Although, the dataset was trained for 600 epochs there was still trainable parameters.

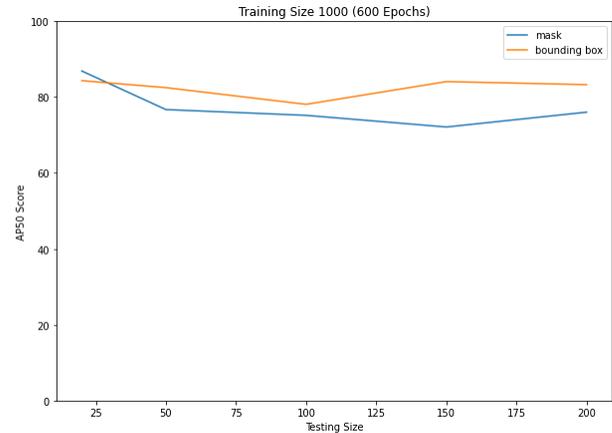


Fig. 14. AP50 Scores Obtained for Dataset of 1000 Images for 600 Epochs.

The model trained utilized the transfer learning concepts and the weights were imported from the “COCO dataset” model. Transfer learning is the concept where the weights are imported by training a model on a different dataset. This should help the new model update weights in less epochs. For the model trained with 600 epochs, observations seen were best bounding box and mask segmentation average AP50 score with 1000 images dataset.

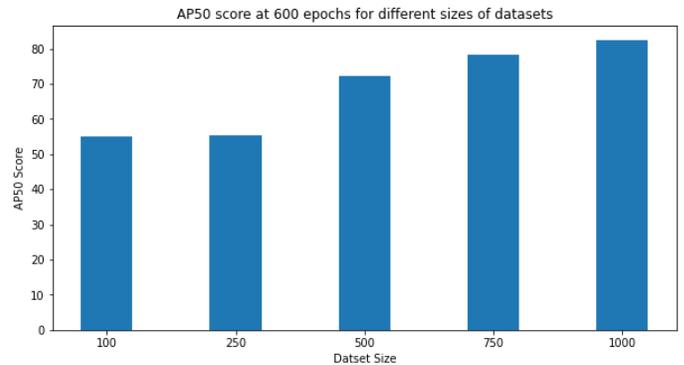


Fig. 15. Comparing AP50 Score of different Dataset Sizes with respect to Bounding Boxes.

As continuing with observations, the 1000 images dataset has obtained AP50 score of 82.4554 for bounding boxes and 77.3842 for mask segmentation at 600 epochs. Fig. 15 compares the AP50 scores of different datasets and it is observed that 1000 images dataset has the best results yet, however it is also inferred that improvement in results with respect to dataset size declines exponentially.

Further, the 1000 images dataset was in two variations:

- With transfer learning (1200 epochs).
- Without transfer learning (1600 epochs).

When trained with transfer learning for 1200 epochs on 1000 images dataset the model gave AP50 scores of 88.4248 and 84.2662, respectively for bounding boxes and mask segmentation as shown in Fig. 16.

Also, for training without transfer learning, the weights are initiated and updated from scratch. Due to which the model needed to be trained for 1600 epochs where the loss stabilizes. The results obtained at this stage are 76.1696 and 72.123 for bounding boxes and mask segmentation as shown in Fig. 17.

In Fig. 18, the results of “with transfer learning” and “without transfer learning” are compared and it is observed that “with transfer learning” model gives better results. Additionally, as observed that with an increase in the dataset size, the results also improve. So, another dataset consisting of 1755 images is considered.

The 1755 images dataset was trained for 1200 epochs with transfer learning and obtained an AP50 score of 88.2416 and 82.1224 respectively for bounding boxes and mask segmentation as shown in Fig. 19.

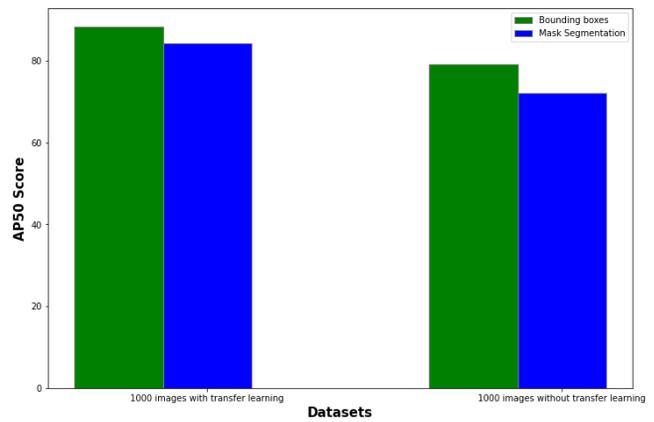


Fig. 18. Comparing Results of 1000 Images with and without Transfer Learning.

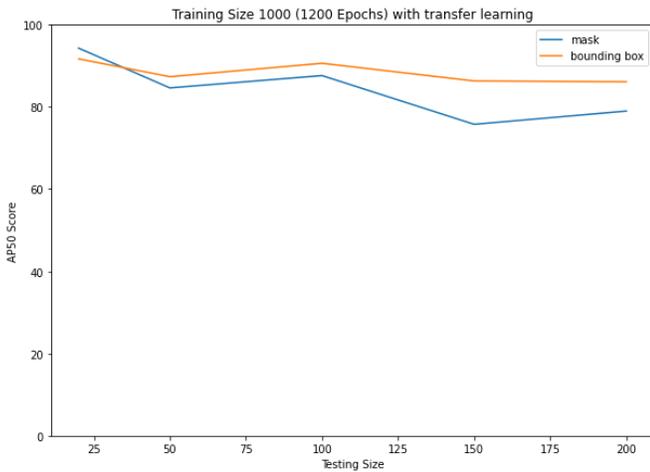


Fig. 16. AP50 Scores Obtained for Dataset of 1000 Images at 1200 Epochs.

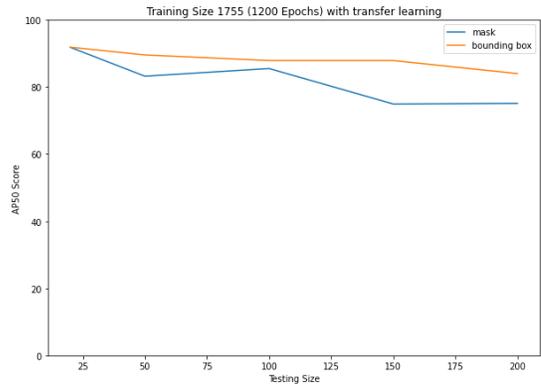


Fig. 19. AP50 Scores Obtained for Dataset of 1755 Images at 1200 Epochs.

Also, the 1755 images dataset is trained without transfer learning for 1600 epochs and obtained 82.3398 and 62.7846 AP50 scores respectively for bounding boxes and mask segmentation as shown in Fig. 20.

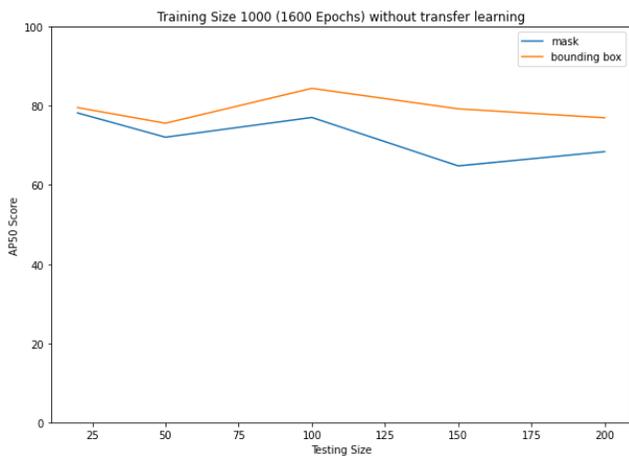


Fig. 17. AP50 Scores Obtained for Dataset of 1000 Images at 1600 Epochs without Transfer Learning.

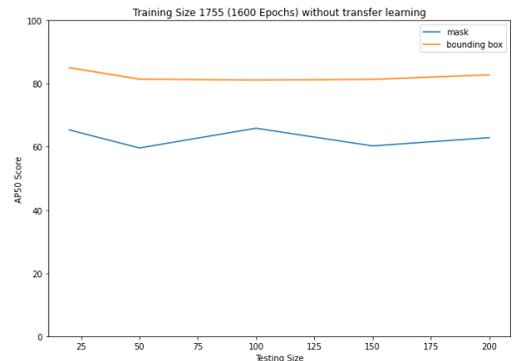


Fig. 20. AP50 Scores Obtained for Dataset of 1755 Images at 1600 Epochs without Transfer Learning.

Although the results obtained seem stable and do not alter much, the size of the dataset showed that the model could be trained further and improved. The 1755 images dataset was trained further for 2400 epochs, and results obtained showed improvement. It obtained AP50 scores of 87.9548 and 76.1272 for bounding box and mask segmentation, respectively as shown in Fig. 21.

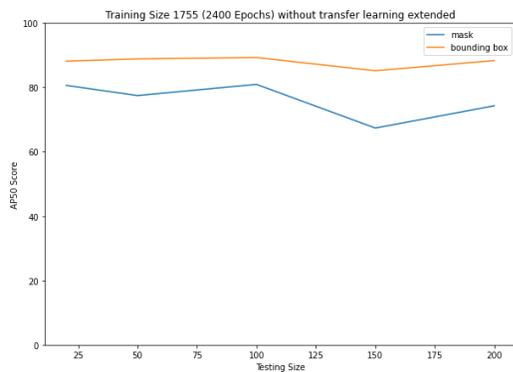


Fig. 21. AP50 Scores Obtained for Dataset of 1755 Images at 2400 Epochs without Transfer Learning.

As observed, the results have improved and altered less, showing that the complexity change in images will not affect the model much. Also, as the 1000 images dataset has obtained better results for mask segmentation, the results may vary depending on the complexity of images but with less intensity.

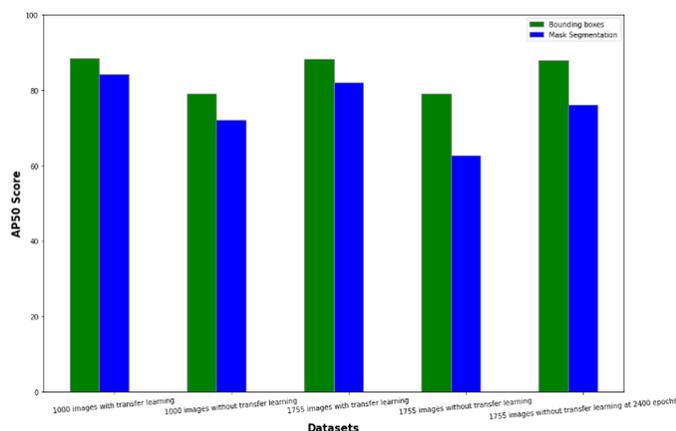


Fig. 22. Comparing AP50 Scores of 1000 and 1755 Images Datasets.

From Fig. 22, one can observe that the bounding box AP50 was highest for the 1755 images dataset trained without transfer learning for 2400 epochs but the mask segmentation AP50 score was highest for the 1000 images dataset with transfer learning at 1200 epochs. One can still observe that results are stable and vary less when there is an increase in dataset size with increased epochs.

## VI. CONCLUSION

The need for expertise in dental clinics is a must. Making the process of taking and reading radiograph must be improved. Also, robotic treatment in dental science needs a system to understand and identify dental objects at the pixel level. This work provides a model that can identify the dental objects at pixel level and has obtained an Average Precision-50 score of 84 and 88 for mask segmentation and bounding boxes respectively for 1000 images dataset at 1200 epochs. The model used in this work is Mask RCNN with RESNET50 architecture. The training was done in two variants of with transfer learning and without transfer learning and with increasing dataset sizes and epochs.

The work demonstrates the mask generated around a tooth with pixel level accuracy which can be further developed for robotic treatment in the future. The model showcases results which are considerable to further explore with more resources for better results that are satisfactory for medical treatment. The AP50 scores of 1000 images dataset prove to be good when trained for 1200 epochs. While the 1755 dataset at 1200 epochs give AP50 scores of 88 and 82 for bounding boxes and mask segmentation. Increasing the number of epochs without transfer learning give similar results for bounding boxes but mask segmentation has reduced by a lot. The results of 1755 dataset trained without transfer learning for 1600 and 2400 epochs give 82 and 87 AP50 scores respectively but the mask segmentation scores have declined to 62 and 76. Further training of model may improve the scores but for more better and practical results it is suggested to increase the dataset size.

The work can be further improved by taking a larger dataset, as observed there is an improvement in results with an increase in dataset size. Also, in this work, the classes of objects have been generalized to three. More specific classes can also be taken for object detection with the help of a dentist or a person with good knowledge in dental science, and work can be improved further.

## REFERENCES

- [1] Abdel-Mottaleb, J. Z. (2005). A content-based system for human identification based on bitewing dental X-ray images. *Pattern Recognition*, 2132-2142.
- [2] Abdel-Mottaleb, M. H. (2005). Classification and numbering of teeth in dental bitewing images. *Pattern Recognition*, 577-586.
- [3] Abdel-Mottaleb, O. N. (2005). A system for human identification from X-ray dental radiographs. *Pattern Recognition*, 1295-1305.
- [4] Anil K. Jain, H. C. (2004). Matching of dental X-ray images for human identification. *Pattern Recognition*, vol. 37, 1519-1532.
- [5] Anny Yuniarti, A. S. (2012). Classification and Numbering of Dental Radiographs for an Automated Human Identification System. *TELKOMNIKA*, 137-146.
- [6] Chen H, Z. K. (2019). A deep learning approach to automatic teeth detection and numbering based on object detection in dental periapical films. *Sci Rep* 9.
- [7] Chen, A. K. (2004). Matching of dental X-ray images for human identification. *Pattern Recognition*, 1519-1532.
- [8] Chen, H., Zhang, K., Lyu, P. et al. A deep learning approach to automatic teeth detection and numbering based on object detection in dental periapical films. *Sci Rep* 9, 3840 (2019). <https://doi.org/10.1038/s41598-019-40414-y>
- [9] Everingham, M. V. (2010). The PASCAL Visual Object Classes (VOC) Challenge. *Int J Comput Vis* 88, 303-338.
- [10] Geert Litjens, T. K. (2017). A survey on deep learning in medical image analysis. *Medical Image Analysis*, 60-88.
- [11] G. Zhu, Z. Piao and S. C. Kim, "Tooth Detection and Segmentation with Mask R-CNN," 2020 International Conference on Artificial Intelligence in Information and Communication (ICAIC), 2020, pp. 070-072, doi: 10.1109/ICAIC48513.2020.9065216.
- [12] He, K. a. (2015). Spatial Pyramid Pooling in Deep Convolutional Networks for Visual Recognition. *IEEE Transactions on Pattern Analysis and Machine Intelligence*, 1904-1916.
- [13] Huang, P. L. (2010). An effective classification and numbering system for dental bitewing radiographs using teeth region and contour information. *Pattern Recognition*, 1380-1392.
- [14] Jindan Zhou, M. A.-M. (2005). A content-based system for human identification based on bitewing dental X-ray images. *Pattern Recognition*, vol. 38, 2132-2142.

- [15] Kaiming He, G. G. (2017). Mask R-CNN. *Clinical Orthopaedics and Related Research*.
- [16] Kandelman, D. a. (2012). Oral health care systems in developing and developed countries. *Periodontology 2000*, 98-109.
- [17] Khalifa, M. L. (2021). Fighting against COVID-19: A novel deep learning model based on YOLO-v2 with ResNet-50 for medical face mask detection. *Sustainable Cities and Society*.
- [18] Kim, C.; Kim, D.; Jeong, H.; Yoon, S.-J.; Youm, S. Automatic Tooth Detection and Numbering Using a Combination of a CNN and Heuristic Algorithm. *Appl. Sci.* 2020, 10, 5624. <https://doi.org/10.3390/app10165624>
- [19] Kim J, L. H. (2019). DeNTNet: Deep Neural Transfer Network for the detection of periodontal bone loss using panoramic dental radiographs. *Sci Rep* 9.
- [20] Kumar, S. R. (2021). Using handpicked features in conjunction with ResNet-50 for improved detection of COVID-19 from chest X-ray images. *Chaos, Solitons & Fractals*.
- [21] Nomir Omaira, A.-M. M. (2007). Human Identification From Dental X-Ray Images Based on the Shape and Appearance of the Teeth. *IEEE Transactions on Information Forensics and Security*, 188-197.
- [22] Omaira Nomir, M. A.-M. (2005). A system for human identification from X-ray dental radiographs. *Pattern Recognition*, 1295-1305.
- [23] S. Tohna, A. M. (2007). Synthesizing Dental Radiographs for Human Identification. *Journal of Dental Research*, 1057-1062.
- [24] Said, E. a. (2006). Teeth segmentation in digitized dental X-ray films using mathematical morphology. *IEEE Transactions on Information Forensics and Security*, 178-189.
- [25] Shashikant Patil, V. K. (2019). Algorithmic analysis for dental caries detection using an adaptive neural network architecture. *Heliyon*, vol. 5.
- [26] Tsung Yi, e. a. (2016). Feature Pyramid Networks for Object Detection. *Clinical Orthopaedics and Related Research*.
- [27] Yang Jie, X. Y. (2018). Automated Dental Image Analysis by Deep Learning on Small Dataset. 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC), 492-497.
- [28] You W, H. A. (2020). Deep learning-based dental plaque detection on primary teeth: a comparison with clinical assessments. *BMC Oral Health* 20.
- [29] Zhang, Z. L. (2018). Large-scale retrieval for medical image analytics: A comprehensive review. *Medical Image Analysis*, 66-84.

# Performance Analysis of Qualitative Evaluation Model for Software Reuse with AspectJ using AHP

Ravi Kumar<sup>1</sup>

Research Scholar, MMICT& BM  
Maharishi Markandeshwar Deemed to be University  
Mullana (Ambala)-133207, Haryana, India

Dalip<sup>2</sup>

Assistant Professor, MMICT& BM  
Maharishi Markandeshwar Deemed to be University  
Mullana (Ambala)-133207, Haryana, India

**Abstract**—Reusability is necessary for developing advance software. Aspect Oriented programming is an emerging approach which understand the problem of arrangement of scattered software modules and tangled code. The aim of this paper is to explore the AOP approach with implementation of real life projects in AspectJ language and its impact on software quality in form of reusability. In this paper, experimental results are evaluated of 11 projects (Java and AspectJ) using proposed Quality Evaluation Model for Software Reuse (QEMSR) and existing Aspect Oriented Software Quality Model (AOSQ). To evaluate AOP quality model QEMSR based on developers AOP projects by using Analytic Hierarchy Process (AHP) tools. Paper provides the evaluation of software reusability and positive impact on software quality. QEMSR model is used to assess Aspect Oriented reusability quality issues, which helps developers to adapt for software development. The overall quality of three models QEMSR, existing AOSQ and PAOSQMO are 0.62552223, 0.5283693, and 0.505815 calculated. According to this, QEMSR model is best in form of quality in same characteristics and sub-characteristics.

**Keyword**—Reusability; AspectJ; software quality metrics; analytic hierarchy process

## I. INTRODUCTION

Various software quality models described the assessment of software quality in software engineering. Quality assessment of software is an interesting research area in software engineering. Several AOSD seminars, workshops and research conferences had considered evaluation of quality of software model is emerging sector in traditional software engineering journals and conferences. According to IEEE/ACM “Software Engineering Curriculum Guidelines list software engineering education” in 2004 as one of the ten specific areas of software engineering education[5][20]. Various international network groups and research communities are working on software evolution. Software evolution concerned issues are very complex because it engages with various dimensions.

This paper focuses performance evaluation of proposed Qualitative Evaluation Model for Software Reuse (QEMSR) by experimentation method using characteristics and its sub-characteristics. We describe some metrics such as WMC, DIT, NOC, LCOM, and CBO for statistical value [10]. We also analyze the existing model such as Aspect Oriented Software Quality Model (AOSQ) and Proposed AO Software Quality Model (PAOSQMO) to examined performance evaluation. The negative impact on software quality is duplication of code.

Crosscutting concerns reduced to have negative effect on understandability, maintainability, operability, modularity because understanding and changing crosscutting concerns requires touched various place in source code.

In existing system, firstly crosscutting concerns are derived after that distinguishes into aspects. Main traditional software reveals crosscutting concern that is called “tyranny of the dominant decomposition.” In existing system, exploration helps to find out aspect. Aspects will help the software developers to examine where and how these tangling and scattering codes are implemented and its effect on quality of software [9]. This process is called aspect mining which is used to examine crosscutting concerns in existing model codes.

Contribution of the paper:

- To examine area of evolution of traditional programming (OOPs) different form evolution of Aspect Oriented Programming (AOP).
- To promote evolution of Object-oriented Programming (OOPs) be implemented to Aspect-oriented Programming (AOP).
- To improve performance evaluation of software quality models in software engineering.

This paper divides into eight sections. First section describe introduction about Aspect-oriented Programming. Related work has been done by the researcher explain in section two. Third section defines the framework or method to achieve research goal and motivation to do that work. Section four and five describe the platform used for practical work and design and result of experiment. Section six describes the analysis of experimental result and qualitative evaluation of 11 research case studies and its impact on quality. Examine performance evaluation of QEMSR model and existing model is described in section seven. In section eight, we discussed major finding of proposed quality model as conclusion and area for future research work for researcher point of view.

## II. LITERATURE REVIEW

In late 1990s, Aspect-oriented Programming (AOP) is an emerging area in evolution of software and it declares the positive impact on software quality; simultaneously, various risks, challenges and paradoxes for AOP adoption for development of software. In 2006, Steimann stated the question:

“Does aspect orientation really have the substance necessary to found a new software development paradigm or is it just another term to feed the old buzzword permutation based research proposal and PhD thesis generator?”

In 1997, Kiczales explore the idea of AOP pattern to modularize the crosscutting concerns in existing system. Table I shows last ten years quality models which is described time to time by researchers. Kumar et. al. extends the ISO/IEC 9126[11] quality model by adding some extra characteristics and sub-characteristics in 2009, called Aspect Oriented Software Quality Model (AOSQUAMO). AOSQUAMO model is first purely based on Aspect Oriented Software Development (AOSD). In 2010 another quality model REASQ is derived by Castillo et.al. REASQ quality model is the combination of ISO/IEC 9126 and ISO/IEC 25030 define by UML.

Simultaneously, Kumar et. al. adds evolvability as an attribute in software quality model for AOP application in 2012 named Aspect-oriented Software Quality (AOSQ) model [1] [18]. This model described four sub-characteristics such as sustainability, design stability, extensibility and configurability [4] [16]. AOSQ model is based on AOSQUAMO and ISO/IEC9126 quality model [23].

G. Suryanarayana et.al. described MIDAS [13] model to analyze design quality assessment method for industrial software in 2013. T. Alrawashdeh and M.I. Muhairat were exploring the quantitative evaluation of enterprise resource planning systems proposing ERPSQM model in 2014[3] [12] [17]. In 2016, Pardeep Kumar Singh and Yugal Kumar assess the empirical evaluation of Aspect-oriented software quality model using multi-criteria decision making approach using PAOSQMO model.

Pankaj Kumar and S.k. Singh also measure a comprehensive evaluation of Aspect-oriented software quality model (AOSQ) using Analytic Hierarchical Process (AHP) [26] [28]. In 2018, Petrus Mursanto and Dameria Christina Pasaribu define software quality rank using AHP and Object-oriented metrics which is used to perform evaluation of quality of QEMSR model[14][24][30].

Sufia Nadeem Chishti explores the quality improvement in small scale projects using Aspect Oriented design in 2019[2] [19]. S. Dixit explores the performance of quality modeling using artificial neural network technique in Aspect Oriented Programming [7]. P. Kumar analyzes the metrics of Aspect Oriented and Object oriented using AspectJ and Java programming languages [8].

Hamed Fawareh proposed the software quality model for maintenance software purposes [6]. Bharti Bisht describes the metric approach to anticipate reusability of object oriented software systems [21].

K. Chitra measures the performance merits of software component using CK metrics [27]. We evaluate quality of QEMSR model using Analytic Hierarchical Process (AHP) that is based on AOS Quality Model (AOSQ) and PAOSQMO [25].

TABLE I. SOFTWARE QUALITY MODEL

Sr. No.	Quality Model	Year
1	Aspect-oriented Software Quality Model(AOSQUAMO)	2009
2	Quality Open Source Software (QualOSS) Model	2009
3	A software Component Quality Framework (Alvaro Model)	2010
4	REquirements, Aspects and Software Quality (REASQ) Model	2010
5	SCQM (Upadhyay Model)	2011
6	Software Quality Evaluation User's View (Al-Badareen Model)	2012
7	Quamoco Quality Meta-Model	2012
8	Aspect Oriented Software Quality Model (AOSQ)	2012
9	Method for Intensive Design Assessments (MIDAS) Model	2013
10	Aspect Oriented Software Reusability Measurement (AOSRM)	2014
11	ERPSQM	2014
12	Proposed Aspect Oriented Software Quality Model (PAOSQMO)	2016
13	Software Quality using AOP based Small Scale Projects	2019
14	AOSQ using Fuzzy Logic Model	2020
15	SQM for Maintenance Software Purposes	2020

### III. MOTIVATION AND METHODOLOGY

Last few years, various researcher working on different software quality model in software engineering. All researcher derived own quality model using some characteristics and metrics. These researchers also evaluate only derived model and not compared other researcher model in respect of quality. Every researcher use different technique to evaluate own quality model like Analytic Hierarchy Process, fuzzy logic, Gang of Four design pattern, etc. No anyone researcher can perform quality evaluation with same parameter with different quality model which is identify best model. So, we decide or motivate that we perform or derive a quality model in respect of reusability and its characteristics and metrics and compare with other model with same parameter. We also extend the qualitative evaluation of a model in more informative form, which helps for software developers to take decision to implement software or applications.

We can assume research methodology for this paper is software reengineering which is comparison analysis technique. Firstly, we can divide our objective into two parts like goals and sub-goals as shown in Fig. 1. In goals part, we define performance evaluation as purpose and concept use reusability. In sub-goals, internal characteristics and metrics are defined which measure the statistical data to evaluate quality. We can re-engineer concept that involve forward and reverse engineering principles. For experimentation purpose, we use quasi-controlled experimentation.

According to QEMSR model, research manipulates one or more independent variables to examine their impact on one or more dependent variables, set of metrics and validation of metrics [15]. We also describe the experimental part using 11 real world projects. We implement these projects in AspectJ and Java language and assign weight of methods and calculate average mean value for qualitative evaluation. All the 11 projects implement to assess contemporary phenomena within its real world situation.

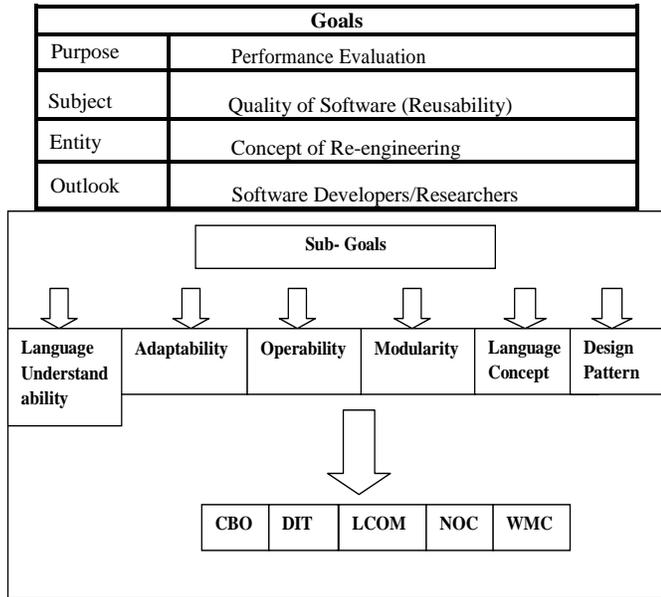


Fig. 1. Framework of QEMSR Model.

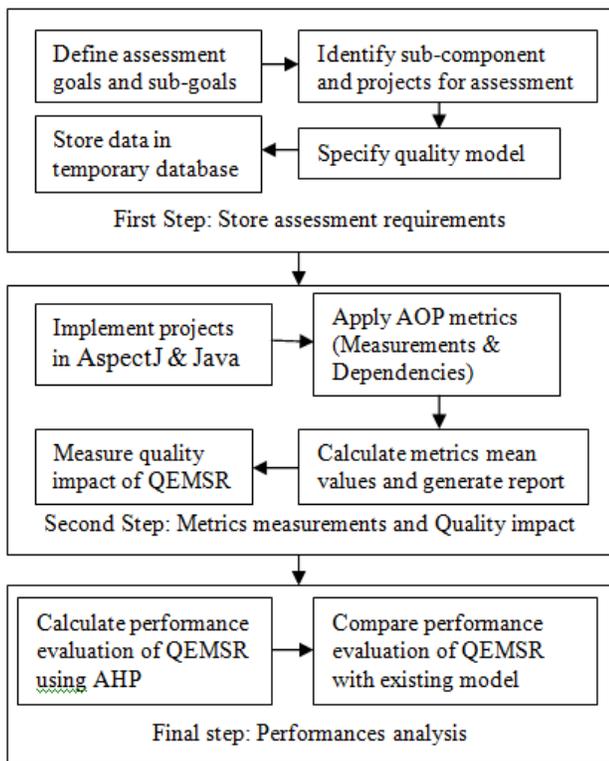


Fig. 2. Methodology for Performance Evaluation of QEMSR.

To achieve goals and sub-goals, we also use R. Marti, Henry and Li, Garcia et. al. and C & K metrics definition and these metrics associated for quality measurement in AOP [29]. QEMSR model proposed to validate metrics and analysis of qualitative evaluation and its impact on quality for AOP. To validate metrics we use experimental results of 11 projects implementations (Java & AspectJ). Experimental result gives intuitive information for the analysis of evolutionary aspects during Aspect-oriented software evolution. Fig. 2 describes the methodology for performance evaluation of QEMSR.

#### IV. EXPERIMENTAL SET-UP

Set-up for experimentation is for 11 projects (AspectJ and Java) to collect descriptive value (metrics) for the analysis of quality of software using AOP metric tools; a common AOP metric tool for both Aspect-oriented and Object-oriented metrics, such as R. Martin, Henry and Li and C & K. For doing experiment operating system required MS Windows XP/7/8, AspectJ 1.6, Java JDK 1.6v and AOP metrics 0.3 binary<sup>20</sup>. Ms-excel sheet generated for manipulation of descriptive data after successful execution of set of list files in a command line for a given source running compile.bat,(.1<sup>st</sup>)(projects) and metrics.bat files. All these descriptive data used for analysis for several AOP characteristics by impact tests and statistical tests.

#### V. EXPERIMENTAL DESIGN AND RESULTS

We can design procedure for 11 projects (AspectJ and Java) implementation for analysis of quality of AOP software consist five steps:

- Description of 11 projects which is used for experimentation or implementation (Java and AspectJ) as shows in Table II.
- Collection of data for experimental results and descriptive data used for AOP metric tools shown in Table IV.
- QEMSR framework which shown in Fig. 1.
- Methodology for performance evaluation of QEMSR shows in Fig. 2.

Ms-excel sheet generated for manipulation of descriptive data after successful execution of set of list files in a command line for a given source running compile.bat, (.1<sup>st</sup>)(projects) and metrics.bat files. All these descriptive data used for analysis for several AOP characteristics by impact tests and statistical tests.

The main goal to provide qualitative evaluation using 11 real world projects implementation (AspectJ and Java) using metric and statistical data with regard to reusability characteristics and sub-characteristics from the software developers view point. Only interesting metrics for this evaluation is DIT, NOC, CBO, LCOM, WMC of reusability characteristics and sub-characteristics. In this paper 11 projects real world system from different size and domain is shown in Table II. Table III shows the description of metrics adapted for QEMSR. Table IV shows the absolute mean values of 11 projects (AspectJ and Java).Using measurement of metrics we evaluate the experimental results on 11 projects and correlation among reusability characteristics and sub-characteristics. Table V shows the difference of average mean value of all 11

projects metrics and also calculate the impact of every metrics as graphically shown in Fig. 3. Table V contains the average mean value of metrics calculated as sum of different module divide by number of module taken for analysis. AHP is applied on these mean values to get corresponding weights of characteristics and sub-characteristics in which total quality weight has been taken as 1.000. These weights used for

comparing for Aspect –oriented projects. Aspect-oriented version of 11 projects shows an improvement in all structured complexity metrics. So for performance evaluation we compare existing AOSQ model and PAOSQMO model to select best suitable model for implementation in Aspect-oriented technology based projects.

TABLE II. DESCRIPTION OF 11 PROJECTS ( ASPECTJ & JAVA)

Name of projects	Description
AJHotDraw	Framework for structured and technical 2D graphics. <a href="http://ajhotdraw.sourceforge.net">http://ajhotdraw.sourceforge.net</a>
AspectTetris	Implementation of Tetris game in AspectJ. <a href="http://www.guzzt.com/coding/aspecttetris.shtml">http://www.guzzt.com/coding/aspecttetris.shtml</a>
PetStore	Demo for the J2EE platform which represent existing applications of E-commerce. <a href="http://java.sun.com/developer/releases/petstore/">http://java.sun.com/developer/releases/petstore/</a>
Eimp	Eclipse plug-in which support collaborative software developments for distributed teams. <a href="http://eimp.sourceforge.net">http://eimp.sourceforge.net</a>
HSQldb	Used for a relational database management system implementation. <a href="http://vrwxv.hsqldb.org">http://vrwxv.hsqldb.org</a>
Hypercast	Software for developing application programs and protocols for overlay network, application layer.
CVS Core	Eclipse plug-in which implements the basic functionalities of a CVS client such as check out and check in system stored in a remote repository. <a href="http://www.eclipse.org/eclipse/platform-cvs/">http://www.eclipse.org/eclipse/platform-cvs/</a>
AJFTPd-Server	Crosscutting concern implementation for security. Application level Server for BLP access control. <a href="http://homepages.wmich.edu/plbijjam/cs555/Projects/">http://homepages.wmich.edu/plbijjam/cs555/Projects/</a>
Telecom AspectJ	Examples of AspectJ <a href="http://www.eclipse.org/aspectJ/">http://www.eclipse.org/aspectJ/</a>
Spacewar Game AspectJ	Examples of AspectJ <a href="http://www.eclipse.org/aspectJ/">http://www.eclipse.org/aspectJ/</a>
Observer Pattern AspectJ	Examples of AspectJ <a href="http://www.eclipse.org/aspectJ/">http://www.eclipse.org/aspectJ/</a>

TABLE III. DESCRIPTION OF METRICS ADAPTED FOR QEMSR

Name of Metrics	Description
WMC	Total number of weighted operation in a class
CBO	Total number of interfaces declaring class or number of class or fields which can be called by a given class
LCOM	Total pairs of operation working on common fields minus total number of pairs of operation working on different
DIT	Longest path length From aspect/ class to the given class hierarchy root
NOC	It measures the total number of class, immediate descendants.

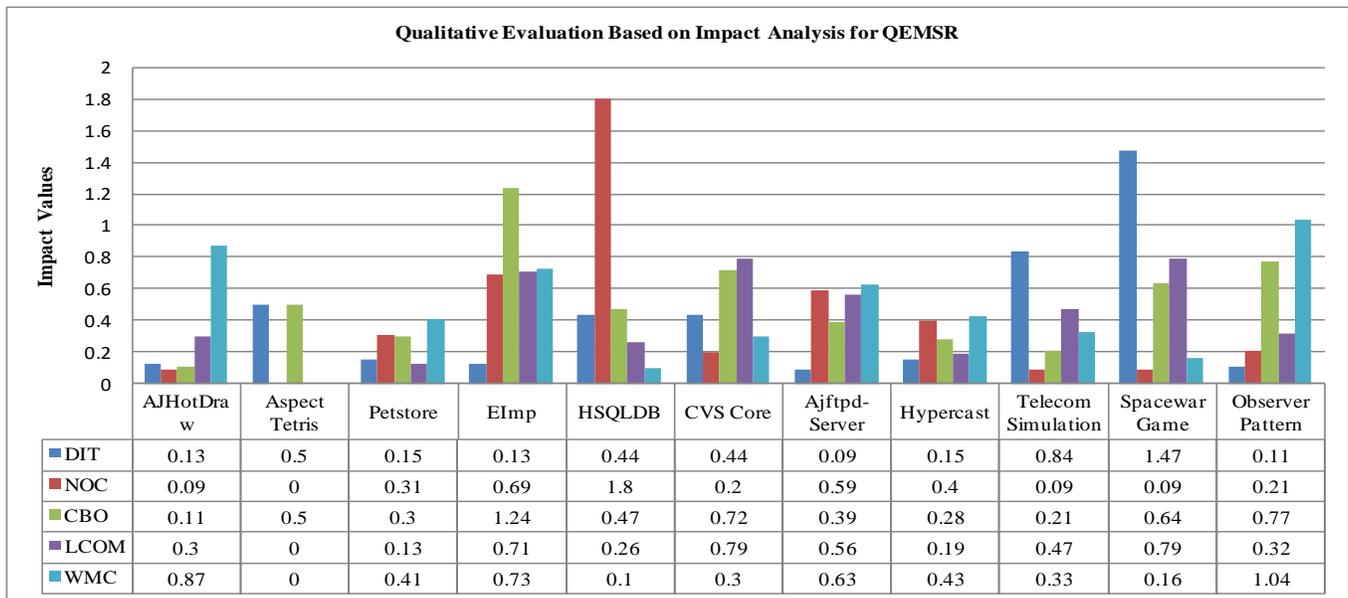


Fig. 3. Qualitative Evaluation based on Impact Analysis for QEMSR.

TABLE IV. ARITHMETIC MEAN VALUES OF QEMSR METRICS OF 11 PROJECTS

Projects /Metrics	Reusability and its Sub-characteristics										
	Modularity				Operability			Adaptability		Understandability	
	DIT		NOC		CBO		LCOM		WMC		
	AO	OO	AO	OO	AO	OO	AO	OO	AO	OO	
AJHotDraw	1.233	1.418	0.4794	0.5288	0.3390	0.3064	0.4567	0.6569	0.4976	0.2663	
Aspect Tetris	0.333	0.667	0.667	0	1.00	0.667	0	0	0	0	
Petstore	1.021	1.208	0.2784	0.4038	1.3904	1.068	1.367	1.5696	0.976	1.663	
EImp	1.233	1.418	0.4794	1.5288	2.3904	1.068	0.4567	1.5696	0.4976	1.863	
HSQLDB	0.233	0.418	1.4794	0.5288	0.967	0.6569	0.1976	0.2663	0.3390	0.3068	
CVS Core	0.233	0.418	0.4294	0.538	0.1567	0.5696	0.2976	0.1663	1.3904	1.068	
Ajftpd-Server	2.1233	1.9418	1.4794	0.9288	1.567	2.5696	0.276	0.63	0.3904	1.068	
Hypercast	2.1233	1.8418	0.8794	0.6288	0.2567	0.3569	0.1976	0.1663	0.3904	0.680	
Telecom-simulation	0.233	1.418	0.4794	0.5288	0.567	0.4696	0.976	0.663	1.3904	2.068	
Spacewar Game	1.033	0.418	0.4794	0.5288	2.567	1.5696	0.2976	0.1663	2.3904	2.068	
Observer Pattern	1.133	1.018	0.4094	0.5188	0.1567	0.6696	0.2976	0.2263	1.3904	0.680	

TABLE V. QUALITATIVE EVALUATION BASED ON IMPACT ANALYSIS FOR QEMSR

Project / Metrics	Reusability and its Sub-characteristics														
	Modularity						Operability			Adaptability			Understandability		
	DIT			NOC			CBO			LCOM			WMC		
	Diff	Impact	Qualitative Evaluation	Diff	Impact	Qualitative Evaluation	Diff	Impact	Qualitative Evaluation	Diff	Impact	Qualitative Evaluation	Diff	Impact	Qualitative Evaluation
AJHotDraw	0.19	0.13	Extremely Helpful	0.05	0.09	Extremely Helpful	0.03	0.11	Extremely Helpful	0.20	0.30	Very Helpful	0.23	0.87	Not so Helpful
Aspect Tetris	0.33	0.50	Helpful	0.67	0.00	Extremely Helpful	0.33	0.50	Helpful	0.00	0.00	Extremely Helpful	0.00	0.00	Extremely Helpful
Petstore	0.19	0.15	Extremely Helpful	0.13	0.31	Very Helpful	0.32	0.30	Very Helpful	0.20	0.13	Extremely Helpful	0.69	0.41	Helpful
EImp	0.19	0.13	Extremely Helpful	1.05	0.69	somewhat Helpful	1.32	1.24	Not at all Helpful	1.11	0.71	somewhat Helpful	1.37	0.73	somewhat Helpful
HSQLDB	0.19	0.44	Helpful	0.95	1.80	Not at all Helpful	0.31	0.47	Helpful	0.07	0.26	Very Helpful	0.03	0.10	Extremely Helpful
CVS Core	0.19	0.44	Helpful	0.11	0.20	Extremely Helpful	0.41	0.72	somewhat Helpful	0.13	0.79	somewhat Helpful	0.32	0.30	Very Helpful
Ajftpd-Server	0.18	0.09	Extremely Helpful	0.55	0.59	Helpful	1.00	0.39	Helpful	0.35	0.56	Helpful	0.68	0.63	somewhat Helpful
Hypercast	0.28	0.15	Extremely Helpful	0.25	0.40	Very Helpful	0.10	0.28	Very Helpful	0.03	0.19	Extremely Helpful	0.29	0.43	Helpful
Telecom simulation	1.19	0.84	Not so Helpful	0.05	0.09	Extremely Helpful	0.10	0.21	Very Helpful	0.31	0.47	Helpful	0.68	0.33	Very Helpful
Spacewar Game	0.62	1.47	Not at all Helpful	0.05	0.09	Extremely Helpful	1.00	0.64	somewhat Helpful	0.13	0.79	somewhat Helpful	0.32	0.16	Extremely Helpful
Observer Pattern	0.12	0.11	Extremely Helpful	0.11	0.21	Very Helpful	0.51	0.77	somewhat Helpful	0.07	0.32	Very Helpful	0.71	1.04	Not at all Helpful

Less than 0.20 = "Extremely Helpful" 0.20-0.40 = "Very Helpful" 0.40-0.60 = "Helpful"  
0.60-0.80 = "somewhat Helpful" 0.80-1.00 = "Not so Helpful" Greater than 1.00 = "Not at all Helpful"

## VI. EVALUATION OF RESULTS

The collection of data for every module (interface, class, aspect) of every system use the extended version of Aspect-oriented metric tools. For every real life project experimental result are represented independent. Crosscutting concerns investigated intensively for all 11 projects which show in Table II. For all project system represent common software problems and solution of those problems. Table IV define the average mean value of Aspect-oriented and Object-oriented implementations of 11 projects. The measurements of metrics have been computed but experimental results of 11 projects. The evaluation of quality of QEMSR model using characteristics and sub-characteristics and metrics adopted from C & K metric suite such as NOC, DIT, LCOM, WMC, and CBO. A smaller average value of lack of cohesion and coupling is between object taken for AOP AspectJ projects. Remaining metrics take same trends variation between values.

We can compare calculated percentage of all 11 project using matrices and determine difference of both AspectJ and Java implementation. 07 (64%) DIT metrics have higher value through Java implementation. 04 (36%) DIT metrics have higher value through AspectJ implementation. 04 (36%) LCO metrics have higher value through Java implementation. 06 (54%) LCO metrics have higher value through AspectJ implementation. 01 (10%) LCO have the same value. 07 (64%) NOC metrics have higher value through Java implementation. 04 (36%) NOC metrics have higher value through AspectJ implementation. 03 (27%) CBO metrics have higher value through Java implementation. 08 (73%) CBO metrics have higher value through AspectJ implementation. 03 (27%) WMC metrics have higher value through Java implementation. 07 (63%) WMC metrics have higher value through AspectJ implementation. 01 (10%) WMC have the same value. CBO and WMC have higher value as compared to NOC and DIT using AspectJ implementation. According to this, coupling is high in AspectJ implementation due to high value of WMC and CBO than the Java implementation. Limited numbers of projects are implemented in this paper, so we can't generalize the experimental results. Experimental results improve the validation of metrics for Aspect Oriented Programming and impact on quality of metrics. QEMSR model supports to take decision or choose the best quality for the applications software.

## VII. PERFORMANCE ANALYSIS OF QEMSR MODEL USING AHP

In this paper, we used two approaches to appraise the AOP and its impact on quality.

1) Qualitative evaluation of Aspect-oriented programming using QEMSR model and Analytic Hierarchy Process technique, similar approach used by Kumar A adapted in this paper [18]. Developer's projects used to determine impact of quality using Aspect-oriented programming (AspectJ) and Object-oriented programming (Java).

2) Describe performance evaluation of QEMSR model using Analytic Hierarchy Process (AHP) with existing model

Aspect-oriented Software Quality (AOSQ) model and Proposed Aspect-oriented Software Quality Model.

Saaty proposed Analytic Hierarchy Process technique uses the pair wise matrix to analyze ambiguity in multi-criterion decision-making problems. In this paper, n elements have main characteristics such as  $mC_1, mC_2, mC_3, \dots, mC_n$  considered, which have compared related weight of  $mC_i$  with respect to  $mC_i$  denoted as  $a_{ij}$ . A square matrix  $A = [a_{ij}]$  of order n as given in equation (1).

$$A = [a_{ij}] = \begin{matrix} & mC_1 & mC_2 & \dots & mC_n \\ mC_1 & \begin{pmatrix} 1 & a_{12} & \dots & a_{1n} \\ 1/a_{12} & 1 & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \\ mC_n & 1/a_{1n} & 1/a_{2n} & \dots & n \end{pmatrix} \end{matrix} \quad (1)$$

Where  $a_{ij} = 1/a_{ji}$ , for i is not equal to j and  $a_{ij} = 1$  for all i.

Matrix is said to be reciprocal metric.

$$A \cdot \omega = \lambda_{\max} \cdot \omega, \lambda_{\max} \geq n \quad (2)$$

Matrix involving human decision making, decision are inconsistent to a lesser or greater degree, in such a case find vector  $\omega$  satisfy the equation (2).

Here  $\omega$  is Eigen Vector and  $\lambda_{\max}$  define Eigen value. The dissimilarity between  $\lambda_{\max}$  and n if any is an indicator of inconsistency of decision. Saaty (1980) describe a consistency Index (CI) and Consistency Ratio (CR) to validate the consistency of the comparison matrix. Following equation is defined for validation:-

$$\text{Consistency Index (CI)} = (\lambda_{\max} - n) / (n - 1) \quad (5)$$

$$\text{Consistency Ratio (CR)} = \text{CI} / \text{RI} \quad (4)$$

Here RI is the average consistency Index over several random entries of same order reciprocal matrix. Saaty (1980) suggested that if the Consistency Ratio exceeds 0.1, set of decision or judgment may be too inconsistent to be reliable. In that condition, a new comparison matrix is required to prepare until Consistency Ratio (CR) is less than equal to 0.1.

In this sequence to determine the sub-characteristics and characteristic for software in Aspect-oriented, we manage a survey from programmer's expert or software developers working in industry and academic experts who have completed their projects and worked in AOP domain. We can identify the weight value of characteristics and sub-characteristics. A table is used to fill the pair wise relative weight value of eight characteristics from  $mC_1$  to  $mC_6$ . The mean of all gathered samples of pair wise relative weight are given in square matrix  $A = [a_{ij}]$  of order eight in equation, which is derived using equation(1) to apply Analytic Hierarchy Process. We have calculated Eigen vector and Eigen value to find the corresponding weight of  $mC_1, mC_2, mC_3, mC_4, mC_5, mC_6$  and CR. We also create a reciprocal matrix after that to calculate Eigen value and Eigen vector for CR and CI.

We assign value it to a square matrix taken from survey. We also assign pair wise relative weight value to all six characteristics using equation (1). Further step to calculate Eigen value and Eigen vector of get corresponding weights and CR. We calculate Eigen vector to multiply all the entries in every row of matrix A and take  $n^{\text{th}}$  root (i.e.  $6^{\text{th}}$  root) of the product helps in getting Eigen vector. Sum of the  $n^{\text{th}}$  root and used to normalize the Eigen vector element.

$$A=[a_{ij}] =$$

$$\begin{bmatrix} 1 & 2.00 & 4.00 & 2.00 & 3.00 & 7.00 \\ 0.50 & 1 & 0.25 & 1.00 & 1.00 & 4.00 \\ 0.25 & 0.33 & 3 & 2.00 & 2.00 & 4.00 \\ 0.50 & 0.33 & 0.5 & 0.33 & 0.05 & 1.00 \\ 0.33 & 2.00 & 1.0 & 2.00 & 1 & 3.00 \\ 0.14 & 0.25 & 0.25 & 0.33 & 0.3 & 1 \end{bmatrix} \quad (5)$$

Table VI shows all calculations and clearly show that  $A_n$ . We calculate  $A \cdot \omega$  and multiply the matrix ( $A_1$  to  $A_6$ ) from Eigen vector. Calculation of first row in Table V shown below:

$$(1 * 0.3499) + (2 * 0.1069) + (4 * 0.2189) + (2 * 0.0695) + (3 * 0.144) + (7 * 0.0342) = 2.2497.$$

The values for remaining five rows are calculated similarly. As per equation (2),  $\lambda_{\max} \geq 6$ , to determine product of  $A \cdot \omega$  Eigen value also determined by using  $\lambda_{\max} = (A \cdot \omega) / \omega$ . All values are greater than six which satisfy the condition  $\lambda_{\max} \geq n$  we calculate Consistency Index using equation (3):

$$CI = (6.46792 - 6) / (6 - 1) = 0.093584$$

After that we calculated CR for set of judgment using CI for considered samples. RI value can be taken from Saaty a scale that is 1.24[22].

$$CR = (0.093584 / 1.24) = 0.07547$$

The calculated value of Consistency Ratio (CR) is 0.1 which indicates estimate is acceptable. The assessment of overall quality of any AOP projects evaluated using below mentioned formula:-

$$AO \text{ Project Quality} =$$

$$\sum_{i=0}^n \text{Comparative value of Sub characteristics } (SC_i) * \text{weight value of } SC_i$$

Where n is the number of sub-characteristics,  $SC_i$  is sub-characteristic  $i$ . We are determining quality of our QEMSR model and existing Aspect-oriented Software Quality (AOSQ) model and existing Proposed Aspect-oriented Software Quality Model (PAOSQMO) as shown in Table VII. The overall quality of three models QEMSR, AOSQ and PAOSQMO are 0.62552223, 0.5283693, 0.505815. According to this, QEMSR model is best in form of quality in same characteristics and sub-characteristics. This calculation shows that overall quality of QEMSR is defined positive impact on software quality. This paper also extends the methodology adapted by Kumar A and based on random choice and decision of experts on AOP technology. Fig. 4 shows the analysis of quality values of all internal characteristics of QEMSR, AOSQ and PAOSQMO model graphically.

TABLE VI. EIGEN VALUES AND EIGEN VECTORS FOR MAIN CHARACTERISTICS

	mC <sub>1</sub>	mC <sub>2</sub>	mC <sub>3</sub>	mC <sub>4</sub>	mC <sub>5</sub>	mC <sub>6</sub>	Eigen Vector ( $\omega$ )	A. $\omega$	$\lambda_{\max} = A \cdot \omega / \omega$
mC <sub>1</sub>	1	2	4	2	3	7	0.3499	2.2497	6.4295513
mC <sub>2</sub>	0.5	1	0.25	1	1	4	0.1069	0.686875	6.425397568
mC <sub>3</sub>	0.25	0.33	3	2	2	4	0.2189	1.343252	6.136372773
mC <sub>4</sub>	0.5	0.33	0.5	0.33	0.5	1	0.0695	0.448812	6.457726619
mC <sub>5</sub>	0.33	2	1	2	1	3	0.144	0.933767	6.484493056
mC <sub>6</sub>	0.14	0.25	0.25	0.33	0.3	1	0.0342	0.235091	6.874005848
							1.00	Mean = 6.467924527	

TABLE VII. PERFORMANCE EVALUATION OF QUALITY OF QEMSR, AOSQ, PAOSQMO

Eigen vector for Main-characteristics	Eigen vector for Sub-characteristics	Weight for Sub-characteristics of QEMSR	Weight for Sub-characteristics of AOSQ	Weight for Sub-characteristics of PAOSQMO	Quality value of QEMSR	Quality value of AOSQ	Quality value of PAOSQMO
0.3499	0.2185	0.321	0.179	0.0137	0.0701385	0.0391115	0.001375
	0.2444	0.112	0.088	0.0053	0.0273728	0.009856	0.0048
	0.3464	0.05	0.05	0.0021	0.01732	0.0025	0.00016
	0.1442	0.132	0.148	0.0304	0.0190344	0.019536	0.00274
	0.0465	0.131	0.169	0.0046	0.0060915	0.022139	0.00046
0.1069	0.2071	0.164	0.236	0.0084	0.0339644	0.038704	0.00075
	0.2929	0.15	0.15	0.0147	0.043935	0.0225	0.00147
	0.2929	0.132	0.168	0.1279	0.0386628	0.022176	0.01023

	0.2071	0.164	0.136	0.0254	0.0339644	0.022304	0.0254
0.2189	0.0849	0.166	0.134	0.0818	0.0140934	0.022244	0.00736
	0.1399	0.154	0.146	0.0703	0.0215446	0.022484	0.0703
	0.1607	0.05	0.05	0.0009	0.008035	0.0025	0.007
	0.1742	0.145	0.155	0.0135	0.025259	0.022475	0.0135
	0.1607	0.054	0.16	0.017	0.0086778	0.00864	0.0017
	0.1399	0.118	0.182	0.0028	0.0165082	0.021476	0.0003
	0.1399	0.151	0.149	0.0131	0.0211249	0.022499	0.0092
0.0695	0.3333	0.154	0.146	0.01	0.0513282	0.022484	0.0008
	0.3333	0.165	0.135	0.01475	0.0549945	0.022275	0.01475
	0.3333	0.034	0.16	0.0249	0.0113322	0.00544	0.0224
0.144	0.0633	0.0567	0.033	0.0253	0.00358911	0.0018711	0.0228
	0.1371	0.0762	0.138	0.1197	0.01044702	0.0105156	0.0083
	0.1514	0.0345	0.155	0.0846	0.0052233	0.0053475	0.0084
	0.1604	0.0651	0.149	0.0356	0.01044204	0.0096999	0.0032
	0.1604	0.0234	0.166	0.0089	0.00375336	0.038844	0.081
	0.1671	0.0765	0.135	0.0039	0.01278315	0.0103275	0.0028
	0.1604	0.0321	0.1679	0.0545	0.00514884	0.0538959	0.0491
0.0342	0.1778	0.0612	0.1388	0.0094	0.01088136	0.00849456	0.0113
	0.2346	0.05	0.05	0.0095	0.01173	0.0025	0.086
	0.2789	0.0532	0.1648	0.0477	0.01483748	0.00876736	0.0334
	0.3087	0.0431	0.1569	0.0546	0.01330497	0.00676239	0.00482
			Total	0.62552223	0.5283693	0.505815	

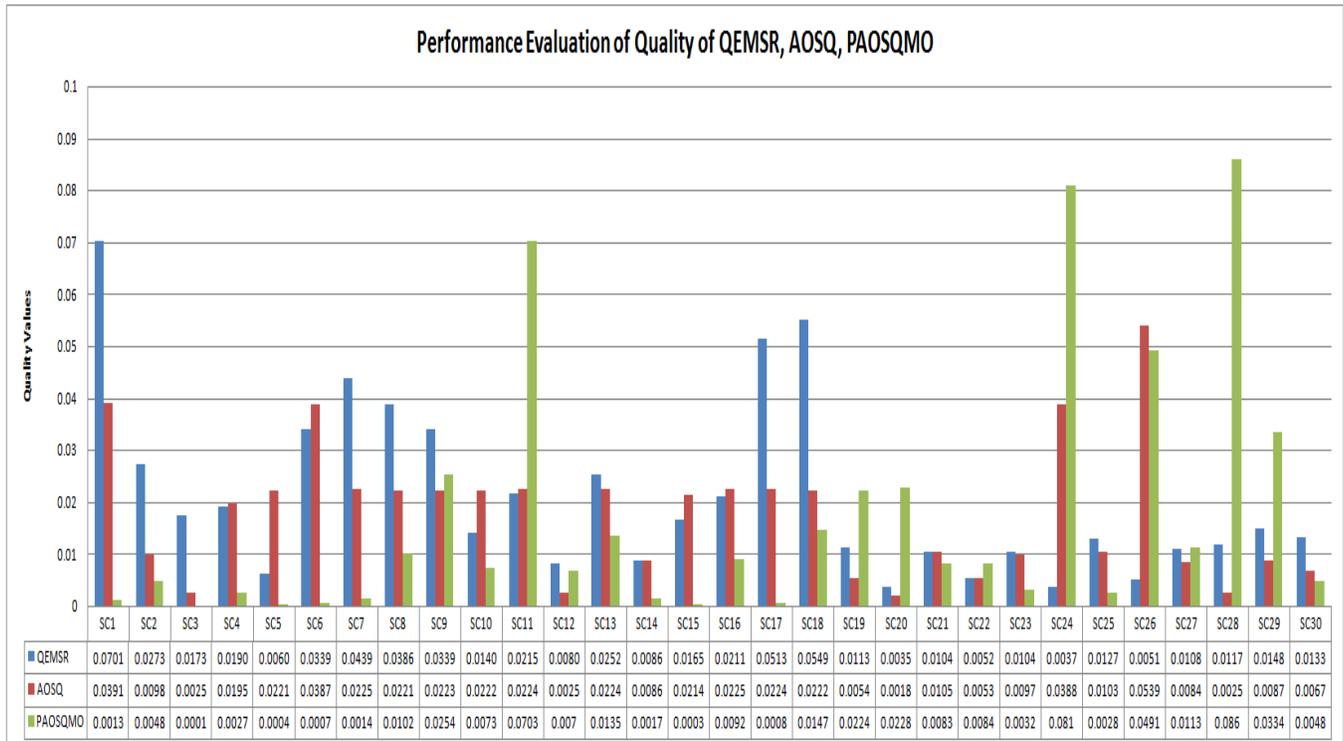


Fig. 4. Performance Evaluation of Quality of QEMSR, AOSQ, PAOSQMO.

### VIII. CONCLUSION AND FUTURE RESEARCH

In AOP, AspectJ is a popular language which provides a support to the software developers to achieve improved quality. AOP is a standard that is trusted for quality improvement. AOP quality measurement has been trusted by evaluation of experimental results using a new QEMSR method and set of metrics for reusability and its sub characteristics. The set of AOP metrics (Coupling, Cohesion, size metrics such as DIT, NOC, CBO, LCOM, WMC, RFC) have authorized to support AspectJ and Java and an authentication of these existing metrics for quality assessment instead of new metrics proposed for AOP. Comparisons of projects are not industrial projects. Nevertheless, this paper provides the evaluation of quality and methodology of comparison as a single unit.

For future research perspective, to validate the quality metrics for large and more complex (commercial) system empirical study require in AOP research. Experimentation on large industrial projects for this domain is very difficult. This paper assessment provides some intuition about AOP and its quality which can't be generalized and it needs supplementary study. The focus of future research is on native programming languages, which is extension of AOP.

#### REFERENCES

- [1] Pankaj Kumar, "Aspect oriented software quality model: The AOSQ model", *Advanced Computing in International Journal*, Vol. 3, No.2, 2012.
- [2] S. N. Chishti and S. K. Singh, "Exploring the quality improvement in small scale project using aspect oriented design", *International Journal of Recent Technology and Engineering*, Vol.8, issue 2, 2019.
- [3] Vinobha A. and Senthil Valan S, "Evaluation of reusability in aspect oriented software using inheritance metrics", *IEEE International Conference on Advanced Communication Control and Computing Technologies (ICACCCT)*, 2014.
- [4] Djamel Meslati and Soumeya Debboub, "Quantitative and qualitative evaluation of aspectJ, Jboss AOP and CaesarJ using Gang-of-Four design patterns", *International Journal of Software Engineering and its Applications*, Vol.7, No. 6, 2013.
- [5] Ghareb M.I. and Gary Allen, "Identifying similar pattern of potential aspect oriented functionalities in software development life cycle", *Journal of Theoretical and Applied Information Technology*, Vol. 80, No.3, 2015.
- [6] Hamed Fawareh, "Software quality model for maintainance software purposes", *International Journal of Engineering Research and Technology*, Vol. 13, No.1, 158-162, 2020.
- [7] S. Dixit, S. K. Singh, "Performance of aspect oriented software quality modeling using artificial neural network technique", *International Journal of Computer Applications*, Vol. 182, Issue 36, 6-10, 2019.
- [8] S. K. Singh and P. Kumar, "An innovative approach to analyze object-oriented and aspect oriented applications metrics using the Java and AspectJ programming language", *International Journal of Advance Research Engineering and Technology*, Vol. 11, Issue 11, 149-158, 2020.
- [9] K. Sirbi and P.J. Kulkarni "Design pattern Vs aspect oriented programming- A qualitative and a quantitative assessment", *International Journal of Computer Science & Communication*, Vol.1, No. 2, pp: 233-237, 2010.
- [10] G. Kiczales, J. Irwin, J. Lamping, "Aspect oriented programming", *European Conference on Object Oriented Programming*, pp: 220-242, ECOOP'1997.
- [11] AL-Badareen, "Software quality evaluation: user's view", *International Journal of Applied Mathematics and Informatics*, Issue 3, Volume 5, 2011.
- [12] Al-Rawashdeh and Feras M. Al'azeh, "Evaluation of ERP systems quality model using AHP technique", *Journal of Software Engineering and Applications*, 7, 225-232, 2014.
- [13] Samarthyam G Ganesh and T. Sharma, "MIDAS: A design quality assessment method for industrial software", *IEEE International Conference on Software Engineering*, San Francisco, USA, 2013.
- [14] A. Przybylek, "An empirical study on the impact of AspectJ on software evolvability", *Empir Software Eng*, 23, 2018-2050, 2018.
- [15] R. Kumar and Dalip, "Implementation of qualitative evaluation model with real life problem using AspectJ", *International Conference on Global Entrepreneurship Trends and Empowerment through Innovation*, Accepted Springer Proceeding, 2021, in press.
- [16] Ram Chatterjee and Ritika Choudhary, "Predilection of reusability over maintainability in aspect oriented system", *International Journal of Computers and Technology*, Vol. 6(3), 2013.
- [17] O. P. Sangwan, P. K. Singh, A. Singh and A. Pratap, "A quantitative evaluation of reusability for aspect oriented software using multi-criteria decision making approach", *World Applied Sciences Journal* 30(12):1966-1976, 2014.
- [18] D. Gotseva and M. Pavlov, "Aspect oriented programming with AspectJ", *International Journal of Computer Science Issue*, Vol.9, Issue 5, No 1, 2012.
- [19] R. Kumar, Dalip and M. Rai, "A comparative study of AOP approaches: AspectJ, Spring AOP, Jboss AOP", *Proceeding of the World Congress on Engineering and Computer Science*, San Francisco, USA, 2019.
- [20] Heba A. Kurdi "Review on aspect oriented programming", *International Journal of Advanced Computer Science and Applications*, Vol. 4, No. 9, 2013.
- [21] Bharti Bisht and Parul Gandhi, "Metric approach to anticipate reusability of object oriented software systems", *Turkish Journal of Computer and Mathematic Education*, Vol.12, No. 6, 2021.
- [22] Saaty, T.L., "The analytic hierarchy process", McGraw-Hill, New York, 1980.
- [23] S. K. Singh and P. Kumar, "An extensive analysis of the characteristics of an AOSQ model using fuzzy logic model", *International Journal of Advance Research and Technology*, Vol.11, Issue 12, 1351-1360, 2020.
- [24] Farhan M. Al Obisat, Zaid T. Alhalhouli, "Review of literature on software quality", *World of Computer Science and Information Technology Journal*, Vol. 8, No. 5, 32-42, 2018.
- [25] Shashank Joshi and Geeta Bagade, "Exploring AspectJ refactoring", *International Journal of Computer Applications*, 2016.
- [26] H. Bindu, Sk. RiazurRaheman and Amiya Kumar Rath, "Dynamic slice of aspect-oriented program: A comparative study" *IJRITCC*, Vol.2, Issue 2, pp: 249-259, 2014.
- [27] K. Chitra and G. Maheswari, "Enhancing reusability and measuring performance merits of software component using CK metrics", *International Journal of Innovative Technology and Exploring Engineering*, Vol.8, 2019.
- [28] Pankaj Kumar and S.K. Singh, "A comprehensive evaluation of aspect-oriented software quality (AOSQ) model using AHP technique", *IEEE, 2nd International Conference on Advances in Computing, Communication & Automation (ICACCA)*, 2016.
- [29] Petrus Mursanto, Dameria Christina Pasaribu, "Defining software quality rank using analytic hierarchy process and object-oriented metrics", *IEEE, International Conference on Advanced Computer Science and Information System (ICACSIS)*, 2018.
- [30] Pankaj Kumar and S.K. Singh, "A comprehensive investigation of quality of AOP based small scale projects using aspect-oriented software quality (AOSQ) model", *IEEE, International Conference on Advances in Computing, Communication Control and Networking (ICACCCN)*, 2018.

# Analysis of the Asynchronous Motor Controlled by Frequency Inverter Applied to Fatigue Test System

Nel Yuri Huaita Ccallo, Omar Chamorro-Atalaya

Faculty of Engineering and Management  
National Technological University of Lima Sur  
Lima, Peru

**Abstract**—This research focuses on analyzing the functional and operational parameters of the three-phase induction motor, squirrel cage type; Where the experimental model consists of a fatigue test system operated by two types of control: Control by Frequency Inverter and Classic star-delta control, where the engine load consists of a standard specimen, corresponding to 61.9% of the nominal load of the object of study. Experimental evaluations of this rotary machine are at regular operating conditions. Managing to Record electrical, mechanical, thermal variables; in a database where they were classified, developed, analyzed and interpreted; Highlighting from the graphs, the quasi-constant behavior of the  $\text{Cos}(\varphi)$  at 0.754 at different regulated frequency values which lead to a low energy consumption of current 1.88 Ampere with variator with respect to the weighted of 2.04 Ampere without inverter; even with improvements in torque when you are opting to use the drive from a 0.71 N-m to a 0.94 N-m. Likewise, the operation of this machine at low frequencies manifests some damages to normal operation, such as the rate of increase in the operating temperature of 78.76 °C in a short time and with projection to increase. Similarly, the injection of harmonic distortion into the network as a result of using electronic equipment, contributes to the detriment of energy quality.

**Keywords**—Induction; torque; frequency inverter (VDF); current; harmonic; temperature

## I. INTRODUCTION

The constitution of an asynchronous electric motor based on the squirrel cage model, presents the condition of gradual variation of speed by controlling the frequency of the stator, and the particularity of modifying the pole numbers in the inductor winding with the automatic adaptation of the same pair of poles in the rotor [1].

According to the constructive differences of electric motors, the types of lower operating speeds require greater torque-motor to deliver the same rotoric power of motors of higher revolutions; this is reflected in the sizing of this type of machine due to the assembly of more solid components for operability [2]. Since, these induction motors are described as a non-linear system because the speed and load condition present sudden jumps [3], so the presence of a special controller that provides vector or scalar control, is useful depending on the application area [4].

Among the different methods of electrical drive of these machines, the establishment of a variable frequency drive (VDF), based on microprocessors and power electronics

components[5, 6, 7]; Of which this operation of speed control in Alternating Current (AC) motors, consequently implies the reduction of wear of electro-mechanical components, such as the rotor conductive bars, which lead to one of the probabilities of failures; and a decrease between 20% and 60% of electrical energy consumption under the same load conditions[8]. The most recurrent VDF model for this application, works under the principle of Power Weight Modulation PWM [9] and this operating mechanism lies explicitly in the reduction or increase of the duration of the series of pulses that allow the control mode depending on the adjustment of the voltage and frequency of the power supply network [10].

Given the significant reduction in energy due to the use of this device, the presence or origin of the harmonic content generated by the grid expressed in the Total Harmonic Distortion (THD) is negligible, although this concept is specified according to the operating conditions and nominal load of the electric motor [11], given that, the VDF is used in specific sectors where they require a negligible THD, it should be noted that these optimal values are exclusive for quasi-stable frequency values; That is, not for applications of continuous velocity variations [12].

It should be noted that this presence of the harmonic spectrum influences the emission of thermal energy, about an additional 5%, in the engine that is operating at nominal load. On the other hand, the rectification of the power factor (f.p.) is developed based on the reduction of the phase angle between the current and voltage established by the VDF [13, 14].

In this sense, this article aims to determine the operational behavior of asynchronous motor controlled by frequency inverter applied in a fatigue test system for analysis of standardized specimens subjected to conditioned tension-compression. Therefore, the purpose of this is to analyze the benefits and particularities caused by the use of controllers such as the frequency inverter.

## II. LITERATURE REVIEW

If we assume that the excessive electronic control equipment consequently generates electrical noises, deformations and harmonics these can be evaluated to counteract them by power electronics, after analysis of the particular, but it is possible when it comes to a line of several motors, the cost is contemplated; Likewise, also ensuring [15].

Electric machines necessarily require reliable protection systems that involve additional expenses; however, among the

advantages of VDF, in addition to speed control, are the safety functionalities where the VDF presents algorithms that guarantee an instant response before possible failure scenarios, as reaffirmed [16] in his case study. These unfavorable scenarios can be: low starting current (ramp), dynamic braking (under reverse magnetic shock), reversal of rotation, absence of phase, imbalance of phases, among others; supplying mechanisms for starting, safety and braking of the electric motor.

### III. RESEARCH METHOD

#### A. Data Logging Processes

The model under study is composed of elements: mechanical, electrical, electronic, among others. Which we can show in Fig. 1, arranged according to their function, being able to be static and/or dynamic. Which we can classify into three systems: Control (command), Actuator (force) and Monitoring; All these are listed in Fig. 2 and Fig. 3 This composition consists of:

- 1) A three-phase network called L1, L2, L3, (220V 60Hz), where only two phases (L1 L2) are used to power the VDF.
- 2) A Siemens Micromaster 440 frequency inverter (attach tab as required), which was preconfigured with the plate data "Parameters"; In addition, peripherals were connected as an external control system composed of: Switch type switch (digital input), which enables the entire external control panel; Switch 1 - 0 - 2 (digital input), makes the so-called rotation inversion; Potentiometer (analog input), Performs the increase or decrease in speed as needed.

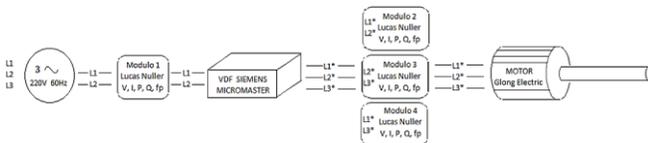


Fig. 1. A Three-phase Network VDF Connection Diagram.

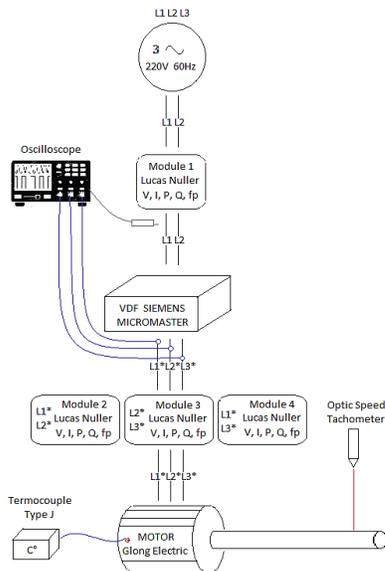


Fig. 2. A Siemens Micromaster 440 frequency inverter (VDF Connection Diagram).

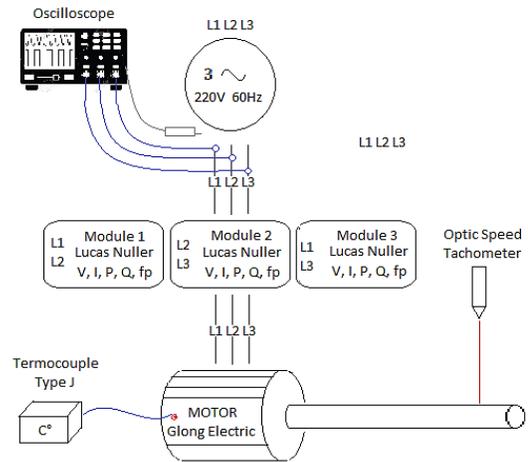


Fig. 3. Direct Boot Connection Diagram.

- 3) A fatigue test machine where a class A-36 specimen was analyzed during the study, see Fig 5; Which consisted of a 61.9% nominal load for the induction motor.
- 4) An optical light tachometer (Standard ST6236B Tachometer) (see Fig. 5).
- 5) A digital oscilloscope (Instek GDS-2064) which registers an admission signal to the drive (L1 L2); drive output signal (L1\* L2\* L3\*)
- 6) Lucas Nuller measurement modules, obtaining (V, I, P, Q, f,p), which were located as follows: Red section – VDF input; VDF – Motor section, one module for each pair of phases (L1-L2/L2-L3/L1-L3); That is, in general it consisted of four modules (see Fig. 4).

#### B. Theoretical Bases

A theoretical part of the subject of the study is based on the behavior of the asynchronous or induction electric motor according to its operability-configuration, which obey laws of electrostatics.

In induction motors the variation of the simultaneous speed developed by the rotating rotor and rotary magnetic field is generated, this behavior of asynchronism is called slippage [17].

The rotor velocity Equation 1 ( $n_r$ ) of these electrical machines is given by the following expression:

$$n_r = \left[ 120 \times f \times \frac{(1-s)}{P} \right] \text{ (r/min)} \quad (1)$$

Where (f) is the wave frequency in units of Hz, (s) is the slippage expressed in percentage value and (P) is the number of magnetic poles.

The difference of this speed with respect to the speed of synchronism is represented according to Equation 2.

$$n_d = n_s - n_r \text{ (r/min)} \quad (2)$$

Where ( $n_d$ ) is the sliding velocity and ( $n_s$ ) is considered precisely the velocity of the magnetic field of the stator.

The description of these motors is similar to a rotary transformer; According to the secondary windings constituted

in the rotor design of the motor, they generate a power flow output mechanically due to the short-circuited system of the coupled windings [18].

This useful power is directly related to the torque induced in the machine, such torque is the result of the difference of the actual torque at the engine terminals and the torque produced by friction and friction with air in this equipment [19]; therefore, the developed mechanical power ( $P_{mec}$ ) is expressed by the following Equation 3:

$$P_{mec} = \frac{\tau_{ind} \times n \times \pi}{30} \text{ (W)} \quad (3)$$

Where ( $\tau_{ind}$ ) is also called motor torque expressed in N-m, and ( $n_r$ ) the rotational speed expressed in RPM.

In asynchronous motors the slip mainly influences the performance result, since the lower the slip value an acceptable efficiency is obtained [1, 17], specifically interpreted in the rotor performance Equation 4 ( $\eta_r$ ):

$$\eta_r = 1 - s = \frac{P_{EM}}{P_S} \quad (4)$$

Where ( $P_{EM}$ ) is the internal mechanical power and ( $P_S$ ) is the interlocking power that reaches the rotor. From the power supply, the motor is supplied with electrical power which is classified as ( $P_{Absorbed}$ ) recorded in the input conductors of the machine, in full operation mechanical power expressed as ( $P_{Util}$ ) is released, this variable differs with the input power due to iron losses, copper and thermally dissipated mechanics.

$$\eta = \frac{P_{util}}{P_{absorbed}} = \frac{P_{output}}{P_{input}} = \frac{P_{Mechanical}}{P_{Electrical}} = \frac{HP \times 746}{\sqrt{3} \times V \times I \times \cos\phi} \quad (5)$$

It is considered that the increase in the feeding frequency influences the decrease in reactive power of magnetization. Since, the reactive energy is consumed when the asynchronous motor performs an operation in vacuum, according to the impedance of the motor, it causes a high angle of lag between voltage and current, consequently, a low  $\cos(\phi)$  [20].

In the mechanism of drive of asynchronous motors, the transient stage is taken into consideration when the change of state is developed by increase or variation of speed where there are various methods of analysis, of which emphasis is taken to the frequency inverter VDF used to control the mechanical speed of rotation of the induction motor.

### C. Basic Concepts

Our model under study is a three-phase squirrel cage type motor in the brand "Glong Electric", asynchronous classification, denomination due to the difference in speed between the magnetic field with respect to the rotational speed, also related to sliding, has an F classification insulation whose working ranges around 155 °C (IEC 60085); Also, a degree of protection with respect to solids and fluids. IP 54 (IEC 60529).

In the Table I, relevant parameters of this electric machine for the present study are detailed, which are collected according to plate data and technical sheet provided by the manufacturer.

TABLE I. ENGINE TECHNICAL SPECIFICATIONS

MODEL - GLONG	
TYPE	MS7132
HP	1
(D) V	220
(Y) V	380
(D) I	3.3
(Y) I	1.93
POLES	2
KW	0.75
HZ	60
RPM	3300
Cos(φ)	0.82
NO.	1111103
η	0.727

Likewise in Table II, the machine would be considered at full load if the consumption was the nominal intensity, but for our case the applied load only represents 61.9%.

TABLE II. ENGINE TECHNICAL SPECIFICATIONS

Rated Load	[A]	3.30
Current Load	[A]	2.04
Percentage Load	[%]	61.90

### D. Overview of Experimental Analysis

During the experimentation, the most relevant electrical parameters were analyzed and documented, which were synthesized in Excel calculation tables, which consist of two analyses, where the Tables III, IV and V correspond to the first analysis; also, for the second analysis consist of two Tables VI and VII. However, these parameters were obtained through different methodologies.



Fig. 4. Experimental Instrumentation System.



Fig. 5. Fatigue Analysis System.

So, we have in Fig. 4: Lucas Nuller modules (V-1Ø, I, f, p (Cos(φ)); Oscilloscope (amplitude, frequency); Tachometer (RPM); parameters obtained through national electrical portals COES SEIN (frequency); Parameters obtained by calculations, using the equations described in the theoretical bases section. powers 3Ø "P-Q-S", Angle(φ°), mechanical power (Equation 3), torque (Equation 3), magnetic field speed, slippage (Equation 2).

In this Fig. 5 we have a partial view of the driving part of the modular fatigue stress analysis system, where in: on the right side, rotating mechanical parts corresponding to the load of the electric machine are observed (rowlocks, specimen, dynamometer, etc.); Similarly, we have on the left side the electric machine, which is the object of study in this article.

#### IV. ANALYSIS

##### A. First Analysis

Tables corresponding to those obtained during the operation of the asynchronous motor by means of a VDF, where Table III corresponds to the supply with two live phases; Also, Table IV corresponds to the output of three quasi-alternating live phases of the VDF which are directed to the terminal box of the three-phase motor.

TABLE III. ELECTRICAL PARAMETERS AT THE VDF INPUT

INPUT OF THE V.D.F. 1Ø VAC - CONNECTION (Δ)					
ENGINE ELECTRIC PARAMETER - EXPERIMENTAL					
f [HZ]	V <sub>(L1-L2)</sub>	I [A]	P [W]	Q	S
59.951	224.10	0.87	96.70	169.29	194.97
60.024	223.40	0.88	96.90	170.82	196.59
59.948	223.70	0.93	104.00	180.17	208.04
60.013	223.50	0.91	101.50	176.49	203.39
60.003	224.40	0.91	101.20	177.20	204.20
59.944	224.20	0.90	100.70	175.09	201.78
60.022	225.10	0.92	103.60	179.59	207.09
59.98	225.30	0.97	109.70	188.88	218.54
59.997	225.00	0.99	112.80	192.39	222.75
60.042	225.20	1.04	119.40	201.74	234.21
60.063	225.00	1.10	127.10	212.75	247.50
60.021	225.10	1.16	133.90	224.29	261.12
60.033	224.80	1.24	145.10	238.10	278.75
60.015	224.50	1.23	142.50	236.20	276.14
60.008	224.10	1.31	153.90	250.22	293.57
60.007	223.80	1.40	164.70	266.47	313.32
59.999	223.90	1.44	170.70	273.61	322.42
59.967	223.50	1.51	179.60	285.55	337.49
60.053	223.40	1.56	185.70	294.43	348.50
60.061	223.50	1.58	196.30	298.12	353.13
60.025	223.40	1.77	215.40	331.79	395.42
59.991	223.40	1.80	218.10	337.67	402.12
60.022	223.20	1.88	230.70	351.00	419.62
60.103	223.00	2.06	254.30	382.75	459.38

TABLE IV. ELECTRICAL PARAMETERS RECORDED AT THE OUTPUT OF THE VDF

OUTPUT OF THE V.D.F. 3Ø VAC' - CONNECTION (Δ)						
ENGINE ELECTRIC PARAMETER - EXPERIMENTAL						
f [HZ]	n <sub>r</sub> [RPM]	V <sub>Fase'</sub> (*)	I <sub>Fase</sub>	P [W]	Q	S
2.26	143.20	15.05	2.60	67.37	7.41	67.78
5.06	243.40	14.20	2.67	-59.43	27.94	65.67
7.53	438.80	20.24	2.75	-87.34	40.81	96.41
10.10	590.90	34.70	2.49	-127.80	77.86	149.65
12.58	737.60	42.50	2.30	-132.23	105.74	169.31
15.08	886.20	51.70	2.16	148.55	123.88	193.42
17.29	1017.00	59.20	2.05	158.49	138.08	210.20
20.00	1180.00	67.40	2.05	179.97	157.75	239.32
22.54	1331.00	76.50	1.99	190.64	182.16	263.68
25.10	1484.00	85.60	1.96	210.97	199.84	290.60
27.51	1628.00	94.40	1.95	232.75	217.91	318.84
30.21	1788.00	103.40	1.90	248.74	232.20	340.28
32.58	1929.00	112.60	1.93	270.26	261.99	376.41
35.19	2084.00	113.50	1.93	281.90	253.94	379.41
37.69	2232.00	121.30	1.93	297.63	275.39	405.49
40.26	2383.00	131.00	1.92	318.02	297.74	435.65
42.45	2518.00	138.80	1.82	321.16	297.16	437.54
45.32	2690.00	147.60	1.92	358.81	334.94	490.85
47.50	2821.00	156.30	1.90	376.52	350.44	514.37
50.50	3000.00	165.70	1.92	403.91	374.83	551.04
52.55	3122.00	183.20	1.86	446.19	386.33	590.20
55.10	3275.00	193.70	1.89	469.86	425.80	634.09
57.54	3420.00	202.60	1.89	495.43	440.93	663.23
59.88	3557.00	218.70	1.88	546.21	456.94	712.14

The Table V, presents six variables under analysis, where the only one obtained experimentally is the Cos(φ); Otherwise with the other variables which are a consequence of the calculations made, based on theoretical bases described above.

Once the values obtained by instrumentation (Table III, Table IV) and calculations in Table V have been admitted and synthesized, we proceed to make graphical representations of the most relevant electrical parameters, including those that are the object of analysis.

In all cases the representations correspond to figures obtained by Module 1 and Module (2, 3 and 4) nomenclature specified in Fig. 1, Fig. 2 and Fig. 3. Parameters represented by IBM SPSS interfaces, corresponding to V, I, P, Q, S and f.p.

TABLE V. CALCULATED ELECTRICAL PARAMETERS OF THE VDF OUTPUT

OUTPUT OF THE V.D.F. 3Ø VAC' - CONNECTION (Δ)					
ENGINE ELECTRIC PARAMETER - CALCULATED					
Cos(φ)	P <sub>rotor</sub> [W]	M [N-m]	n <sub>s</sub>	n <sub>d</sub>	PAR Axis
0.064	2.748	0.183	135.6	-7.6	6.13
-0.897	-38.140	-1.496	303.6	60.2	2.66
-0.877	-62.479	-1.360	451.8	13.0	2.93
-0.029	-2.845	-0.046	606.0	15.1	3.25
-0.768	-88.163	-1.141	754.8	17.2	3.26
0.752	96.376	1.039	904.8	18.6	3.25
0.745	104.240	0.979	1037.4	20.4	3.26
0.736	116.345	0.942	1200.0	20.0	3.20
0.716	125.036	0.897	1352.4	21.4	3.23
0.716	138.424	0.891	1506.0	22.0	3.25
0.718	151.480	0.889	1650.6	22.6	3.27
0.723	163.605	0.874	1812.6	24.6	3.25
0.715	178.154	0.882	1954.8	25.8	3.29
0.726	181.360	0.831	2111.4	27.4	3.06
0.726	192.424	0.823	2261.4	29.4	3.05
0.730	208.379	0.835	2415.6	32.6	3.09
0.727	213.574	0.810	2547.0	29.0	3.11
0.725	233.116	0.828	2719.2	29.2	3.10
0.727	243.788	0.825	2850.0	29.0	3.12
0.728	261.079	0.831	3030.0	30.0	3.12
0.739	285.699	0.874	3153.0	31.0	3.31
0.734	303.833	0.886	3306.0	31.0	3.33
0.737	319.061	0.891	3452.4	32.4	3.34
0.754	351.097	0.943	3592.8	35.8	3.47

For Fig. 6, the intake voltage at all analysis points is within the maximum permissible ranges of +/- 5%. However, at the output of the VDF in all cases it presents a stable increase, corresponding to the directly proportional increase of the frequency in selected analysis.

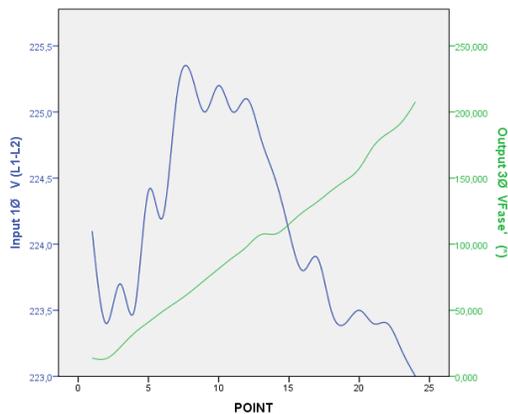


Fig. 6. Analysis of 1Ø (V) and 3Ø (V).

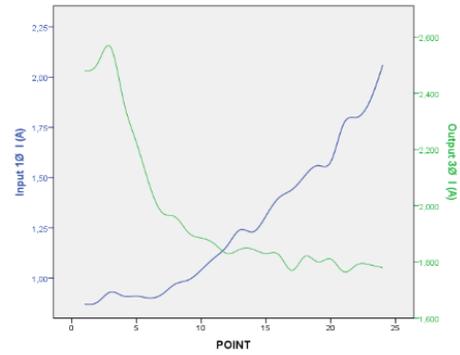


Fig. 7. Analysis of 1Ø (A) and 3Ø (A).

The output intensity of the VDF presents an increase in peak value, due to the low starting frequency, in addition to the natural inertial load of the rotor and including the load; however, this peak is temporary, since it presents a beneficial decrease in time, in inverse relation to the frequency. However, in the admission of the VDF presents a quasi-constant proportional increase.

Likewise; Regarding the Fig. 7, we can affirm that the use of VDF is profitable at low frequencies, since the consumption of the network is lower than the output of the VDF. Where the point of non-profitability would be around 12 where the frequency is around 30.21 HZ.

Given this representation Fig. 8, we can reaffirm one of the greatest virtues of the VDF, which consists in the reduction of energy consumption of the electricity grid. Where according to the graph at all times the active power of the network is lower, than that of the output of the VDF.

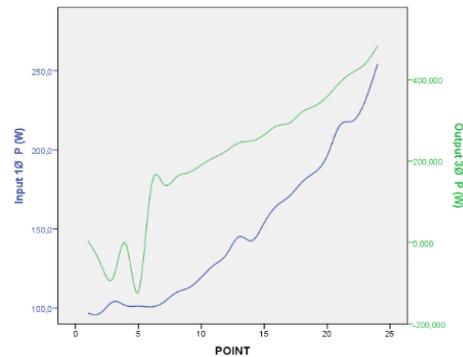


Fig. 8. Analysis of 1Ø (W) and 3Ø (W).

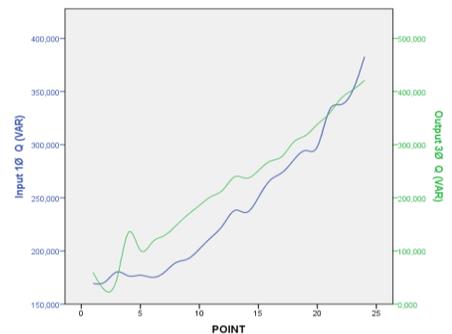


Fig. 9. Analysis of 1Ø (VAR) and 3Ø (VAR).

Given the interpretation of the graph (Fig. 9), we can affirm that the reactive power in the output of the VDF is greater than that of the network for all the frequencies analyzed, which has similitude to a circuit with a reactive energy compensation system.

Apparent powers are also considered one of the most important parameters of a power triangle. This is a consequence of vector considerations of the f.p, active and reactive powers that is why we can affirm through its graph (Fig. 10), that the use of a VDF reduces energy consumption, without affecting the electrical or mechanical power of the induction motor.

Having simulated several representative waves of ideal waves using software PSIM, we make available the waveforms obtained by the function generator, which we show in Fig. 11. Being able to show the distortions caused in the fundamental wave by the use of a VDF.

Similarly in Fig 12, the waveforms generated by a frequency inverter; That is, the one we make available to the cargo.

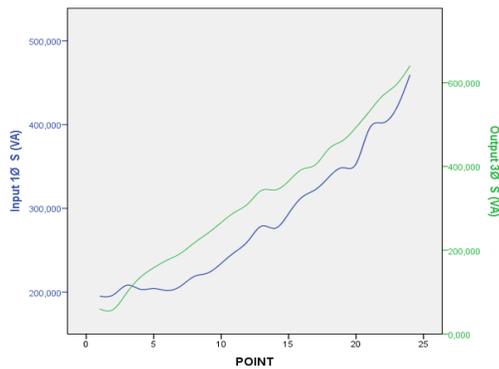


Fig. 10. Analysis of 1Ø (VA) and 3Ø (VA).

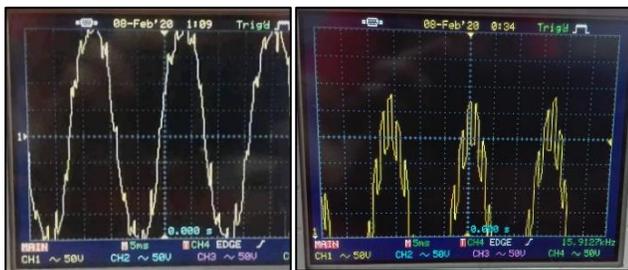


Fig. 11. Harmonic Distortion Caused by the use of a Variable Frequency Drive.

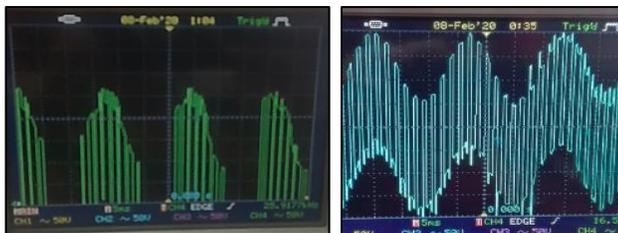


Fig. 12. Quasi-Sine Waveform Generated by the Variable Frequency Drive to make the Load Available.

B. Second Analysis

From now on we start a new analysis; where we compare the rotary machine, operating on a regular basis with a direct starting system using contactors Fig. 3 and a second using a VDF with ramp starting system Fig. 2; but, both with delta connection. The electrical parameters obtained were arranged in tables, respectively (Table VI and Table VII).

TABLE VI. ELECTRICAL PARAMETERS IN SINGLE-PHASE AND THREE-PHASE REGISTERED WITHOUT VDF

WITHOUT V.D.F. VAC				
ENGINE ELECTRIC PARAMETER				
CONNEC.	TRIANGLE (**)			
	1Ø			3Ø
	LINE 1	LINE 2	LINE 3	
f [HZ]	59.94	59.94	59.94	59.94
n <sub>r</sub> [RPM]	3560.00	3560.00	3560.00	3560
V <sub>(L1-L2)</sub> [V]	224.80	225.20	224.00	224.67
I [A]	1.99	2.04	2.10	2.04
P [W]	360.00	364.80	370.00	364.93
Q [VAR]	280.00	288.50	300.00	289.50
S [VA]	447.00	456.90	470.00	457.97
Cos(φ)	0.79	0.77	0.78	0.78
φ °	37.44	39.24	38.92	38.54
Sen(φ)	0.61	0.63	0.63	0.62
P <sub>Mechanics</sub> [W]	261.72	265.21	268.99	265.307
M [N -m]	0.70	0.71	0.72	0.712
n <sub>s</sub>	3596.64	3596.64	3596.64	3596.64
n <sub>a</sub>	36.64	36.64	36.64	36.64
PAR <sub>Axis</sub>	3.75	3.76	3.74	3.75

In the Table VII, we make the comparison under similar operating conditions with the exception of considering in the installation a VDF "C/VDF" (see Fig. 2) or not using it "S / VDF" (see Fig. 3).

From now on we proceed to perform the validation of the results obtained by Power Simulation Software (PSIM), for this we start by making the representative equivalent diagrams in the software interfaces, where we also declare the nomenclatures and denominations of the instruments, to analyze subsequent representations that preserve the same nomenclatures.

We can deduce the following diagram as the electrical interpretation of Fig. 2. Where modules (2, 3 and 4) are presented as a composition of instruments specific to each parameter. In addition to performing the electrical representation of a rotating electric machine by its equivalent impedance (resistance "r" and inductive reactance "xl") Of similar characteristics to the previous wing, the present representation corresponds to the electrical interpretation of Fig. 3 with similar contemplations with respect to instruments and equivalent electrical circuits described in Fig. 13.

TABLE VII. COMPARATIVE ANALYSIS OF THE C/S VDF TESTS

CONNEC.	C/ VDF	S/VDF
	TRIANGLE	
	3Ø VAC'	3Ø VAC
f [HZ]	59.88	59.94
n <sub>r</sub> [RPM]	3557.00	3560.00
V <sub>(L1-L2)</sub> [V]	207.75	224.67
I [A]	1.78	2.04
P [W]	482.94	420.73
Q [VAR].	420.73	289.50
S [VA]	640.50	457.97
Cos(φ)	0.75	0.78
φ °	41.06	38.54
Sen(φ)	0.66	0.62
P <sub>Mechanics</sub> [W]	351.10	265.31
M [N-m]	0.94	0.71
n <sub>s</sub>	3592.80	3596.64
n <sub>d</sub>	35.80	36.64
PAR <sub>Axis</sub>	3.47	3.75

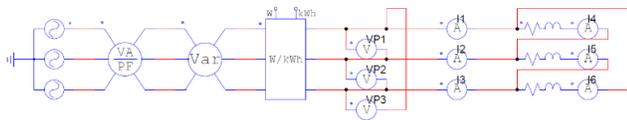


Fig. 13. Electrical Parameter Measurement Diagram with VDF.

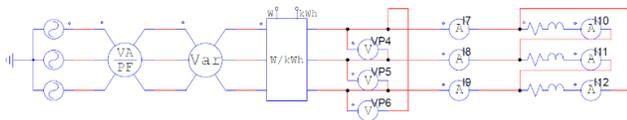


Fig. 14. Electrical Parameter Measurement Diagram without VDF.

The Fig. 15 correspond to those obtained by instruments called voltmeters with the nomenclature VP1, VP2, VP6 (Fig. 13 and Fig 14), with respect to effective values. However, the exposure of the sine curves responds to those of an oscilloscope, evaluating in the first harmonic or fundamental wave.

In the Fig. 16, are represented the electrical intensities collected by ammeter for effective values. Also, for those corresponding to that of an oscilloscope, where they provide maximum, minimum values and other characteristics of this generator. In all cases they represent the line intensities in both analyses.

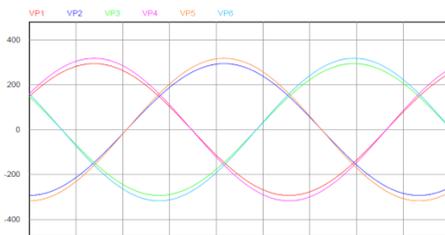


Fig. 15. Line Voltage Curves c/s VDF.

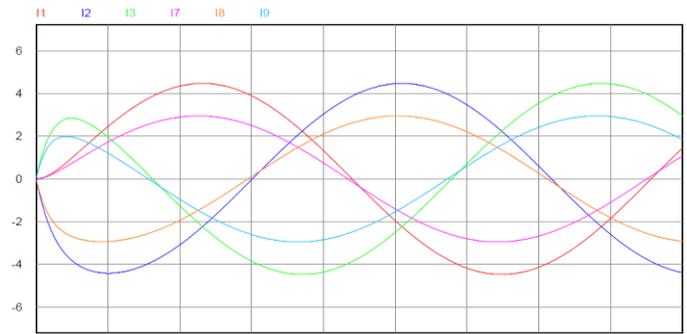


Fig. 16. Curves of the Line Current c/s VDF.

The following graph called Fig. 17 corresponds to those obtained from similar conditions to the previous figures, with the exception that these represent the electrical intensities of phase. If we remember in a typical connection of an electric machine of 6 terminals, connected in delta (triangle), the line intensities are root of three times phase wings.

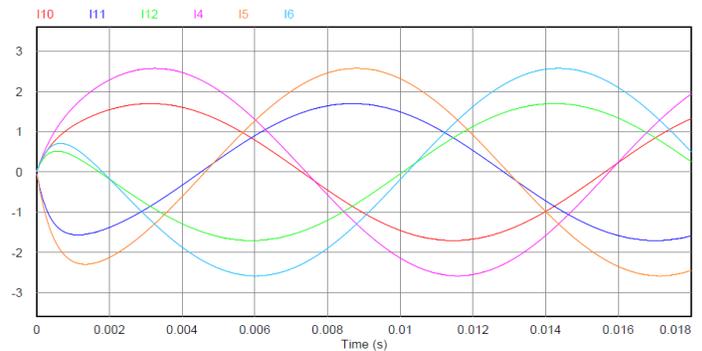


Fig. 17. Curves of the Phase Current c/s VDF.

This Fig. 18 corresponds to the effective values and maximum values of voltage and current. Obtained by the instrumentation modules and equivalent measuring instruments in Fig. 13 and Fig 14. In addition, these values can be contrasted with those obtained experimentally in Table VII.

RMS Value

Time From	1.0000000e-005
Time To	1.7940000e-002

VP1	2.0746762e+002	I7	2.0149252e+000
VP2	2.1393670e+002	I8	2.0910262e+000
VP3	2.0166419e+002	I9	2.0594404e+000
VP4	2.2436163e+002	I10	1.1843110e+000
VP5	2.3135749e+002	I11	1.2095659e+000
VP6	2.1808563e+002	I12	1.1657161e+000
I1	3.0526435e+000	I4	1.7870206e+000
I2	3.1420231e+000	I5	1.8168283e+000
I3	3.1049799e+000	I6	1.7653063e+000

Fig. 18. Effective Parameters c/s VDF.

Temperature [°C] VS Frequency [Hz]

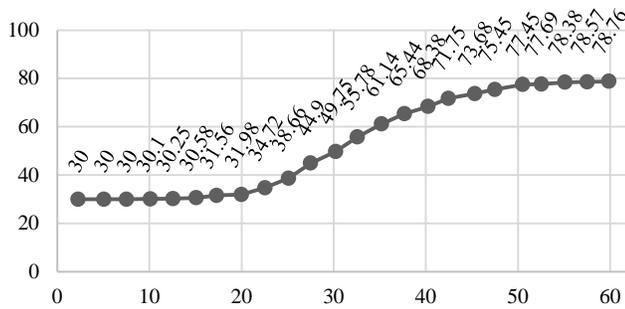


Fig. 19. Temperature Values of the Induction Motor with VDF.

One of the parameters considered of high importance in the useful life of electrical machines is the working temperature, since this is responsible for the physical state of the insulation (windings, rotoric core, statoric core, etc.). This parameter has an impact on efficiency. Which relates the power that is absorbed from the electrical network, materializing it in losses per joule effect and minimizing the useful power; also, with respect to this we can deduce given Equation 5.

That said, in this table data collected during experimentation were synthesized, where they are in units of S.I. [°C], these were collected by ammeter Prasek (PR-103), in the temperature function with connection of external receiver peripheral called thermocouple type J, where the thermocouple was fixed to motor housing (see Fig. 2 and Fig. 3)

#### V. DISCUSSION

If we consider between the option of controlling the speed of a rotating machine and we opt for only 2 possibilities such as changing the number of poles or installing a vdf according to a Cost-benefit analysis, the second option would be the most convenient for the benefits of varying any RPM value with only the variation of frequencies, in addition to having protection algorithms. Likewise, it states in [7], in addition to other options that are not the subject of study.

There are control systems based on fuzzy logic in which they focus directly on the torque of the engine in the condition of operation or of certain regimes [21]; however, these would only be applicable to machines of regular work regime, the exception being those of intermittent work or irregular periods. Since these would necessarily have the phenomenon of vibrations of high torque and of different magnitudes in this regard, in [22], they point out that the claims were even higher, but for regular work regimes.

The asynchronous rotary machines have a self-coupled cooling system by constitution and composition, where the first refers to the fins of the housing, whose function is to dissipate the temperature by conduction, the temperature increases produced by the core and winding of the stator; Also, the second refers to the fan coupled to the rotary axis which directs the flow of cold air to the fins by means of the principle of forced convection; However, this fan is conditioned to the rotational speed of the rotor, where the nominal speed guarantees its efficiency; Also in [23] it is sated in regard. In the case of speed variations, they strongly impair the efficiency

of this. Therefore, according to the machine dimensions, power, environmental factors, programmed rotational speeds, external ventilation systems must be chosen, guaranteeing the working temperature. Avoiding exceeding these recommended values even of “F” insulation which guarantees us a maximum optimal work at the temperature of 155 °C (IEC 60085); in this regard in [24] they also assure the same.

#### VI. CONCLUSION

Electric machines have as a fundamental purpose to transform electrical energy into mechanics. So, in this article, two analyses were performed: The first, using a VDF, the torque was evaluated at different speeds (Table V); the second, making a functional comparison of the engine with and without VDF (Table VII), in both situations, only operating at nominal speeds. consequently, we can assert that, in the first case, under any frequency value assigned in the VDF the mechanical torque of the electrical machine is preserved almost constant, oscillating between 0.88 (N-m); However, in the second case the electric machine has a higher torque when using the VDF; that is, with VDF 0.94 N-m and without VDF 0.71N-m.

Rotary electric machines have standardized operating temperatures, which meet criteria of rotational speed, mechanical load, type of bearings, insulation class, among others; Given the importance of this parameter, in our experimentation with VDF, it was determined that the working temperature increased drastically in shorter operating time, and with possibilities of increase, establishing itself at 78.76 °C (see Fig. 19); However, when the use of VDF is ignored, the engine is set to a temperature of 40 °C, during any operating time. For both cases: First, the evaluation period was similar, corresponding to approximately 30 minutes, until stability was evident; Second, the percentage of mechanical load is less than the nominal, see Table II.

The power factor is directly related to the powers (P, Q, S), arranged in a triangle, in relation to their nominal parameters. lower load corresponds to lower f.p. consequently greater unnecessary energy consumption, making possible alternatives such as reactive energy compensation. however, among the advantages of a VDF drive is to preserve a Cos(φ) as high as possible, but at the cost of injecting harmonics into the network. Likewise, we can see the manifestation of this event in Table VII in the electrical current apparatuses (I[Ampere]).obtaining a Cos(φ) of 0.754 despite reducing energy consumption, against a Cos(φ) of 0.782 with higher consumption. Both in equal operating conditions at 61.9% load. This value is optimal if we consider that such a machine is not operating at nominals.

The slippage is increased directly proportional to the rotational and statoric velocities (magnetic field); Then, according to the analysis carried out in Tables IV and V. We can affirm that this increase is very small, but it is preserved over time; that is, the use of a VDF does not alter its main characteristic of this type of electrical machines asynchronous. However, this slide has an average of approximately 30 rpm.

Given the analysis to Fig. 7 we can affirm, that despite the configuration of acceleration ramp, the electrical intensity presents a visible peak, because the engine starts its march in

zero frequency; In addition to including the inertia of the natural rotor axis with load included; However, this peak will be settling as the speed increases; Likewise, the machine has optimal energy efficiency at low frequencies, where the breaking point is approximately 12 and the corresponding frequency is around 30.21 HZ. This energy reduction can be evidenced as the curve of the intensity admitted in the VDF is lower, regarding the one supplied to the engine.

The injection of harmonics into the network is directly related to the operating frequencies of the rotating machine Fig. 12, even more so at low frequencies, the manifestation of this phenomenon is reflected in the waveform obtained by the function generator; so, we have in Fig. 11, which shows the distortion caused in the fundamental wave.

According to the analysis in Table VI we can deduce that the dependence on reactive energy is much higher when you choose to use a VDF; however, this variable is relatively debatable, only for specific sectors where energy regulations consider in addition to active energy, reactive energy. Current regulations that contemplate tariffs and penalties, regarding consumption or injection into the interconnected electricity grid depending on whether the sector is used, distributed or transmitted.

#### REFERENCES

- [1] M. A. Pozueta "Speed variation in asynchronous motors". University de Cantabria-Department of Electrical and Energy Engineering, Spain, 2017.
- [2] H. G. ENRÍQUEZ, "Control of electric motors". Editorial Limusa. 2015.
- [3] M.A. Hannan, " Optimization techniques to enhance the performance of induction motor drives." Renewable and Sustainable Energy Reviews, vol.2, no.3, pp.56-72, 2017.
- [4] W. L. Bermeo, A. B de Souza, T. R. Fernandes, D. A. Honorio, L. L Nogueira-dos Reis, and L. H. Barreto "Slider mode control applied on the current mesh for an application of a base-DSP for position control of a squirrel cage induction motor". Colombian Journal of Advanced Technologies, vol. 1 no. 27, pp. 26-32, 2016.
- [5] R. Bharti, M. Kumar and B. M. Prasad, "V/F Control of Three Phase Induction Motor," International Conference on Vision Towards Emerging Trends in Communication and Networking, vol. 5 no. 12, pp. Vellore, India, pp. 31-44, 2019.
- [6] J. Girisha and J. Pinto, "Fuzzy Logic Controller for Indirect Vector Control of Induction Motor," Advances in Communication, Signal Processing, VLSI, and Embedded Systems, vol. 614, pp. 519-534, 2019.
- [7] R. Amanz, J. Garcia and L. Miguel "Induction Motor Control Techniques: Synthesis of Current Situation." Ibero-american magazine automatic informatic industrial, vol. 13, no.2, pp.381-392, 2016.
- [8] M. Ballesteros, F. Cadena and A. Jaramillo. "Signal processing techniques used for the analysis of harmonic distortion generated by variable frequency drives in induction motors." Networks of Engineering, vol. 6, no. 1, pp. 72-84, 2015.
- [9] J. A. A. Gallardo, J. L. D. Rodríguez, and A. Guerrero, "Simulated annealing optimization of a single-phase multilevel converter with multi-carrier sinusoidal PWM", modulation. Colombian Journal of Advanced Technologies, vol. 1, no. 27, pp. 91-97, 2016.
- [10] O. P. Ardila, "Spatial vector modulation for three-phase inverters with four switch branches". Colombian Journal of Advanced Technologies, vol. 2, no. 26, pp. 99-107, 2015.
- [11] J. V. Gragger, A. Haumer, C. Kral and F. Pirker "Efficient Analysis of Harmonic Losses in PWM Voltage Source Induction Machine Drives with Modelica". Proceedings of the 6th Modelica Conference 2018, Bielefeld, Germany. 2018
- [12] R.. Taleb, D. Benyoucef, M. Helaimi, Z. Boudjemaa, and H. saidi. "Cascaded H-bridge asymmetrical seven-level inverter using THIPWM for high power induction motor". Energy Procedia Journal, vol. 74, no. 4, pp. 844-853. 2015.
- [13] G. Wang and L. Song. "Performance assessment of variable frequency drives in heating, ventilation and air-conditioning systems" , Science and Technology for the Built Environment Journal, vol. 12, no. 4, pp. 456-472, 2018.
- [14] Z. B. Duranay, H. Guldemir. "Selective harmonic eliminated V/f speed control of single-phase induction motor," IET Power Electronics, vol. 11, no. 3, pp. 477-483, 2017.
- [15] Z. B. Duranay, H. Guldemir, "Fuzzy logic based harmonic elimination in single phase inverters". 2017 IEEE XXVI Int. Scientific Conf. "electronicsET2017", Sozopol, Bulgaria, September 2017.
- [16] D. Panasetsky, A. Osak, D. Sidorov, L. Yong. "Simplified Variable Frequency Inducton – Motor Drive Model for Power System Stability Studies and Control." Elsevier. IFAC- Papers Online. Vol. 49, no. 27 pp. 451-454, 2016.
- [17] A. Hughes. "Electric Motors and Drives". Newnes Butterworth-Heinemann. 3da. ed. 185-186, 2006.
- [18] S. Chapman. "Electrical Machines", 5ta ed. Mc Graw Hill.1. pp. 415-416. 2012.
- [19] K. S. Hoon, "Electric motor control", 1st ed. Elsevier Science, 2017.
- [20] F. Petruzella. "Electric Motors and Control Systems", 2nd Edition, McGraw-Hill, 2016.
- [21] O. Chamorro, N. Huaita, L. Vicuña, R. Ilizarbe, J. Torres, J. Rupay. "Experimental Analysis in Alternate Current and Direct Current of the Operating Parameters of a Universal Single-Phase Engine." Advances in Science, Technology and Engineering Systems Journal. vol. 4, no. 6, pp. 360-370, 2019.
- [22] Z. Mekrini, B. Seddik. "Fuzzy Logic Application for Intelligent Control of an Asynchronous Machine," Indonesian Journal of Electrical Engineering and Computer Science, vol. 7, no. 1, pp. 61-70, 2017.
- [23] E. Gundabattini, R. Kuppan, D Gnanaraj, A. Kalam, D. Kothari, R. Abu. "A Review on Methods of Finding Losses and Cooling Methods to Increase Efficiency of Electric Machines.", Ain Shams Engineering Journal. vol. 12 no. 1, pp 497-505, 2021.
- [24] T. Sato, M. Enokizono. " Evaluation Of Stator Core Loss of High-Speed Motor by Using Thermography Camera.", American Institute of Physics, vol. 8, no. 4, 2017.

# Heuristic Algorithm for Automatic Extraction Relational Data from Spreadsheet Hierarchical Tables

Arwa Awad<sup>1</sup>

Faculty of Computer and Information Sciences  
Ain Shams University, Cairo, Egypt

Rania Elgohary<sup>2</sup>

Faculty of Information Technology  
Misr University for Science and Technology, Cairo, Egypt

Ibrahim Moawad<sup>3</sup>

Faculty of Computer Science and Engineering  
Galala University, New Galala City, Suez, Egypt

Mohamed Roushdy<sup>4</sup>

Faculty of Computer and Information Technology  
Future University in Egypt, Cairo, Egypt, Cairo, Egypt

**Abstract**—Spreadsheets are contained critical information on various topics and were most broadly utilized in numerous spaces. There are a huge amount of spreadsheet clients everywhere in the world. Spreadsheets provide considerable flexibility for data structure organization. As well as it gives their makers an enormous level of opportunity to encode their data as it is simple to utilize and easy to store the data in a table format. Because of this flexibility, tables with very complex and hierarchical data structures could be generated. Thusly, such complexity makes table processing and reusing this data is a difficult task. Therefore, the expansion in volume and complexity of these tables has prompted the necessity to preserve this data and reuse it. As a result, this paper implemented a novel algorithm-based heuristic technique and cell classification strategy to automate relational data extraction from spreadsheet hierarchical tables and without need any programming language experience. Finally, the paper does experiments on 2 different real public datasets. The percentage of average accuracy using the proposed approach on the two datasets is 95 % and 94.2% respectively.

**Keywords**—*Spreadsheet table analysis; hierarchal table structure; cell classification; heuristic algorithm; relational data extraction*

## I. INTRODUCTION

A spreadsheet is an interactive application tool for organization charts, storage, and analysis of data. It contains data that is viewed in a tabular form. It consists of information orchestrated during a two-dimensional (2-D) cell. Normally, fragments during a table address the table name, and each line addresses the attributes or the values. The primary line or lines may contain segment attributes or variable names. Cells may contain numbers, text, dates, and other data types. Past this fundamental model, Spreadsheets are utilized by an enormous number of clients as a typical generally useful data management tool. Because of this flexibility, tables with very complex data structures could be generated. Thusly, such complexity makes automatic table processing and data extraction a difficult task. Therefore, the table pre-processing step is regularly needed in the data extraction pipeline [1].

Unfortunately, an enormous amount of spreadsheet tables are unstructured tabular data with simple or hierarchical and

sophisticated table structures. The attributes or the header of simple tables [2] acts in only the first line or only in the left column (rule). The hierarchical table structures [3] act in hierarchical attributes at the top lines (highest rows) of spreadsheet tables or multi-dimensional levels of left attributes (left columns). As shown in “Fig. 1”, the complex table structure [4] acts within the top and left attributes together. These attributes of complex table structures could also be hierarchical or simple (top and left) without hierarchy. They are intended to be explicitly understood by humans but not by a machine which makes it implicit to understand and process these hierarchal and unstructured data. Nowadays, there is an explosion of computation intelligence vision that requires the data to be understood by machine and extracted in a structured form like an electronic database. The automatic extraction of hierarchical table header structure is the initial step of converting unstructured data to structure data form.

The data stored in spreadsheets is unstructured, inconsistent, has low quality, and lacks data integration operations. Spreadsheets do not observe a standard data model (definite structure or schema), thus it is difficult to integrate with other data sources. The spreadsheet tables contain a huge amount of high value that needs to convert to a relational form to reuse and integrate. The first logical step to make such data relational is to extract the relational table structure from a spreadsheet.

According the literature, there are three main types of approaches that are responsible for extracting relational data from the spreadsheets:

1) *Schema-based approach*: It is a traditional schema mapping system used to extract or convert from spreadsheets to relational data by specifying the source and target attributes mapping.

2) *Rule-based approach*: It requires explicit user-provided conversion rules.

3) *Visualization-based approach*: It provides the users with an interactive visualization interface to extract or manage the underlying data that exist in the spreadsheets.

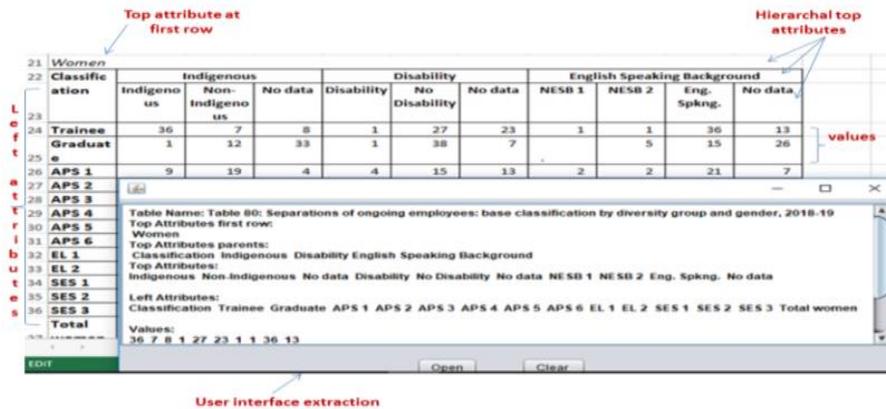


Fig. 1. A Running Example of Complex Table Structure with user Interface Extraction.

However, there are three common draw-backs of these three main approaches:

- a) Challenges to handle hierarchal spreadsheet tables.
- b) The extraction process cannot be accomplished automatically.
- c) Most of the approaches require the users to learn a new language or pre-defined operators to describe the extraction rules.

Therefore, the paper used an automatic approach based-heuristic algorithms and cell classification strategy to accurately extract relational data from hierarchal and complex spreadsheet tables.

The importance of this research lies in the future vision of the relational data extracted from a spreadsheet includes computer agents searching for information, making decisions, and taking actions on behalf of human users. Thus, it is needed to automate extracts for collected complex table header structure in the spreadsheet (semi-structured format) to improve spreadsheet quality as it is the precondition for investigating and utilizing information and for ensuring the estimation of the information.

The main contribution of this research is developing variant techniques and algorithms that allow discovering tables in spreadsheets to infer their layout and their relational data. However, most of the existing approaches and techniques cannot achieve the extraction process automatically for hierarchal table structure extraction. It often required some user efforts to accomplish this process. As a result, this paper developed an automatic approach that is accompanied by some heuristic rules and cell classification features.

As extension of our previous work [5, 6], a new method was developed to extract multiple tables from the Excel sheets. Also, extended to extracts implicit and relational data from complex and hierarchy structure tables not only from simple table structure based on:

Proposed an algorithm based on heuristic rules and classification cell features for selecting complex and hierarchal section header lines and data values. This methodology provides a way to extract a more and more organized structure data from spreadsheets.

This paper is organized as follows. Section 2 discusses the related work as well as the relational data extraction. Whereas Section 3 introduces the proposed approaches with the process extraction of relational data from spreadsheet tables, Section 4 presents the proposed algorithms. Section 5 presents the results and analysis of the experiment of the accuracy of complex table structure. Finally, the paper is concluded in Section 6.

## II. RELATED WORK

Spreadsheet table discovery is the assignment of identifying all tables on a given sheet and finding their reaches. Table detection header is the stage of detection mechanism that achieves state-of-the-art results in computer vision [7, 8] based on the convolutional neural networks approach. On the other hand, [9] presented a multi-task learning method to extract a semantic structure of a table. [10] Includes heuristics on the structure and textual content of a table that is designed for three model table types. [11] Combines various heuristic-based algorithms that classify spreadsheet cells into four functional groups (roles; headings or data values). [12] Used rules-based language for table analysis and interpretation. [13] Assumes that all content in one cell is either a label or an entry. [14] Proposed a classification approach and training the data to discover only the layout of tables in spreadsheets above cell level structure. [15] Presented a predictive synthesis algorithm to helpfully automating the data wrangling process. [16] Used the heuristic approach for table header to correct and achieve matching between the physical and visual presentation of the table structure. However, authors in [17] used programming by examples for hierarchal data conversion to a relational table. The authors of [18] applied the cell features algorithm to classify and identify the table spatial in the spreadsheet. The authors of [19] generate a flash relate algorithm and the user must use the input-output examples for the relational data required. In addition, the authors in [20] used a heuristic method to correct a physical structure to the table header by merging the empty cell with the neighboring ones that are not empty. Most of these algorithms require user efforts for relational data extraction or conversion.

Through reviewing previous work, the research has covered this point from different angles, including automation like the proposed work [21], which does not need any user intervention. However, they automatically infer some

spreadsheet structure, but they cannot process hierarchical spreadsheets. Semi-automation [22,23] who needs user intervention, and sometimes needs to understand the user to a specific programming language, and what needs to be programming language [24,25]. The current study is consistent with past investigations in its principle subject and the general objective, yet it differs from it in the application strategy.

### III. RESEARCH METHOD

As depicted in “Fig. 2”, the initial phase for the extraction process of research approach is to detect the tables found in the Excel sheet. The spreadsheet may contain only one table or multiple tables. After that, the algorithm starts to detect the tables' names if found. Then the algorithm begins to distinguish between tables' headers and their values. Finally, the proposed algorithm extracts tables found in the spreadsheet with their names and their attributes besides their values. The detailed process of each phase can be described in the next sub-section as the following steps:

#### A. Table Detection and Extraction Phases

Spreadsheet table detection and discovery is the first step needed to complete the process of changing over information put away in spreadsheets into organized information in a database that can be questioned and handled to applied decision making and knowledge discovery rules. Table detection is the errand of recognizing all tables on a given sheet and finding their separate reaches as shown in “Fig. 3”.

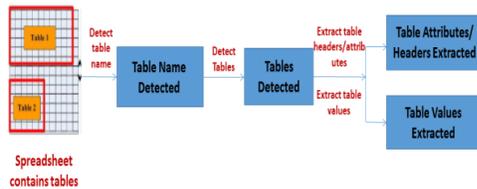


Fig. 2. The Research Methodology.

```
1- Iterate upon all sheets
for (int i = 0; i < workbook.getNumberOfSheets(); i++) {XSSFSheet
sheet = workbook.getSheetAt(i);
2- Detect rows [max-written rows number].
sheet.getPhysicalNumberOfRows()
3-Read number of merge region and detect it's address.
CellRangeAddress address = new CellRangeAddress(first column ,last column
,first row , last row);
address = sheet.getMergedRegion(region number);
4-Iterate on all rows
Iterator<Row> rowIterator = sheet.iterator();
while (rowIterator.hasNext())
Row row = rowIterator.next();
5-Iterate on every cell in all rows.
Iterator<Cell> cell iterator = row.cellIterator();
while (cellIterator.hasNext())
Cell cell = cellIterator.next();
6-Read cell value and detect which it value or attribute.
7-Get last row number at every sheet int lastRow =
sheet.getLastRowNum();
```

Fig. 3. Table Detection Process.

After detecting the table in the spreadsheet, the algorithm starts to extract table name, attributes, and values based on the heuristic rules and cell features as shown in “Fig. 4”, “Fig. 5”, and “Fig. 6”.

1. If this cell Attribute cell
2. Only one cell at this row
3. Next row is empty blankRow == null
4. No table name yet TablNm == false
5. Cell value contains substring "Table"  
CelValue.contains("Table")

Fig. 4. Extract Table Name.

1. If this cell Attribute cell
2. Extract table name before TablNm == true
3. There are other attribute cells at the same row
4. Check if this merged region and get its address (parent attribute)
5. sheet.getNumMergedRegions() \\  
calculate NUMBER of merged region
6. CellRangeAddress address = new  
CellRangeAddress(firstRow,endow,firstColumn,endCo  
lumn) \\  
return address of merged region
7. There is an empty cell in the same row
8. If the next row has an attribute cell, this is a hierarchal  
attribute
9. Every cell in the next row has the same address of  
merged cell be a child of parent Attribute

Fig. 5. Extract Top Attributes.

1. If this cell Attribute cell
2. First cell at row columnIndex == 0
3. There are not any attribute cells at the same row  
phNumOfCell == 1
4. If the rest of the row blank is parent left Attribute
5. If there are other data at the same row value left  
attribute

Fig. 6. Extract Left Attributes.

#### B. Extract more than One Table from One Datasheet

In the case of the existence of more than one table in the same datasheet, there are two possible causes for the positioning of them. Case (A), if these tables were placed side by side separated by one or more empty columns. Case (B), if these tables were placed over each other separated by one or more empty rows.

### IV. HORIZONTAL SYNCHRONIZATION

In this case, if the algorithm found an empty column before the maximum number of the filled data columns, that means there is another table in the same rows. The algorithm will implement a new matrix to store the new table.

### V. VERTICAL SYNCHRONIZATION

In this case, if the algorithm found an empty row before the maximum number of the filled data rows, that mean there is another table below. The algorithm will finalize and send the current table then starts to explore the new one.

## VI. ALGORITHMS USED

### A. Header Inference Algorithm based on Heuristic Rules and Cell Classification Features

1) The spreadsheet table has its exceptional trait of being a structure of vertically on a level plane extended segments, which are table name, attributes, and values. The paper displays a calculation for table identification in spreadsheets. The calculation utilizes three kinds of cells as its premise: table name cell, attribute cell, and value cell. As shown in "Fig. 7", the cell classification identification proof was based on its heuristic features and the number of cells, one cell or more than one cell.

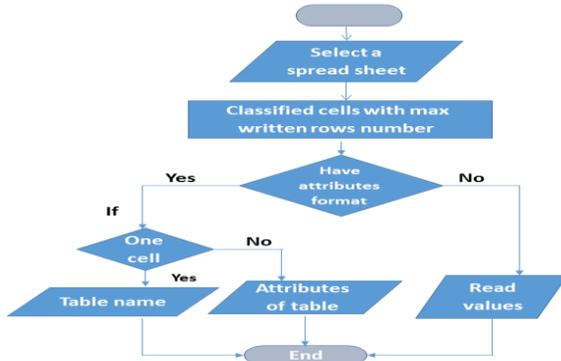


Fig. 7. Cell Classification Flow Chart.

Once the user opened the selected spreadsheet, the algorithm begins to detect all tables found in the spreadsheet using the method of cell classification based on detect max written rows number. This method detects the first row that contains data and the last row that contains data which makes a table frame. After that, the algorithm will check the cell formats for example if it is bold, italic, justified, capitalized, or colored to detect if this cell has an attribute's format or not. The attribute's format detects based on the cell classification numbers as well as one cell and has attributes format, it will be table name. However, if there is more than one cell and contains the format of the attributes, it will be attributes or headers of the detected table. However, table attributes detection is divided into two phases, top and left attributes. Top attributes are the first row that is not empty and contains data with attributes format and the left attributes are in the first left column within attributes format. The Top and Left attributes may be extended in a multi-level of rows or columns respectively which makes it a hierarchal attribute. Otherwise, the algorithm detects and extracts table values based on a cell type if it is the numeric type which means the cell contains numbers or the string cell is not an attribute cell.

Heuristic rules for complex and hierarchal table structures are found in the top first row and first left column. Also, Heuristic rules for hierarchal table attributes extended for multi-level rows or columns. Excel relational data extraction for table structure can be summarized as shown in Algorithm 1.

Physical layout features (the cell has right border, the cell has bottom border, the row has bottom border, if there is a table, the table has outside border, the table has a bottom

double border, the table has thick bottom border, the table has top and double bottom border, the row has a top and double border, the cell has all borders, the column has a right border if there are merged cells).

---

#### Algorithm 1. Excel relational data extraction

---

```
Input: Exc
el workbook with multiple sheets A = {S1, S2, ..., Sn} and contains
complex and hierarchal tables structure
Output: Separate tables each include TBL: Table name as a variable
TblNm and Attributes as an array list Att = {att1, att2, ..., attn}, values
as Val[m,n] = {valm1n1, valm1n2, ..., valm,n}

Begin A
  For every sheet in A Do
    Begin new TBL // row 3
    For every filled row Do
      For every filled column Do
        For every cell Do
          If the cell has attributes format and no other data in
this row or column // one cell
            TblNm <- cell data
          Else if a cell has attributes format and there is other
data in this row or column // more than one cell contains the same
format // top or left attribute
            Att <- cell data
          Else if the cell in the next line have Attributes format
// next line column or row
            Att <- cell data // Hierarchal attributes
          If a cell does not have attributes format or it is a numeric
value
            Val[m,n] <- cell data
          Else if an empty row or an empty column go to row 3
            End if
          End if
        End for
      End for
    End for
  End for
End for
```

---

Semantic content features for cells ( bold, italic, underline, different font or content style, different background cells color ( fill color or cell format), alignment ( top, middle, bottom, left, center, right), attribute contains keyword such as: "Total", "Name", "ID", "Average", "Avg", "Date", Year...etc., attribute letters are all capitalized, attribute contains a colon, attributes font size is bigger than values font size, the attribute has blank cells in the middle( blank row or column inside the detected frame), child's row index is greater than parents, parent row index is smaller than children, in left attributes the child's indentation is greater than parents, attribute cell is long width, if there are the same features on multiple rows or column until finding deferent features, etc.

## VII. RESULTS AND DISCUSSION

The evaluations of the accuracy of the approach are used and illustrate it by utilizing the gov.au.data dataset [26]. The paper downloaded two different public datasets with Excel (.xlsx) Formats. The datasets contain multiple sheets (61 and 82 sheets, respectively) and every sheet may contain only one table or multiple tables as illustrated in Table I. The evaluation supported relational data detected and extraction from the spreadsheet tables.

TABLE I. EXPERIMENTAL RESULTS

Datasets	Number of sheets	Number of randomly selected sheets, tables	Number of successfully identified relational data	Percentage of successfully extracted relational data %
1- Australian Public Service Statistical Bulletin - December 31, 2016	61 sheets	20 sheets with 20 tables	Table name: 20 Top attributes: 19 Left attributes: 18	Table name: 100% Top attributes: 95% Left attributes: 90%
2- APS Employment Data 30 June 2019 release	82 sheet	20 sheets with 29 tables	Table name: 29 Top attributes: 27 Left attributes: 26	Table name: 100% Top attributes: 93.1% Left attributes: 89.6%

REFERENCES

The experimental results showed that the percentage of accuracy to the first dataset of table name detection and extraction is 100%, top attributes are 95%, and left attributes are 90%. However, the second dataset results accuracy is 100% for the table name detected and extraction, 93.1% of top attributes, and 89.6% of left attributes. In summary, It is important to need to understand the nature of the Excel sheet that will be working on because each excel sheet has a different structure from the other one, and therefore the difficulty of extracting data from it comes from here. Therefore, it needs to know the structure of the Excel sheet that will be work on, and if there is any structure other than this, the extraction algorithm will be stopped working, or it will not work correctly to extract the data from it. Thus, to extract a large corrected number of relational tables successfully from spreadsheets, you have to identify a variety and of heuristic tables' cells features and rules.

The algorithms are written in JAVA as a programming language, connected with SQL server as an analysis tool, and Windows 7 as an operating system. To test it, an executable jar file is created. The hardware specifications for the system are, Intel® Core™ 2 Duo CPU with 4 GB of RAM. The version of Microsoft Excel installed on the machine is 2013. However, the proposed tool works only with new version of Excel (.xlsx' format).

VIII. CONCLUSION AND FUTURE WORK

This paper presents a detailed algorithmic data processing method for automatically extracting relational data in complex and hierarchal table structures from spreadsheets. The automatic approach is accompanied by some heuristic rules, features, and cell classification categories. The experimental results showed that the accuracy of relational data detected and extracted from the spreadsheet tables for the tested two datasets are 95% and 94.2% respectively. In the future work, the proposed method can be extended to integrate the extracted data into an existing relational database.

IX. CONFLICTS OF INTEREST

The paper declares that it has no conflict of interest and no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

ACKNOWLEDGMENT

We would like to thank the "Future University in Egypt" for its continuous support and efforts to improve the scientific research results for publication.

- [1] N. Mohamad, N. Ahmad, and S. Sulaiman. "Data pre-processing: a case study in predicting student's retention in MOOC." Journal of Fundamental and Applied Sciences, 9.4S, (2017), pp.598-613.
- [2] L. Irina, and A. Begler. "A method of semi-automated ontology population from multiple semi-structured data sources." Journal of Information Science, (2020): 0165551520950243 , pp.1-14.
- [3] K. Elvis, et al. "A machine learning approach for layout inference in spreadsheets." IC3K 2016: Proceedings of the 8th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management: volume 1: KDIR. SciTePress, 2016, pp.77-88.
- [4] C. Zhe, and M. Cafarella. "Automatic web spreadsheet data extraction." Proceedings of the 3rd International Workshop on Semantic Search over the Web. 2013, p.1-8.
- [5] Awad, A., Roushdy, M. I., ElGohary, R. A. E., & Moawad, I. F. "Metadata extraction for low-quality semi-structured spreadsheets." Joint European-US Workshop on Applications of Invariance in Computer Vision. Springer, Cham, 2020, p. 448-457.
- [6] Awad, A., Roushdy, M. I., ElGohary, R. A. E., & Moawad, I. F. An interactive tool for extracting low-quality spreadsheet tables and converting into relational database. International Journal of Intelligent Computing and Information Sciences, 21(1), (2021), 1-18.
- [7] G. Ross, et al. "Rich feature hierarchies for accurate object detection and semantic segmentation." Proceedings of the IEEE conference on computer vision and pattern recognition. 2014, p. 580-587.
- [8] D. Haoyu, et al. "Tablesense: Spreadsheet table detection with convolutional neural networks." Proceedings of the AAAI Conference on Artificial Intelligence. Vol. 33. No. 01. 2019, pp. 69-76.
- [9] D. Haoyu, et al. "Semantic structure extraction for spreadsheet tables with a multi-task learning architecture." Workshop on Document Intelligence at NeurIPS 2019. 2019.
- [10] P. Aleksander, et al. "Transforming arbitrary tables into logical form with TARTAR." Data & Knowledge Engineering 60.3 (2007): 567-595.
- [11] RA. Robin, and M. Erwig. "UCheck: A spreadsheet type checker for end users." Journal of Visual Languages & Computing 18.1 (2007): 71-95.
- [12] S. Alexey, and A. Mikhailov. "Rule-based spreadsheet data transformation from arbitrary to relational tables." Information Systems 71 (2017): 123-136.
- [13] TT. Cui, and D. Embley. "Automatic hidden-web table interpretation, conceptualization, and semantic annotation." Data & Knowledge Engineering 68.7 (2009): 683-703.
- [14] KK. Elvis, et al. "A machine learning approach for layout inference in spreadsheets." IC3K 2016: Proceedings of the 8th International Joint Conference on Knowledge Discovery, Knowledge Engineering and Knowledge Management: volume 1: KDIR. SciTePress, 2016, p. 77-88.
- [15] VV. Gust, and L. Raedt, "Towards automated relational data wrangling." Proceedings of AutoML 2017@ ECML-PKDD: Automatic selection, configuration and composition of machine learning algorithms 1998 (2017): 18-26.
- [16] PP. Viacheslav, A. Shigarov, and V. Vetrova. "Table header correction algorithm based on heuristics for improving spreadsheet data extraction." International Conference on Information and Software Technologies. Springer, Cham, 2020, p. 147-158.
- [17] YY. Navid, X. Wang, and I. Dillig. "Automated migration of hierarchical data to relational tables using programming-by-example." Proceedings of the VLDB Endowment 11.5 (2018): 580-593.

- [18] KK. Elvis, et al. "Table identification and reconstruction in spreadsheets." International Conference on Advanced Information Systems Engineering. Springer, Cham, 2017, p. 527-541.
- [19] BB. Daniel, et al. "FlashRelate: Extracting relational data from semi-structured spreadsheets using examples." ACM SIGPLAN Notices 50.6 (2015): 218-228.
- [20] PP. Viacheslav, et al. "Heuristic algorithm for recovering a physical structure of spreadsheet header." International Conference on Information Systems Architecture and Technology. Springer, Cham, 2019, p. 140-149.
- [21] JJ. Cunha, J. Saraiva, and J. Visser. From spreadsheets to relational databases and back. In PEPM, 2009, p. 179-188.
- [22] AA. Nikita, D. Turdakov, and N. Vassilieva, "Semi-automatic data extraction from tables." RCDL, 2013, p. 14-20.
- [23] KK. Sean, et al. "Wrangler: Interactive visual specification of data transformation scripts." Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. 2011, p. 3363-3372.
- [24] GG. Sumit, W. Harris, and R. Singh, "Spreadsheet data manipulation using examples." Communications of the ACM 55.8 (2012): 97-105.
- [25] LL. Vu, and S. Gulwani, "Flashextract: A framework for data extraction by examples." Proceedings of the 35th ACM SIGPLAN Conference on Programming Language Design and Implementation. 2014, p. 542-553.
- [26] [https://data.gov.au/data/dataset?organization=australianpublicservicecommission&res\\_format=excel+%28.xlsx%29&res\\_format\\_limit=0](https://data.gov.au/data/dataset?organization=australianpublicservicecommission&res_format=excel+%28.xlsx%29&res_format_limit=0).

# Effective Controlling Scheme to Mitigate Flood Attack in Delay Tolerant Network

Hanane ZEKKORI, Saïd AGOUJIL, Youssef QARAAI

Dept. of Computer Science of Faculty of Sciences and Techniques, University of Moulay Ismail  
Errachidia, Morocco

**Abstract**—Conventional routing protocols breaks down in opportunistic networks due to long delays, frequent disconnectivity and resource scarcity. Delay Tolerant Network (DTN) has been developed to cope with these mentioned features. In the absence of connected link between the sender and the receiver, in DTN mobile nodes replicate bundles and work cooperatively to improve the delivery probability. Malicious nodes may flood the network as possible by a huge number of unwanted bundles (messages) or bundle replicas which waste the limited resources. DOS (Denial of Service) attack especially Flooding attack attempt to compromise the availability service of the network. Traditional congestion control strategies are not suitable for DTN, so developing new mechanisms to detect and to control flooding attack is a major challenge in DTN network. In this paper, we presented a comprehensive overview of the existing solutions for dealing with flooding attack in delay tolerant network, and we proposed an effective controlling mechanism to mitigate this threat. The main goal of this mechanism is first to detect malicious nodes that flood the network by unwanted messages, and then to limit the damage caused by this attack. We also ran a large number of simulations with the ONE simulator to investigate how changing buffer capacity, message lifetime, message size, and message replicas affect DTN network performance metrics.

**Keywords**—DTN; flooding attack; DOS; congestion; buffer capacity; bundle; ONE

## I. INTRODUCTION

Nowadays, the use of wireless technology has invaded the mobile network market. MANET (Mobile Ad hoc Network) [1] is a wireless network that does not rely on a pre-existing infrastructure. This traditional mobile network, on the other hand, does not support packet transfer in an environment characterized by an intermittent connectivity between the transmitter and the receiver. Which results in the birth of the DTN (Delay tolerant network) [2], that comes to cope with these challenges by the help of a Bundle layer added on top of lower-layer protocols (see Fig. 1). The bundle layer ensures interoperability between network regions and the transfer of bundles (messages) via a technique known as store carry and forward [2], in which network mobile nodes collaborate with each other to increase the message delivery rate.

Contacts in the DTN network are opportunistic [3]; nodes meet with no prior knowledge about the movement and the mobility of the other nodes in the network. So, flooding based routing strategy can be opted to improve the probability of delivery and to reduce the average latency. This routing strategy consists of flooding the network with multiple copies

or replicas for each single bundle to increase the likelihood that one of these copies will reach its destination. This strategy, however, consumes more network resources.

DTN uses the store-carry and forward paradigm [2] to avoid data loss if the upstream path is interrupted. When a source node creates a bundle, it stores it in its persistent buffer until a contact opportunity with an intermediate node occurs. The mobile nodes exchange bundles in a hop-by-hop manner, and the process is repeated until each bundle arrives at its final destination. Each node has a persistent buffer B in which it stores the received bundles, and it is defined by its limited capacity C.

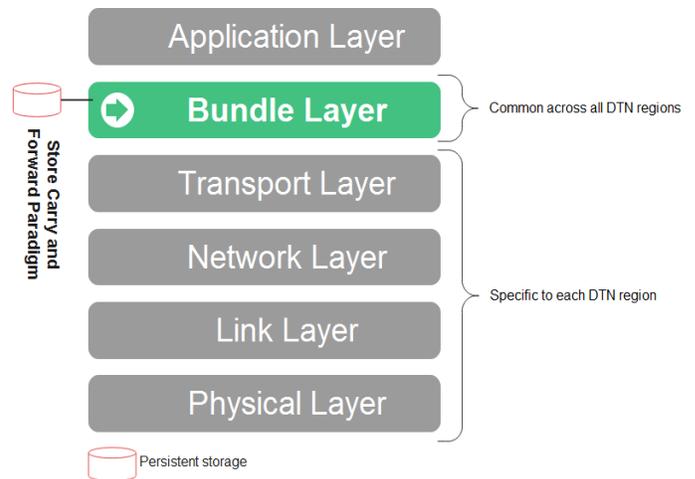


Fig. 1. Illustration of DTN Layered Architecture.

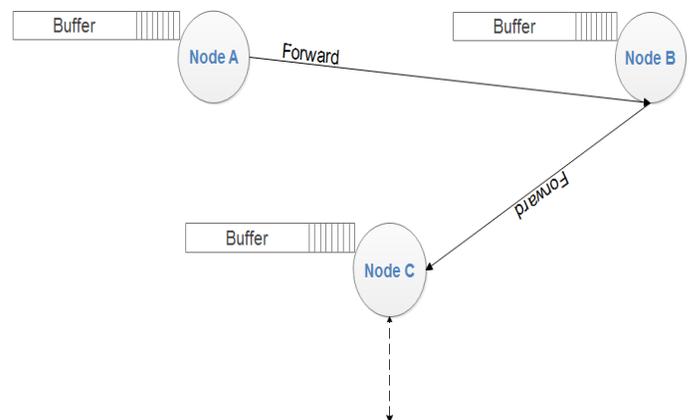


Fig. 2. Illustration of the Store Carry and Forward Transport Technique.

We have schematized the technique Store and Forward in the Fig. 2: to deal with the DTN network's intermittent connectivity, each node keeps the bundle in its buffer (store phase) while waiting for a future communication opportunity with a relay node to transmit that bundle (forward phase).

#### A. Security Requirements

The fundamental security requirements for DTN [4] are similar to those for wired and wireless networks with infrastructure. Security services are based on five fundamental concepts: Authentication, confidentiality, data and network traffic integrity, availability, and non-repudiation (see the Fig. 3 below) [5] [6].



Fig. 3. The Five Fundamental Security Requirements.

#### B. The Five Fundamental Security Requirements

- Authentication

Authentication verifies the identity of network entities or nodes. This is a crucial step in controlling network resource access. Without authentication, a malicious node can easily spoof another node in order to gain the privileges assigned to that node, or attack using that node's identity in order to harm its reputation. The authentication process in wired or wireless networks with infrastructure is based on a trusted third party which has been approved by all network entities. The trusted third party is simply the certificate authority, which distributes certificates to nodes with access to specific network services. This centralized authentication scheme is known as Public Key Infrastructure (PKI) [7]. It is nearly impossible to apply the PKI model directly to the DTN network because the DTN network topology changes frequently and dynamically and the connectivity is intermittent, the nodes are autonomous, and their capabilities (energy, computation, buffer space, etc.) are limited.

- Confidentiality

The fundamental service for ensuring private communication between nodes is confidentiality. It is about protecting against threats that could lead to unauthorized disclosure or viewing of private information. It is fundamentally based on cryptography, specifically encryption algorithms. Encryption algorithms, whether symmetric or asymmetric, require an encryption key to encrypt a message

before it is sent to its destination. However, in order to decrypt the message, the destination must have a decryption key. As a result, a key management and sharing mechanism tailored to the DTN network is required, however due to the DTN network's unique characteristics (intermittent connectivity...), it is a significant challenge to implement these traditional encryption algorithms.

- Integrity

This service ensures that traffic from the source to the destination has not been altered or modified without prior authorization during transmission. The risk that a malicious node modifies a message is always present in the DTN network. The goal of integrity service is to ensure that resources are working properly. This service protects information from unauthorized modification (ensure data integrity). Indeed, this service can be used in conjunction with security protocols that provide confidentiality and authentication.

- Availability

Availability refers to ensuring the continuity of a node's services even in the face of an attack. In other words, nodes must ensure network services continuity (such as routing, data access, and so on) in the event of a flooding attack. To accomplish this, it is necessary to protect against threats that may disrupt network functions to ensure that all nodes have access to network resources without any restriction.

- Non-Repudiation

The ability to verify that the sender and the receiver are the parties claiming to send or receive messages is referred to as non-repudiation security requirement. In other words, the undeniable source demonstrates that data was sent, and the undeniable destination demonstrates that data was received. Non-repudiation, in other words, ensures that the transaction (transmission/reception) cannot be denied. This is extremely helpful to detect and isolate infected nodes. Any node that receives an incorrect message can use evidence to accuse the sender, which helps other nodes believe in the sending node's compromise.

Because of long delays [5], frequent disconnections, and resource scarcity, traditional routing protocols fail in opportunistic networks. To address these issues, the Delay Tolerant Network (DTN) was created. In the absence of a connected link between the sender and the receiver, DTN mobile nodes replicate bundles and collaborate to improve the probability of delivery. Malicious nodes may flood the network with as many unwanted bundles or bundle replicas as possible, wasting the network's limited resources. A flood attack attempts to compromise the network's availability service. Because of the unique characteristics of DTN networks, traditional mechanisms are ineffective for detecting and controlling flooding attacks, so developing new mechanisms to detect and control flooding attacks is a major challenge in DTN.

In this paper we examined the impact of changing buffer capacity, message lifetime, message size, and message replicas on flooding-based routing protocols in terms of the following

performance metrics: delivery probability, overhead ratio, and latency average, and we proposed an effective controlling mechanism to mitigate the flooding attack. The primary goal of the proposed mechanism is to detect malicious nodes that flood the network with unwanted messages and then limit the damage caused.

This paper is structured as follows: Section 2 discusses related work on the existing security solutions against selfish behavior in Delay Tolerant network and presents flooding attack in DTN. Section 3 gives our proposed work whereas section 4 focuses on the simulation setting used to discuss the performance of routing protocols in DTN, also this section emphasizes and analyzes the obtained results. Finally, Section 5 concludes the paper providing a final summary of the study and suggests additional research topics for the future.

## II. RELATED WORK

### A. Flooding Routing Protocols

To improve the delivery probability and to reduce the average latency, flooding-based routing protocols can be used (see the Table I). Flooding-based routing strategy [8] involves flooding the network with multiple copies or replicas of each single bundle (message) in order to increase the likelihood that one of these copies will reach its destination. This, however, consumes more network resources.

TABLE I. DESCRIPTION OF THE FLOODING BASED-ROUTING PROTOCOLS

Routing Algorithm	Description
Epidemic[9]	In the epidemic routing protocol, each mobile node stores a copy of each message in the network in its buffer. When it makes a contact with another node, all its messages are routed to that node, and so on. Each bundle is labeled with a unique identifier (ID) and listed in a list known as a "state vector." When two nodes communicate, the list of bundle IDs is exchanged; at the end of this operation, both nodes should have the same bundles in their buffers. There is no prior network knowledge required for the epidemic routing protocol. This protocol, on the other hand, necessitates a substantial amount of buffer space, bandwidth, and energy.
Spray and Wait[10]	Spyropoulos et al proposed the Spray and Wait routing protocol, which works on the principle of starting the transmission with a limited number of copies L (with $L > 1$ ) in order to preserve the DTN network's limited resources. For each bundle in the network, the Spray and Wait protocol algorithm consists of two phases: <ul style="list-style-type: none"><li>• The spray phase: The source node sends L copies of each bundle to the L relay nodes during the spray phase.</li><li>• The wait phase: When each bundle has a single copy, each node will wait for a direct meeting with the destination node before sending the bundle copy to its destination.</li></ul>
Binary-Spray and Wait[10]	The spray phase here differs from the one described above (the spray phase of Spray & Wait protocol); in Binary-Spray & Wait protocol, the source node sends $L/2$ copies to the neighboring nodes, and when there is only one copy left in each node's buffer, it enters in the wait phase, as described above in the wait phase of Spray & Wait protocol.

### B. The Queue Management

When the DTN runs out of storage space, it discards old bundles because they are likely to have arrived at their destinations. When storage resource becomes insufficient, the Bundle layer has only a certain amount of freedom in managing the situation, so it can drop older ( $TTL \approx 0$ ) bundles in order to receive new bundles.

There are several service disciplines (Buffer management policies) to manage a queue, the simplest way to manage a queue is the FiFo (First in First out) discipline[11].

- DLR (Drop Least Received): is identical to FiFo, the first message to arrive will be the first served.
- DOA (Drop Oldest Arrive): deletes the oldest message because there is a high probability that this message has reached its destination.
- DLE (Drop Last Encountered): drops the message that has the smallest predictability.

### C. Problem Statement: Flooding Attack

A Denial-of-Service (DOS) [12] attack is an active attack that aims to make a network's services unavailable for an extended period of time. The purpose of this type of attack is not to modify or drop bundles. But the goal is to disrupt or harm the reputation of a network service. This attack consumes resources such as bandwidth, energy, and storage space.

The basic idea behind this attack is to send bundles in an unusual pattern, causing saturation or instability in the victim nodes and preventing them from providing the network services that they are supposed to provide. When several nodes cause a Denial-of-Service attack. This is referred to as a "Distributed Denial of Service (DDOS)". A DDOS attack has the same goal as a DOS attack, except that the attack is launched from more than one node at the same time.

Such attacks are classified into two types [13]:

- a) Denial of service by saturating a node's buffer to the point where it can no longer receive other bundles.
- b) Denial of service by exploiting vulnerabilities, which involves exploiting a network flaw to render it inoperable.

### D. Overview of the Existing Solutions for Detecting the Flooding Attack in Delay Tolerant Network

Table II summarizes the fundamental three techniques used in the literature to detect and prevent the flooding attack in DTN.

TABLE II. SURVEY OF THE EXISTING SECURITY SCHEMES USED FOR MITIGATING THE FLOODING ATTACK IN DTN

Scheme	Its process	Its limitation
Claim-Carry and Check scheme[14]	A rate limiting was proposed, each node has a limit on the number of messages that it can generate in each time interval and a limit on the number of replicas that it can generate for each message. When a node violates its rate limiting, a claim is generated as an alarm, and each node receiving the alarm must check for the inconsistency between the received claims.	False claims and inconsistency of the received claims.
Encounter Records (History of encounters) (ERs) scheme[14]	This scheme is based on recording the history of encounters. In order to record the messages sent during previous contacts, nodes must exchange their ER (Encounter Record) history. Malicious nodes will be identified, resulting in a flooding attack.	Removing favorable ERs. ERs falsification and modification.
Stream-Check scheme[14]	The streaming node is used in this scheme to monitor the network environment. Three tables must be maintained by the monitor node. The first contains the rate limits of all nodes in the network, the second contains the delivery probability of each node in the network, and the third contains the blacklisted nodes. The streaming node compares estimated probability of delivery to actual probability of delivery; if the difference is greater than the assigned limit value, the node is added to the blacklist by the streaming node.	A large number of resources are required by the streaming node.

### III. THE PROPOSED MECHANISM TO CONTROL THE DISTRIBUTED FLOODING ATTACK

In this paper we are interested in the first type of DOS [12] (saturation of a node's buffer) in the DTN network because it appears to be more severe than the second due to DTN's scarcity of resources. Consider the scenario in which the attack is launched from multiple DTN nodes. In a brief, we are interested in a distributed flooding attack. This attack is carried out by several network nodes with the goal of disrupting the availability service of the nodes. The figure below (Fig. 4) depicts a node's inability to transmit messages due to the saturation of its buffer by unwanted bundles (bundles mean messages in DTN network).

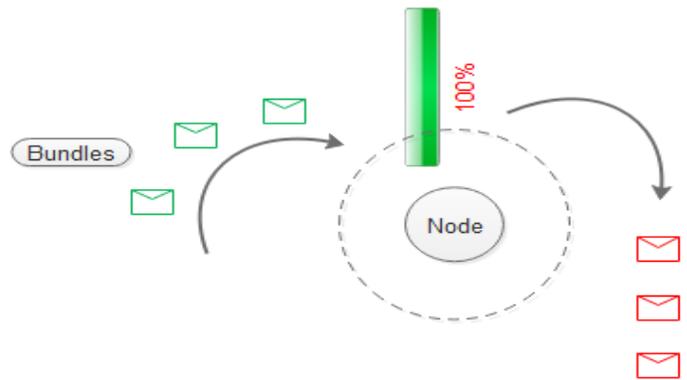


Fig. 4. Unwanted Bundles Saturating a DTN Node's Buffer.

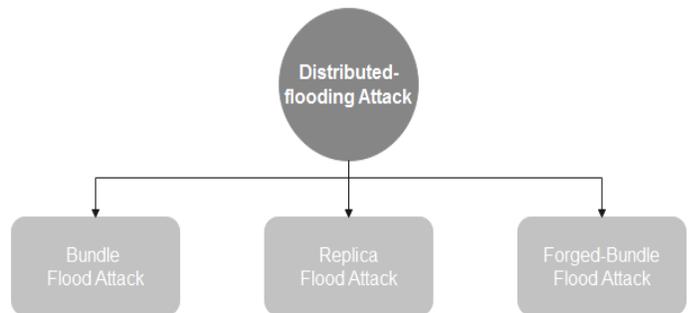


Fig. 5. Classification of the Flooding Attack.

The flooding attack [15] [16] can be classified into three types based on the type of bundles, as shown in the figure below (Fig. 5):

- Bundle-Flood Attack: when the attacker nodes flood the network by normal messages.
- Replica-Flood Attack: when the attacker nodes flood the network by replicas of each message.
- Forged Bundle-Flood Attack: when the attacker nodes flood the network by fake messages.

#### A. Our Assumptions

- A partition of the network is affected all by distributed flooding attack.
- Malicious nodes flood the network by bogus bundles, so we need to filter the traffic by filters.
- There are three groups of bundles which circulate into the network: Normal Bundles, Replica Bundles and Forged Bundles.
- Nodes are classified into three main groups, Nodes that are nearer to their destinations, they transfer very important (urgent) bundles, Nodes that are partially near to their destinations, they transfer important but not urgent bundles and finally, nodes that are far to their destinations, they transfer unimportant bundles.
- According to the priority of each bundle into the network, bundles are classified into three main groups: Urgent bundles, important bundles, and unimportant bundles.

TABLE III. TABLE OF THE USED NOTATIONS FOR OUR PROPOSED WORK

Notation	Signification
N	The total number of nodes in the network
TTL (Time To Live)	Bundle lifetime
$d_i, i = \{1,2,3\}$	Node classes based on their proximity to the destination with ( $d_1 < d_2 < d_3$ ).
$P_i, i = \{1,2,3\}$	Priority classes of bundles.

**B. Our basic Idea**

Each DTN node generates different bundles and then commits to prioritizing them as follows (More information about the notations used can be found in Table III):

- It classifies messages that are very important (urgent) in the set P1.
- It classifies the messages that are important but not urgent in the set P2.
- It classifies the messages that are less important than P2 in the set P3.

Nodes are classified into three categories based on their distances from the destination nodes:  $d_1$ ,  $d_2$  and  $d_3$  with ( $d_1 < d_2 < d_3$ ).

- Nodes that are closer to the destination, their distance to the destination is  $d_1$ .
- Nodes that are partially close to the destination, their distance to the destination is  $d_2$ .
- Nodes that are far away from the destination, their distance to the destination is  $d_3$ .

The priority of each message is determined according to its lifetime (messages with a short TTL have a high priority because they must be transmitted before their TTL expires), its size (messages with a smaller size have a high priority than large messages because the latter may saturate the limited storage space) and its number of replicas (Messages with a small number of replicas have a higher priority than messages with a large number of replicas).

The distance of each node from its destination is determined by referring to the movement history of the DTN nodes (the hop-by-hop count taken before arriving at the destination). The value of this distance is predictive because DTN nodes are mobile.

Our basic idea is first to distribute the bundles to the various nodes based on their priorities in the following manner:

- The nodes whose distance to the destination is  $d_1$  agree to receive only messages with priority P1 and agree to forward them to their destinations.
- The nodes whose distance to the destination is  $d_2$  accept to receive only the messages of priority P2 and agree to transfer them to their destinations.
- The nodes whose distance to the destination is  $d_3$  accept to receive only the messages of priority P3 and agree to forward them to their destinations.

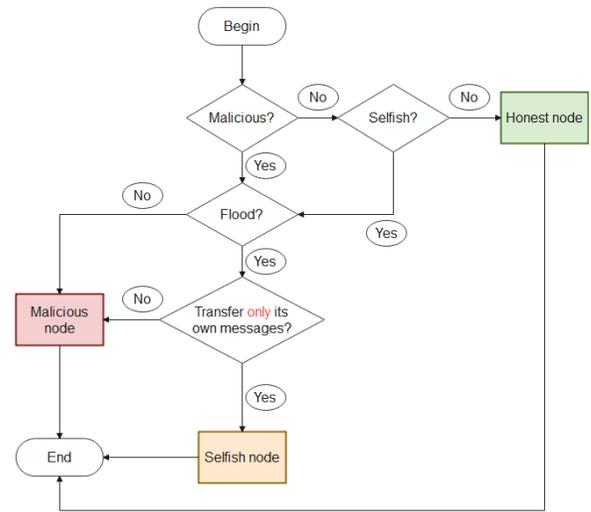


Fig. 6. Overall Flowchart.

Then, to identify malicious nodes that flood the network by unwanted bundles, we have proposed an effective scheme (see the below flowchart, Fig. 6).

**C. The Objectives of our Proposed Work**

1) Identify the nodes that flood the network with unwanted messages so that the other nodes in the network do not accept their messages the next time they contact them.

2) Reduce and optimize the network load by categorizing nodes and messages (as explained above in section 3). When exchanging messages between two neighboring nodes, it is not necessary for the receiver node to accept all the messages from the sender node; instead, it must accept a subset of these messages based on its type (close to the destination or not) and based on the priority class of the messages (P1, P2 or P3).

**IV. SIMULATION AND ANALYSIS**

The ONE (Opportunistic Network Environment Simulator) simulator [17] is an opportunistic networking simulator that provides several tools for creating complex mobility scenarios that are more realistic than many other synthetic mobility models. ONE supports various node movement models and simulates a variety of DTN routing algorithms. The ONE simulator is written in Java, and it allows to add routing algorithms by extending the built-in routing classes.

**A. Simulation Environment Setup**

The ONE simulator (Opportunistic Network Environment Simulator) [17] was used, as shown in Fig. 7. Our scenario includes a network of 140 DTN nodes (an average density): 120 pedestrians and 20 trams. The simulation time was 12 hours, with a 0.1 second update interval. The effect of changing the buffer capacity, bundle lifetime, bundle size and bundle replicas on flooding protocols was investigated. To make our simulation more realistic, we used a cluster-based mobility model with three clusters or regions (each cluster can be a remote village) spread across an area of  $4.5 \times 3.4$  Km. The pedestrians within each cluster were moving at a speed ranging from 0.5 to 1.5 m/s. See the table below (Table IV) for more information on the simulation parameters that were used.

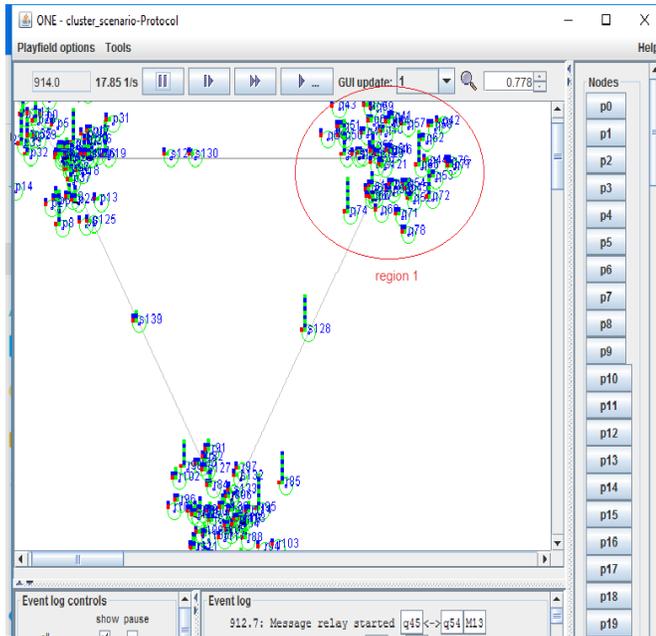


Fig. 7. The Screenshot of our Scenario on the ONE Simulator's GUI.

TABLE IV. SIMULATION PARAMETERS

Parameter name	Value(s)
Simulation time	43200s
Number of Nodes	140
TTL	60Min-300Min (step 60)
BufferSize	20MB-180MB (step 20)
MsgSize	50kB-550kB
NBOOfReplicas	20-100 (step 20)
movementModel	ClusterMovement
RoutingProtocols	Epidemic, Spray & Wait, Binary-Spray & Wait

The following performance metrics are considered in analyzing the effect of changing buffer capacity, bundle lifetime, bundle size, and number of replicas on the flooding protocols:

- **Delivery\_prob**: this metric describes the probability of message delivery at the end of the simulation. It is also known as the delivery ratio because it is the ratio of delivered messages to created messages. One of the primary goals of the DTN network is to maximize the value of this parameter. This metric's value is scaled in

[0,1]. It is computed using the following formula:  $(\text{NumberOfDeliveredMessages}/\text{NumberOfCreatedMessages})$ .

- **Overhead\_ratio**: it denotes a bandwidth efficiency evaluation during the simulation. The primary goal of the DTN network is to reduce the value of this metric. It is computed using the following formula:  $((\text{NumberOfRelayedMessages}-\text{NumberOfDeliveredMessages})/\text{NumberOfDeliveredMessages})$ .
- **Latency\_avg**: it is the average message delay from the time a message is created at the source to the time it is delivered to the destination. In a DTN network, the terms delay and latency are used interchangeably. The DTN network's primary goal is to reduce the value of this metric.

### B. Simulation Results and Discussions

#### a) The impact of BufferSize on flooding-based routing protocols

Fig. 8 (a) depicts the delivery probability obtained by using the flooding-based routing protocols: Epidemic, Spray & Wait (S&W), and Binary-Spray & Wait (B-S&W) in terms of BufferSize (MB). When the Epidemic routing protocol is used, the delivery probability increases with the increase of the BufferSize (MB) since buffer space means more nodes can carry more copies of messages, as opposed to the B-S&W and S&W routing protocols, which have approximately similar invariant values. This is because the Epidemic protocol's message transmission logic necessitates a large buffer size as compared to the B-S&W and S&W routing protocols. While the overhead-ratio falls (Fig. 8 (b)) particularly when using the Epidemic protocol. This is due to an increase in buffer size, which means more free space is available to transmit and to carry more messages. Fig. 8 (c) shows that when using the Epidemic protocol, the average latency decreases as the buffer size increases thanks to the multiple-copy nature of this protocol, which spreads replicas blindly, as opposed to the spraying protocols (S&W and B-S&W), which spread limited replicas into the network. Briefly, the Epidemic protocol benefits the most because its process of exchanging messages is quick, lowering average latency, thereby improving performance.

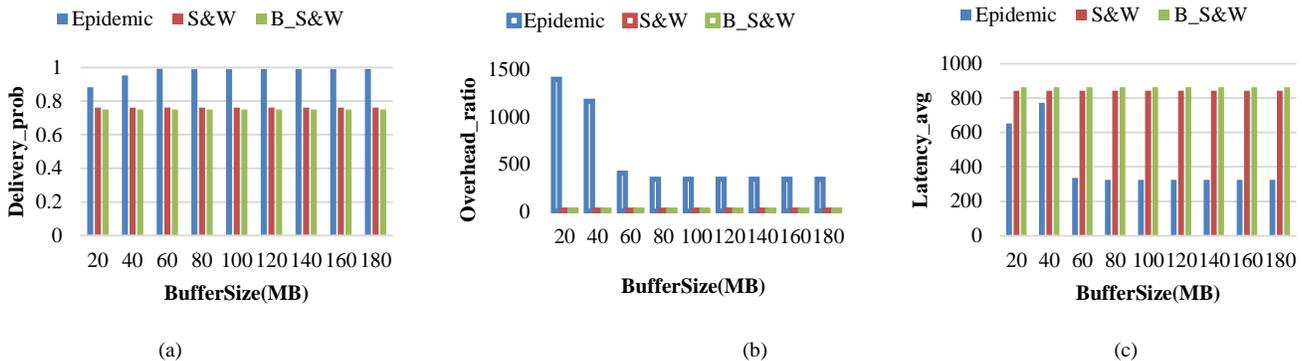


Fig. 8. The Effect of Changing the Buffer Size on Three Performance Parameters, (a) Delivery Probability, (b) Overhead Ratio, and (c) Average Latency, when using Flooding-based Routing Protocols (Epidemic, Spray&Wait and Binary-Spray&Wait).

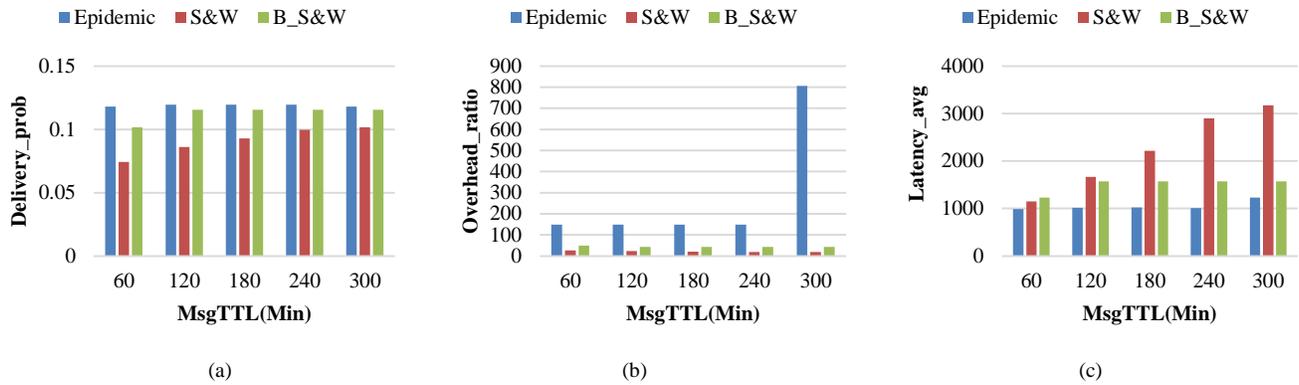


Fig. 9. The Effect of Changing the Message TTL on Three Performance Parameters, (a) Delivery Probability, (b) Overhead Ratio, and (c) Average Latency, when using Flooding-based Routing Protocols (Epidemic, Spray&Wait and Binary-Spray&Wait).

b) The impact of MsgTTL on flooding-based routing protocols (with BufferSize=5M)

Fig. 9 (a) shows that there is some progress in delivery probability as message TTL improves but the value of Delivery probability does not exceed 0.2 for the three protocols because messages with high MsgTTL values are classified as P3 Priority class (not important messages for transmission, see the third section) which lowering the delivery ratio. Furthermore, messages with a high MsgTTL value have a high chance of being delivered because these messages tolerate long RTT (Round Trip Time). However, increasing MsgTTL leads to an improvement in the network's overhead ratio, as shown in Fig. 9 (b). The epidemic protocol has higher values than the other protocols because it is possible that the replicas of each delivered message are still circling in the network, which increase the overhead ratio. Fig. 9 (c) depicts the effect of message TTL on average latency. The average latency for the three protocols has higher values. When the message lifetime is long, the average latency increases significantly. This behavior is easily explained by the fact that when a message has a large TTL value, it means that the transmission of this message is not a critical or urgent task. According to the third section, the priority class of the message is P3, and the nodes whose distance to their destinations is d3 are the nodes who accept to receive and transmit that category of messages. Because these nodes are so far away from their destinations, the average latency rises, which conform to our assumptions (see the third section).

c) The impact of MsgSize on flooding-based routing protocols (with BufferSize=5M)

Fig. 10 (a) shows the effect of varying Message size on the delivery probability for flooding-based routing protocols. When the message size increases, it seems that the delivery probability significantly decreases especially in the case of

using Epidemic as a routing protocol, but it does not have much effect on the other protocols (S&W and B-S&W). Increase message size, reduce the limited buffer size, and make congestion and cause continuous buffer space occupation. Which force relay nodes to accept to store only a small number of messages in their buffers, lowering the delivery rate. According to our assumptions, messages with a small size have a higher priority than messages with a large size. As a result, the delivery ratio has low values when large messages circulate in the network (as Fig. 10 (a) depicts). The priority class of messages with large sizes is P3, and the nodes transmitting these messages are far from their destination nodes (with distance d3), which explains the decrease in the delivery probability (see the third section). Fig. 10 (b) shows how changing the size affects the overhead ratio. As we can see, increasing the message size reduces the overhead ratio, especially when using Epidemic routing protocol. The overhead ratio is defined as  $(\text{NumberOfRelayedMessages} - \text{NumberOfDeliveredMessages}) / \text{NumberOfDeliveredMessages}$ , and as shown in Fig. 10 (a), the delivery ratio decreases as message size increases, implying that the number of relayed messages decreases as MsgSize increases. This behavior can be explained by the loss of large messages. Therefore, to avoid saturating their buffers, nodes rarely accept large messages (these large messages have a low priority class P3), resulting in a decrease in the delivery rate and a decrease in the network overhead ratio that can only be explained by the loss of large data. However, because large-sized messages are considered to have the lowest priority class (P3) according to our assumptions, and the nodes whose distance to their destinations is d3 are the nodes who accept to receive and transmit this category of messages, and because these nodes are so far away from their destinations that their transmission will take a long time, the average latency increases which conform to our assumptions see Fig. 10 (c)).

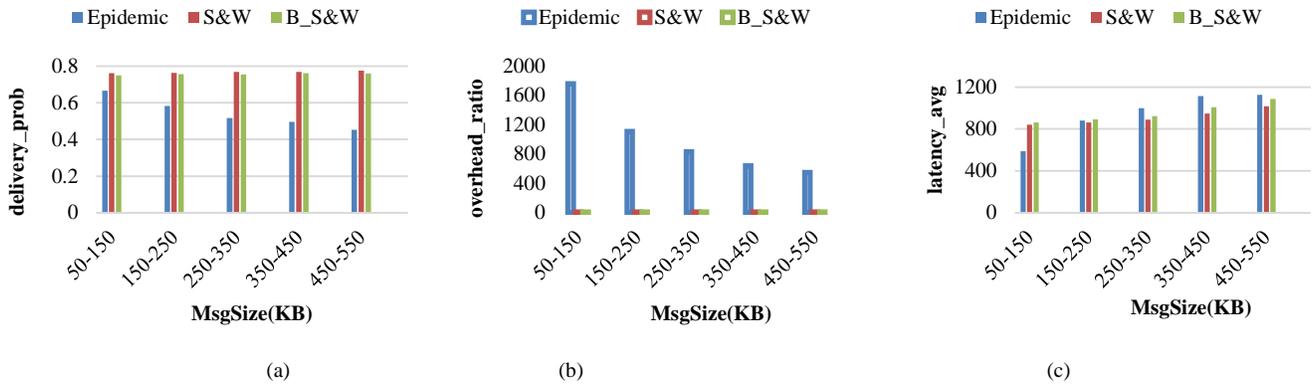


Fig. 10. The Effect of Changing the Message Size on Three Performance Parameters, (a) Delivery Probability, (b) Overhead Ratio, and (c) Average Latency, when using Flooding-based Routing Protocols (Epidemic, Spray&Wait and Binary-Spray&Wait).

d) The impact of NBOfReplicas on flooding-based routing protocols (with BufferSize=5M)

Fig. 11 depicts the message delivery, network overhead, and latency ratios when flooding-based routing protocols were used with different replica number values. The delivery rate, overhead ratio, and latency average for the Epidemic protocol are invariant to the number of replicas, which is due to the nature of this protocol, which floods the network with an unbounded number of copies (replicas); in comparison to the spraying protocols (Spray & wait protocol and Binary-spray & wait protocol), it has a higher value of the overhead ratio because it floods the network with unlimited replicas and the buffer space is limited in size (5M). As a result, we will concentrate on the comparison between Spray & Wait protocol and Binary-Spray & Wait protocol. For S&W and B-S&W the delivery rate shows an increasing trend up to a certain extent beyond which it saturated but B-S&W has higher values of delivery probability compared to S&W, see Fig. 11 (a). Fig. 11 (b) shows that the overhead ratio for S&W is invariant to the number of replicas, whereas the overhead ratio for B-S&W always increases continuously with the increase of the number of replicas. Messages with a small number of replicas have a higher priority than messages with a large number of replicas, according to our assumptions, and nodes whose distance to their destination is d1 (close to the destination) agree to receive

and to forward only messages with priority P1 (highest priority class). This means that as the number of replicas increases, the delivery probability must decrease (because messages are transmitted by nodes located far from their destinations) and the overhead must increase. Fig. 11 (a) shows, however, that the increase of the number of replicas leads to the increase in the probability of delivery, which contradicts our assumption. Fig. 11 (b), on the other hand, depicts the increase in overhead as the number of replicas increases, which is a natural result of the increase in delivery probability (as shown in Fig. 11 (a)). Fig. 11 (c) shows that as the number of replicas increases, the average latency decreases, particularly when using the B-S&W, implying that nodes have a short Round Trip Time (RTT) before being delivered to their destinations.

e) Message Graphs by using graphviz (with MsgTTL=60min)

The graphs below (Fig. 12, Fig. 13, Fig. 14) depict the node connections as well as the network paths that the delivered messages took. The MessageGraphviz [18] report module creates directed graphs of delivered message paths. The figures below show three examples of delivered messages graphs that contain all the messages sent from one network node to another during the simulation (Fig. 12, Fig. 13, Fig. 14). The figures show an example of a message graph, which contains all the messages sent from node to node during the simulation.

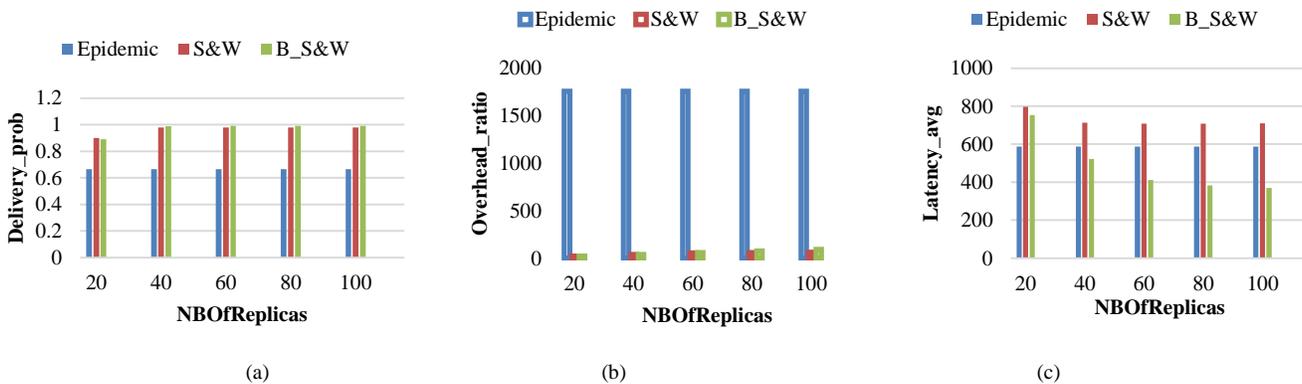


Fig. 11. The Effect of Changing the Number of Replicas on Three Performance Parameters, (a) Delivery Probability, (b) Overhead Ratio, and (c) Average Latency, when using Flooding-based Routing Protocols (Epidemic, Spray&Wait and Binary-Spray&Wait).

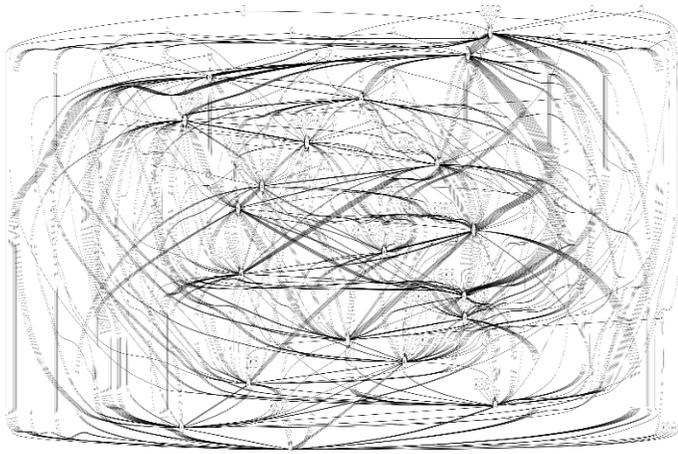


Fig. 12. Graph of the Messages that were sent from r113 to s128 for Epidemic Routing Protocol (173 Messages Delivered).

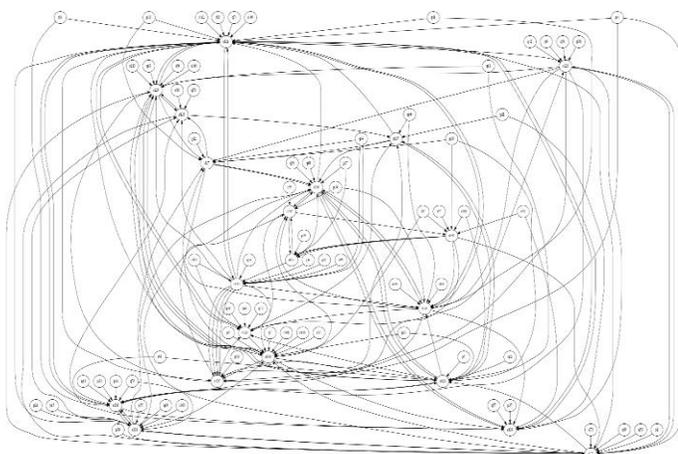


Fig. 13. Graph of the Messages that were sent from r112 to s121 for Spray and Wait Routing Protocol (109 Messages Delivered).

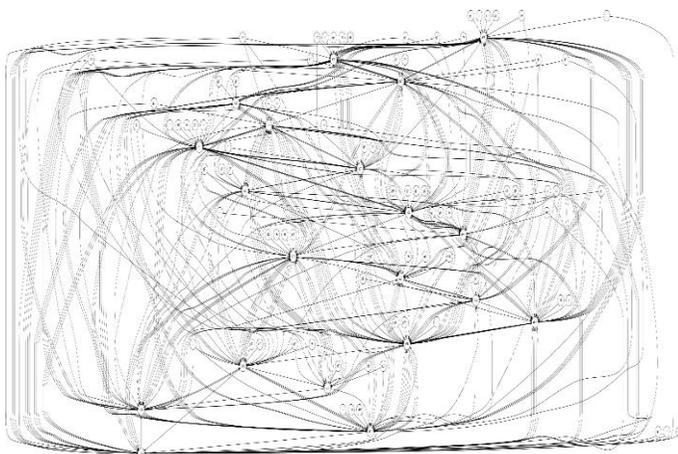


Fig. 14. Graph of the Messages that were sent from r113 to s128 for Binary-Spray and Wait Routing Protocol (149 Messages Delivered).

The graphs show that the Epidemic routing protocol's delivered message graph (Fig. 12) has more edges than the other graphs (when using the S&W and B-S&W protocols), resulting in an increase in delivered messages when using the

Epidemic protocol, as evidenced by the way Epidemic protocol messages are transmitted.

## V. CONCLUSION

Security is still a major concern in the Delay Tolerant Network. The DTN network lacks a centralized authority in charge of network filtering, and each mobile network node functions as both a router and a host. Malicious nodes can quickly flood the network with unwanted messages. Flooding attacks, in particular, disrupt the availability of network services. In this paper, we have proposed a security mechanism for controlling the distributed flooding attack, as well as a security scheme for detecting malicious nodes that flood the network. Then, in terms of three important metrics: delivery probability, overhead ratio, and latency average, a comprehensive study of the impact of changing buffer capacity, message lifetime, message size, and message replicas on flooding-based routing was presented. The simulations validate our most important hypotheses. In future work, we intend to improve our mechanism for dealing with flooding attack in order to improve the network performance in DTN, and we intend to design and implement a collaborative trust management protocol with an integrated buffer management scheme for dealing with flooding attack.

## REFERENCES

- [1] P. M. Jawandhiya, M. M. Ghonge, M. S. Ali, and J. S. Deshpande, "A survey of mobile ad hoc network attacks," *Int. J. Eng. Sci. Technol.*, vol. 2, no. 9, pp. 4063–4071, 2010.
- [2] F. Warthman, "Delay-and disruption-tolerant networks (DTNs)," *Tutor. V 0 Interplanet. Internet Spec. Interest Group*, pp. 5–9, 2012.
- [3] V. Kushwaha and R. Gupta, "Delay tolerant networks: architecture, routing, congestion, and security issues," in *Handbook of research on cloud computing and big data applications in IoT*, IGI Global, 2019, pp. 448–480.
- [4] P. Kumar, N. Chauhan, and N. Chand, "Security framework for opportunistic networks," in *Progress in Intelligent Computing Techniques: Theory, Practice, and Applications*, Springer, 2018, pp. 465–471.
- [5] P. K. BVSP, S. Sarma, and G. B. Prasad, "A BRIEF SURVEY ON SECURITY IN DELAY/DISRUPTION TOLERANT NETWORKS," *Int. J. Pure Appl. Math.*, vol. 118, no. 14, pp. 157–162, 2018.
- [6] R. Di Pietro, S. Guarino, N. V. Verde, and J. Domingo-Ferrer, "Security in wireless ad-hoc networks—a survey," *Comput. Commun.*, vol. 51, pp. 1–20, 2014.
- [7] S. Chokhani, W. Ford, R. Sabett, C. Merrill, and S. Wu, "RFC3647: Internet X. 509 Public Key Infrastructure Certificate Policy and Certification Practices Framework." RFC Editor, 2003.
- [8] E. P. Jones and P. A. Ward, "Routing strategies for delay-tolerant networks," *Submitt. ACM Comput. Commun. Rev. CCR*, vol. 1, 2006.
- [9] R. Wang, Z. Wang, W. Ma, S. Deng, and H. Huang, "Epidemic Routing Performance in DTN with Selfish Nodes," *IEEE Access*, vol. PP, pp. 1–1, May 2019, doi: 10.1109/ACCESS.2019.2916685.
- [10] T. Spyropoulos, K. Psounis, and C. S. Raghavendra, "Spray and wait: an efficient routing scheme for intermittently connected mobile networks," in *Proceeding of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking - WDTN '05*, Philadelphia, Pennsylvania, USA, 2005, pp. 252–259. doi: 10.1145/1080139.1080143.
- [11] J. A. Davis, A. H. Fagg, and B. N. Levine, "Wearable computers as packet transport mechanisms in highly-partitioned ad-hoc networks," in *Proceedings Fifth International Symposium on Wearable Computers*, 2001, pp. 141–148.
- [12] P. Pathak, A. Shrivastava, and S. Gupta, "A Survey on Various Security Issues in Delay Tolerant Networks," *J. Adv. Shell Program.*, vol. 2, no. 2, pp. 12–18, 2015.

- [13] D. S. Eswari, "A Survey On Detection Of Ddos Attacks Using Machine Learning Approaches," *Turk. J. Comput. Math. Educ. TURCOMAT*, vol. 12, no. 11, pp. 4923–4931, 2021.
- [14] M. Shah and P. Khanpara, "Survey of Techniques Used for Tolerance of Flooding Attacks in DTN," in *Information and Communication Technology for Intelligent Systems*, Springer, 2019, pp. 599–607.
- [15] R.-T. Lee, Y.-B. Leau, Y. J. Park, and M. Anbar, "A Survey of Interest Flooding Attack in Named-Data Networking: Taxonomy, Performance and Future Research Challenges," *IETE Tech. Rev.*, pp. 1–19, 2021.
- [16] K. Salunke and U. Ragavendran, "Shield Techniques for Application Layer DDoS Attack in MANET: A Methodological Review," *Wirel. Pers. Commun.*, pp. 1–27, 2021.
- [17] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," presented at the 2nd International ICST Conference on Simulation Tools and Techniques, Rome, Italy, 2009. doi: 10.4108/ICST.SIMUTOOLS2009.5674.
- [18] A. Keränen, J. Ott, and T. Kärkkäinen, "The ONE simulator for DTN protocol evaluation," in *Proceedings of the 2nd international conference on simulation tools and techniques*, 2009, pp. 1–10.

# Efficient DNN Ensemble for Pneumonia Detection in Chest X-ray Images

V S Suryaa, Arockia Xavier Annie R, Aiswarya M S

Department of Computer Science and Engineering  
College of Engineering, Guindy Anna University, Chennai, India

**Abstract**—Pneumonia is a disease caused by a variety of organisms, including bacteria, viruses, and fungi, which could be fatal if timely medical care is not provided. According to the World Health Organization (WHO) report, the most common diagnosis for severe COVID-19 is severe pneumonia. The most common method of detecting Pneumonia is through chest X-ray which is a very time intensive process and requires a skilled expert. The rapid development in the field of deep learning and neural networks in recent years has led to drastic improvement in automation of pneumonia detection from analysing chest x-rays. In this paper, a pre-trained Convolutional Neural Networks (CNN) on chest x-ray images is used as feature extractors which are then further processed to classify the images in order to predict whether a person has pneumonia or not. The different pre-trained Convolutional Neural Networks used are assessed with various parameters regarding their predictions on the images. The results of pre-trained neural networks were examined, and an ensemble model was proposed that combines the predictions of the best pre-trained models to produce better results than individual models.

**Keywords**—Deep neural networks; ensemble learning; pneumonia detection using x-ray images; transfer learning

## I. INTRODUCTION

Pneumonia is an infection in one or both lungs. Bacteria, viruses, and fungi cause it. The infection causes inflammation in the alveoli. The alveoli fill with fluid or pus, causing difficulty in breathing. Pneumonia and lower respiratory tract infections like influenza and respiratory syncytial virus are the leading cause of death worldwide. WHO Child Health Epidemiology Reference Group reported that the median global incidence of clinical pneumonia is 0.28 episodes per child- year. This statistic converts to an annual incidence of 150.7 million new cases, of which 11-20 million (7-13%) are severe enough to require hospital admission [1]. Majority of the episodes of clinical pneumonia in young children worldwide occur in developing countries due to lack of proper timely diagnosis. In 2015, More than half of all global pneumonia cases were from India, Nigeria, Indonesia, Pakistan, and China alone [2]. Chest X-rays are used by radiologists to identify pneumonia among patients. They look for white spots in the lungs (called infiltrates) that identify an infection. Medical imaging accounts for more than 90% of the entire available medical. Radiologists are required to analyse large quantities of medical images which is a time-consuming and exhaustive process. With the development of deep learning methods, it would be possible to sift through the data and analyse medical exams more efficiently.

Machine learning algorithms like Logistic Regression, Support Vector Machines (SVM) do not learn any hidden representation in the images and directly use the image data provided. On the contrary, deep learning in computer vision has shown great success in decoding hidden representations and extracting features from them with the help of Convolutional Neural Networks. Convolutional Neural Networks (CNN) can extract and process data at very high speeds. The recent advancement in deep learning frameworks [3] have enabled faster and more accurate detection, while the increased CPU and GPU processing power available allows radiologists to improve their diagnostic efficiency.

In this work, pre-trained CNN architectures proposed in the past few years taken into consideration and try to assess their prediction on various parameters to identify the ideal one. All architectures used in the paper are CNNs which were pre-trained on ImageNet dataset previously. The CNNs were fine-tuned with the pneumonia chest x-ray dataset which was then used for feature extraction. The CNNs were connected with a common fully connected layer to assess their predictions from extracted features.

Lower image resolution helps lower training time on very large dataset and also decreases computational needs and device capacities due to relatively lesser number of parameters. With the advent of technology, it is easier to transfer image files over the phones which could be taken to advantage if the image is of lower resolution as it decreases the file size drastically. This also helps storing a large database of X-ray images over a device without much hassle.

The related works section discusses the various pre-trained networks. The third section discusses the strategies and hyper parameters considered for the comparison of these deep neural networks. The proposed ensemble model is discussed in the fifth section and it is followed by result analysis in the next section and finally the sixth section concludes.

## II. RELATED WORK

In recent years, there has been significant research in automation of Pneumonia detection through deep learning and neural networks which has yielded impressive results.

The study in [4] contributed a voting ensemble (AlexNet, ResNet18, InceptionV3, DenseNet-121 and GoogleNet) classification approach to Pneumonia detection. In [5] proposes a customized VGG16 model for the detection with an accuracy of 96.2%. The work done in [6] asserts that DenseNet201

architecture outperforms AlexNet, ResNet18 and SqueezeNet with an accuracy of 98% and AUC score of 0.98.

Kernany et al. (2018) in [7] used InceptionV3 pre-trained model for classification. They have also worked on bacterial and viral pneumonia classification in addition to normal and pneumonia. Saraiva et al. (2019) in [8] used cross validation technique in a customized 4 fully connected layer neural network to obtain an accuracy of 94.4% and compared it with MLP network.

D.Varshini et al (2019) [9] used different pre-trained CNN feature extractors combined with classifiers SVM with RBF kernel, Naive Bayes, k-nearest neighbours and Random Forests. They conclude that DenseNet-169 for the feature extraction stage and SVM for the classification stage provide statistically better results. Quan et al (2021) [10] proposed DenseCapsNet, a capsule network for detection of Covid-19 from X-ray images. DenseCapsNet reached 90.7 % accuracy and 96% sensitivity in test set results.

#### A. Transfer Learning

Transfer learning is a machine learning method that involves using an already developed model on a new problem task as the initial model in [11]. It is a popular approach used in computer vision and other arduous deep learning tasks.

When transfer learning is used, the model parameters start with good initial values due to the previous training and do not require huge modifications to be better adapted to the new task. The pre-trained model weights are treated as the initial values for the new task in hand, and updates are performed on that during training [12].

In proposed work, due to limited availability a new classifier is fitted on the top layers and fine tune only the last few convolutional layers in the model and use that for feature extraction purposes. The performance of some famous pretrained networks such as ResNet-50, ResNet-101 ResNet-152, VGG- 16, VGG-19, MobileNetV2 and DenseNet-201 also evaluated.

#### B. VGG Architecture

VGG16 is a convolutional neural network model proposed in the paper “Very Deep Convolutional Networks for Large-Scale Image Recognition” in [13]. The model achieves 92.7% top-5 test accuracy in ImageNet dataset. The model was submitted to ILSVRC-2014 and gained huge popularity. It makes improvements over its previous works by replacing large kernel-sized filters with multiple 3×3 kernel-sized filters one after another. The network is characterized by stacking 3×3 convolutional layers on top of each other to increase network depth. The convolution layers increase the volume size which is handled by max-pooling. Max-pooling is performed over a 2×2-pixel window, with stride 2.

The VGG-19 Neural Network is defined as that type of neural network which is also specifically trained on more than a million images from the ImageNet database, but the difference between the VGG-19 Neural Network and the VGG-16 Neural Network is its network layer depth level as 19 and 16, respectively.

#### C. ResNet Architecture

The main idea behind ResNet is adding more layers without degrading the performance of the whole network due to vanishing gradient problems. Vanishing gradient problem was caused due to repeated application of chain rule during back propagation which made the gradient too small and eventually disappears. This led to no actual learning in the networks.

ResNet introduced, “Identity Shortcut Connection” that skips one or more layers [14]. It stacks up identity mappings which are initially skipped and the activations from the previous layers are used instead. This enables faster learning in the compressed network. Later when the network trains again, the skipped layers are included to understand the feature space. The main difference between ResNet-50, ResNet-101 and ResNet-152 are the number of layers in them. ResNet-50 has  $3.8 \times 10^9$  floating point operations in total compared to  $7.6 \times 10^9$  in ResNet-101 and  $11.3 \times 10^9$  in ResNet-152.

#### D. DenseNet Architecture

The increasing depth of convolutional neural networks caused a problem of vanishing information about the input or gradient when passing through many layers. In order to solve this, authors introduced architecture [15] with a simple connectivity pattern to ensure the maximum flow of information between layers both in forward computation as well as in backward gradients computation. Each layer in the network adds its own feature-maps to the input received from its previous layers, which are then passed on to the subsequent layers in the network.

In DenseNet,  $H_i$  ( $i$  refers to the layer index) is a composite function of operations like ReLU, pooling, convolution and batch normalization. Each layer implements  $H_i(x_0, x_1, x_2, \dots, x_{i-1})$  where,  $[x_0, x_1, x_2, \dots, x_{i-1}]$  refers to concatenation of the feature-maps produced in layers 0 to  $i-1$ . Variable size of feature-maps does not allow concatenation operation. Down-sampling layers are the most important aspect of convolutional neural network. To facilitate the downsampling in the architecture, the complete architecture has been divided into multiple densely connected dense blocks. The layers between dense blocks are transition layers which perform convolution and pooling. Convolution and pooling operations are performed in transition layers between the dense blocks.

The main advantages of DenseNet are decreasing vanishing gradient issue, improving feature propagation, both forward and backward, increase feature reuse and reducing the number of parameters.

#### E. MobileNetV2 Architecture

MobileNetV2 has three convolutional layers in a block: the first is a 1x1 convolution called the expansion layer. The main purpose of the expansion layer is to increase the number of channels in the data before it is passed on to the next layer. The expansion factor is 6 by default. The next layer is the depth wise convolution which is used to filter inputs. Finally, a 1x1 projection layer is used which projects data with higher dimension into a tensor with lower dimension and it reduces the amount of data that flows through the network.

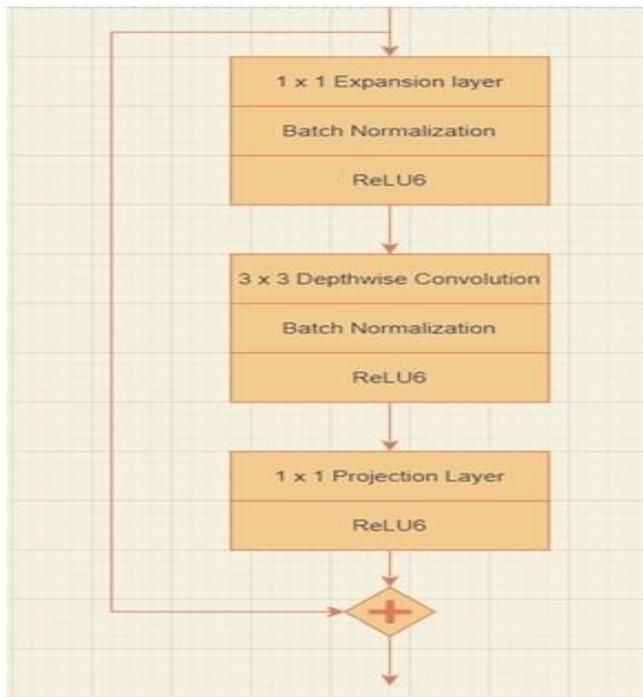


Fig. 1. MobileNetV2 Architecture Description.

As observed in Fig. 1, the architecture introduces residual connection which helps the flow of gradients through the networks. All the layers have batch normalization and ReLU6 activation function (except for projection layer). The authors in [16] report that due to low dimensional data produced in the layer, using a non-linearity affects the information obtained.

The dataset used is from Labeled Optical Coherence Tomography (OCT) and Chest X-Ray Images for Classification” released by Daniel et al. in 2018 published on the Kaggle platform [17], which consists of 5,863 X-Ray images. Chest X-ray images (anterior-posterior) were selected from retrospective cohorts of pediatric patients of one to five years old from Guangzhou Women and Children’s Medical Center, Guangzhou.

For this work, following the approaches from the past, the labels are treated as ground truth for the purpose of pneumonia detection. Out of the complete Radiographic image dataset, 4608 images were used as a training set which contains 1115 normal X-ray images and 3493 images labeled as Pneumonia. The test data and validation data both contains 624 X-ray images with 234 normal X-ray images and 390 images labeled as Pneumonia. The images were downscaled to 184 x 184 size for computational purposes before using it for analysis.

The training of all the models was done using a computer with 16 GB RAM and Nvidia Tesla P100 GPU. The figures shows sample chest X-ray images taken from dataset used for training, where, Fig. 2 is a chest X-ray of a normal patient and Fig. 3 is a chest X-ray of a patient affected by Pneumonia.

#### F. Pre-processing Stage

The images were scaled down to 3 channel 184 x 184 resolution and data normalization techniques were deployed to improve computational efficiency. The values were scaled

between 0 and 1 with random zooming on the images for image augmentation [18].

#### G. Feature Extraction and Classification

The pre-trained neural networks considered for feature extraction in the experiment are ResNet-50, ResNet-101, ResNet-152, VGG-16, VGG-19, MobileNetV2 and DenseNet-201.

Further on the features extracted are classified using a fully connected layer fitted to the network. All the networks were fine-tuned by freezing earlier layers and unfreezing the rest for the network to adapt well to the dataset considered for the experiment.

1) *Resnet pre-trained networks:* All the Resnet networks considered for the experiment- ResNet50, ResNet101 and Resnet152 were networks pre-trained on the ImageNet dataset and were fed in with input of 184 x 184 x 3 chest x-ray images. All three had been fit with a fully connected layer for classification. The fully connected layer consists of a dense layer of 2048 units and another dense layer of 64 units with ReLU activation function, dropouts and batch-normalization.

2) *VGG pre-trained networks:* Both VGG-16 and VGG-19 taken for consideration were pre-trained networks on the ImageNet dataset. The output of the network without top layers was further classified with a fully connected layer containing two dense layers of 4096 units with ReLU activation. Then the fine-tuned network shown in Fig. 4, was later trained on the dataset to obtain the results on the test data

3) *DenseNet201 pre-trained network:* The feature extracted from the ImageNet pre-trained network was subjected to global average-pooling and fed into a fully connected layer consisting of 1024 unit dense layer and 512 units dense layer with ReLU activation function which was then classified with a Softmax function.

4) *MobileNetV2 pre-trained network:* The ImageNet pre-trained network was used for feature extraction which was then fed into a fully connected layer after global average-pooling with dense layers of 4096 units and 512 units and ReLU activation function. The output of that was classified with a Softmax function.



Fig. 2. Chest X-Ray of a Normal Patient.



Fig. 3. Chest X-Ray of a Patient affected by Pneumonia.

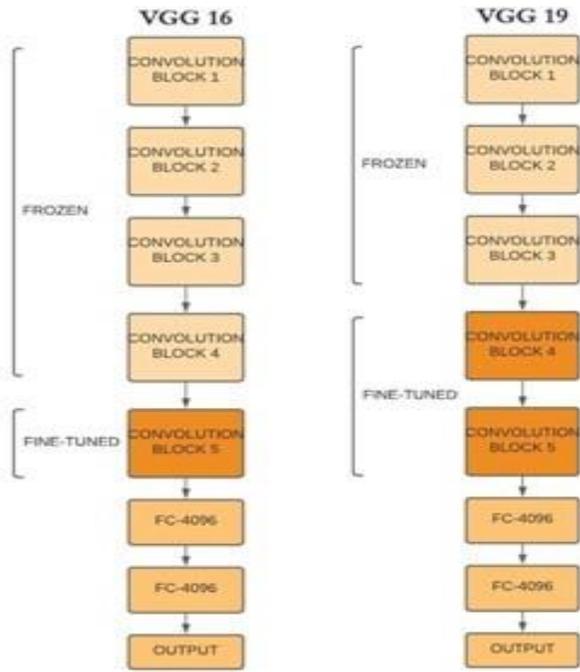


Fig. 4. Transfer Learning Approach through Fine Tuning during Training for VGGNet.

### III. STRATEGIES AND HYPER-PARAMETERS OF THE NETWORK

#### A. Learning Rate

The learning rate controls the ease of the model to adapt to the problem [19]. Smaller learning rates require more epochs during training given the smaller changes made to the weights each update as mentioned in Equation 1, whereas larger learning rates result in rapid changes and require fewer training epochs.

Large learning rates can cause the model to converge too quickly to a non-optimal solution or might lead to exploding gradient, whereas a small learning rate can cause the training to get stuck or lead to vanishing gradient issue.

$$w'_i = w_i - \gamma \frac{\partial L}{\partial w} \quad (1)$$

where

$\gamma$  - Learning rate.

L - Loss function.

$w_i$  - weights.

The equation shows as to how the weight gets updated. The learning rate used in training is 0.001, generally the learning rate ranges from 0.00001 to 1.

#### B. Optimization Algorithm

Batch gradient descent recomputes gradients for similar samples before each parameter update which leads to drastic increase in redundant computations for large datasets. Stochastic Gradient Descent [20] does away with this redundancy. Stochastic Gradient Descent frequently updates with a high variance that cause the objective function to

fluctuate heavily, on the other hand, it allows it to find better local minima. With SGD estimating loss function using a small batch it potentially may not lead us in an optimal direction. Hence, usage of exponentially weighted averages can help us with a better estimate which is closer to the actual derivative. This explains the better performance of SGD with momentum than the classic SGD. SGD tends to find it difficult to find the optimum in cases of ravines (area where surface curves much more steeply in one dimension than other) and oscillates around them. This issue is overcome with momentum as it accelerates gradients [21] in the optimal direction. Hence, Stochastic Gradient Descent is used with momentum. This is shown in Equation 2 and 3.

$$V_t = \beta V_{t-1} + (1 - \beta) \nabla_w L(w, x, y) \quad (2)$$

$$w = w - \alpha V_t \quad (3)$$

where,

$\beta$  - Coefficient of momentum.

L - Loss function.

V - Retrained gradient.

$\nabla$  - Learning rate.

w - weight.

x - Feature vector.

y - Output.

Using lower values of momentum implies averaging over much lesser values and more than 0.9 averages over a large data previously encountered. Hence, 0.9 is generally said to be a good estimate and is used in the experiments.

#### C. Dropout

Dropout involves removing some nodes so that the neural network does not overfit and can be implemented during the training process [22]. This enables the network to understand and distinguish redundant features. For each training stage, each node can be selected with probability P or drop it with probability (1-P). A dropout of 0.3 is applied on both the hidden layer units in the fully connected layers.

#### D. Batch Size

The batch size defines the number of samples that will be propagated through the network in one forward and backward propagation. Networks train faster with mini batches because the weights get updated after each propagation. It requires less memory. Since, the network is trained using fewer samples, the overall training procedure requires less memory. That's especially important when using large image datasets for training. A batch size of 32 is used for this work.

#### E. Activation Function

An activation function is a function that is added into an artificial neural network in order to help the network learn complex patterns in the data, it takes in the output signal from the previous cell and converts it into some form that can be taken as input to the next cell. It is like adding non-linear layers in between linear layers because non-linearity is required for

the network to understand complex data. In the fully connected layers, ReLU activation [23] is applied for the hidden dense layers and softmax function [24] in the prediction layer. Softmax is used in multiclass classification problems, as in equation 4.

$$\sigma(\vec{z}_i) = \frac{e^{z_j}}{\sum_{j=1}^K e^{z_i}} \quad (4)$$

where,

$\sigma$  - softmax.

$e^{z_j}$  - standard exponential function for output vector.

$z$  - input vector.

$K$  - no. of classes in multi-class classifier.

$z_i$  values are the elements of the input vector and can take any real value. The denominator is the normalization term used so that the summation of the output values results in 1 and a valid probability distribution is maintained. ReLU (Rectified Linear Unit) is a type of activation function. ReLU is defined as  $y = \max(0, x)$  in mathematical terms and the graphical representation is provided in Fig. 5. It is most commonly used activation function in convolutional neural network.

### F. Loss Function

The loss function used in the experiment is sparse categorical cross-entropy. Cross-entropy is defined as the measure of the difference between two probability distributions for a given random variable or set of events.

A skewed probability distribution has lower entropy than a balanced probability distribution. In this work, sparse

categorical cross-entropy is considered because the classes are mutually exclusive from each other unlike the categorical cross-entropy which is used in the case of samples having multiple classes or soft probabilities.

### G. Inference from Individual Models

The classification accuracy for each model has been plotted on a graph with respect to the number of epochs used for training. Both validation and training set accuracy has been plotted for each epoch. This helps us to see how the model has been fitting input data. The model loss for each of the models has been plotted for both validation and training set for every epoch.

Loss and Accuracy from the various Network models are tested and depicted as graphs in Fig. 6(a – g). The network models evaluated are ResNet-50, ResNet-101, ResNet-152, VGG-16, VGG-19, DenseNet-201 and MobileNet-V, respectively.

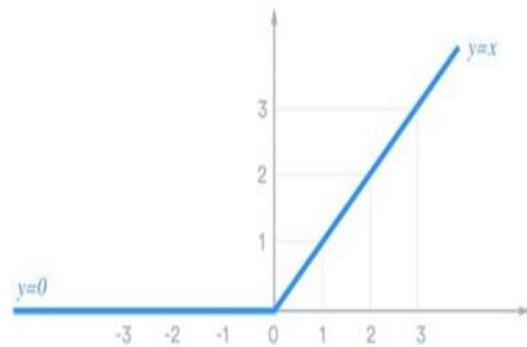


Fig. 5. ReLU Function.

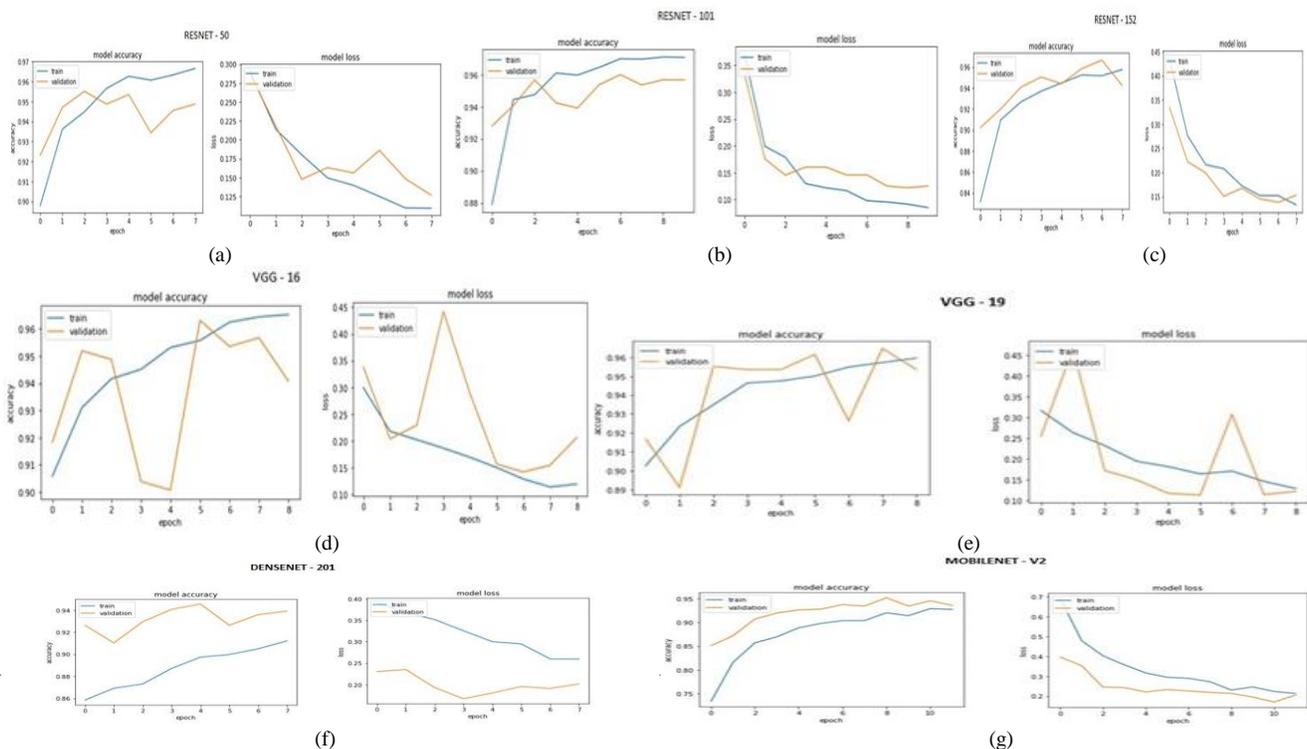


Fig. 6. Loss and Accuracy from the Various Network Models (a) ResNet-50 (b) Resnet-101 (c) Resnet-152 (d) VGG-16 (e) VGG-19. (f) DenseNet-201 (g) MobileNet V2.

#### IV. ENSEMBLE NETWORK MODEL

The ensemble model works on combining predictions and decisions of different models to augment the overall performance and generalization of the models. The main idea is to reduce noise, bias and variance in different models. The ensemble model can employ simple methods like mode and weighted average or resort to advanced techniques like bagging and boosting depending on the requirements and constraints for the task in hand. Although it drastically increases the complexity of the model and the design time, it generally improves on the accuracy, stability and robustness of the model.

Weighted average predictions involving the multiple models are employed to obtain an ensemble model in the experiment. Ensemble model of which is proposed has the following models:

- a) VGG-16
- b) ResNet-50
- c) ResNet-101
- d) ResNet-152
- e) VGG-19

- f) DenseNet-201
- g) MobileNet-V2

As shown in Fig. 7, the trained models are loaded with their respective weights and the prediction on the test set is obtained for all the models.

Then the model predictions are combined through weighted average, with 30% weightage VGG16 and 20% for VGG19 as they have a relatively higher accuracy and AUC score compared to others. All other models are given 10% weightage for computation of ensemble prediction value.

The proposed model has an accuracy of 95.03% and an AUC score of 0.9441 which is higher than any model considered by a good margin. The ROC curves used to compute the AUC scores have been compiled in Fig. 8. ROC graph [25] is a plot with the false positive rate on the X axis and the true positive rate on the Y axis. It is a visual approach for analysing the trade-off between the ability of a classifier to correctly identify positive cases and the number of negative cases that are incorrectly classified. ROC graph captures all information contained in the confusion matrix, since, FN is the complement of TP and TN is the complement of FP. Fig. 8 shows the different ROC curves for all the models.

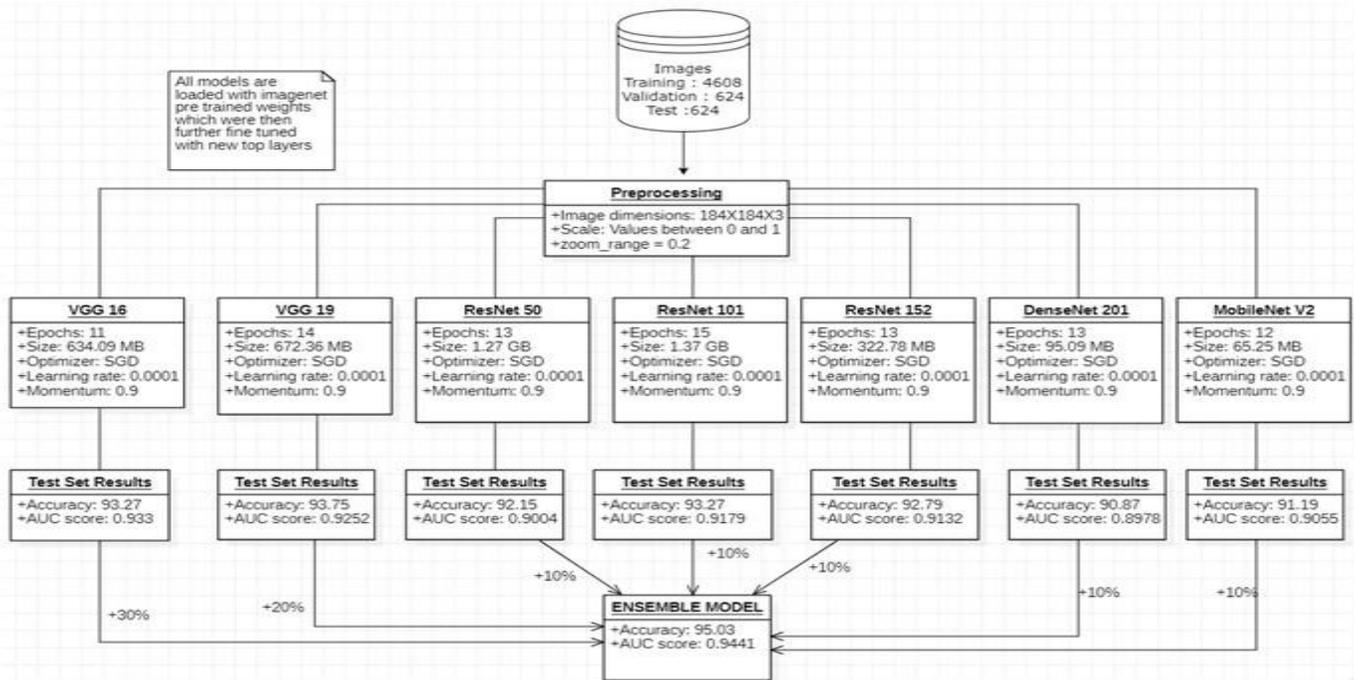


Fig. 7. Proposed Ensemble Model.

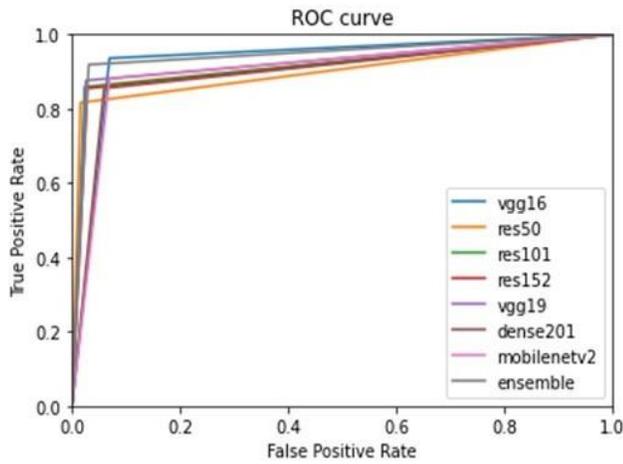


Fig. 8. ROC Curve Comparison of all the Individual Models with Ensemble Model.

### V. RESULT ANALYSIS

In this section, a comparison of the ensemble model and other models are done with different metrics. The following sections gives the performance metrics used, and provides discuss on how the Ensemble model provides better results than other models.

#### A. Performance Metrics for Evaluation

The Results have the study on Accuracy impact with various models as described in [26]. The various metrics used are as follows:

Confusion matrix, Classification accuracy, Precision, Sensitivity and Specificity, F1-Score and Area Under Curve AUC - ROC curve.

#### B. Result and Discussion

Table I shows that the ensemble model does better than all the models considering the different metrics of evaluation used and the ensemble network has an accuracy of 95.03 and AUC score of 94.41. The ensemble model is based on weighted voting, with each model's output being assigned a different weightage. The results assert that the combination of different results with appropriate weightage improves the overall prediction significantly. This can be attributed to the tendency of a particular model being biased towards a particular region of interest or feature. The bias can be avoided in an ensemble model. Moreover, it aids the evaluation by accounting different niche aspects of the image.

Different models have been trained in accordance to the validation result analysis using early stopping technique as observed in Fig. 6. Among individual models, VGG-16 and VGG-19 have comparatively better results with accuracy of 93.27% and 93.75%, respectively, and with an AUC score of 93.30 and 92.52 for VGG16 and VGG19. AUC score is generally used for binary classification models and is taken as the main parameter to assess the models because of the class imbalance between normal and pneumonia affected X-ray images. AUC score is not in consistent with the accuracy which avoids evaluating the model from a narrow perspective.

TABLE I. COMPARISON OF METRICS OF ENSEMBLE MODEL WITH OTHER INDIVIDUAL NETWORK

Model	Accuracy	Sensitivity	Specificity	Precision	F1score	AUC
DenseNet-201	90.87	91.52	89.69	94.1	0.927	89.78
ResNet-50	92.15	89.93	96.95	98.46	0.94	90.04
MobileNet-V2	91.19	92.84	88.41	93.08	0.929	90.55
ResNet-152	92.79	91.77	94.79	97.18	0.944	91.32
ResNet-101	93.27	92.03	95.71	97.69	0.947	91.79
VGG-19	93.75	92.91	95.35	97.44	0.951	92.52
VGG-16	93.27	96.03	89.02	93.08	0.946	93.3
<b>Ensemble</b>	<b>95.03</b>	<b>95.21</b>	<b>94.71</b>	<b>96.92</b>	<b>0.961</b>	<b>94.41</b>

TABLE II. COMPARISON OF ENSEMBLE MODEL WITH BASELINE MODELS

Models from Literature	Accuracy	Precision	Sensitivity	AUC
Rajaraman et al. [5]	96.2	97.7	96.2	99.3
Rahman et al. [6]	98	97	99	98
Chouhan et al. [4]	96.39	93.28	99.62	99.34
Enes Ayan et al. [27]	84.5	91.3	89.1	87
Saraiva et al. [8]	94.4	94.3	94.5	94.5
Kermany et al. [7]	92.8	-	93.2	-
<b>Ensemble Model - Proposed</b>	<b>95.1</b>	<b>96.92</b>	<b>95.21</b>	<b>94.5</b>

On the comparison study for previous works in Table II, the works of Kermany et al. in [7], Rajaraman et al. in [5] and Rahman et al. in [6] have been significant in automation of pneumonia detection. They have also compared their works with other authors who have published their results in the same problem. Rahman reported 98% classification accuracy and AUC score of 98 for an input image size of 224 x 224 for ResNet18 and DenseNet201 and 227 x 227 for AlexNet and SqueezeNet architectures. Rajaraman et al. [5], provided a study of the better results of cropped ROI (Region of Interest) data when compared to baseline data and proposed a customized VGG 16 model for the problem. Vikash et al proposed an ensemble model with an AUC score of 99.34 and 96.39 accuracy. Saraiva et al. in [8] evaluated a CNN network with an input image size of 150 x 150 pixels and reported 94.4% accuracy and 94.5 AUC score.

The slight dip in both [8] and proposed Ensemble results can be attributed to low training image resolution which affects the classification performance of the CNN. This has been supported and reasoned in the works of Sarkar et al. in [28], Kozierski et al. in [29], Dodge et al. in [30] and Kannoja et al. in [31]. The work in [29], reports that models that achieved high accuracy on the original, undistorted images were also more resilient to low image resolution and the pattern was observed across almost all the architectures. In our work, the relative dip in performance on testing with images of lower resolution would be less compared to the previous works due to the lower training set image resolution. This is also confirmed by the works of [31] in the reported values for MNIST and CIFAR-10 datasets where we could observe the drastic lowering of performance in models when the resolution of training and testing images vary vastly. They also state that improved results on low quality images need models trained with lower quality images which is the core idea behind our work.

For a 224 x 224-pixel image of 8-bit depth, file size is 6.125 KB whereas a 184 x 184-pixel image of 8-bit depth is 4.132 KB, which is nearly 150% increase in file size. In addition to it, it adds on to the computation time due to the increased number of parameters in the CNN leading to poor efficiency. With COVID-19 pandemic causing damages on a global scale, deep learning solutions using X-ray images are being actively proposed by researchers. Sridhar et al. in [32] evaluated a ResNet model to identify the similar regions between the X-rays of different lung disease and reported Atelectasis, Consolidation, Emphysema, and Pneumonia are most similar in nature to COVID-19. The result augments the need for more extensive research in Pneumonia detection to help distinguish the disease from COVID-19 which would help provide timely and appropriate treatment.

## VI. CONCLUSION

The study presents a transfer-learning based ensemble model to automate Pneumonia detection using Chest X-rays. Different CNN architectures were fine-tuned, trained and the results analyzed to finally propose an ensemble model. The other core idea focused on the work is to lower the resolution and size of the images used while balancing the trade-off with the performance of the model. The final ensemble model

evaluated had an accuracy of 95.03 and AUC score of 94.5 with a precision of 96.92. With significant research in the problem yielding promising results, such models can be deployed in real life to reduce the workload on physicians and bring down human error levels. With lower storage capacity and computing device needs, the implementation can be taken to remote rural areas globally that lack proper diagnoses and treatment for such illness due to lack of skilled doctors and radiologists, poor connectivity and lack of infrastructure. Although it cannot replace a physician, it can aid the diagnosis process and reduce the crucial time taken.

## ACKNOWLEDGMENT

Acknowledge Dr. T.V.Geetha Prof (retd.), Department of Computer Science and Engineering, CEG, Anna University, for motivating us to carry out this work during 2020, COVID'19 pandemic.

## FUNDING STATEMENT

Not received any financial support from any sources.

## CONFLICTS OF INTEREST

All the authors declare that they have no conflicts of interest to report regarding this study.

## REFERENCES

- [1] I. Rudan, L. Tomaskovic, C. Boschi-Pinto, H. Campbell, and WHO Child Health Epidemiology Reference Group, "Global estimate of the incidence of clinical pneumonia among children under five years of age," *Bull. World Health Organ.*, vol. 82, no. 12, pp. 895–903, 2004.
- [2] D. A. McAllister et al., "Global, regional, and national estimates of pneumonia morbidity and mortality in children younger than 5 years between 2000 and 2015: a systematic analysis," *Lancet Glob. Health*, vol. 7, no. 1, pp. e47–e57, 2019.
- [3] J. Gu et al., "Recent advances in convolutional neural networks," *Pattern Recognit.*, vol. 77, pp. 354–377, 2018.
- [4] V. Chouhan et al., "A novel transfer learning based approach for pneumonia detection in chest X-ray images," *Appl. Sci. (Basel)*, vol. 10, no. 2, p. 559, 2020.
- [5] S. Rajaraman, S. Candemir, I. Kim, G. Thoma, and S. Antani, "Visualization and interpretation of convolutional neural network predictions in detecting pneumonia in pediatric chest radiographs," *Appl. Sci. (Basel)*, vol. 8, no. 10, 2018.
- [6] T. Rahman et al., "Transfer learning with deep Convolutional Neural Network (CNN) for pneumonia detection using chest X-ray," *Appl. Sci. (Basel)*, vol. 10, no. 9, p. 3233, 2020.
- [7] D. S. Kermany et al., "Identifying medical diagnoses and treatable diseases by image-based deep learning," *Cell*, vol. 172, no. 5, pp. 1122–1131.e9, 2018.
- [8] A. Saraiva et al., "Models of learning to classify X-ray images for the detection of pneumonia using neural networks," in *Proceedings of the 12th International Joint Conference on Biomedical Engineering Systems and Technologies*, 2019.
- [9] D. Varshni, K. Thakral, L. Agarwal, R. Nijhawan and A. Mittal, "Pneumonia Detection Using CNN based Feature Extraction," 2019 IEEE International Conference on Electrical, Computer and Communication Technologies (ICECCT), 2019, pp. 1-7, doi: 10.1109/ICECCT.2019.8869364.
- [10] Quan H, Xu X, Zheng T, Li Z, Zhao M, Cui X. DenseCapsNet: Detection of COVID-19 from X-ray images using a capsule neural network. *Comput Biol Med.* 2021; 133:104399. doi:10.1016/j.combiomed.2021.104399.
- [11] S. J. Pan and Q. Yang, "A survey on transfer learning," *IEEE Trans. Knowl. Data Eng.*, vol. 22, no. 10, pp. 1345–1359, 2010.

- [12] S. Rajaraman et al., "Pre-trained convolutional neural networks as feature extractors toward improved malaria parasite detection in thin blood smear images," *PeerJ*, vol. 6, p. e4568, 2018.
- [13] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," *arXiv [cs.CV]*, 2014.
- [14] K. He, X. Zhang, S. Ren, and J. Sun, "Deep residual learning for image recognition," in 2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016.
- [15] G. Huang, Z. Liu, L. Van Der Maaten, and K. Q. Weinberger, "Densely connected convolutional networks," in 2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2017.
- [16] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, "MobileNetV2: Inverted residuals and linear bottlenecks," in IEEE/CVF Conference on Computer Vision and Pattern Recognition, 2018.
- [17] Kermany, Daniel, Kang Zhang, and Michael Goldbaum. "Labeled optical coherence tomography (oct) and chest X-ray images for classification." *Mendeley data* vol.2, 2018.
- [18] S. Lakshmanan, "Towards AI, How, When, and Why Should You Normalize/Standardize/Rescale Your Data?" *Towards AI-The Best of Tech, Science, and Engineering*.
- [19] D. R. Wilson and T. R. Martinez, "The need for smaller learning rates on large problems," in *IJCNN'01. International Joint Conference on Neural Networks. Proceedings (Cat. No.01CH37222)*, IEEE, 2001, p. vol. 1, pp. 115–119.
- [20] S. Ruder, "An overview of gradient descent optimization algorithms," *arXiv [cs.LG]*, 2016.
- [21] I. Sutskever, J. Martens, G. Dahl and G. Hinton, "On the importance of initialization and momentum in deep learning," in *International conference on machine learning*, May 26 2013, PMLR, pp. 1139–1147.
- [22] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, R. Salakhutdinov, "Dropout: a simple way to prevent neural networks from overfitting" *The journal of machine learning research.*;15(1):1929-58, 2014.
- [23] A. F. Agarap, "Deep learning using rectified linear units (relu)," *arXiv preprint arXiv:1803.08375.*, 2018.
- [24] B. Gao and L. Pavel, "On the properties of the softmax function with application in game theory and reinforcement learning," *arXiv [math.OC]*, 2017.
- [25] Fawcett and Tom, "ROC graphs: Notes and practical considerations for researchers," *Machine learning*. 2004 Mar 16;31(1):1-38, 2004.
- [26] G. R. Cogalton and M. Story M, "Accuracy assessment: a user's perspective." *Photogrammetric Engineering and remote sensing*.52(3):397-9, 1986.
- [27] E. Ayan and H. M. U" nver, "Diagnosis of pneumonia from chest x-ray images using deep learning," *Scientific Meeting on Electrical-Electronics and Biomedical Engineering and Computer Science (EBBT)*, pp. 1–5, 2019.
- [28] R. Sarkar, A. Hazra, K. Sadhu, and P. Ghosh, "A novel method for pneumonia diagnosis from chest X-ray images using deep residual learning with separable convolutional networks," in *Computer Vision and Machine Intelligence in Medical Image Analysis*, Singapore: Springer Singapore, 2020, pp. 1–12.
- [29] M. Koziarski and B. Cyganek, , Impact of low resolution on image recognition with deep neural networks: An experimental study, vol. 28, no. 4. *International Journal of Applied Mathematics and Computer Science*, 2018.
- [30] S. Dodge and L. Karam, "Understanding how image quality affects deep neural networks," *Eighth International Conference on Quality of Multimedia Experience(QoMEX)*, vol. 19, pp. 1–6, 2016.
- [31] S. P. Kannoja and G. Jaiswal, "Effects of varying resolution on performance of cnn based image classification: An experimental study," *International Journal of Computer Sciences and Engineering*, vol. 6, no. 9, pp. 451–456, 2018.
- [32] S. Sridhar, S. Mootha, R. Seetharaman and A. X. A. Rayan, "A Study on Co-occurrence of various Lung Diseases and COVID-19 by observing Chest X-Ray Similarity using Deep Convolutional Neural Network," in *2020 Fourth International Conference On Intelligent Computing in Data Sciences (ICDS)*, 2020, pp. 1–8.

# Delivery of User Intentionality between Computer and Wearable for Proximity-based Bilateral Authentication

Jaeseong Jo<sup>1</sup>, Eun-Kyu Lee<sup>2\*</sup>, Junghee Jo<sup>3\*</sup>

Department of Information and Telecommunication Engineering, Incheon National University, Incheon, Korea<sup>1,2</sup>  
Department of Computer Education, Busan National University of Education, Busan, Korea<sup>3</sup>

**Abstract**—Recent research discovers that delivering user intentionality for authentication resolves a random authentication problem in a proximity-based authentication. However, they still have limitations – energy issue, inaccurate data consistency, and vulnerability to shoulder surfing. To resolve them, this paper proposes a new method for user intent delivery and a new proximity-based bilateral authentication system by adopting it. The proposed system designs a protocol for authentication to reduce energy consumption in a power-constrained wearable, applies a Needleman-Wunsch algorithm to the matching of time values as well, and introduces randomness to a user behavior that a user must perform for authentication. We developed a prototype of our authentication system on which a list of experiments was conducted. Experimental results show that the proposed method results in more accurate data consistency than conventional methods for user authentication intent delivery. Eventually, our system reduces authentication failure rate by 66.7% compared to conventional ones.

**Keywords**—Security; authentication; internet of things; user intentionality; proximity-based authentication; bilateral

## I. INTRODUCTION

An ID-password authentication has enjoyed a variety of applications for a long time. While it is simple to use, it requires mental efforts to remember IDs and passwords as well as physical efforts to input them directly. It is recommended to use different passwords for different IDs. However, people in real life use the same password for multiple IDs because it is easy to remember one password. Once the password is exposed, however, user's accounts can be exposed to security risks.

With advancement of Internet of Things (IoT) technologies and pervasive computing, recent proximity-based authentication performs without requiring both mental and physical from users. The proximity-based authentication initiates authentication when a wearable user approaches a certain distance from the authentication device (say, a computer). We note that once the user is within the distance, the authentication automatically proceeds regardless of the user's intention to authenticate. That is, the user proceeds with authentication that she does not know, named a random authentication problem. Moreover, the user's lack of understanding of authentication intent leads to the problem of continuing authentication; an authentication process starts whenever the user passes a certain distance of the computer that she wanted to authenticate.

A user authentication intent delivery solves the problems. It proceeds with authentication via a user's specific behavior, enabling proximity-based authentication to work with the sensor values in the wearable and data collected from the computer for this behavior. Conventional methods for user authentication intent delivery use a mouse in the computer to calculate acceleration values using mouse position values and distance traveled values to collect them with time values and use a keyboard to press the keyboard and time to press the time. The wearable collects acceleration sensor values and the time values and transmit them to the computer. The computer checks the consistency of these data to determine whether to authenticate.

However, the conventional methods have limitations as follow. First, they require the wearable device to keep running built-in sensors and recording data, which consumes energy faster in the small, power-constrained device. Next, they predefine the type of behavior that a user must perform for authentication and the number of actions that the user repeats the behavior, which could be vulnerable to external attackers. Last, the conventional methods do not make use of time values when checking data consistency, which may result in less accurate matching.

This paper proposes a new method that delivers user intentionality for authentication and resolves the limitations and eventually proposes a new proximity-based bilateral authentication system by adopting the new method. To address the energy concern, the proposed system designs a new protocol for authentication where an authentication process is initially detected by the wearable. The system resolves the second limitation by applying randomness to the number of actions; that is, it changes the number each time a user proceeds with authentication. Last, our system enhances accuracy of data consistency by applying a Needleman-Wunsch algorithm to the matching of time values as well as acceleration sensor data.

A prototype is developed where we use a Galaxy Watch as a wearable, and experiments are conducted to evaluate performance of the proposed system. Experimental results show that the proposed system reduces error in data consistency by 46.6% on average (from 0.3593 to 0.1918). The improved accuracy affects performance of authentication; our system reduces authentication failure rate by 66.7% compared to the conventional method.

\*Corresponding Author.

The rest of the paper is composed as follows. Section II reviews two popular authentication methods and their limitations. Section III describes a conventional method for a user authentication intent delivery in detail. Section IV proposes a new proximity-based authentication system that delivers user's intentionality for authentication in an accurate manner. Experiments and performance evaluation of the proposed system are discussed in Section V. The last section concludes the paper.

## II. RESEARCH BACKGROUND

This section reviews a widely used authentication method, an ID-Password authentication, and discusses limitations. It also describes a proximity-based authentication method that can resolve the limitations.

### A. ID-Password Authentication

The most popular user authentication method has been an ID-password authentication [1]. It determines whether these data are equivalent to the values stored in the database by the user entering their own ID and password. Recently, authentication security through secondary authentication has been strengthened. The security of authentication is increasing with the addition of various secondary authentication methods, including authentication methods using existing ID passwords [2], sending messages using smartphones to enter additional code of messages [3], and user verification methods using specific applications.

Limitations: The ID-Password authentication method has limitations; it requires mental and physical efforts from users. In the case of mental effort, it is likely to be resolved if the passwords and IDs of all accounts are unified, but if passwords and IDs are exposed, all accounts may be at risk. On the contrary, if all IDs and passwords are set differently, mental efforts are needed too much because one should remember the whole thing. In the case of physical effort, the process of entering an ID and password is more mobile than expected because it uses a mouse and keyboard to enter characters. Recently, additional authentication methods using secondary passwords and QR codes [5] have been utilized by utilizing smartphones [4] to increase security. This method is certainly highly reliable in security, but there is a hassle of unlocking a smartphone, using an application, or checking a message and entering it back into the computer.

### B. Proximity-based Authentication

Proximity-based authentication is a technology that logs in or out users from applications, devices, websites, etc. using the distance between users and authentication devices as a key value [6]. To be successful in authentication, it is necessary to have auxiliary devices such as smartwatches and wearables near devices that users want to authenticate. Proximity-based authentication automatically initiates authentication when a user approaches a certain distance of the authentication device. At this time, authentication devices and users use wireless communications such as Bluetooth and Wi-Fi. The proximity-based authentication system is shown in Fig. 1. A computer and a user proceed with authentication by exchanging authentication tokens with each other [7] when the user is within a certain distance of the server.

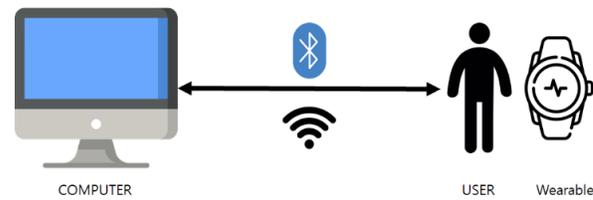


Fig. 1. Proximity-based Authentication Initiates as a user Approaches a Computer.

Limitations: Proximity-based authentication automatically begins a process when a user approaches a certain distance of the authentication device. The authentication that occurs at this time proceeds regardless of the user's intention to authenticate. In other words, authentication proceeds even if a user approaches a device within a certain distance without any intention of authentication, so the user proceeds with authentication that he or she does not know [8]. Authentication fails if the user deviates from the effective distance for authentication with the authentication device while the authentication is in progress. This is an important part of the authentication process that is irrelevant to the user's intentions described earlier. Authentication is attempted if the user passes the effective distance of the authentication device, at which point authentication attempts-authentication failures [9] are repeated because authentication fails if it is outside the effective distance. If this process is repeated, certain devices lock down the authentication and cause problems that prevent users from proceeding with authentication in the situation they want to authenticate. The following section describes how one can communicate users' authentication intent in proximity-based authentication in detail.

## III. DELIVERY OF USER INTENTIONALITY FOR AUTHENTICATION: CONVENTIONAL APPROACH

In proximity-based authentication, a user authentication intent delivery allows accurate authentication to proceed by delivering authentication intention from assistive devices (e.g., wearables and smartwatches) or authentication devices (e.g., computers). Two typical technologies for user authentication intent delivery include wristband-based authentication for desktop computers (SAW) [10] and proximity-based user authentication on voice-powered Internet-of-Things devices (PIANO) [11]. This section describes a conventional approach that accurately conveys users' authentication intent in proximity-based authentication. Since our scenario sees authentication between a wearable and a computer, a review in this section is mainly based on the former.

### A. User Authentication Intent Delivery

A user authentication intent delivery is generally based on near-field based authentication, where wearable users and computers are paired over wireless communication within a certain distance, then double-click a specific button on the computer keyboard to confirm the user's intention to authenticate. Afterwards, values for a user's specific behavior are collected from wearable and computer, and authentication is carried out by matching these data [12].

1) *System architecture*: After wearing a wearable device, the user double-taps the computer's keyboard to verify the computer's authentication intent. When the computer confirms the authentication intent, it requests data about the acceleration sensor of the wearable. Users take certain actions, using a mouse or keyboard. On wearable devices, the acceleration sensor value and the gravitational sensor value are calculated and sent to the server using a specific program to calculate the value of the mouse and keyboard movement. When transmitting, it is carried out through wireless connections such as Bluetooth and Wi-Fi. The matching of the sensor value of the wearable device sent to the server is verified using a mouse or keyboard, and user authentication is performed on the computer with an authentication completion message. Request to measure again if authentication fails.

Unlike traditional proximity-based authentication, the user authentication intent delivery conveys the user's authentication intent, which allows the user to approach within a certain distance, verify the authentication intent, and authenticate. Differences from proximity-based authentication methods are shown in Table I [13].

2) *Operation*: In a conventional method for user authentication intent delivery, a computer and a wearable is paired via Bluetooth communication [14]. After pairing, authentication starts by pressing the computer's keyboard specific key twice, and the computer requests acceleration sensor values and time data from the wearable. The worm transmits the requested acceleration sensor data [15] to the computer. When the data is transferred, the computer checks data consistency; it successfully authenticates upon successful data matching or fails to authenticate upon data matching failure. In the event of a data matching failure, the sensor data transfer request is re-requested. If the data is not sent within 5 seconds of pairing, the pairing is canceled and then the pairing is requested again.

3) *Detection of user intent on computer*: The computer uses data values for wrist movements of wearable users to check the consistency with acceleration sensor data of wearable [16]. To collect data on the user's wrist movement from a computer, conventional methods use a mouse-wiggle [17] and/or a TAP [18]. Fig. 2 illustrates these two ways.

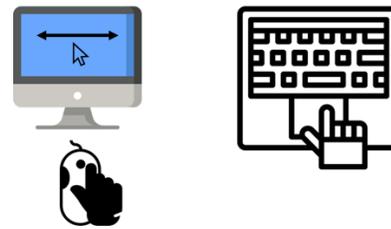


Fig. 2. Mouse-Wiggle (Left) and Keyboard Tab (Right) Methods.

When authentication begins, a user in the mouse-wiggle method moves the mouse from side to side on the screen, which is recorded. The computer measures the mouse's position values and time values with which it computes acceleration values. Finally, the acceleration value is calculated by dividing the time value by the distance traveled previously obtained. The TAP method makes use of the time value when the keyboard was pressed a certain number of times and difference between the current time value and the time value when the keyboard was first pressed. This value indicates the time when the user's hand presses and releases the keyboard. The computer uses this time value to verify that the value of the highest point of the acceleration sensor value in the wearable matches the recorded time.

4) *Detection of user intent on wearable*: After pairing with a computer, a wearable is asked to send sensor data. When a user performs a mouse-wiggle and keyboard-TAP method, the wearable transmits the value of the acceleration sensor of the device itself to the computer [19].

*B. Limitations of User Authentication Intent Delivery*

A delivery of explicit user intentionality for authentication solves the random authentication problem [20] that can occur in proximity-based authentication methods, thus enabling more accurate authentication. However, conventional methods for user authentication intent delivery have limitations that hinder optimal authentication operations. First, the methods make a computer to detect a user intent for authentication initially. Once detected, the computer tries to communicate with a wearable device on the user side to obtain sensor records. This implies that the device remains on a ready state all the time, which makes it hard to save energy consumption on the device. Next, conventional methods use fixed forms of user behaviors as intent. For instance, the TAP-5X method pushes a computer's keyboard five times to collect data for matching data between computers and wearables. Because TAP-5X performs exactly five actions by the user, it is possible for an external attacker to observe and analyze the user's behavior and authenticate by taking the same action [24]. Wearable devices may not be problematic because they are usually worn by the user, but if the user is away for a while or if the wearable is stolen 15 times, the computer cannot verify whether the user is a user or an attacker, making the TAP-5X vulnerable to external attackers. Last, conventional methods prioritize the matching of acceleration sensor values in data matching for authentication between computers and wearables for authentication. Data obtained from computers and wearables include time values and acceleration sensor values. A Needleman-Wunsch algorithm [21] has been used to match the

TABLE I. DIFFERENCES BETWEEN TRADITIONAL AUTHENTICATION METHODS AND USER AUTHENTICATION INTENT DELIVERY BASED METHODS

<i>Proximity-based authentication</i>		<i>User authentication intent delivery</i>	
Advantages	Authentication system operation when user approaches within a certain distance	Characteristics	Complement the absence of a user authentication intent verification method of traditional proximity-based authentication by identifying the intent through specific actions.
Weakness	Continuously operates the authentication system when accessing within a certain distance without identifying the user's authentication intent.		

acceleration sensor values, increasing the accuracy of the acceleration sensor data values. However, algorithms for data matching were not used for time values while time values have been used as one of the most significant metrics in previous research on user authentication intent delivery [22, 23]. This can cause problems in the process of identifying data matching.

#### IV. PROPOSED SYSTEM: USER-INTENDED PROXIMITY AUTHENTICATION

This section proposes a new proximity-based authentication system that explicitly delivers user intentionality for authentication. To resolve the first limitation, an authentication process in the proposed system is initially detected on a user side instead of on a computer. To this end, the user is required to touch her wearable twice first. The next limitation is resolved by applying a one-time password concept that proposes a new criterion for the number of actions that a user must perform each time he or she proceeds with authentication. To resolve the last limitation, our system improves accuracy in the data matching process by applying the Needleman-Wunsch algorithm to time values as well.

##### A. System Architecture

The proposed system consists of two entities, a user and a computer, as shown in Fig. 3. The user is with a wearable that is paired with the computer via Bluetooth communication. The user starts behaving an intent action, and her behavior is detected both on the wearable and on the computer and processed. Fig. 4 helps us describe how accurately the system measures data on the behavior and determines that the measured values on both sides are matched.

The computer in Fig. 4 opens a Bluetooth server and connects it to Intelligent Unit that calculates data matching and Action Detector that is responsible for detecting the movement of a keyboard and a mouse on the computer and for measuring corresponding data. The wearable uses Bluetooth Server on the computer and a Bluetooth socket to make a UUID connection. Sensor Manager keeps monitoring values from built-in sensors. Once an authentication process is triggered, Sensor Manager transmits the sensor records to the computer via the Bluetooth communication. At the same time, Action Detector measures the movement of the computer's mouse and keyboard and records related data. Upon collecting data from both Sensor Manager and Action Detector, Intelligence Unit checks the match between the two data. Authentication is completed if the data is matched, or retransmission is requested if authentication fails due to data mismatch.

##### B. Protocol

The proposed system designs a protocol for authentication between the computer and the wearable, and Fig. 5 depicts flows and processes of the protocol.

The computer makes a pairing request to the wearable by transmitting its UUID. The wearable checks the validity of the UUID received and transmits its own UUID to the computer to proceed further with pairing. Once they are paired, a user is allowed to request authentication to the computer.

An authentication process in the proposed system is initially detected by the wearable unlike conventional methods

for user authentication intent delivery. The user double-touches the wearable to communicate her authentication intent to the computer. Then, authentication begins when the computer confirms the intent. The computer requests the wearable to transmit sensor records. At the same time, it generates a random number (a nonce) and piggybacks the nonce on the request message.

Upon receiving the message, the user takes an action; she moves a mouse or pushes a key in a keyboard connected to the computer. The nonce received guides her behaviors; that is, she repeats the movement or the push multiple times corresponding to the nonce value. When the user performs an action, Sensor Manager in the wearable records acceleration values and corresponding time values and transmits them to the computer. After sending the request message to the wearable, Action Detector in the computer starts collecting data of mouse movement (changes of the pointer's positions and corresponding timestamps) and/or data of keyboard (numbers of key presses and timestamps of pressing and releasing).

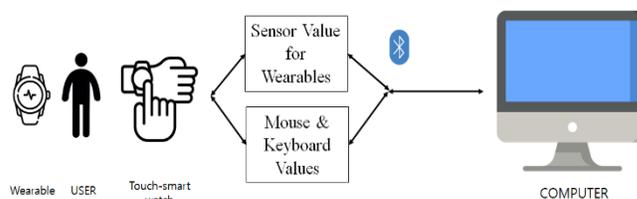


Fig. 3. The Proposed Authentication System Consists of Two Entities, a user and a Computer. They do Authentication by Delivering the user's Authentication Intent.

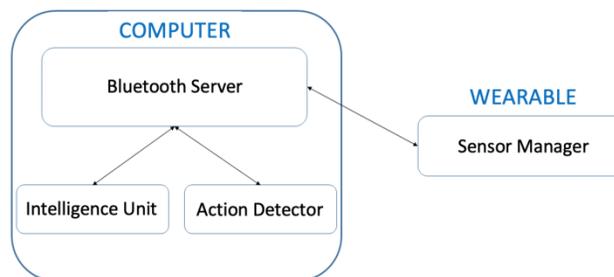


Fig. 4. Two Entities in the Proposed System Include a List of Components, and they are Responsible for Exchanging Data Regarding user's behavior and Processing it for Data Matching.

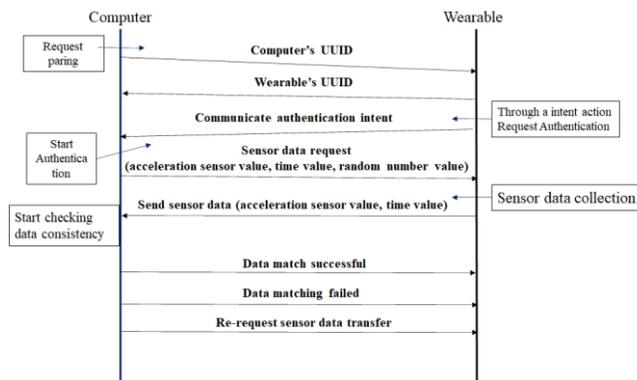


Fig. 5. The Proposed System Designs a Protocol for Authentication between Computer and user, where user's Intentionality for Authentication is Delivered Explicitly.

Intelligence Unit in the computer collects data from both Sensor Manager and Action Detector. These data are supposed to represent the user's behavior for authentication intent commonly but recorded by two different devices. It then checks the consistency of the data using the Needleman-Wunsch algorithm. If two data are matched, the user is authenticated. If they are not matched or the collected data is not received, the computer retransmits the request message. If there is no response within timeout period, authentication fails.

### C. Accuracy of Data Consistency

Conventional methods for user authentication intent delivery, like our system, apply the Needleman-Wunsch algorithm to the data consistency check; it matches data from user-worn wearables with data measured on the computer. It is observed that the methods use the matching algorithm only to determine the matching of sensor values and do not care for corresponding time values. However, time values in general authentication have played an important role especially when computing data consistency and data matching [25]. Matching of sensor data may result in failure of authentication unless corresponding time values are matched. To resolve the limitation, this paper proposes applying the Needleman-Wunsch algorithm to the matching of time values as well as acceleration sensor data, enhancing accuracy of data consistency.

### D. Randomness of user behavior

In a behavior-based authentication, data consistency is verified using data obtained by a user taking an action. Conventional methods for user authentication intent delivery define criteria in their specific behaviors [26]. This criterion is an essential part of users' behavior but can be abused for attacks. An external attacker can observe certain behaviors that a user performs when authenticating to a computer and then mimic the same action with a wearable device to carry out an authentication attack [27]. The criteria for users' behavior serve as fixed ID-Password values in a popular authentication. Thus, if data is leaked, constant data can be analyzed and attacked with authentication using fake data.

To tackle the challenge, the proposed system adopts the concept of OTP in the existing ID-Password authentication method [29]. The computer in our system sends a random number together when requesting data for authentication to a wearable [28]; this changes the required number of criteria for each authentication of a user's specific behavior. More technically, the computer sends two random values that are applied separately to the mouse and keyboard actions. To reduce the time required for certification as much as possible, a random number for the mouse is between 3 and 5 and that for the keyboard is between 3 and 7, which is based on numbers of existing authentication methods. This allows users to defend against authentication attacks because each authentication requires different numbers of certain behaviors. Even if external attackers observe and analyze users' behavior, they are inconsistent. We note that an optimal range of random values could be an interesting topic for further research.

## V. DEVELOPMENT AND PERFORMANCE EVALUATION

This section develops a prototype of the proposed system, runs experiments, and evaluates its performance. To assess accuracy of data consistency, we compare error values both in a traditional (conventional) method reviewed in Section III and in the proposed system that applies the matching algorithm to the time values additionally. Regarding randomness of user behavior, we measure data on how much user behaviors are matched when using randomized criteria. The initial result is then used to see whether an external attacker is authenticated when he imitates a particular behavior in both systems.

### A. Development

The test environment was modeled on the way that a user performs authentication at a personal computer, and a wearable was worn on the user's right wrist. We use a computer running Linux Ubuntu 16.04.04 LTS on a system of Intel® Core™ i5-9600KF CPU @ 3.70GHz and 16GB of memory. When recording mouse movements, the computer calculates the acceleration value using the position change value and the time change value [30]. When recording keyboard input, the time when the keyboard is inputted and the time when it is inputted is recorded. We use a Galaxy Watch (smartwatch) as a wearable, and Table II shows its technical specification. The smartwatch samples the accelerometer sensor at 200 Hz and transmits the data to the Bluetooth server in real time.

### B. Experiments on Traditional Method

For traditional methods, we use a mouse and keyboard to collect data about a user's specific behavior. Participants wear smartwatches on their right wrist to conduct experiments. In the smartwatch, acceleration sensors are used to collect acceleration values for wrist movements, and in the computer, mouse and keyboard are selected sequentially from Python-based programs. When selecting a mouse, the mouse moves from side to side on the screen to collect the mouse's location data and time data and calculate the acceleration. We then collect the time when the keyboard button is pressed once the keyboard is selected, or the time when the keyboard button is pressed [31]. The computer uses the matching algorithm to determine the data match for the acceleration value of the collected data.

For accurate verification of consistency of the data collected via the mouse-keyboard method of the participants, the data values are graphically represented to confirm the consistency of the values directly. This section compares the two graphs with the largest error in the experimental results as representatives, and the overall experimental results are tabulated.

TABLE II. SPECIFICATIONS OF SMARTWATCH

	Spec OF Galaxy Watch
<b>O.S</b>	Tizen-based wearable OS 4.0
<b>CPU</b>	Dual-core 1.15 GHz Cortex-A53
<b>Memory</b>	4GB 768MB RAM, 4GB 1.5GB RAM
<b>SENSOR</b>	Accelerometer, gyro, heart rate, barometer
<b>BATTERY</b>	Up to 72 h (mixed usage)

Fig. 6 shows the mouse experiment results of participant 1. The x-axis of the graph is the time in seconds, and the y-axis uses the acceleration value ( $m/s^2$ ). The graph for acceleration values in computers and smartwatches shows a similar graph in the peak, but in the last peak in the computer, the computer shows an acceleration value of 0.47264 and 0.168671 in the smartwatch, with an error value of 0.303969. In the SAW paper, the criterion for the error value of the data is 0.3. Existing systems determine that certification failed for the current participant.

Fig. 7 shows the results of a keyboard experiment for the same participant. In the figure, the part marked in red squares takes time for the keyboard to press and hit. The data consistency check on the keyboard first determines whether the acceleration value on the smartwatch is the value of the peak point at the time the keyboard is pressed on the computer. The keyboard checks the pressed and hit time and determines that it is the same if there are no other pick points within this time interval. However, the above graph shows that the value is peak at the time the keyboard was pressed on the second computer, but the exact data matching was not achieved because another pick point was displayed in the red square section, which represents the interval where the keyboard was pressed and hit. For the first experimental participant, neither mouse-keyboard nor mouse-keyboard matched the data.

Fig. 8 shows a graph of the mouse results of participant 6. The graph on the mouse results of the 6th experimental participant shows significantly similar appearance and matching values in computers and smartwatches than the graph of the first participant in the preceding one. However, the maximum value on a computer at 2.5 seconds in the graph is 1.62745, and the minimum value for a smartwatch is 1.10937. In this experiment, the error value at the peak point has a maximum value of 0.51808. This value is also determined to be an authentication failure because it does not match the data with more than twice the error tolerance value of 0.3 in [10].

Fig. 9 shows the results of the same participant's keyboard experiment. By checking the graph above, the sixth experimental participant was able to see the matching of the data in the keyboard experiment because the time the keyboard was pressed on the computer was all peak value of the smartwatch's acceleration value and no other peak value was included in the red square section.

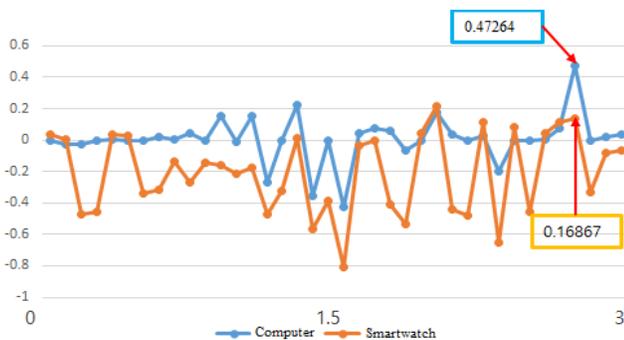


Fig. 6. An Experimental Result of Mouse Movement on Participant 1.

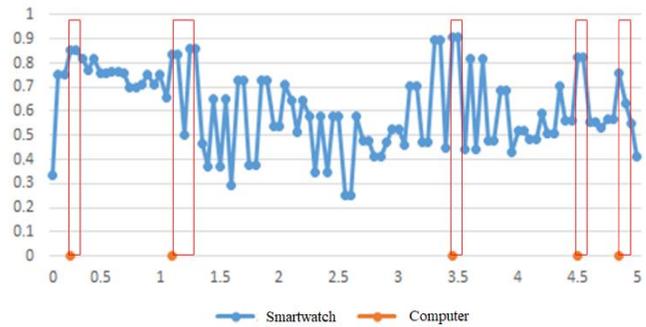


Fig. 7. An Experimental Result of Keyboard Press on Participant 1.

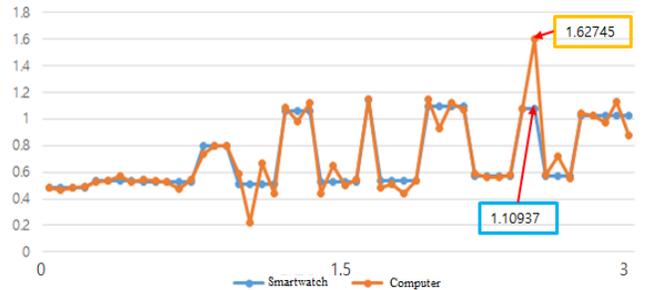


Fig. 8. An Experimental Result of Mouse Movement on Participant 6.

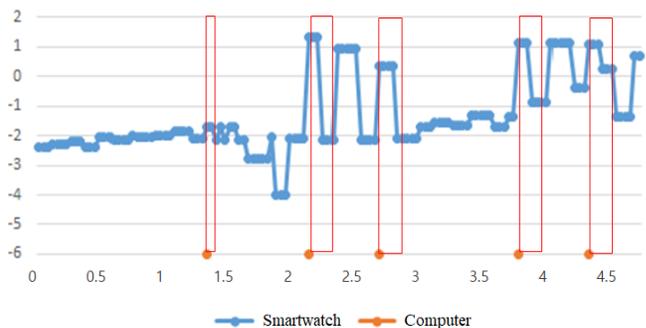


Fig. 9. An Experimental Result of Keyboard Press on Participant 6.

Table III summarizes mouse experiment results of a total of eight experimental participants in the traditional method. Five of the eight participants in the experiment are close to the tolerance value of 0.3, of which three are accurately included in the tolerance value, with one exceeding some.

Table IV shows eight participants are certified through the results of a keyboard experiment. There were five successful participants in the experiment, and three unsuccessful participants. Authentication via keyboard rather than mouse is the main method. All participants matched the time the keyboard was pressed on the computer with the peak point of the acceleration value on the smartwatch, but three failed to authenticate, including the other peak value in the keyboard's pressing and hitting interval. These results confirm that when the matching algorithm for time values is not applied during the authentication process through the user authentication intent transfer method.

TABLE III. EXPERIMENTAL RESULTS OF EIGHT PARTICIPANTS USING TRADITIONAL METHODS

	Computer	Smartwatch	Error value
Participant 1	0.47264	0.16867	0.30396
Participant 2	0.25175	-0.18172	0.43347
Participant 3	0.84264	0.28839	0.55425
Participant 4	-0.02481	-0.39514	0.37033
Participant 5	0.64428	0.41439	0.22989
Participant 6	1.62745	1.10937	0.51808
Participant 7	0.75613	0.52571	0.23042
Participant 8	0.40917	0.17514	0.23403

TABLE IV. KEYBOARD EXPERIMENT RESULTS FROM EIGHT PARTICIPANTS USING TRADITIONAL METHODS

	Authentication success	Authentication failed
Participant Number	2, 3, 6, 7, 8	1, 4, 5

C. Experiments on Proposed System

Unlike traditional methods, a smartwatch in the proposed system verifies the user's authentication intent, sends it to the computer, and verifies this intention on the computer to proceed with authentication. In this case, random values are transferred to the smartwatch together to provide a baseline for a specific behavior for the user's authentication, and experimental participants take a specific behavior through the mouse and keyboard according to this number.

With these data values, the computer applies the Needleman-Wunsch algorithm to verify the consistency of the data, and then applies the algorithm to the time value to perform authentication with more accurate data matching. Experiments conducted by experiment participants are the same as previous experiments, and only new parts are added that initiate authentication by touching the smartwatch twice. The graph also displayed the results of the experimenter with the largest error value and the experimenter with the smallest error value, just like the previous experiment, and the results for the entire experiment were tabulated.

Fig. 10 shows a graph of the acceleration sensor values of participant 5. The random number of mouse experiments occurred was 4, and the user moved the mouse left and right for 4 seconds to measure acceleration sensor data, time data, and acceleration and time values through the computer's mouse movement. In the above graph, the graphs for acceleration values of computers and smartwatches are not completely consistent, but we can confirm that the two data are much more consistent than those of conventional methods. At this point, a peak value of 0.33762 was recorded on the 1.2-second computer, while the smartwatch recorded a value of 0.25983. At this point, the error of the two values is 0.07779, showing a significantly lower value than 0.3 which was represented by the error value in the existing user authentication scheme.

Fig. 11 shows the results of a keyboard experiment of the same participant. At this point, the displayed random numbers represent the same 5 as the existing experiments, and the user conducted an experiment of pressing the keyboard five times.

In the graph above, the time when the keyboard was pressed on the computer and the peak point of the acceleration value of the smartwatch are the same, and the red section for the time when the keyboard was pressed and hit does not include other peak points. In the case of keyboard experiments, there was no problem with data matching, unlike previous conventional methods experiments among participants. In other words, authentication was carried out by applying the need only-one algorithm to the time value, matching the section where the keyboard was pressed and hit to the time when the peak point of the smartwatch was stamped.

Fig. 12 is a mouse experimental graph of participant 1 in the proposed method. Unlike the results of one previous experiment, graphs for acceleration values of smartwatches and computers show more consistency. The computer's acceleration value is 0.50388 and the smartwatch recorded acceleration sensor value is 0.25983. The error value for this is 0.22284, which is lower than the error range of 0.3. However, the values shown this time showed similar values in previous experiments.

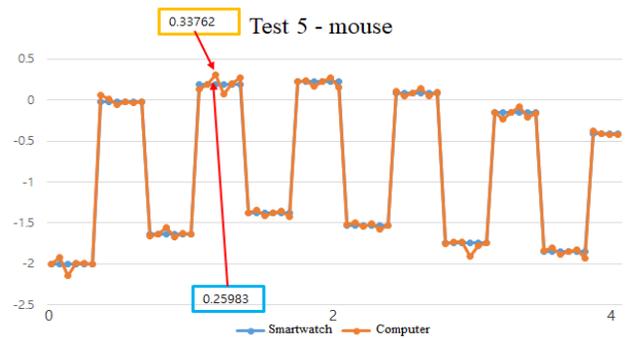


Fig. 10. An Experimental Result of Mouse Movement on Participant 5 in the Proposed Method.

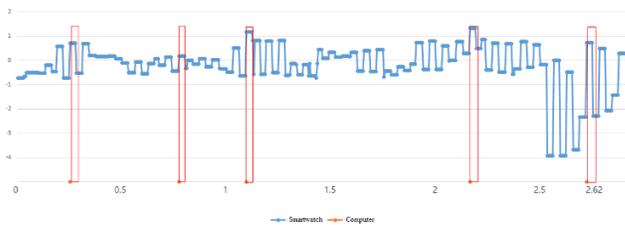


Fig. 11. An Experimental Result of Keyboard Press on Participant 5 in the Proposed Method.

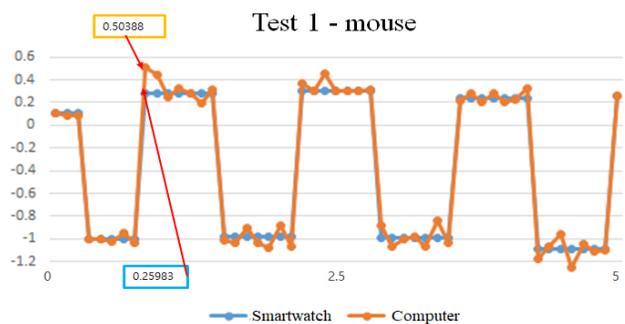


Fig. 12. An Experimental Result of Mouse Movement on Participant 1 in the Proposed Method.

The results of the overall participants in the proposed scheme are presented in Table V. There were seven participants who did not correspond to the error value of 0.3, and only one failed to authenticate beyond the error value. It shows higher accuracy than data matching experiments in which three people in the previous existing method succeeded and five failed. This is the result of applying the need-one-value algorithm to the time value, which makes the comparison between computers and smartwatch data more accurate. It shows a lower error value than the error value shown in the experiments of the existing method, and is reliably successful in data matching, enabling authentication.

TABLE V. EXPERIMENTAL RESULTS OF 8 PARTICIPANTS IN THE PROPOSED SYSTEM

	Computer	Smartwatch	Error value
Participant 1	0.50388	0.28104	0.22284
Participant 2	-0.02944	0.09978	0.12922
Participant 3	0.27756	0.23265	0.04491
Participant 4	0.98824	1.09113	0.10289
Participant 5	0.33762	0.25983	0.07779
Participant 6	0.8537	1.3054	0.4517
Participant 7	1.2084	0.98841	0.21999
Participant 8	0.74269	1.02772	0.28503

#### D. Performance of Data Consistency

We confirm the experimental results of the existing and proposed methods in the previous subsection. In mouse authentication, we show that the existing method succeeds in 3 out of 8 and 5 fails, and that the proposed method fails only 1 out of 7 people. Furthermore, we show that the error value of the proposed scheme is also significantly lower, and we can confirm that it is a more suitable method for data matching. This can be confirmed through the graph in Fig. 13.



Fig. 13. Comparison of Error Values between Existing and Proposed Methods.

By checking the graph in the figure, the maximum value of the error in the existing scheme is 0.55425 and the minimum value is 0.21989 and the maximum value of the error in the proposed scheme is 0.4517, with a minimum value of 0.04491.

The mean of each error value shows a significantly lower value of 0.359304 in the existing method, 0.191796 in the proposed method, and since the data error value for successful authentication must be less than 0.3 it is appropriate to use the proposed method focusing on matching time values over the existing method.

Keyboard-experiments also showed results of five successful and three unsuccessful using conventional methods, but the proposed method showed results of seven successful and one failure. However, because the proposed method can only authenticate when both the mouse and keyboard have a data match, one failed to authenticate through a match at the mouse value. Comparing only keyboard values, all eight showed accurate data matching.

#### E. Comparison of Behavioral Matching with Randomness

Traditional methods operate by setting criteria for specific behaviors of users. For instance, SAW in [10] used the TAP-5X, a five-press keyboard method. However, as previously stated, certain behaviors with these criteria can allow an external attacker to observe the user's movements and take the same action to make an authentication attack [32-34]. In this paper, random numbers are transferred from the computer to the smartwatch to perform the mouse-keyboard behavior at different times per authentication, rather than the criteria set for a particular number of actions. To confirm this, eight participants observed other people's experiments and examined whether they could perform the same behavior.

In experiments with existing methods, all eight participants answered that all users could do the same because they used the same authentication method of mouse movement and keyboard No. 5 tab. However, the experimental participants failed to take the same action because the proposed authentication method applied different random numbers to the mouse-keyboard method. Through this, authentication methods through randomness have an advantage in attacks through the observation of external attackers than when there is a set standard for a specific number of actions for authentication of existing users.

## VI. CONCLUSION

This paper proposed a new proximity-based authentication system that delivered user's intentionality for authentication in an accurate manner. Conventional methods for user authentication intent delivery solve a random authentication problem that can occur in proximity-based authentication. But, they still have limitations; (i) a wearable device may consume energy much faster, (ii) conventional methods proceed based on the number of actions fixed to a specific behavior for user authentication, which could be vulnerable to external attackers, and (iii) the methods do not match time values, which results in less accurate data consistency process.

To overcome the limitations, the proposed system designs a new protocol for authentication where an authentication process is initially detected on a user side instead of on a computer. The system adopts a randomness that changes the number of actions that a user should perform each time she proceeds with authentication. It increases the accuracy of the matching of the data by applying a Needleman-Wunsch

REFERENCES

algorithm to time values when verifying data consistency. Experimental results showed that authentication was succeeded 5 times and failed 3 times with conventional methods, but the proposed system showed 7 successes and 1 failure. Results in the mouse experiments showed that the maximum error value in the conventional methods was 0.55425 and the minimum value was 0.21989, while the proposed system showed the maximum of 0.4517 and the minimum of 0.04491, which was much lower.

A. Discussion

Verifying user intentionality is one of the most important goals in authentication process. In traditional patterns of authentication interaction (human-machine, human-human, and machine-human authentication), human beings have been involved directly in authentication and delivered authentication intent explicitly [35]. Examples include password-based methods and biometric-based methods. By touching on a finger scanner, a user presents her intent for authentication in a fingerprint authentication. With increasing development of IoT technologies and pervasive computing, however, a new pattern of a machine-machine authentication becomes popular [22, 36-37]. For instance, a user carrying a wireless authentication token approaches a target computer that authenticates the user whenever the token is within a certain distance. In such a new pattern of the proximity-based authentication, the user intentionality is often omitted or not verified explicitly.

Delivering the intent and verifying it on both sides of authentication entities may delay processing and degrade convenience of the machine-machine authentication [38]. That is, a new authentication method is on between accurate verification and user convenience. The proposed authentication system is somewhat intended to high accuracy and high protection level. It diminishes risks from external attackers by randomizing user behaviors in authentication, increases accuracy of data consistency process by handling time values, and takes care of energy consumption of a power-constrained IoT device by designing a new authentication protocol.

The proposed system may not provide an excellent benefit of user convenience. Our authentication may be recognized as an interruptive step in a user's normal workflow. That is, a user should start explicitly authentication after stopping what she is doing. Once authentication done, she gets back to her normal work that she was on before authentication. A future work may include development of an advance authentication that blends seamlessly into users' workflow. One possible approach is to make use of the workflow for authentication [26]. It would be optimal if she is being authenticated while she is doing her work; that is, seam between authentication and workflow are blurred.

Delivery of users' authentication intent is expected to enable faster and safer authentication through user behavior analysis if machine learning, which has recently been utilized in various fields, is applied. Furthermore, as the demand for wearable devices such as smartwatches is increasing, further research is required to analyze user behavior patterns in more detail and to quickly authenticate based on them.

- [1] L. Lamport, "Password authentication with insecure communication", Communications of the ACM, November 1981.
- [2] T. Petsas, G. Tsirantonakis, E. Athanasopoulos, S. Ioannidis, "Two factor authentication: is the world ready?: quantifying 2FA adoption", European Workshop on System Security (EuroSec), Article No.:4, pp.1-7, 2015.
- [3] S. Ma, R. Feng, J. Li, Y. Liu, S. Nepal, Diethelm, E. Bertino, R. Deng, Z. Ma, and S. Jha, An empirical study of SMS one-time password authentication in Android apps, ACM Annual Computer Security Applications Conference, Dec. 2019.
- [4] B. Rodrigues, A. Chaudhari and S. More, "Two factor verification using QR-code: A unique authentication system for Android smartphone users," International Conference on Contemporary Computing and Informatics (IC3I), 2016.
- [5] B. Zhou, J. Lohokare, R. Gao, and F. Ye, EchoPrint: Two-factor Authentication using Acoustics and Vision on Smartphones, ACM Annual International Conference on Mobile Computing and Networking, Oct. 2018.
- [6] J. Zhang, Z. Wang, Z. Yang and Q. Zhang, "Proximity based IoT device authentication," IEEE Conference on Computer Communications (INFOCOM), 2017, pp. 1-9.
- [7] A. Kalamandeen, A. Matthew Scannell, E. De Lara, Anmol Sheth, Anthony LaMarca, "Ensemble: cooperative proximity-based authentication", ACM International conference on Mobile systems, applications, and services (MobiSys), pp. 331-344, 2010.
- [8] M Horton, 2016, "Proximity based device security", US Patent 9,443, 071, AT&T Intellectual Property I, L.P, Atlanta, GA (US).
- [9] A. Varshavsky, A. Scannell, A. LaMarca, E. de Lara "Amigo: Proximity-Based Authentication of Mobile Devices", Ubiquitous Computing, pp 253-270, 2007.
- [10] S. Mare, R. Rawassizadeh, R. Peterson, D. Kotz, "SAW: Wristband-based Authentication for Desktop Computers", ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies, 2018, Article No:125.
- [11] N. Z. Gong et al., "PIANO: Proximity-Based User Authentication on Voice-Powered Internet-of-Things Devices," IEEE International Conference on Distributed Computing Systems (ICDCS), 2017, pp. 2212-2219.
- [12] D. E. Bernard, 2008, " Multimodal natural language query system and architecture for processing voice and proximity-based queries ", US Patent 7,376,645, The Intellection Group, Inc, Duluth GA (US).
- [13] Li et al, Los Altos, CA (US), 2018, " Methods and Apparatus for User Authentication and Human Intent Verification in Mobile Devices ", US Patent 9,877,193, Apple Inc., Cupertino, CA(US).
- [14] R. Boughenguel, I. Mahgoub and M. Ilyas, "Bluetooth Security in Wearable Computing Applications," International Symposium on High Capacity Optical Networks and Enabling Technologies, 2008, pp. 182-186.
- [15] J. Rekimoto, "GestureWrist and GesturePad: unobtrusive wearable interaction devices," International Symposium on Wearable Computers, 2001, pp. 21-27.
- [16] S. Khan, S. Parkinson, L. Grant, N. Liu, S. McGuire, "Biometric Systems Utilising Health Data from Wearable Devices: Applications and Future Challenges in Computer Security", ACM Computing Surveys , Article No:85, July 2020.
- [17] R.Raya, J. Roa, E. Rocon, R. Ceres, J. Pons, "Wearable inertial mouse for children with physical and cognitive impairments", Sensors and Actuators A: Physical, Vol. 162, Issue 2, pp. 248-259, August 2010.
- [18] N. Kern, B. Schiele, and A. Schmidt "Multi-Sensor Activity Context Detection for Wearable Computing", European Symposium on Ambient Intelligence, pp 220-232, 2003.
- [19] S. Li, A. Ashok, Y. Zhang, C. Xu, J. Lindqvist and M. Gruteser, "Whose move is it anyway? Authenticating smart wearable devices using unique head movement patterns," IEEE International Conference on Pervasive Computing and Communications (PerCom), 2016, pp. 1-9.

- [20] L. Xiao, Q. Yan, W. Lou, G. Chen and Y. T. Hou, "Proximity-Based Security Techniques for Mobile Users in Wireless Networks," *IEEE Transactions on Information Forensics and Security*, 8(12), pp. 2089-2100, Dec. 2013.
- [21] Needleman, Saul B. & Wunsch, Christian D. (1970). "A general method applicable to the search for similarities in the amino acid sequence of two proteins". *Journal of Molecular Biology*. 48 (3): 443–53.
- [22] X. Li, Q. Zeng, L. Luo, T. Luo, "T2Pair: Secure and Usable Pairing for Heterogeneous IoT Devices", *ACM Conference on Computer and Communications Security*, pp. 309–323, 2020.
- [23] S. Mare, R. Rawassizadeh, R. Peterson, D. Kotz, "Continuous Smartphone Authentication using Wristbands", *Workshop on Usable Security*, 2019.
- [24] A. Bianchi, I. Oakley, "Wearable authentication: Trends and opportunities", 2016, it - *Information Technology* 58(5).
- [25] F. De Arriba-Pérez, M. Caeiro-Rodríguez, J. Santos-Gago, "Collection and Processing of Data from Wrist Wearable Devices in Heterogeneous and Multiple-User Scenarios", *Sensors*, 16(9), 1538, 2016.
- [26] A. Huang, D. Wang, R. Zhao, Q. Zhang, Au-Id: Automatic User Identification and Authentication through the Motions Captured from Sequential Human Activities Using RFID, *ACM on Interactive, Mobile, Wearable and Ubiquitous Technologies*, 3(2), Article No.: 48, June 2019.
- [27] L. E. Boyd, X. Jiang, G. R. Hayes, "ProCom: Designing and Evaluating a Mobile and Wearable System to Support Proximity Awareness for People with Autism", *Conference on Human Factors in Computing Systems (CHI)*, pp. 2865–2877, 2017.
- [28] J. Jacob, K. Jha, P. Kotak and S. Puthran, "Mobile attendance using Near Field Communication and One-Time Password," *International Conference on Green Computing and Internet of Things (ICGCIoT)*, pp. 1298-1303, 2015.
- [29] C.-H. Ling, C.-C. Lee, C.-C. Yang, and M.-S. Hwang, "A Secure and Efficient One-time Password Authentication Scheme for WSN", *International Journal of Network Security*, Vol.19, No.2, PP.177-181, Mar. 2017.
- [30] C. Shen, Z. Cai, X. Guan, Y. Du and R. A. Maxion, "User Authentication Through Mouse Dynamics," in *IEEE Transactions on Information Forensics and Security*, vol. 8, no. 1, pp. 16-30, Jan. 2013.
- [31] F. Ciuffo and G. M. Weiss, "Smartwatch-based transcription biometrics," *IEEE Annual Ubiquitous Computing, Electronics and Mobile Communication Conference (UEMCON)*, pp. 145-149, 2017.
- [32] X. Li, "Smart Sensing Enabled Secure and Usable Pairing and Authentication. Doctoral dissertation, 2020. Retrieved from <https://scholarcommons.sc.edu/etd/6068>.
- [33] X. Liu, Z. Zhou, W. Diao, Z. Li, K. Zhang, "When Good Becomes Evil: Keystroke Inference with Smartwatch", *ACM Conference on Computer and Communications Security*, October 2015.
- [34] J. Voris, Y. Song, M. Salem, S. Hershkop, S. Stolfo, "Active authentication using file system decoys and user behavior modeling: results of a large scale study", *Computers & Security*, Volume 87, November 2019.
- [35] S. Peisert, Ed Talbot, and T. Kroeger, *Principles of Authentication. ACM Workshop on New Security Paradigms Workshop (NSPW)*, 2013.
- [36] C. Li, X. Ji, B. Wang, K. Wang, and W. Xu, SenCS: Enabling Real-time Indoor Proximity Verification via Contextual Similarity, *ACM Transactions on Sensor Networks*, 17(2), pp 1–22, June 2021.
- [37] W. He, M. Golla, R. Padhi, J. Ofek, M. Durmuth, E. Fernandes, and Blase Ur, Rethinking Access Control and Authentication for the Home Internet of Things (IoT), *USENIX Security Symposium*, Baltimore, MD, 2018.
- [38] I. Chenchev, A. Aleksieva-Petrova, and M. Petrov, *Authentication Mechanisms and Classification: A Literature Survey*, *Intelligent Computing, Lecture Notes in Networks and Systems*, vol 285. pp 1051-1070, Springer, 2021.

# Digital Preoperative Planning for High Tibial Osteotomy using 2D Medical Imaging

Norazimah Awang<sup>1\*</sup>, Faudzi Ahmad<sup>2</sup>  
Rosnita A. Rahaman<sup>3</sup>  
Computing Department, Universiti Selangor  
Malaysia

Azrulhizam Shapi'i<sup>5</sup>  
Centre for Artificial Intelligence Technology  
Universiti Kebangsaan Malaysia  
Selangor, Malaysia

Riza Sulaiman<sup>4</sup>  
Institute IR 4.0  
Universiti Kebangsaan Malaysia  
Selangor, Malaysia

Abdul Halim Abdul Rashid<sup>6</sup>  
Orthopaedic Department  
Universiti Kebangsaan Malaysia Medical Center  
Selangor, Malaysia

**Abstract**—The pre-operative planning process for High Tibial Osteotomy (HTO) is vital to correct the deformity of the long bones. The most important process is needed to find the Centre Of Rotation of Angulation (CORA) and display the forecast result based on the value of the correction angles simultaneously. Presently, these practices should be done manually because current software only can define either CORA's point or correction angle at one time. This paper proposed to use computer-aided software to make the fully digitized process of pre-operative planning for HTO to be done. For this purpose, we introduced OsteoAid software. This software enables the user to define the mechanical or anatomical axes and define the CORA's point and the angle at one time. For testing purposes, we compared the reliability of osteotomy's correction angle between this two software (MedWeb and OsteoAid) in preoperative planning open-wedge high tibial osteotomy. This is to ensure that the new software is reliable for the correction. Thirteen digital long leg radiographs with long-standing positions from the frontal axis showing patients with both tibia deformities were examined using intra-class correlation. Those images are accessed from the picture archiving and communication system (PACS). Three medical officers (raters) who were involved in an osteotomy used the same medical image format twice with a two-week interval. Using the MedWeb software, the mean correction angle score of each rater is at excellent level: 0.989 (intra-rater1), 0.982 (intra-rater2) and 0.972 (intra-rater3). Scores of each rater for OsteoAid are also excellent: 0.949, 0.987 and 0.986 respectively. The inter-rater reliabilities of the correction angle were 0.820 and 0.979 ( $p < 0.001$ ) respectively for each software. The principal finding of this study was that the new software (OsteoAid) showed excellent reliabilities and good consistency in preoperative planning in finding CORA and correction angle.

**Keywords**—Center of rotation of angulation; CORA; HTO; software; digital; medical image

## I. INTRODUCTION

The High Tibial Osteotomy (HTO) is one of the trusted methods and an effective medical treatment option for correction in ensuring the success of HTO surgical procedures [1], [2]. HTO is an acceptable and common procedure to treat symptomatic osteoarthritis of the medial compartment of the

knee with varus alignment. HTO is considered a very successful surgical procedure with low complication rates. The goal of surgical treatment is to shift the weight-bearing axis from the medial compartment to the lateral compartment [3]. It is becoming increasingly important nowadays in the treatment of cartilage pain or central osteoarthritis with varus deformity [4].

Proper planning, especially the height of the wedge base and osteotomy correction angle, is also a crucial aspect of effective HTO. Usually, preoperative planning of HTO will be done before the real surgery to ensure optimum correction and to avoid malalignment that can lead to under-correction or over-correction, even with navigation systems [5]. Inaccurate preoperative planning will produce inadequate correction during surgery and loss of correction in the postoperative period [6].

Previously, conventional preoperative planning for HTO was done by tracing out the x-ray film on paper. When the technology was replaced from X-ray film to digital, the full digital procedure for preoperative planning should also be produced. Current software is reliable for preoperative planning for HTO in a part of procedure such as finding CORA's point or angle at one time only, it does not visualise the forecast result as needed by surgeon. This motivates researchers to develop a new software that can fulfil all the requirements needed by surgeon.

Computer-assisted planning gives the advantages to the higher accuracy and reliability in many ways such as digital storage, infrastructure and technology [7], digital planning [3], better result [8], real-time feedback [9] and possible to display future results [10]. In optimizing a digital radiographic image in the orthopaedic department, the researcher developed digital preoperative planning for high tibial osteotomy software.

A previous study from Awang et al [11] shows five different specification software namely TraumaCad, MediCad, Sectra, MedWeb, and Photoshop applied to implement preoperative planning for an osteotomy. However, certain software is usually equipped with advanced equipment

\*Corresponding Author

(computer navigation) and exorbitantly costly and it is difficult for developing countries such as Malaysia to purchase. On the other hand, current software implemented in Universiti Kebangsaan Malaysia Medical Center (UKMMC), as an example, has limited functions and does not provide a forecast image for postoperative.

OsteoAid software was developed to overcome the current limitation that occurred during the planning process, such as, the current software does not provide a centre of rotation of angulation and it does not provide visualisation for correction. The new software enables the user to easily find out an angle for correction and rotate a part of the image and visualise it. This paper aims to determine the CORA and correction angle at one time. It also aims to compare the accuracy of new software, in order to ensure the reliability of the new software in doing preoperative planning for HTO.

Meanwhile, the CORA is the point of intersection between two straight lines at the proximal and distal [12]. According to Kim et al., [3] CORA is determined by the intersection of the transverse dividing line between the proximal and distal tibial anatomical axes and the posterior tibial cortex. Moreover, it allows accurate analysis of lower limb angular defects [13].

CORA is the most important assessment for angular defect correction. The line that crosses the CORA and divides the lateral and medial angles formed by the proximal and distal axes of the bone is called the transverse bisector line (tBL).

The intersection of these straight lines involves mechanical [14], [15] or anatomical axes [16] It is also influenced by the need or regulation of the osteotomy itself i.e. varus gene defect [14], valgus [17] or recurvatum [18]. This selection also depends on the selection of wedges to be used that is whether open wedge, closed, dome and also a combination.

Thus, this study is focusing on the requirements needed to develop the digital planning for HTO. CORA as the main requirement in this study is needed to guide the surgeon to cut the proximal tibia with dedicated correction angle. Then the correction angles founded from the same images using two different software were then tested and compare their ICC to prove that it is also equivalent among MedWeb and OsteoAid. This section also contains the background of the current research. Section II discussed the materials and methods needed in this study. Section III discussed the evaluation followed by the results, discussion and conclusion.

## II. MATERIALS AND METHODS

This new software was developed based on the user requirements. The main focus of this development is on the defining CORA's location and correction angles' value. Besides, this software enables end user to see a picture based on the previous result of CORA point and the angle of the correction.

A retrospective case series was conducted between 2016 and early 2018, 26 tibia's radiographic images from 13 patients have already undergone osteotomy surgery. The patients were five men and eight women with aged between two to 15 years old. To ensure good quality results, two identical tests will be

conducted by the same three evaluators for all two tests, within a two-week interval at the PPUKM Orthopaedic Clinic by medical officers in specialist training in the osteotomy field.

The three medical officers (evaluators) will test the Medweb software and also OsteoAid using medical images (Dicom). All of the images were tested to compare CORA's angle finding from two different software; MedWeb which is the current software used in that hospital and OsteoAid, new proposed software that was developed to overcome MedWeb's deficiency.

### A. Preoperative planning

Since this study focused only on the genu varum and valgus, all radiographic images were from the coronal plane which required a long lower limb. The aim is in preoperative planning for high tibial osteotomy by realigning the deformity leg to the normal weight-bearing line. This study only focuses on comparing results in finding CORA based on two different softwares. Here, CORA was defined based on two intersections of lines produced from proximal and diaphyseal anatomical axis to produced lateral open wedge for high tibial osteotomy. Fig. 1 shows how to produce CORA and the correction angle.

### B. Radiographic Evaluation

There are many records of patients who had undergone osteotomy, but to ensure that the testing can be done fairly and transparently, several things need to be concentrated. Those requirements are long leg radiograph with long-standing position from the frontal axis and using the same Movement Reference Number (MRN) of each patient from picture archiving and communication system (PACS).

### C. Correction Angle

A correction angle is an angle produces based on the percentage of anatomy or mechanical axis. An example, based on [19], the target mechanical axis were calculated as much as 62.5% using radiographs in the standing and supine positions based on Fujisawa technique. The author in [17] defines correction angle based on the drawn line from the hinge point to the line connecting the center of the femoral head and 55, 60, and 65% weight-bearing line.

In this study, two straight lines of T-shaped and T-downward which are known as T1 and T2's markers were used to produce the angles. T1 as by default is at a zero angle of degrees while T2 is at an angle of 180 degrees. If the user clicks on the right arrow key for any marker, the current value of the marker will be added to five degrees, while if the user clicks on the left arrow key, the current value of the marker will be subtracted to negative five degrees. Those markers are shown in Fig. 1.

Similarly, if the user clicks on the up-arrow key, the current value of the marker will be added to one degree, while if the user clicks on the down arrow key, the current value of the marker will be subtracted to negative one degree. The two markers will then be continuously updated with the value of their respective findings. Fig. 2 shows the programming language used to calculate the angles.



Fig. 1. CORA's Location and Correction Angle.

```
if DeltaTheta ~= 0 || dAlpha ~= 0
    handles.data.Alpha = handles.data.Alpha + dAlpha;
    if ID == 1
        handles.data.Theta1 = handles.data.Theta1 +
DeltaTheta;
        handles.data.Marker1 =
imrotate(imresize(handles.data.MarkerRef,handles.data.Alpha,
'bicubic'),-handles.data.Theta1,'bicubic');
        handles.data.bMarker1 =
any(handles.data.Marker1>0.1,3);

set(handles.Theta1,'String',num2str(handles.data.Theta1));
    else
        handles.data.Theta2 = handles.data.Theta2 +
DeltaTheta;
        handles.data.Marker2 =
imresize(imrotate(handles.data.MarkerRef,-
handles.data.Theta2,'bicubic'),handles.data.Alpha,'bicubic')
;
        handles.data.bMarker2 =
any(handles.data.Marker2>0.1,3);

set(handles.Theta2,'String',num2str(handles.data.Theta2));
```

Fig. 2. Algorithm of the Selection and Rotation a Part of Image.

#### D. Rotating a Part of Image

As the correction angle is produced, they want to display the prediction of correction. Based on the CORA correction's angle obtained, the next task is to mark an area of the image of the tibia to be rotated and visualize the expected result of the rotation. This is done to get the satisfaction of the surgeon in obtaining the best picture of point and angle results before the operation. In addition, it is also important to provide an initial overview to patients and family members about the treatment methods that the patient will receive.

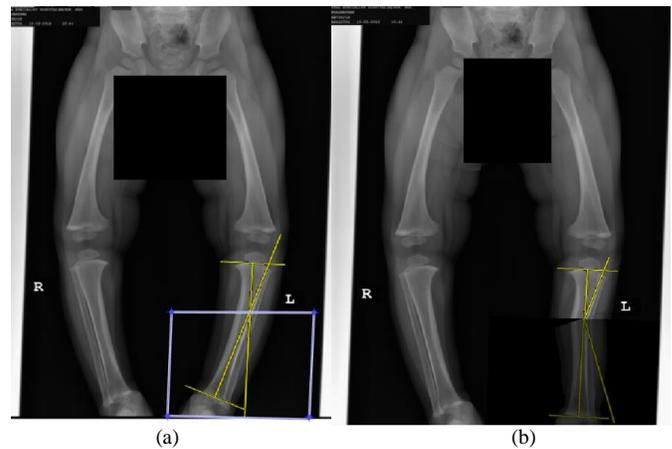


Fig. 3. (a) Process of Selection a Part of the Area, (b) Result Displayed based on the Correction Angle.

Fig. 3(a) shows an example where a part of the area was selected for cropping and rotation. Here, the user needs to mark four corners of the part of the image to be rotated and it must cross the line at the CORA point. In the last corner, which is the fourth corner, the user has to click the mouse twice to finish the process of selection. Then the result will display as shown in Fig. 3(b).

#### E. Statistical Analysis

Normality tests were performed using Kolmogorov – Smirnov on all variables before determining parametric statistics. This test is made to determine the compatibility between the two methods is also tested by comparing the mean of the correction angle obtained. Kolmogorov – Smirnov testing was performed to confirm the normal distribution. This test was chosen to test the normality of the data when the data were in small numbers and less than 50.

If the data is normal, then the researcher can use a T-test to run a further test. Else, Wilcoxon signed-rank test can be used. Then, the intra-class correlation was used to test the reliability of the results (ICC). Inter- and intra-rater reliabilities using the IntraClass Correlation Coefficient method were accessed. For statistical analysis, the IBM SPSS software for Windows version 17 was employed to determine if statistically significant similarities were present between the group studied. A p-value of 0.05 or less was considered to be a significant difference.

### III. EVALUATION

After the development of the system was completed, one simple test will be done to evaluate the accuracy of the system. Testing has been conducted on 13 patients with impairment on both legs who had undergone osteotomy treatment from 2016 to early 2018 at Universiti Kebangsaan Malaysia Medical Center (UKMMC). The respondents comprised of three medical officers who practice osteotomy correction planning and the tests were conducted at UKMMC. They tested on this system themselves in conducting osteotomy preoperative planning procedures and obtained the results based on the given patient. To determine the sample size, an a priori power analysis was performed using the null hypothesis test at  $\alpha$  level

of .05. It had been hypothesized that the reliability of intra- and inter-rater for the dedicated software was zero.

As the study involves the field of medicine that leads to orthopaedic, the test is based on the guidelines obtained from the International Society of Arthroscopy, Knee Surgery and Orthopaedic Sports Medicine (ISAKOS), in which the results lead to the reliability of new techniques based on existing techniques.

The reliability of this new software will be evaluated. The current software is regarded as a gold standard, and consistency was evaluated for the examination of the accuracy of the new system PACS-OsteoAid method. Coronal alignment and posterior tibia slope were evaluated and excluded to sagittal alignment. The reliability of the measurement was accessed, by examining the intra-rater and inter-rater reliability, using intra-class correlation coefficient (ICC) to determine each component score [20]. Three medical officers, who were involved in osteotomy, measured the correction angle twice with a two-weeks interval.

#### IV. RESULTS

A few standards on the development that have been done were listed to be followed before testing could be executed as followed:

- 1) the software can use the medical image in Dicom format.
- 2) surgeons are free to define CORA.
- 3) the software can visualise CORA for correction.
- 4) software is tested by the medical officer who is involved in osteotomy.

Based on the standard proposed, one evaluation was done to accept the level of accuracy achieved from the usage of OsteoAid. The demographic data based on thirteen patients with both tibia's patients underwent preoperative planning in finding CORA angle are in age 2-15 based on the data available in the PACS is shown in Table I.

Table II shows the two tests (Test1 and Test2) that need to be performed by all evaluators. Result shows that all of the significant value is 0.00. This indicates that Test1 and Test2 are not significantly different from the normal distribution based on statistics. Thus, non-parametric testing such as Wilcoxon Rank-Marked Test will be conducted.

The Wilcoxon Signed-Rank Test was chosen to make a comparison between Test1 and Test2. If a pair of scores has the same value, then it is considered bound and dropped from the analysis and the sample size will be reduced taking into account the value of  $P < 0.05$  is considered significant. For this study, the Wilcoxon Rank-Marked Test was used to compare scores from two tests performed at two different time points.

The finding of MedWeb's for Rater1 and Rater2 from two weeks apart for Rater1 did not show a statistically significant change ( $p = .444, 0.71$ ) compared with alpha value = 0.05. For Rater3, it shows a statistically significant change ( $p = .036$ ) compared with alpha value = 0.05. For the OsteoAid, all raters did not show a statistically significant change ( $p = .545, .224, .932$ ) compared with alpha value = 0.05.

TABLE I. DEMOGRAPHIC RESULT

Item	Number
Total tibia examined	26
Total number of patients	13
Right tibia	13
Left tibia	13
Age	2-15
Gender (M/F)	5/8

TABLE II. NORMALITY TEST BY KOLMOGOROV-SMIRNOV

	Kolmogorov-Smirnov		
	Statistic	df	Sig
Test1	.111	234	.000
Test2	.090	234	.000

As shown in Table III, the finding of MedWeb's for Rater1 and Rater2 is there is no difference between Testing1 and Testing2 whereas for Rater3, there is a difference between Testing1 and Testing2. For the OsteoAid, the findings for each rater are there was no difference between Test1 and Test2. The factor that contributes to the difference between Testing1 and Testing2 for Rater3 was due to the factor of variability between users where this factor is out of control. Thus, the number of evaluators of three people has helped to reduce the biased results.

TABLE III. WILCOXON SIGNED-RANK TEST

Rater	MedWeb		OsteoAid	
	z value	p Value	z value	p Value
Rater1	-.765	.444	-.605	.545
Rater2	-1.806	.071	-1.217	.224
Rater3	-2.102	.036	-.086	.932

Z Asymp. Sig (2-tailed) at 0.05

Table IV shows the intra-rater result for each rater towards each software. For intra-raters, three raters would test two different software which is (a) MedWeb and (b) OsteoAid. Every rater had done the testing twice every fortnight. Meanwhile, the inter-rater testing was done by all three raters towards the two software. Through the statistics software package SPSS version 21 (SPSS Inc.), an estimation of ICC and Confidence interval (CI) of 95%, absolute-agreement and two-way mixed-method model were chosen.

Each rater scored excellent level: 0.989 (0.975-0.995), 0.982 (0.961-0.992) and 0.972 (0.938-0.987) respectively for MedWeb. As for OsteoAid, the scores were also excellent: 0.949 (0.882-.0978), 0.987 (0.970-0.994) and 0.986 (0.969-0.994) respectively. The finding from the usage of each software to get the CORA angles of the preoperative planning for osteotomy by all three raters is excellent.

The statistics for the inter-rater reliability between MedWeb and OsteoAid showed that the ICC of the latter is higher compared to the former. The ICC for OsteoAid is 0.979 while the ICC for MedWeb is at 0.820. Therefore, both figures can be accepted. OsteoAid method is in the range of good and acceptable reliability for preoperative planning of high tibial osteotomy.

TABLE IV. INTRA-CLASS CORRELATION FOR INTRA-RATERS

Rater	Correction Angle
Intra-rater 1(a)	0.989 (0.975-0.995)
Intra-rater 2(a)	0.982 (0.961-0.992)
Intra-rater 3(a)	0.972 (0.938-0.987)
Intra-rater 1(b)	0.949 (0.882-0.978)
Intra-rater 2(b)	0.987 (0.970-0.994)
Intra-rater 3(b)	0.986 (0.969-0.994)
Inter-rater (a)	0.820 (0.663-0.901)
Inter-rater (b)	0.979 (0.967-0.987)

Intra-rater 1 means ICC of rater 1 for first and second measurements. Intra-rater 2 means ICC of rater 2 for first and second measurements. Intra-rater 3 means ICC of rater 3 for first and second measurements. (a) refers to MedWeb, while (b) refer to OsteoAid. Inter-rater (a) means the ICC using MedWeb, between rater 1, 2 and 3. Inter-rater (b) means the ICC using OsteoAid between rater 1, 2 and 3.

## V. DISCUSSION

The most important finding of this study was that new software (OsteoAid) had a significant reliability in finding CORA's angle rather than current software (MedWeb). This study successfully compares measurement angles of digital radiographic images among two softwares. In addition, there was excellent intra- and inter-rater correlation.

Planning techniques need to be reliable [21]. This study was done because existing software can only perform one of the procedures at a time. It is difficult for surgeons to define the CORA and propose the correction angle at one time. Fig. 4 shows the CORA that was produced based on the intersection of two lines, and the correction angle is automatically displayed when the user rotates the line based on the desired location.

Other studies have discussed the preliminary planning of high tibial osteotomy [14], [22]. Based on different osteotomy problems, the need for planning also varies. For example, based on the difference of deformity whether genu varum, valgus or recurvatum, selection of frontal and sagittal planes, selection of mechanical or anatomical axis [22] in planning, open or close wedge, as well as CORA cuts are also different is based on the needs and determined by the surgeon himself. This study is reassuring concerning the reliability of preoperative planning, but it does not cover the reliability of intra- and post-operative.



Fig. 4. Finding CORA and Automatically Software will Define Correction Angle.

The outcome was that both current and newly developed software had outstanding reliabilities and consistency in finding CORA for preoperative planning open wedge high tibial osteotomy. In addition, the finding of this paper are comparable to that of Sivertsen [23] in their study comparing the correction angle between Dugdale and Miniaci method found that both Intra- and inter-rater reliability was excellent for the correction angle with 0.992 and 0.991 and 0.988 and 0.987 respectively. So et al [24] ICC for medial proximal tibial angle MPTA is 0.844 (0.774–0.892).

Schroter et al [25] conducted an ICC comparison between two software, namely PreOPlan and mediCAD with ICC values of 0.993 (0.990-0.995) and 0.995 (0.992-0.996) respectively on the wedge angle. Elson et al. [19] in turn compared the results obtained on digital planning using the Miniaci method where the ICC values for interrater 0.980–0.986 and intra-rater 0.968–0.985, respectively.

## VI. CONCLUSION

Preoperative planning for HTO has proven useful in producing the best decision needs to be taken in the surgery. However, manual procedures become obsolete and take time. We have developed a new digital preoperative planning for HTO to assist the developer to assist surgeon in their task. The digital method undertakes the manual procedure hence to reduce the time for decision making and giving the more effective way to provide a solution.

Based on the testing that has been done shows that the existing software also has similar results to the new software. This makes the new software can be adopted to conduct testing for future osteotomy prenatal planning as well as provide added value such as post-surgical expectation display and planning that can be repeated using fully digital. This finding also contributes in medical field especially in the digital preoperative planning of HTO.

The principal finding of this study is that, the new software OsteoAid method showed excellent reliabilities and good consistency in preoperative planning. This proves that all hypotheses have failed to reject the null hypothesis meaning to accept the hypotheses. Consequently, it shows the reliability of each rater for all tested software is zero. Thus, the use of the OsteoAid enables direct measurement of the angle measurement with high reliability.

There were various flaws in this study. The clinical results of patients after surgery were not studied, but that was not the study's major goal. The other limitation was this software is focusing on the HTO only. The future study should expand to other practices in orthopedics. It also should enhance 3D medical images in future.

## ACKNOWLEDGMENT

This research project was conducted in collaboration with Prof Dr Abdul Halim Abdul Rashid from the Department of Orthopaedic and Traumatology, Medical Centre of University Kebangsaan Malaysia. University Grants GP-2019-K007341.

REFERENCES

- [1] C. Jin, E. K. Song, A. Santoso, P. S. Ingale, I. S. Choi, and J. K. Seon, "Survival and Risk Factor Analysis of Medial Open Wedge High Tibial Osteotomy for Unicompartement Knee Osteoarthritis," *Arthrosc. - J. Arthrosc. Relat. Surg.*, vol. 36, no. 2, pp. 535–543, 2020, doi: 10.1016/j.arthro.2019.08.040.
- [2] R. M. A. Raja Izaham, M. R. Abdul Kadir, A. H. Abdul Rashid, M. G. Hossain, and T. Kamarul, "Finite element analysis of Puddu and Tomofix plate fixation for open wedge high tibial osteotomy," *Injury*, vol. 43, no. 6, pp. 898–902, 2012, doi: 10.1016/j.injury.2011.12.006.
- [3] H. Kim, H. Lee, J. Shin, K. Park, S. Min, and H. Kyung, "Preoperative planning using the picture archiving and communication system technique in high tibial osteotomy," vol. 25, no. 1, pp. 1–6, 2017, doi: 10.1177/2309499016684701.
- [4] X. Liu, Z. Chen, Y. Gao, J. Zhang, and Z. Jin, "High Tibial Osteotomy: Review of Techniques and Biomechanics," *J. Healthc. Eng.*, vol. 2019, no. December 2018, 2019, doi: 10.1155/2019/8363128.
- [5] F. Gebhard et al., "Reliability of computer-assisted surgery as an intraoperative ruler in navigated high tibial osteotomy," *Arch Orthop Trauma Surg*, vol. 131, pp. 297–302, 2011, doi: 10.1007/s00402-010-1145-9.
- [6] B. Zampogna et al., "Assessing Lower Limb Alignment: Comparison of Standard Knee Xray vs Long Leg View," *Iowa Orthop. J.*, vol. 35, pp. 49–54, 2015, [Online]. Available: [http://www.ncbi.nlm.nih.gov/pubmed/26361444%0Ahttp://www.ncbi.nlm.nih.gov/pmc/articles/PMC4492139/pdf/IOJ\\_2015\\_49.pdf](http://www.ncbi.nlm.nih.gov/pubmed/26361444%0Ahttp://www.ncbi.nlm.nih.gov/pmc/articles/PMC4492139/pdf/IOJ_2015_49.pdf).
- [7] Q. L. H. T. T. Nguyen, P. T. Nguyen, V. D. B. Huynh, and L. T. Nguyen, "Application Chang's extent analysis method for ranking barriers in the e-learning model based on multi-stakeholder decision making," *Univers. J. Educ. Res.*, vol. 8, no. 5, pp. 1759–1766, 2020, doi: 10.13189/ujer.2020.080512.
- [8] C. A. S. Velando and E. G. C. Gutierrez, "2D/3D registration with rigid alignment of the pelvic bone for assisting in total hip arthroplasty preoperative planning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 5, pp. 681–688, 2020, doi: 10.14569/IJACSA.2020.0110583.
- [9] M. F. Alrifai, Z. H. Ahmed, A. S. Hameed, and M. L. Mutar, "Using Machine Learning Technologies to Classify and Predict Heart Disease," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 3, pp. 123–127, 2021, doi: 10.14569/IJACSA.2021.0120315.
- [10] A. Shapi, "Digital Preoperative Planning for Total Hip Replacement using Two Dimensional X-ray Imaging," *Int. J. Comput. Appl.*, vol. 17, no. 2, pp. 20–27, 2011.
- [11] N. Awang, R. Sulaiman, A. Shapi, M. F. M. A. Abdul Halim Abdul Rashid, and S. Osman, "A Comparative Study of Computer Aided System Preoperative Planning for High Tibial Osteotomy," *Springer Int. Publ. Switz.*, vol. LNCS 9429, pp. 189–198, 2015, doi: 10.1007/978-3-319-25939-0.
- [12] D. Paley, *Principles of Deformity Correction*. Maryland: Springer, 2003.
- [13] J. A. Fixsen, R. A. Hill, F. Grill, J. A. Fixsen, and R. A. Hill, *Leg Deformity and Length Discrepancy Part I: Classification and Management of Lower Limb Reduction Anomalies*. 2010.
- [14] P. Gupta, V. Gupta, B. Patil, and V. Verma, "Angular deformities of lower limb in children: Correction for whom, when and how?," *J. Clin. Orthop. Trauma*, vol. 11, no. 2, pp. 196–201, 2020, doi: 10.1016/j.jcot.2020.01.008.
- [15] K. Igarashi et al., "Distal Tibial Tuberosity Focal Dome Osteotomy Combined With Intra-Articular Condylar Osteotomy (Focal Dome Condylar Osteotomy) for Medial Osteoarthritis of the Knee Joint," *Arthrosc. Tech.*, vol. 9, no. 8, pp. e1079–e1086, 2020, doi: 10.1016/j.eats.2020.04.004.
- [16] P. Mazdarani, M. B. M. Nielsen, R. S. Gundersen, A. von Wenck, and J. E. Miles, "Geometric modelling of CORA-based levelling osteotomy in the dog," *Res. Vet. Sci.*, vol. 135, no. June 2020, pp. 127–133, 2021, doi: 10.1016/j.rvsc.2021.01.005.
- [17] J. E. Kim et al., "Difference of preoperative varus–valgus stress radiograph is effective for the correction accuracy in the preoperative planning during open-wedge high tibial osteotomy," *Knee Surgery, Sport. Traumatol. Arthrosc.*, vol. 29, no. 4, pp. 1035–1044, 2021, doi: 10.1007/s00167-020-06076-4.
- [18] J. Kim, H. Kim, and D. Lee, "Leg length change after opening wedge and closing wedge high tibial osteotomy: A meta- analysis," pp. 1–10, 2017.
- [19] D. W. Elson, T. G. Petheram, and M. J. Dawson, "High reliability in digital planning of medial opening wedge high tibial osteotomy, using Miniaci's method," *Knee Surgery, Sport. Traumatol. Arthrosc.*, vol. 23, no. 7, pp. 2041–2048, 2015, doi: 10.1007/s00167-014-2920-x.
- [20] J. Karlsson et al., *A Practical Guide to Research: Design, Execution, and Publication*, vol. 27, no. 4. Elsevier Inc., 2011.
- [21] J. Blackburn, A. Ansari, A. Porteous, and J. Murray, "Reliability of two techniques and training level of the observer in measuring the correction angle when planning a high tibial osteotomy," *Knee*, vol. 25, no. 1, pp. 130–134, 2018, doi: 10.1016/j.knee.2017.11.007.
- [22] S. Galal, "The Resolution Axis Method (RAM) for lengthening of the femur with or without associated frontal plane deformity (a new method)," *Strateg. Trauma Limb Reconstr.*, vol. 13, no. 2, pp. 109–118, 2018, doi: 10.1007/s11751-018-0312-3.
- [23] E. A. Sivertsen, J. Vik, A. S. V. Meland, and T. K. Nerhus, "The Dugdale planning method for high tibial osteotomies underestimates the correction angle compared to the Miniaci method," *Knee Surgery, Sport. Traumatol. Arthrosc.*, 2021, doi: 10.1007/s00167-021-06663-z.
- [24] S. Y. So, S. S. Lee, E. Y. Jung, J. H. Kim, and J. H. Wang, "Difference in joint line convergence angle between the supine and standing positions is the most important predictive factor of coronal correction error after medial opening wedge high tibial osteotomy," *Knee Surgery, Sport. Traumatol. Arthrosc.*, vol. 28, no. 5, pp. 1516–1525, 2020, doi: 10.1007/s00167-019-05555-7.
- [25] S. Schroter, C. Ihle, J. Mueller, P. Lobenhoffer, U. Stockle, and R. van Heerwaarden, "Digital planning of high tibial osteotomy . Interrater reliability by using two different software," vol. 21, pp. 189–196, 2013, doi: 10.1007/s00167-012-2114-3.

# Using Transfer Learning for Nutrient Deficiency Prediction and Classification in Tomato Plant

Vrunda Kusanur<sup>1</sup>

Research Scholar, Visvesvaraya Technological University  
Bengaluru, Karnataka, India

Dr. Veena S Chakravarthi<sup>2</sup>

Professor, Department of Electronics and Communication  
Engineering, BNMIT, Bengaluru, Karnataka, India

**Abstract**—Plants need nutrients to develop normally. The essential nutrients like carbon, oxygen, and hydrogen are obtained from sunlight, air, and water to prepare food and plant growth. For healthy growth, plants also need macronutrients such as Potassium, Calcium, Nitrogen, Sulphur, Magnesium, and Phosphorus in relatively great quantities. When a plant doesn't find necessary nutrients for its growth inadequate amount, deficiency of plant nutrients occur. Plants exhibit various symptoms to indicate the deficiency. Automatic identification and differentiation of these deficiencies are very important in the greenhouse environment. Deep Neural Networks are extremely efficient in image categorization problems. In this work, we used the part of the pre-trained deep learning model i.e. Transfer Learning model to detect the nutrient stress in the plant. We compared three different architectures including Inception-V3, ResNet50, and VGG16 with two classifiers: RF and SVM to improve, classification accuracy. A total of 880 images of Calcium and Magnesium deficiencies in the Tomato plant from the greenhouse were collected to form a dataset. For training, 704(80%) images are used and for testing, 176(20%) images are used to examine the model performance. Experimental results demonstrated that the largest accuracy of 99.14% has resulted for the VGG16 model with SVM classifier and 98.71% for Inception-V3 with Random Forest Classifier. For a batch size of 8 and epochs equal to 10, the Inception -V3 architecture attained the highest validation accuracy of 99.99% and the least validation loss of 0.0000384 on an average.

**Keywords**—Nutrient deficiency; plant nutrients; deep neural networks; transfer learning; random forest (RF); support vector machine (SVM)

## I. INTRODUCTION

A proper combination of nutrients is required for plants to live, develop and reproduce. So, plant analysis is a necessary tool that assists farmers by providing significant information about the nutritional description of the growing plant to obtain a better yield. Generally, plant analysis indicates the analysis of magnesium (Mg), sulphur (S), phosphorous (P), calcium (Ca), nitrogen (N), potassium (K), etc. Normally, plants show signs of being unhealthy when they suffer from undernutrition. For example, yellow around the edges of its leaves are a sign of magnesium deficiency. Yellow spots between the leaf veins and Blossom End Root denote the absence of calcium. Brown edges along the plant leaves indicate a deficiency of potassium. Yellow or pale green leaves imply the need for nitrogen [1]. These nutrient deficiency symptoms will help growers to identify the nutrient status of plants for a better crop yield. Manually diagnosing these deficiencies is a difficult task. So,

the key objective of this work is to automate the identification of nutrient deficiencies in plants using Convolutional Neural Networks (CNN).

Artificial Intelligence has numerous applications in multiple industries, healthcare, environment, finance, education, agriculture, etc. to solve complex problems and make our daily life more secure and fast.

G. Madhulatha et al. [2] proposed an automatic plant disease detection on the plant leaves to decrease crop loss and increase productivity. Plant diseases are predicted and classified with 96.50% accuracy based on visual symptoms using deep CNN. The authors used a dataset from the "Plant-Village" dataset for plant leaf diseases. The model was pre-trained using AlexNet. Muhammad Hammad Saleem et al. [3] developed three Deep Learning meta-architectures namely; Faster Region-based Convolutional Neural Network (RCNN), Single Shot MultiBoX Detector (SSD), and Region-based Fully Convolutional Networks (RFCN) to recognize plant disease and healthy leaves. All three models include a feature extractor and a base network. This research used Gradient Descent with its Momentum version, Adaptive Moment Estimation (Adam), and Root Mean Square Propagation (RMSProp) optimization algorithms to increase the performance of the Deep Learning meta-architectures. The authors examined that all the Deep Learning meta-architectures needed 126 epochs (200,000 iterations) for training convergence. When the SSD model was trained using Adam optimizer, the maximum means Average Precision (mAP) of 73.07% was obtained. Guan Wang et al. [4] suggested a deep learning model for control plant disease application. The authors used the apple leaf black rot images produced by the fungus Botryosphaeria obtuse from the PlantVillage dataset for disease severity classification. The highest overall accuracy of 90.4% was obtained for the VGG16 model. Sharada P. Mohanty et al. [5] established a smartphone-assisted application to detect the disease using a deep convolutional neural network. In this research, GoogLeNet architecture performs better and provides 99.35% accuracy as compared to AlexNet architecture. The presently available deep learning methods to identify the plant disease were reviewed by M. Nagaraju and Priyanka Chawla [6].

Many previous works have considered Image Recognition and Machine Learning models to classify the images into healthy and unhealthy images. However, most of these algorithms require image segmentation and feature extraction. But, from the many extracted features, it is difficult to judge

the important and dominant features for plant disease detection. Moreover, under difficult background circumstances, many techniques fail to successfully segment the leaf and will lead to unreliable deficiency recognition. So, image segmentation and feature extraction are still challenging tasks. Therefore, automatic plant disease detection and nutrient deficiency recognition are still challenging tasks. Recently, Convolutional Neural Network (CNN) is becoming the preferred scheme to overcome few challenges.

The main objective of this research is to diagnose nutrient deficiency in plants and take several measures like adjusting the pH value of water to achieve a quality yield, providing the right amount of fertilizer, etc. using deep learning models. For nutrient deficiency classification, we employed the Transfer Learning method, where pre-trained models are used as the entry point to develop the neural network models. In this research, we have used these models to predict Calcium (Ca) and Magnesium (Mg) deficiency in tomato crops grown under a greenhouse environment.

The key advantage of transfer learning is that instead of beginning the learning process from the scratch, the model commences from the characteristics that have been educated when resolving other problems which are analogous to the one being resolved. We have used three pre-trained models- InceptionV3, VGG16, and ResNet50 as a base model and SVM or Random Forest classifier on top of it to attain better results.

The rest of this paper is structured in the following fashion. Section II introduces the images collected to form the dataset of Ca and Mg deficiencies followed by related concepts. This section also presents Inception V3, ResNet50, and VGG16 architectures, and the proposed model to identify and classify the deficiencies. Section III dedicated to the evaluation, and the comparative analysis of results obtained in this experiment. In Section IV, the paper is summarized and future work is mentioned.

## II. MATERIALS AND METHODS

### A. Data Acquisition

Tomato plants were grown in a greenhouse of a size 10x4 sq.ft. to study and gather the dataset for lack of nutrients in tomato leaves and fruits. The calcium and magnesium deficiencies were induced for the plants in different stages and their images were captured from the camera for training and testing the performance of the model. The dataset was developed with two classes for classification and prediction: Calcium and Magnesium. Altogether, there are 880 images in the dataset. Out of 880 images, 704 (80%) images are for training the model, and 176 (20%) images are for testing the model. There are 374 calcium deficiency and 330 magnesium deficiency images in the training dataset. Further, out of 176 testing images, 94 images are of calcium, and the remaining 82 images are of magnesium deficiency images. To enhance the dataset, the data augmentation methods including image resizing, flipping, random rotation, shearing, etc., are applied. The details of calcium and magnesium nutrient deficiency symptoms in tomatoes are presented in Table I. 256 x 256

pixels is the size of all the resized images. These sample images are input to the convolutional neural network for training the model. The trained model is applied for the class prediction of unseen images. These phases are explained in detail in the following sections. Machine learning algorithms including SVM, Decision-Tree and, RF are excellent in resolving classification problems [10]. However, they go wrong in extracting the proper features from the image. Alternatively, Convolutional Neural Networks receives the raw pixel of the images directly as inputs instead of extracting certain features manually [12-14]. CNN learns how to take out these features from the actual image.

### B. Convolutional Neural Networks

CNN's are a class of Deep Neural Networks that can identify and categorize specific features in images and are generally used for examining visual images. Significantly, CNN can yield good results than the traditional feature extraction algorithms in plant disease diagnosis [15-18]. In CNN, the filters are learnable. A classic CNN consists of two components: The Convolution Block and the Fully Connected block, which are detailed as follows.

TABLE I. CALCIUM AND MAGNESIUM NUTRIENT DEFICIENCY SYMPTOMS IN TOMATO

Nutrients	Description	Deficiency Symptoms on Leaf/ Fruit
Calcium (Ca)	Young leaves curl inwards and cause dry decaying areas at Blossom End of the fruit (BER) in Tomatoes.	
Magnesium (Mg)	Interveinal chlorosis (Veins of Leaf remains green whereas the areas between the leaves go yellow). Elder leaves drip their color excluding in the veins. It does not affect the fruit.	

### C. Convolutional Neural Networks

CNN's are a class of Deep Neural Networks that can identify and categorize specific features in images and are generally used for examining visual images. Significantly, CNN can yield good results than the traditional feature extraction algorithms in plant disease diagnosis [9, 11]. In CNN, the filters are learnable. A classic CNN consists of two components: The Convolution Block and the Fully Connected block, which are detailed as follows.

1) *Convolution block*: The convolution block contains the Convolution Layer and the Pooling Layer. In this block, the task of feature extraction is accomplished. The convolutional layer produces the feature maps or activation maps by applying filters to input images using the ReLU activation function. The ReLU function returns  $x$  for all the values of  $x > 0$ , and returns 0 for all values of  $x \leq 0$  and is given in equation 1.

$$F(x) = \max(0, x) \quad (1)$$

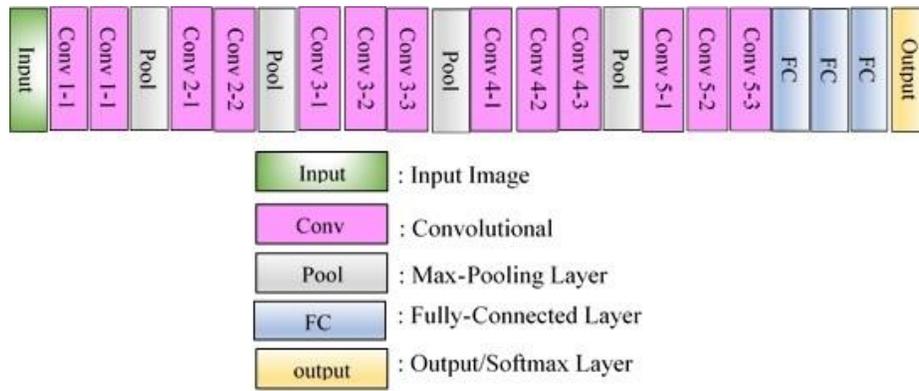


Fig. 1. VGG16 Architecture

Fig. 1. VGG16 Architecture.

The convolutional layer uses filters kernels to recognize various features like edges, horizontal lines, vertical lines, etc., in an image. To extract more composite and thoughtful features, the same size convolution kernel is used again and again multiple times. The pooling layer is enforced next to a convolution layer in which a down sampling operation is performed on a convolved feature to scale down the number of dimensions of the feature map. Commonly, the average and maximum values are selected by the pooling layer for this task.

2) *Fully connected block*: The Fully Connected block comprises of fully connected simple neural network design which does classification depending on convolutional block inputs. Convolutional Neural Network has one or more fully connected layers at the end of it. At the end of the fully connected layer, there is a softmax activation function whose output is a probability (from 0 to 1) for every classification label.

#### D. VGG16 Model Architecture

VGG is a pre-trained model and has 138 Million parameters. VGG is trained over 14 million images belonging to 1000 classes and learned to detect generic features from images. There are 16 and 19 weight layers in the network for VGG-16 and VGG-19 respectively.

This research work uses VGG-16 as the base model and altered it to create a different network. As VGG16 attains 92.7% test accuracy in ImageNet, and because of its high performance, the pre-trained weights are retained and only the top three Fully Connected Layers or Dense Layers are modified to fine-tune the neural network. In this work, the features extracted from VGG16 are given as input to RF or SVM Classifiers to reduce the training time and increase the classification accuracy. Fig. 1 describes the VGG16 scheme. All the resized images in this model are of fixed size 244x244.

The VGG16 model used NVIDIA Titan Black GPUs and was trained for weeks. The VGG16 model can categorise the images into 1000 classes. The VGG model handles the input image and yields the vector of 2 values.  $y^\wedge$  denotes the probability of classification for the corresponding class and is given by equation 2.

$$y^\wedge = \begin{bmatrix} y_0^\wedge \\ y_1^\wedge \end{bmatrix} \quad (2)$$

Where,  $y_0^\wedge$  represents the probability with which class 0 (Ca) is predicted and  $y_1^\wedge$  represents the probability with which class 1(Mg) is predicted. The RGB image of constant size 224x224 is the input to the conv1 layer. The image is moved through several convolutional layers. Each layer uses a small 3x3 or 1x1 filter. Five max-pooling layers perform spatial pooling. A 2x2 pixel window with a stride of 2 is used to implement max-pooling. There are three Fully-Connected (FC) layers where there are 4096 channels in each of the first two layers and the third layer comprises 1000 channels. The softmax layer is the terminating layer. All networks have a similar configuration of the fully connected layers. A non-linear ReLu activation function is used by all hidden layers.

#### E. Inception-V3 Model Architecture

Inception-V3 is the most generally used CNN architecture and achieved more than 78.1% accuracy for image prediction on the ImageNet dataset. The model comprises Convolution Layers, Max pooling Layers, Average pooling Layers, Concat Layers, Dropout Layers, and Fully Connected Layers. In Inception V3, the resized images are of size 299x299x3 pixels. The structure of Inception-V3 is analogous to Inception-V2 with few modifications including Label Smoothing Regularization, Batch normalization, Auxiliary Classifier. Use of Factorized 7x7 convolutions. Inception-V3 is a CNN with 48 layers in depth. The inception model is a concatenation of parallel convolution layers with 1x1, 3x3, 5x5, etc. sized filters and a max pooling layers of 3x3 matrix. The error rate improved to 0.2 % by adding label smoothing in Inception-V3 architecture. Fig. 2 describes the Inception-V3 scheme.

Inception-V3 model used RMSProp optimizer that offered significant results in connection with accuracy and time to achieve it. RMSProp is fixed as a default optimizer. The update dynamics in the Inception-V3 model are given by equation 2 and equation 3.

$$g_{k+1}^{-2} = \alpha g_k^{-2} + (1 - \alpha) g_k^2 \quad (3)$$

$$w_{k+1} = \beta w_k + \frac{\eta}{\sqrt{g_{k+1}^{-2} + \epsilon}} \nabla f(w_k) \quad (4)$$

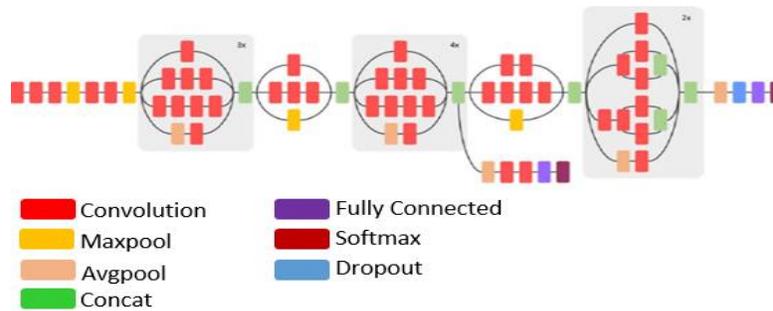


Fig. 2. Inception V3 Architecture.

Where,  $g_k$  is gradient descent at time  $k$ ,  $g_{k+1}$  is gradient descent at time  $k+1$ ,  $w_k$  is the weight at time  $k$ ,  $w_{k+1}$  is the updated weight at the time  $k+1$ , ' $\alpha$ ' is the step size, ' $\beta$ ' is known as momentum and ' $\epsilon$ ' is small positive constant to avoid division by zero in implementation, ' $\nabla$ ' is the gradient, which is taken of  $f$ , ' $\eta$ ' is learning rate.

In RMSProp, the parameters ' $\alpha$ ', ' $\beta$ ', and ' $\epsilon$ ' are set as decay  $\alpha = 0.9$ , momentum  $\beta = 0.9$ , and  $\epsilon = 1.0$

#### F. ResNet50 Model Architecture

ResNet (Residual Network) is presented by Kaiming He, Xiangyu Zhang, Shaoqing Ren, and Jian Sun in 2015 in their paper "Deep Residual Learning for Image Recognition". The development of ResNet improved the problem of training deep neural networks. The simple element in ResNet is as depicted in Fig. 3. In the Residual network, there is a straight connection called 'skip connection' which skips some in between layers.

The 'skip connection' is used to resolve the vanishing gradient problem and to learn the identity functions. The output  $H(X)$  with the introduction of skip connection is given by the equation  $H(X) = F(X) + X$ . Table III shows the elements of the ResNet50 model. The ResNet model was tested on the ImageNet set and attained a 20.47% top-1 error rate also 5.25% top-5 error rate.

The proposed model used these transfer learning techniques for feature extraction and altered their basic structures by adding Random Forest or SVM classifiers to improve the classification ability of the models as illustrated in Fig. 4.

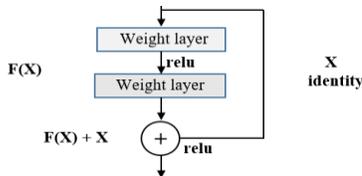


Fig. 3. A Basic Residual Network.

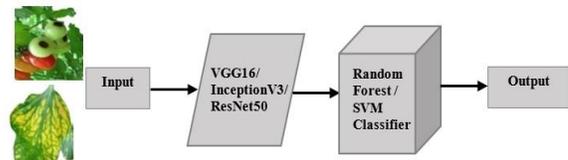


Fig. 4. Proposed Model.

### III. EXPERIMENTAL RESULTS AND ANALYSIS

In this work, image pre-processing techniques, data augmentation, and implementation of Convolutional Neural Network algorithms were conducted using Jupyter notebook(Python 3.9), Keras API, OpenCV library, Matplotlib visualization library, OS module, glob module, and so on. The hardware specifications in this experiment to train and test our model includes Intel(R) Core (TM) i7-4210U CPU, 4.00 GB RAM. In this experiment, the CNN is developed using InceptionV3, ResNet50, and VGG16 Transfer Learning Models.

All three models used pre-trained weights from the ImageNet dataset by eliminating the upper layer and redefining a fresh fully connected Softmax layer with 2 classes for classification [7, 8]. In this experiment, the batch size was fixed to 8 and the number of epochs was set to 10 with Adam optimizer. The features extracted from the Transfer Learning technique were used by SVM and Random-Forest classifiers. 80% of the total images were used to form a training dataset to train the model and 20% were used to form a testing dataset. For the Inception-V3 model, all the images were resized to 299x299x3, the input image size for ResNet-50 and VGG16 was 224x224. Inception V3 attained the validation accuracy of 99.99 % and the validation loss of 0.0000384 as depicted in Table II out of the three models.

The accuracy and loss obtained from three different Transfer Learning models are presented in Fig. 5 to 7.

TABLE II. ACCURACY AND LOSS OF DIFFERENT TRANSFER LEARNING MODELS AFTER 5 AND 10 EPOCHS

Transfer Learning Model	Training Accuracy (%)		Validation Accuracy (%)		Training Loss		Validation Loss	
	5 Epochs	10 Epochs	5 Epochs	10 Epochs	5 Epochs	10 Epochs	5 Epochs	10 Epochs
Inception V3	99.23	100	98	99.99	0.1364	0.000264	0.3685	0.0000384
ResNet-50	89.40	82.28	87.00	82.10	0.2632	0.5541	0.2568	0.4783
VGG16	100	100	98.86	98.86	0.000001	0	0.3572	0.2220

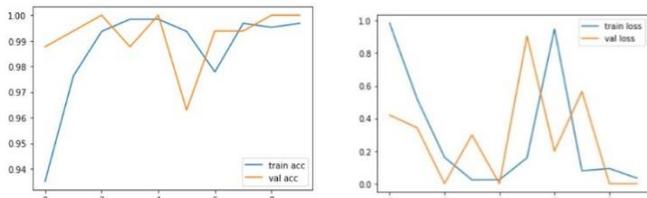


Fig. 5. Inception V3: Accuracy and Loss Model.

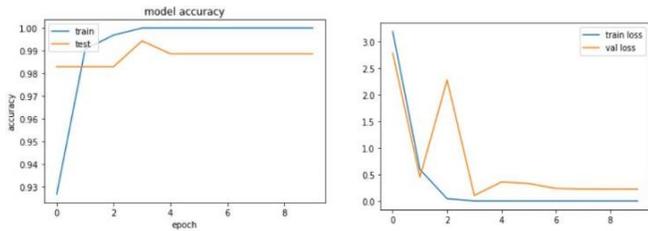


Fig. 6. ResNet50: Accuracy and Loss Model.

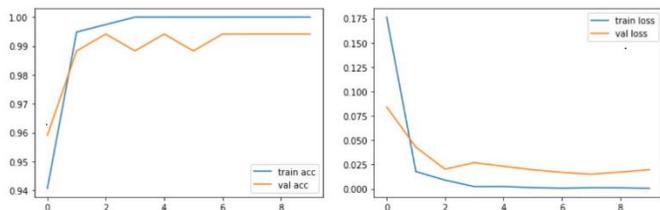


Fig. 7. VGG16: Accuracy and Loss Model.

Fig. 8 to 10 represents the confusion matrix of plant nutrient deficiencies identification using three Transfer Learning models with RF and SVM classifiers. The classification accuracy chart of plant nutrient deficiency identification in tomato plants using Transfer Learning models with Random Forest and SVM classifiers is presented in Fig. 11. It is noticed from the chart that the largest accuracy of 99.14% has resulted using the VGG16 model with SVM classifier and 98.71% for Inception-V3 with Random Forest Classifier.

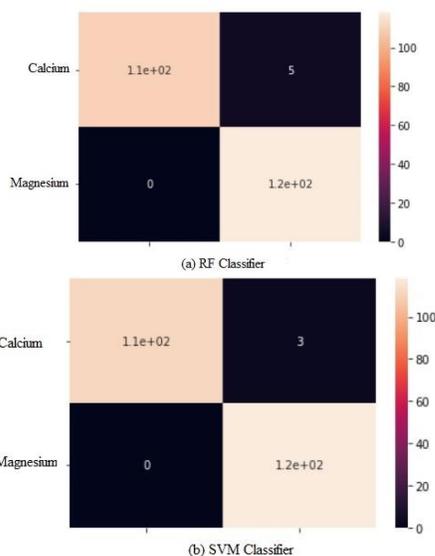


Fig. 8. Confusion Matrix using Inception V3.

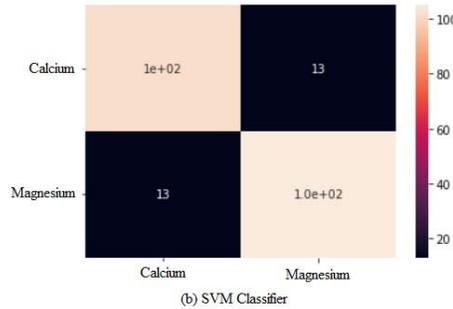
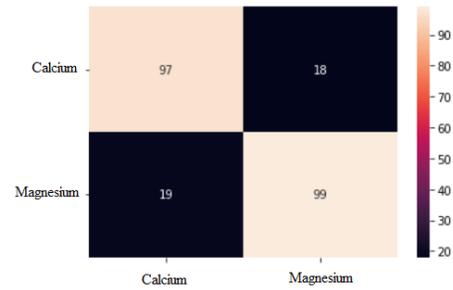


Fig. 9. Confusion Matrix using ResNet50.

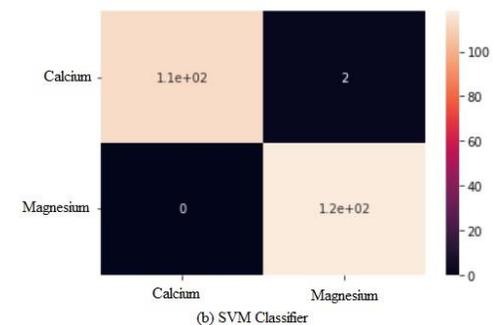
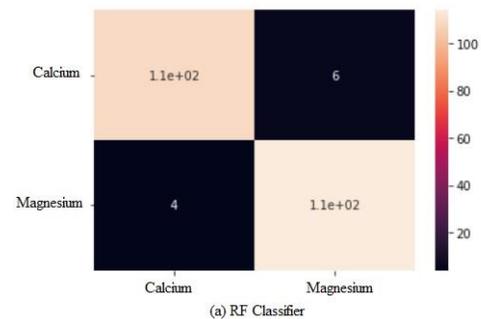


Fig. 10. Confusion Matrix using VGG16.

The results of lack of nutrients predicted from three different models with RF and SVM classifiers on few samples are displayed in Fig. 12. From Table II, it can be observed that almost calcium and magnesium deficiencies were detected properly by all three Transfer Learning models with RF and SVM classifiers. The average classification accuracy is high for InceptionV3 and VGG16 models in various experiments. These models could be extended for the identification of other nutrient deficiencies.

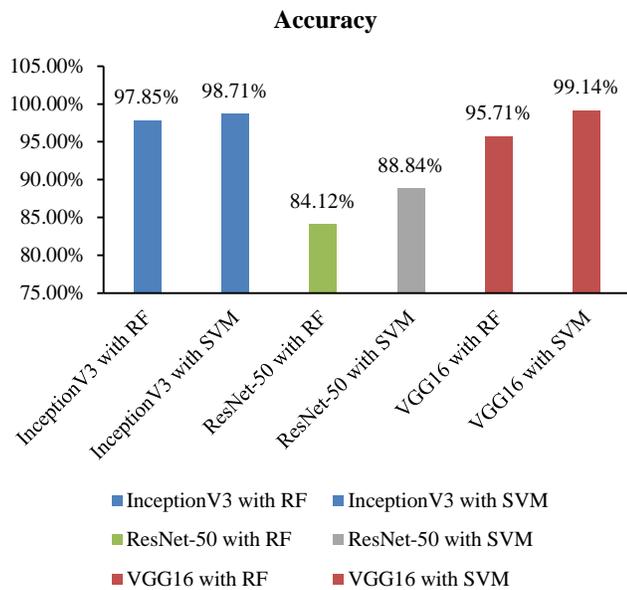


Fig. 11. Comparison Efficiency for Transfer Learning Models with RF and SVM Classifiers.

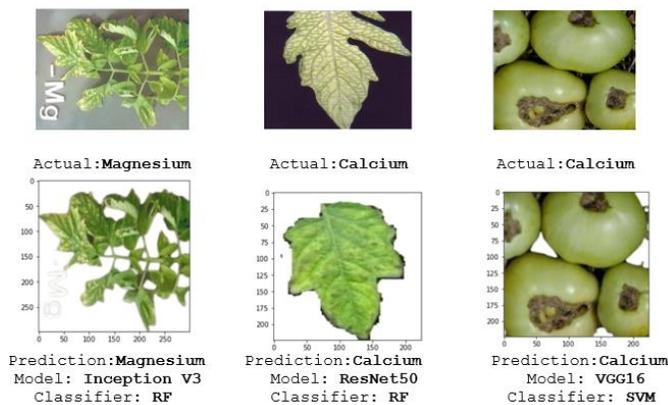


Fig. 12. The Predicted Samples of Plant Nutrient Deficiency Images.

#### IV. CONCLUSION

Quick identification of plant nutrient deficiency is necessary for a greenhouse environment. Manual inspection of these deficiency symptoms in a large greenhouse requires more effort. Consequently, automated plant nutrient deficiency diagnosis is required in greenhouse technology. With technology growth, a CNN using Transfer Learning models such as Inception V3, ResNet50, and VGG16 were proposed along with Random Forest (RF) and SVM classifiers to improve the efficiency. These models are pre-trained on ImageNet dataset and are modified for our tomato dataset with images of calcium and magnesium deficiencies in this research. On average, out of all the three Transfer Learning techniques, Inception V3 attained the highest validation accuracy of 99.99 % and the least validation loss of 0.0000384 for 10 epochs. Further, when the experiment was conducted for Random Forest (RF) and SVM classifiers, results show that the largest accuracy of 99.14% has resulted using the VGG16 model with

SVM classifier and 98.71% for InceptionV3 with Random Forest Classifier.

To control these plant nutrient deficiencies, the tomato greenhouse environmental factors such as humidity, temperature, pH, and soil moisture need to be monitored to find out the right quantity of fertilizer to be applied. Hence, in the future, this work can be improved by monitoring the greenhouse parameters by Wireless Sensor Network (WSN) to apply fertilizer precisely in a greenhouse.

#### ACKNOWLEDGMENT

We extend our heartfelt gratitude to the management of the BNM Institute of Technology, Bengaluru for providing us with all the necessary sources to accomplish this work and all the support to do the subsequent publications. We are also grateful to Visvesvaraya Technological University for giving us an appropriate platform to complete this research.

#### REFERENCES

- [1] Gaganjot Kaur, "Automated Nutrient Deficiency Detection In Plants: A Review", *Palarch's Journal of Archaeology Of Egypt/Egyptology*, vol. 17, no. 6, pp. 5894-5901.
- [2] G. Madhulatha, O. Ramadevi, "Recognition of Plant Diseases using Convolutional Neural Network", *International Conference on IoT in Social, Mobile, Analytics and Cloud (I-SMAC)*, 2020, ISBN: 978-1-7281-5464-0, DOI: 10.1109/I-SMAC49090.2020.9243422.
- [3] Muhammad Hammad Saleem, Sapna Khanchi, Johan Potgieter and Khalid Mahmood Arif, "Image-Based Plant Disease Identification by Deep Learning Meta-Architectures", *Plants* 2020,9,1451, MDPI Publication, DOI: 10.3390/plants9111451.
- [4] Guan Wang, Yu Sun, and Jianxin Wang, "Automatic Image-Based Plant Disease Severity Estimation Using Deep Learning", *Computational Intelligence and Neuroscience*, Volume 2017, Article ID 2917536, <https://doi.org/10.1155/2017/2917536>.
- [5] Sharada P. Mohanty, David P. Hughes, and Marcel Salathe, "Using Deep Learning for Image Based Plant Disease Detection", *Frontiers in Plant Science*, 7, 1419, 2016.
- [6] M. Nagaraju, Priyanka Chawla, "Systematic review of deep learning techniques in plant disease detection", *Int J Syst Assur Engg Manag.* 11(3), 547-560, 2020.
- [7] Nafees Akhter Farooqui and Ritika, "An Identification and Detection Process for Leaves Disease of Wheat Using Advance Machine Learning Techniques", *Bioscience Biotech Research Communication*, vol. 12, no.4, pp. 1081-1091, 2019, DOI: 10.21786/bbrc/12.4/31.
- [8] Zhe Xu, Xi Guo, Anfan Zhu, Xiaolin He, Xiaomin Zhao, Yi Han, and Roshan Subedi, "Using Deep Convolutional Neural Networks for Image- Based Diagnosis of Nutrient Deficiencies in Rice", *Computational Intelligence and Neuroscience*, Hindawi Publications, vol. 2020, 12 pages, DOI: 10.1155/2020/7307252.
- [9] Shima Ramesh, Mr. Ramachandra Hebbbar, Niveditha M, Pooja R, Prasad N, Shashank N, Mr. P V Vinod, "Plant Disease Detection Using Machine Learning", *International Conference on Design Innovations for 3Cs Compute*, 2018, ISBN: 978-1-5386-7523-6, DOI: 10.1109/ICD13C.2018.00017.
- [10] Jayme Garcia Anal Barbedo, "Detection of nutrition deficiencies in plants using proximal images and machine learning: A review", *Computers and Electronics in Agriculture*, Elsevier Publications, vol. 162, pp. 482-492, 2019, DOI: <https://doi.org/10.1016/j.compag.2019.04.035>.
- [11] Aravind Krishnaswamy Rangarajan, Raja Purushothaman, Anirudh Ramesh, "Tomato crop disease classification using pre-trained deep learning algorithms", *International Conference on Robotics and Smart Manufacturing (RoSMa2018)*, 2018, pp. 1040-1047, DOI: 10.1016/j.procs.2018.07.070.
- [12] Yan Guo, Jin Zhang, Chengxin Yin, Xiaonan Hu, Yo Zou, Zhipeng Xue, Wei Wang, "Plant Disease Identification Based on Deep Learning

- Algorithm in Smart Farming”, *Discrete Dynamics in Nature and Society*, vol.2020, no.7, pp.1-11, 2020. DOI: 10.1155/2020/2479172.
- [13] Lili Ayu Wulandhari, Alexander Agung Santoso Gunawan, Aie Qurania, Prihastuti Harsani, Triastinurmiatingsih, Ferdy Tarawan, and Riska Fauzia Hermawan, “Plant Nutrient Deficiency Detection Using Deep Convolutional Neural Network”, *ICIC International Conference, ICIC Express Letters*, pp. 971-977, vol. 13, no. 10, 2019.
- [14] G.Chu, “How to use transfer learning and fine-tuning in keras and tensorflow to build an image recognition system and classify (almost) any object”, *Deep Learning Sandbox*, 2017.
- [15] A. M. G. J. Hanson, A. Joy, and J. Francis, “Plant leaf disease detection using deep learning and convolutional neural network”, *International Journal of Engineering Science*, vol. 7, no.3, pp.5324-5328, 2017.
- [16] G.L. Grinblat, L.C. Uzal, M.G. Larese and P. M. Granitto “Deep learning for plant identification using vein morphological patterns”, *Computers and Electronics in Agriculture*, vol.127, pp. 418-424, 2016.
- [17] K. P. Ferentinos, “Deep learning models for plant disease detection and diagnosis”, *Computers and Electronics in Agriculture*, vol. 145, pp.311-318, 2018.
- [18] D. Story, M. Kacira, C. Kubota, A. Akoglu and L. An, Lettuce calcium deficiency detection with machine vision computed plant features in controlled environments, *Computers and Electronics in Agriculture*, vol. 74, no.2, pp. 238-243, 2010.

# A New Protection Scheme for Biometric Templates based on Random Projection and CDMA Principle

Ayoub Lahmidi<sup>1</sup>, Khalid Minaoui<sup>2</sup>, Mohammed Rziza<sup>4</sup>  
LRIT Laboratory, Associated unit to CNRST (URAC29),  
IT Rabat Center Faculty of Sciences in Rabat,  
Mohammed V University, Rabat, Morocco

Chouaib Moujahdi<sup>3</sup>  
Scientific Institute  
Mohammed V University  
Rabat, Morocco

**Abstract**—Although biometric technologies have revolutionized the world of communication and dematerialized exchanges, authentication by biometrics still has many limitations, particularly in terms of privacy concerns, due to the various potential threats to which biometric templates are subject. The existence of these vulnerabilities has created an enormous need for biometric data protection. Indeed, several protection schemes have been proposed, which are normally supposed to offer certain guarantees, including the confidentiality of the collected personal data and the reliability of the recognition system. The challenge for all these techniques is to achieve a trade-off between performance accuracy and robustness against vulnerabilities, which is not always obvious. In this paper, we propose a theoretical protection model dedicated to biometric authentication systems. The objective is to ensure a high level of security for the stored reference data in such a way that it complies with the non-invertibility and revocability properties. The main idea is to incorporate a discretization tool, namely the spread spectrum technology and in particular the Code Division Multiple Access (CDMA), into a biometric system based on Random Projection. We introduce and demonstrate the proposed scheme as a non-invertible transform, while proving its effectiveness and ability to meet the requirements of revocability and unlinkability.

**Keywords**—Biometric template; security; authentication; CDMA; random projection

## I. INTRODUCTION

In a society where the risk of fraud continues to increase, the security of individuals within authentication systems has become a major concern. Despite the development in this sector, which has experienced a qualitative leap in terms of surveillance and access control, the traditional authentication systems, namely those based on knowledge (use of passwords) or possession (use of badges and keys) are ineffective against attacks of fraud and identity theft. Over the years, this kind of system has shown great weaknesses because of its inability to differentiate between an authorized person and an impostor who fraudulently acquires knowledge of the authorized person. Thus, the use of an authentication system that was both efficient and secure was essential, hence the emergence of biometric authentication.

In just a few years, biometrics has become the only way for authentication to guarantee rigorous access control since it is based primarily on the morphological and behavioral aspects specific to each person. Indeed, biometric systems exploit the physical characteristics (such as fingerprints, face, iris, etc.) or the behavioral aspects (such as voice, writing, the rhythm of typing on a keyboard, etc.) to construct an identity representing

an individual. Commonly called modalities, these biometric identifiers are often universal, unique to each person, and permanent in time [1]. Moreover, they ensure great robustness since it is very difficult for them to be lost, forgotten, stolen, copied, or falsified. The main objective of biometrics is to provide a more secure alternative to traditional access control systems, in the sense that it avoids the use of a large number of complex passwords, concerns about loss, theft and other falsifications of keys [2].

Although biometric authentication systems provide a much higher level of security compared to traditional systems, they are not safe from tampering. The use of this kind of system has given rise to new challenges related to the protection of biometric data [3]. Biometric information is generally considered sensitive since it is specific to each individual, and through which it can identify the owner. The inappropriate use of biometrics may involve risks to respect for fundamental rights and freedoms. Some risks of privacy violation are presented as follows:

- **Absence of secrecy:** Biometric data can expose very sensitive information, simply because the data are publicly available, so they can serve as a basis for unjustified discrimination.
- **Traceability:** the tracking and monitoring of an individual identified by the same biometric data across different databases, to perform profiling of the user.
- **Irrevocability:** In case of a compromise of the reference biometric template, it is impossible to revoke it because of its uniqueness.
- **Function creep / Misuse:** extending a specific use of the biometric identifier for another unintended or unauthorized use.

The issue of preserving biometric data deserves special attention to ensure respect for privacy when using biometric data. It should be noted that despite the advantage of biometric features being virtually impossible to steal, and difficult to guess by a tier, biometric systems are still vulnerable to attacks that target this kind of system [4]. Indeed, any component of the biometric system may be susceptible to a specific attack: the sensor, the feature extractor, the biometric reference templates stored and the final decision [5, 6]. The storage and security of reference data remain among the most crucial issues for a biometric system, as it can lead to serious security and invasion problems compared to other modules such as:

- The handling sensitive information.
- The regeneration of the original biometrics from the stored template.
- The construction of a falsified biometric sample.
- The secondary use of biometric information (surveillance, discrimination, etc.).
- The inability to revoke the biometric identifier when identity theft occurred.

These tasks require imperative attention, especially in the absence and necessity of an effective protection mechanism based on biometric templates. This has undoubtedly motivated us to multiply our thoughts on this point. The challenge is to design, implement and use a cancellable biometric system that improves authentication services without unduly compromising privacy.

Each protection approach for biometric templates must be designed with strong security analysis while taking into account the scenarios where the risk of fraud threatens the stored templates, and must also offer the possibility of revoking a biometric data set in the case of interception [7]. As specified by Jain et al. [3], template protection techniques are generally divided into two families: (i) Feature Transformation and (ii) Biometric Cryptosystem. The common feature of these methods is that they do not directly store the raw biometric data in databases, but rather they are either stored on an external medium or stored after an alteration due to a transformation function.

The principle of feature transformation approach [3, 8] consists in transforming the original biometric template  $X$  by using a function  $\mathfrak{F}$  which depends on a random data  $K$ . This specific information that should normally be secret is assigned to each legitimate user of the system. Thereafter, only the transformed template  $\mathfrak{F}(X, K)$  will be stored. At authentication, the query features  $X'$  will be transformed in the same way using the same transformation function  $\mathfrak{F}$ , then is directly matched with the reference template. Authentication will succeed if  $\mathfrak{F}(X', K)$  is sufficiently close to  $\mathfrak{F}(X, K)$  using some measures of similarity. To guarantee the notion of revocability in case of compromise of the transformed data, it is sufficient to change the parameters of the transformation function, and this is done by directly replacing the user key  $K$ , the reason for which biometric transformations generally use secret data in addition to the original biometric data [9, 10]. The choice of the transformation function remains the paramount element in the design of a protection approach belonging to this category. The function used can be either invertible in case of *Salting*, where security is relative to the knowledge of the transformation parameters [11], or is non-invertible when a one-way function is applied to the template [12, 13], in this case, it is computationally infeasible to reconstruct the original template, even if the transformation parameters are known.

Biometric cryptosystems [14, 15] provide the means to adapt cryptographic protocols to biometric data which are very sensitive and intrinsically noisy. The use of this kind of system consists either in securing the cryptographic keys using the biometric features or else indirectly generating cryptographic

keys from biometric features. They are also based on user-linked help data extracted from the biometric feature vector, which is needed during matching to extract the cryptographic key from the query biometric features. The helper data is public information that should not, in any case, reveal any significant information about the original biometric template. Biometric cryptosystems in their turns can be classified into key generation schemes, where binary keys are directly created from the acquired biometrics, and key binding schemes, which store information obtained by combining biometric data with randomly generated keys.

All evoked protection schemes have their advantages and limitations in terms of performance, accuracy, and robustness, but generally do not yet respond effectively to all desired requirements. The difficulty is that the transformation is in most cases entirely or partially invertible. Moreover, the desired criterion of revocability is not obvious to achieve without creating other risks. This is why we are motivated to design a generic transformation, in which the protected reference templates will be easy to revoke, difficult to reverse, and will not degrade performance. In this paper, we present a demonstration of a new protection model for reference templates by adapting the security aspect of a multiplexing technique defined as spread spectrum called *Code Division Multiple Access (CDMA)* within a system based on random projection. The proposal aims to verify and prove the identity of an individual only through its provided identifier while ensuring agreement with the properties of revocability, unlinkability, and non-invertibility. This paper is organized as follows. Section 2 presents related works. Section 3 is devoted to preliminary knowledge. Section 4 describes in detail the steps required to build the templates. Analysis and discussion of the revocability, diversity, and non-invertibility requirements produced by our proposal are given in Section 5. Finally, Section 6 is dedicated to the conclusion and future work.

## II. RELATED WORK

In biometric protection schemes, privacy preservation is related to the protection of the biometric templates. Ideally, as defined in several references [16], these schemes are designed to meet the requirements of non-invertibility, unlinkability, and revocability. Among the solutions that have been proposed by the research community to further protect the biometric templates, we can quote:

Ratha et al. [17] have proposed an interesting solution. The main idea is to apply geometric transformations on the fingerprint minutiae representation. Three types of transformations have been tested: Cartesian, polar and functional. This solution offers great security, as it is difficult to recover the original minutiae representation from the transformed template. However, these transformations increase the rate of intra-class variations in the protected representation, which considerably degrades the performance.

Tulyakov et al. [18] made use of symmetric hash functions as means of protecting fingerprint templates. The hash functions were constructed from the minutiae locations, considering the random shifting of the minutiae during the acquisition phase. The security of the generated templates is improved in [19] using a combination of various hash functions. How-

ever, it seems that the enhanced approach also suffered from computational complexity.

Wang and Hu [20], proposed a non-invertible transformation that can be applied to vectors derived from pair-minutiae. The proposal is an infinite-to-one mapping approach which is able to generate revocable templates. The performance of the system is very promising except that the consistency of the user key matrix leads to certain storage problems.

Moujahdi et al. [21] have developed a protected fingerprint representation that relies on the distances between fingerprint global features (Singular points) and all other fingerprint minutiae. The principal is to build special spiral curves, which will represent the final protected template rather than the features of minutiae. The accuracy performance is supposed to be maintained, however, The risk is that when a fingerprint template is compromised, it may reveal the distances used to generate the protected template.

There are a variety of other methods in this context, many of which are recent [22, 23].

### III. PRELIMINARY KNOWLEDGE

In this section, we focus on the main pillars on which our approach is based. For this, we will detail both *Random projection* and *CDMA*.

#### A. Random Projection

*Random Projection* is a technique that allows in a way to hide data in a certain space, it is considered in several works [24, 25, 26] as one of the most secure transformations concerning biometric template protection [27], as it ensures unlinkability and revocability. The principle of *Random projection* is to project a data vector  $X \in \mathbb{R}^n$  onto a random matrix  $R$ , to generate a vector  $M \in \mathbb{R}^m$  of reduced dimension  $m < n$  (from the product  $M = RX$ ). In biometry, the utility of such a projection depends on whether the distances between the different feature vectors of the same user will be preserved or not. For that purpose, S. Kaski [28] has proved that if the matrix  $R$  is orthonormal then the similarity between vectors is preserved, and therefore the matrix  $R$  becomes a basis of projection. To get an orthonormal matrix, we have to go through the Gram-Schmidt process [29], which requires that the set of randomly generated vectors must be linearly independent.

According to the literature, the *Random projection* was always a basis for many approaches that deal with biometric template protection, specifically *BioHashing* [11] and *BioPhasor* [12] approaches. The use of such a technique was to produce transformed biometric data that may be used for authentication purposes, given that it provides an impressive diversification effect for biometric templates protection. Moreover, through the *Random projection*, we can also reinforce the property of non-invertibility using quantization. This step consists in transforming the result of the projection  $W = (w_1, \dots, w_m)$  to a vector with binary values, by using a one-way transformation such that the resulting transformed biometric data cannot be used to reveal the original biometric data. However, the quantization requires the definition of a threshold  $\tau_b$  for the

computation of the resulting vector  $B = (b_1, \dots, b_m)$ , from the following formula:

$$b_i = \begin{cases} 0 & \text{if } w_i \leq \tau_b \\ 1 & \text{if } w_i > \tau_b \end{cases} \quad (1)$$

Generally, the threshold  $\tau_b$  is chosen equal to zero as the results of the projection have the same probability of being negative or positive.

#### B. Code Division Multiple Access (CDMA)

*CDMA* is a multiplexing technique that is widely used in the radiofrequency domain, where it provides multiple access and resource sharing that is both flexible and secure [30]. This method of access is derived from the spread transmissions used in the context of military transmissions for many years, where their objective was to resist at best narrow-band interferers and to carry out discrete transmissions. Subsequently, this technique has seen a surprising emergence and a great evolution over the following years [31].

The principle of *CDMA* consists in transmitting a set of messages coming from several transmitters simultaneously on the same physical medium. On receiving, each recipient collects the received data and then tries to retrieve only the message originating from his corresponding transmitter, notably through a code that was allocated to him at the beginning of the communication. The use of spreading sequences as codes provides a way of distinguishing between the different given users. This makes the transmission less vulnerable to selective fluctuations in frequencies, and as well as a secure transmission [32]. This results in better management of available resources. It was thus stressed that the *CDMA* technique based on the use of orthogonal spreading sequences, was theoretically very satisfactory so that the different trains emitted by the users do not interfere with one another [30]. The generation of orthogonal codes is such a crucial step for resistance against interferences with multiple users. According to [33], there are two important properties of spreading sequences that must be respected: autocorrelation and cross-correlation. The autocorrelation property refers to the correlation between time-shifted versions of the same code while cross-correlation concerns if the codes which are used are completely orthogonal or not, if it was not the case, the different users are interferers to each other, hence the near-far problem appears. There are several code expansion techniques to generate orthogonal codes. Probably Hadamard transform [34] is the best-known technique. According to our reflection, we will adopt the same strategy as the *CDMA* by multiplexing all the reference templates in the same instance. During the authentication, the code corresponding to the user is calculated and then used to extract the specific reference template to perform the matching. We discuss the approach in detail in the following section.

### IV. THE PROPOSED APPROACH

In this section, we introduce a new protection scheme for the biometric template, which consists of applying a non-invertible transformation on the biometric features in order to generate a unique compact binary code. The secure transformation is based essentially on the principle of multiplexing provided by *CDMA* and the principle of *Random projection*.

Furthermore, we made sure during the design phase, that our approach meets the requirements of revocability, unlinkability, and non-invertibility. Generally, cancellable biometrics [35] is mainly based on two factors that must be presented at each authentication [36], namely the biometric trait and the seed (which can be seen as a secret key). The seed is a user-specific component through which the transformation of the original template is carried out, this element must indeed be secret and out of the way of impostors. For this reason, we have made sure that the transformation only relies on the biometric modality as [13] to avoid any vulnerabilities that may arise in case of seed theft [37]. So, to keep the seed secure and unknown to adversaries, we integrated its generation intuitively during template generation as shown in Fig. 1. In general, biometric systems consist of two main phases: 1) enrollment and 2) authentication (which can take the form of either identity verification or identification [20]). During Enrollment, the user biometric trait is captured (acquisition) and the features are extracted and stored in a database as a reference template. At authentication, the same biometric trait is captured again, the features are extracted and compared with those previously stored in the database for an eventual matching and then produce a decision (match/no match). In the following, we outline the stages that make up our processes.

#### A. Enrollment Stage

Our proposed protection scheme consists of two main steps:

- 1) Associate for each enrolled user a unique seed, through which we can always access the same projection space.
- 2) Projection of the extracted original biometric features onto a secure domain generated from the seed used in the previous step.

During processing, we used *CDMA* to discretize the seed associated with each user. As mentioned above, *CDMA* is a mechanism that requires the use of spreading sequences to avoid interferences. For this reason, our thinking has led us to apply the *QR decomposition*, which decomposes a matrix into two components  $Q$  and  $R$ , where  $R$  is an upper triangular matrix and  $Q$  is orthogonal with orthonormal columns  $Q^T \cdot Q = I$  (where  $I$  is the identity matrix). When the decomposed matrix is square, then firstly it will always have a decomposition and secondly  $Q$  will be orthogonal  $Q^T \cdot Q = Q \cdot Q^T = I$ . In our approach, this decomposition assumes an important part, not only in the generation of orthogonal sequences but also in linking each identity to a unique orthogonal code. All steps of the proposed revocable approach are described in the Algorithm 1.

The enrollment phase involves the storage of three elements, namely the matrix  $R$  from which the orthogonal code is recovered, the sum  $S$  relative to the *CDMA* technique, and finally the protected templates.

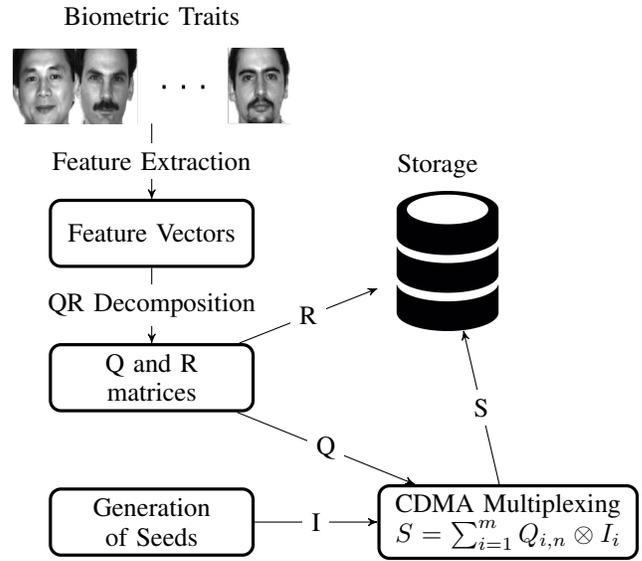


Fig. 1. Binding and Discretization of Seeds.

#### B. Authentication Stage

During the authentication phase, the system scans the biometric trait of the enrolled user  $k$ , hence the extraction of the feature vector  $V_k$ . Thereafter, the orthogonal code  $Q_k$  is recovered using the stored triangular matrix  $R$  according to the following formula:

$$Q_k = R^{-1} \cdot V_k \quad (4)$$

(It should be noted that making the matrix  $M$  squared during the enrollment phase, was very useful when selecting orthogonal sequences residing at the rows of the orthogonal matrix  $Q$ ). Then, the sum  $S$  is multiplied by the recovered orthogonal code  $Q_k$  to separate the seed  $I_k$  corresponding to the user  $k$ . Applying the same process of random projection during the enrollment phase, the protected template will thus be obtained. The system computes then the Hamming distance between the resulting template and the reference one stored in the database to either accept or reject the claimer. Concerning the determination of the threshold, it depends on the system design, and it is chosen such that the desired false rejection rate (FRR) and false acceptance rate (FAR) are satisfied.

#### V. ANALYSIS AND DISCUSSION

Our scheme is considered as a one-way function since it is computationally infeasible to reconstruct the original template starting from the stored elements. It is true that the sum  $S$  contains all the orthogonal codes and their associated seeds, but it is almost impossible to extract them in case of compromise. Even the knowledge of the triangular matrix  $R$  can not reveal the orthogonal codes  $Q_i$ , especially with the absence of the feature vectors, knowing that  $M = QR$ . So the security of our scheme is ensured as long as it is difficult to reverse the transformation to obtain the original biometric template. Furthermore, the scheme meets also the requirements of revocability and unlinkability, properties for which an ideal biometric template protection technique is founded. Thus, if a

---

**Algorithm 1** Stages of the enrollment phase

---

**Step 1.** Extraction of the biometric features vector  $x \in \mathbb{R}^n$  from a raw biometric image where  $n$  is the feature vector dimension.

**Step 2.** Assemble the set of feature vectors on a matrix  $M_{m \times n}$ , where  $m$  represents the user index during enrollment phase and  $n > m$ .

$$M_{m \times n} = \begin{pmatrix} x_{1,1} & x_{1,2} & \cdots & x_{1,n} \\ x_{2,1} & \ddots & & \vdots \\ \vdots & & \ddots & x_{m-1,n} \\ x_{m,1} & \cdots & x_{m,n-1} & x_{m,n} \end{pmatrix}$$

**Step 3.** Make  $M$  a square matrix by complementing it with random numbers in a way to avoid the case where  $\det(M) = 0$  (the order of the new matrix becomes  $n \times n$ ).

**Step 4.** Apply the *QR Decomposition* on the matrix  $M$ , which it can be expressed as  $M_{n \times n} = Q_{n \times n} R_{n \times n}$

**Step 5.** Generate for each identity a random vector representing the seed,  $\{I_k \mid k = 1, \dots, m\}$ .

**Step 6.** Application of *CDMA* combining all the generated seeds  $\{I_k \mid k = 1, \dots, m\}$  with the first  $m$  orthogonal sequences residing at the first  $m$  rows of the orthogonal matrix  $Q$  into a single data as :

$$S = \sum_{i=1}^m Q_{i,m} \otimes I_i \quad (2)$$

**Step 7.** Generate a set of pseudo-random vector,  $\{r_i \in \mathbb{R}^n \mid i = 1, \dots, m\}$  from each seed  $I_k$ , through a random number generator (RNG), in our case we used Blum-Blum-Shub [38].

**Step 8.** Apply the Gram-Schmidt process on the previous set of random vectors to get an orthonormal set of  $r$ ,  $\{or_i \in \mathbb{R}^n \mid i = 1, \dots, m\}$  thereby forming a projection base.

**Step 9.** Project each acquired biometric vector on its associated projection base, by computing the inner product of feature vecteur  $x \in \mathbb{R}^n$  and each orthonormal vector  $or_i$ , such that  $\langle x, or_i \rangle$ .

**Step 10.** Quantify the transformed template as follow:

$$b_i = \begin{cases} 0 & \text{if } \langle x, or_i \rangle \leq \tau \\ 1 & \text{if } \langle x, or_i \rangle > \tau \end{cases} \quad (3)$$

where  $\tau$  is a predefined threshold, and  $m$  is the dimension of the protected template.

---

stored template is compromised, it can be protected by using a new seed instead of the one corresponding to the identity of the compromised template. The revocation requires both the storage of a new protected template resulting from the use of the new seed and also the update of the stored sum  $S$  as:

$$S_{new} = S_{stored} - (Q_{identity} \otimes I_{old}) + (Q_{identity} \otimes I_{new}) \quad (5)$$

That is how we will be able to generate multiple protected templates for the same biometric identity by using different seeds, which ensures the unlinkability or diversity property. The advantage of the proposed technique lies not only in the fact that it is perfectly secure but also in that the scheme does

not require the repetition of the enrollment phase in case of a compromise of a protected biometric template.

On another hand, it should be noted that biometric identifiers are very sensitive and are affected by the variations that can occur during acquisition thus leading to a considerable degradation in accuracy performance [39]. This lack of accuracy is due to several factors: variability during capture (i.e. acquisition noise, use of multiple acquisition sensors, etc.), intra-class variability (variability of biometric data for an individual), and inter-class similarity (i.e., the similarity of biometric data for multiple individuals). The work we have proposed at this stage is dedicated to biometrics that represents high stability during the acquisition phase or non-biometric digital data to demonstrate the effectiveness of the provided discretization mechanism.

## VI. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a new scheme for biometric template protection. We have indeed exploited the multiplexing property provided by the Code Division Multiple Access (CDMA) to generate a certain discretization for biometric templates as a non-invertible transformation in a system based on random projection. Our proposal is a kind of biometric protection approach, which only requires the user biometric identifier to perform the authentication of individuals. We have demonstrated that it meets the requirements of a revocable biometric system, namely, the properties of revocability, unlinkability, and non-invertibility. It must be mentioned that the nature and sensitivity of the biometrics have a crucial impact on performance preservation after the application of the non-invertible transformation. Through this work, our proposal has been proven to be effective for stable digital data. In this perspective, future work will focus on adapting sensitive biometrics and then evaluating them through experiments using public biometric databases, as well as a comparative study with some classical protection schemes in terms of revocability, unlinkability, non-invertibility, and accuracy performance.

## REFERENCES

- [1] A. K. Jain, A. Ross, and S. Prabhakar, "An introduction to biometric recognition," *IEEE Transactions on circuits and systems for video technology*, vol. 14, no. 1, pp. 4–20, 2004.
- [2] A. K. Jain, A. Ross, and S. Pankanti, "Biometrics: a tool for information security," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 2, pp. 125–143, November 2006.
- [3] A. K. Jain, K. Nandakumar, and A. Nagar, "Biometric template security," *EURASIP Journal on Advances in Signal Processing*, vol. 8, no. 2, pp. 1–17, 2008.
- [4] N. Bartlow and B. Cukic, "Biometric system threats and countermeasures: A risk-based approach," in *Proceedings of the Biometric Consortium Conference (BCC 05)*, Crystal City, VA, USA, September 2005.
- [5] N. K. Ratha, J. H. Connell, and R. M. Bolle, "An analysis of minutiae matching strength," in *Proceedings of the Third International Conference on Audio- and Video-Based Biometric Person Authentication (AVBPA'01)*, Halmstad, Sweden, June 2001, pp. 223–228.
- [6] W. Yang, S. Wang, J. Hu, G. Zheng, and C. Valli, "Security and accuracy of fingerprint-based biometrics: A review," *Symmetry*, vol. 11, no. 2, p. 141, 2019.
- [7] N. K. Ratha, J. H. Connell, and R. M. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614–634, 2001.
- [8] A. B. J. Teoh, Y. W. Kuan, and S. Lee, "Cancellable biometrics and annotations on biohash," *Pattern Recognition*, vol. 41, no. 6, pp. 2034–2044, June 2008.

- [9] J. B. Kho, J. Kim, I.-J. Kim, and A. B. Teoh, "Cancelable fingerprint template design with randomized non-negative least squares," *Pattern Recognition*, vol. 91, pp. 245–260, 2019.
- [10] S. S. Ali, I. I. Ganapathi, S. Prakash, P. Consul, and S. Mahyo, "Securing biometric user template using modified minutiae attributes," *Pattern Recognition Letters*, vol. 129, pp. 263–270, 2020.
- [11] A. B. J. Teoh, D. C. L. Ngo, and A. Goh, "Two factor authentication featuring fingerprint data and tokenized random number," *Pattern recognition*, vol. 37, no. 11, pp. 2245–2255, November 2004.
- [12] A. Teoh and D. Ngo, "Biophasor: Token supplemented cancellable biometrics," in *9th International Conference on Control, Automation, Robotics and Vision(ICARCV '06)*, Singapore, December 2006, pp. 1–5.
- [13] C. Moujahdi, G. Bebis, S. Ghouzali, M. Mikram, and M. Rziza, "Biometric template protection using spiral cube: performance and security analysis," *International Journal on Artificial Intelligence Tools*, vol. 25, no. 01, p. 1550027, 2016.
- [14] U. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948–960, 2004.
- [15] E. Maiorana and P. Campisi, "Fuzzy commitment for function based signature template protection," *IEEE Signal Processing Letters*, vol. 17, no. 3, pp. 249–252, March 2010.
- [16] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of fingerprint recognition*. Springer Science & Business Media, 2009.
- [17] N. K. Ratha, S. Chikkerur, J. H. Connell, and R. M. Bolle, "Generating cancelable fingerprint templates," *IEEE Transactions on pattern analysis and machine intelligence*, vol. 29, no. 4, pp. 561–572, 2007.
- [18] S. Tulyakov, F. Farooq, P. Mansukhani, and V. Govindaraju, "Symmetric hash functions for secure fingerprint biometric systems," *Pattern Recognition Letters*, vol. 28, no. 16, pp. 2427–2436, 2007.
- [19] G. Kumar, S. Tulyakov, and V. Govindaraju, "Combination of symmetric hash functions for secure fingerprint matching," in *2010 20th International Conference on Pattern Recognition*. IEEE, 2010, pp. 890–893.
- [20] S. Wang and J. Hu, "Alignment-free cancelable fingerprint template design: A densely infinite-to-one mapping (ditom) approach," *Pattern Recognition*, vol. 45, no. 12, pp. 4129–4137, 2012.
- [21] C. Moujahdi, G. Bebis, S. Ghouzali, and M. Rziza, "Fingerprint shell: Secure representation of fingerprint template," *Pattern Recognition Letters*, vol. 45, pp. 189–196, 2014.
- [22] A. K. Trivedi, D. M. Thounaojam, and S. Pal, "Non-invertible cancellable fingerprint template for fingerprint biometric," *Computers & Security*, vol. 90, p. 101690, 2020.
- [23] A. Lahmidi, K. Minaoui, C. Moujahdi, and M. Rziza, "Fingerprint template protection using irreversible minutiae tetrahedrons," *The Computer Journal*, 2021.
- [24] J. K. Pillai, V. M. Patel, R. Chellappa, and N. K. Ratha, "Sectorized random projections for cancelable iris biometrics," in *Proc. IEEE Int. Conf. Acoustics, Speech, Signal Processing*, Dallas, TX, USA, March 2010, pp. 1838–1841.
- [25] —, "Secure and robust iris recognition using random projections and sparse representations," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 33, no. 9, pp. 1877–1893, September 2011.
- [26] A. Teoh and C. T. Yuang, "Cancelable biometrics realization with multispace random projections," *IEEE Transactions on Systems, Man, and Cybernetics*, vol. 37, no. 5, pp. 1096–1106, October 2007.
- [27] S. Jassim, H. Al-Assam, and H. Sellahewa, "Improving performance and security of biometrics using efficient and stable random projection techniques," in *Proceedings of 6th International Symposium on Image and Signal Processing and Analysis (ISPA 2009)*, Salzburg, Austria, September 2009.
- [28] S. Kaski, "Dimensionality reduction by random mapping," in *Int. Joint Conf. on Neural Networks Proceedings*, vol. 1, Anchorage, AK, USA, May 1998, pp. 413–418.
- [29] W. Hoffmann, "Iterative algorithms for gram-schmidt orthogonalization," *Computing*, vol. 41, no. 4, pp. 335–348, December 1989.
- [30] M. Z. Mushtaq, M. Ahsan, and M. S. Jamil, "Improving quality of security for cdma using orthogonal coding method," in *International Conference on Computer Science and Network Technology (ICCSNT)*, Harbin, China, December 2011, pp. 2649–2653.
- [31] R. Prasad and T. Ojanpera, "An overview of cdma evolution toward wideband cdma," *IEEE Communications Surveys*, vol. 1, no. 1, pp. 2–29, First Quarter 1998.
- [32] O. B. Wojuola, S. H. Mneney, and V. M. Srivastava, "Cdma in signal encryption and information security," in *Information Security for South Africa (ISSA)*, Johannesburg, South Africa, August 2016, pp. 56–61.
- [33] V. P. Ipatov, *Spread Spectrum and CDMA : Principles and Applications*. Jhon wiley and Sons, 2005.
- [34] R. L. Peterson, R. E. Ziemer, and D. E. Borth, *Introduction to Spread Spectrum Communications*. Prentice Hall International Editions, 1995.
- [35] V. M. Patel, N. K. Ratha, and R. Chellappa, "Cancelable biometrics: A review," *IEEE Signal Processing Magazine*, vol. 32, no. 5, pp. 54–65, 2015.
- [36] M. Ferrara, D. Maltoni, and R. Cappelli, "A two-factor protection scheme for mcc fingerprint templates," in *2014 International Conference of the Biometrics Special Interest Group (BIOSIG)*. IEEE, 2014, pp. 1–8.
- [37] A. Lahmidi, K. Minaoui, and M. Rziza, "A variant of biohashing based on the chaotic behavior of the logistic map," in *2019 International Conference on Systems of Collaboration Big Data, Internet of Things & Security (SysCoBioTS)*. IEEE, 2019, pp. 1–7.
- [38] L. Blum, M. Blum, and M. Shub, "A simple unpredictable pseudo-random number generator," *SIAM Journal on Computing*, vol. 15, no. 2, pp. 364–383, May 1986.
- [39] A. K. Jain, P. Flynn, and A. A. Ross, *Handbook of biometrics*. Springer Science & Business Media, 2007.

# Verifiable Homomorphic Encrypted Computations for Cloud Computing

Ruba Awadallah  
School of Computer Sciences  
Universiti Sains Malaysia  
Penang, Malaysia

Azman Samsudin  
School of Computer Sciences  
Universiti Sains Malaysia  
Penang, Malaysia

Mishal Almazrooie  
School of Computer Sciences  
Universiti Sains Malaysia  
Penang, Malaysia

**Abstract**—Cloud computing is becoming an essential part of computing, especially for enterprises. As the need for cloud computing increases, the need for cloud data privacy, confidentiality, and integrity are also becoming essential. Among potential solutions, homomorphic encryption can provide the needed privacy and confidentiality. Unlike traditional cryptosystem, homomorphic encryption allows computation delegation to the cloud provider while the data is in its encrypted form. Unfortunately, the solution is still lacking in data integrity. While on the cloud, there is a possibility that valid homomorphically encrypted data beings swapped with other valid homomorphically encrypted data. This paper proposes a verification scheme based on the modular residue to validate homomorphic encryption computation over integer finite field to be used in cloud computing so that data confidentiality, privacy, and data integrity can be enforced during an outsourced computation. The performance of the proposed scheme varied based on the underlying cryptosystems used. However, based on the tested cryptosystems, the scheme has 1.5% storage overhead and a computational overhead that can be configured to work below 1%. Such overhead is an acceptable trade-off for verifying cloud computation which is highly needed in cloud computing.

**Keywords**—Cloud computing; computation verification; data confidentiality; data integrity; data privacy; distributed processing; homomorphic encryption

## I. INTRODUCTION

The demanding needs of modern computing have prompted many enterprises to outsource their data solution to cloud service providers (CSP). CSP provides services that improve performance efficiency and ease of maintenance to the adopters. On top of the improvements, adopting cloud services also offers savings in information technology infrastructure costs, in which most of the infrastructure cost is transferred to the CSPs, and clients only pay for what are used. Thus, enterprises can conveniently store, maintain, and manage data files remotely with reduced operation costs [1]. The CSP market is currently brimming with CSPs and their innovative and competitive products. In general, the current success of cloud services is mostly on cloud storage. However, the market for cloud computing is also building up in momentum. Implementing cloud computing empowers enterprises to become more competitive by having computing platforms that are scalable, agile, and reliable. As a result, the growth in the cloud computing market is projected to reach US 623.3 billion by 2023 [2].

A typical cloud computing ecosystem consists of cloud users (client), CSP, and the network infrastructure that connects the client and the CSP. Models of CSP architecture consist of

software as a service, infrastructure as a service, and platform as a service. In addition, there are a few CSP designs that include private, public, hybrid, and community clouds [3].

Even though the outlook for cloud computing is positive, this technology is always being plagued with the trade-offs between cost and security. The issue lies in the principle of cloud computing, where enterprises need to delegate the task of protecting their data to CSP [4]. Subsequently, data sovereignty is lost once the data is stored in a remote CSP. This absence of control for data security presents data protection problems. According to the Cloud Security Alliance (CSA) analysis, for the third time in a row [5], [6], [7], data breaches topped the list of threats in the cloud. Data is considered breached once its information is disclosed, manipulated, or used by unauthorized parties. A data breach may be the primary goal of a targeted attack or merely the result of human error. However, the management of CSP is central, and it cannot guarantee the reliability of its employees [8]. [9] found that the occurrence of internal breaches is more serious and costly than foreign attacks. The reason behind this result is that insiders know the system and attack valuable information, while outsiders steal what they have access to [10].

As part of the security risk assessment, data privacy, confidentiality, and integrity must be considered to mitigate potential risks. Privacy refers to the access control that the clients have over their data. Confidentiality means only authorized parties can access the data. In comparison, data integrity refers to the assurance of data consistency over its entire life-cycle [11].

In order to ensure privacy and confidentiality in cloud computing, researchers have indicated that homomorphic encryption (HE) is one of the promising methods for remote manipulations over encrypted data [12], [13]. However, although HE makes computation delegation possible, it has security flaws that can affect the validity of outsourced calculations. Specifically, HE is malleable in nature, which makes it non-compliance to the indistinguishability under adaptive chosen-ciphertext attack (IND-CCA2) security notation [14]. Therefore, data integrity is at stake with only HE itself versus centralized cloud data management. For cloud computing, the threats to data integrity can be numerous and varied. This paper addresses the problem of data integrity verification (DIV) of CSP computations over homomorphically encrypted data. The focus of this paper is on the CSP behavior that stores and computes sensitive data. Specifically, the threats from the CSP can be enumerated as follows:

- 1) An attacker (CSP) violates the data integrity by directly substituting the given ciphertext with another valid ciphertext.
- 2) An attacker (CSP) maliciously substitutes a given computation query with another valid query.

Integer-based HE has been extensively researched and used. Therefore, this research aims to achieve the computational integrity of HE over an integer finite field. That contributes to strengthening the security of HE against data tampering and thus achieving privacy, confidentiality and integrity of the processed data.

The rest of the paper is organized as follows. Section II presents the current DIV methods with their limitations. Section III illustrates the candidate HE cryptosystems and presents the proposal scheme. The results and discussion are shown in Section IV. Finally, Section V provides the conclusion.

## II. RELATED WORK

Researchers are still looking for a comprehensive security solution that can bring cloud computing to the mainstream. HE with different approaches have been utilized to address the DIV problem. Classical auditing methods on single data copy had a broad resonance in addressing this problem, which represented by provable data possession (PDP) techniques [15], [16], [17], [18], [19], [20] and proving the possibility of retrieval (POR) techniques [21], [22], [23], [24], [25], [26], [27]. However, these methods are ineffective in the case of data loss or corruption on the servers. Another alternative is to archive multiple replicas of each file to use if the original copy has compromised, this model is known as data integrity auditing under distributed such as [28], [29], [30], [31].

As the previous schemes by their nature allow for a limited number of queries, there are proposing solutions [32], [33], [34], [35] that assign auditing tasks to a single third-party auditor (TPA) that independently manages the data audits. There are also works [36], [37], [38] where the auditing task is assigned to multiple TPAs to benefit from simultaneous synchronous audit sessions. Nevertheless, all the aforementioned schemes focus on checking the data integrity stored in cloud computing servers without verifying the validity and efficiency of CSP computations over the data.

In the field of verifiable computing, a variety of methods, including such [39], [40], [41], [42], [43], [44], [45], [46], [47], [48], [49], [50], [51]. [52] the basic of many variants of the verifiable computing proposal afterward, that developed based on fully homomorphic encryption (FHE). Although FHE appears theoretically ideal, it is inefficient for practical implementations due to the difficulty of the requirements of high storage usage and heavy overhead computing, therefore it is not very powerful for use in many power-limited devices. Likewise, these schemes [53], [51], [54], [55], [56], [57] proposed impractical methods based on FHE.

Otherwise, [46] presented a verifiable scheme that implements a commitment utilizing probabilistically checkable proofs. At the same time, [44] extended the scope of verifiable computation in two essential directions: public delegation and public verifiability. While [47] used a quadratic arithmetic

program and Elliptic curve encryption to obtain public verification commitment with a constant size however the number of executed operations. Also, [40] suggested a verifiable method of computations of quadratic polynomials over a large number of variables. Meanwhile, [45] tried to solve possible collusion attacks in the El-gamal scheme by re-encrypting the ciphertext using the receiver's public key. After that, [41] present a general Incremental verifiable database system by integrating the primitive vector commitment and the encrypted-then-incremental MAC encryption mode. And [48] suggested a framework using a hash function over ciphertext and dual-CSPs to check data duplication. [43] scheme promised an improved deduplication system in a hybrid cloud architecture. Furthermore [58] introduced the IKGSR scheme to improve the RSA key generation function based on the use of four giant prime numbers to generate encryption and decryption keys. In short, all of these proposals have the same framework idea of bounding the CSP generate a commitment, and accordingly, the client used this commitment to verify the CSP performance over his ciphertexts.

Whereas [50] proposed a public evaluation verification scheme over ciphertexts by interacting with the trusted authenticator (TA) and a public auditor proxy (PAP). Although they reduce the overload of both the cloud users and the verifier, it inefficient for practical applications due to using FHE's complicated scheme.

While numerous attempts have been made to overcome the CSP's computation cheating attack problems, they remain subject to certain fundamental flaws. First of all, most of the previous works are constructed for particular structures and cannot be included in other environments. This means that even a minor alteration can cause the schemes to fail due to their particular layouts. Furthermore, all the proposed models believe in the centralization of the CSP's authority or any third party over the data. As CSP can manipulate the computations applied to the data, it can generate the commitment value to match the applied computations. Thus, the client still receives an adequate commitment to computed ciphertexts, while the CSP perform the computation fraud attack.

In different ways, some researchers, such as [11] and [4], sought to use blockchain technology to prove the work of cloud service providers on cloud data. [11] relied on fiat cryptocurrencies such as Bitcoin and Ethereum to store the hash of the database issued by at least four cloud service providers and compare all the issued results. [4] used the proof of work consensus to delay the creation of a new record in the database to 6 minutes to create a single record as a minimum.

Despite the security effectiveness of the proposed schemes, they are pretty expensive; i.e. in addition to the cost of the required computations, blockchain implementation costs will be added as additional costs that clients will have to pay. Moreover, adopting the Byzantines Fault Tolerance consensus for both proposals would at least quadruple both costs. Also, using proof of work consensus in scheme [4] will impact cloud computing business performance. Therefore, our proposal will be based on modular arithmetic to provide a verification mechanism for the processes applied to the data at the lowest costs. Furthermore, the use of modular arithmetic dramatically increases digital signal processing performance in algorithms with extensive use of addition and multiplication. Thus, it

provides speed and low energy consumption and promises high reliability and fault tolerance [59], [60], [61]. The analysis of the latest scientific papers [62], [63], [64], [65], [66] confirms that the use of modular computation is continuously expanding. They ascribe that to the modular arithmetic's ability to increase the reliability of monitoring systems and their tolerance of errors significantly by increasing the resources used while preserving the operating time. As a result, many major companies such as Cisco and Kabushiki Kaisha Toshiba are rushing to research and apply modular arithmetic [67].

### III. VERIFICATION SCHEME DESIGN

The migration of sensitive data into CSP is a source of security issues. If sensitive data are migrated into CSP, the client must be assured that proper data security measurements are in place. In order to ensure data privacy and confidentiality, this paper assumes the use of HE. Subsequently, this section presents the proposed scheme which enables the client to verify the integrity of the applied computations over the encrypted data. Fig. 1 shows the flow diagram of the proposed scheme.

#### A. Scheme Preliminaries

This paper proposes the use of HE over  $\mathbb{Z}_p^*$  in encrypting the data before sending them to CSP, thus allows CSP to perform operations on the encrypted data at the client's request, without disclosing its content. In the context of this paper, the HE is briefly defined as follows. An HE over operation ' $\diamond$ ' in a finite field  $\mathbb{Z}_p^*$  is an encryption scheme that supports the following equation:

$$Enc_{k_e}(m_1) \diamond Enc_{k_e}(m_2) = Enc_{k_e}(m_1 \diamond m_2), \quad \forall m_1, m_2 \in \mathbb{Z}_p^*, \quad (1)$$

where  $Enc(\cdot)$  is an encryption algorithm,  $k_e$  is the encryption key and  $(m_1, m_2)$  are plaintexts. An HE scheme is primarily characterized by four operations: KeyGen, Enc, Dec, and Eval. Eval is an HE-specific operation, which takes ciphertexts as input and outputs a ciphertext corresponding to the plaintexts [68]. The Eval function in this paper supports both addition and multiplication operations over  $\mathbb{Z}_p^*$ . Table I summarizes the math notations used in this article. Depending on the supported homomorphism features, HE schemes can perform different type of operations. At any given time, the Partial Homomorphic Encryption (PHE) scheme can only perform one type of computation operation. It can be either a multiplicative homomorphism; e.g. RSA [69], and ElGamal [70], or additive homomorphism; e.g. Benaloh [71], Paillier [72], and Okamoto-Uchiyama (OU) [73]. While Somewhat Homomorphic Encryption (SWHE) scheme is a cryptosystem which supports both properties but for limited number of operations. Such as Boneh-Goh-Nissim (BGN) [74] which allowing unlimited number of additions, but only one multiplication. In this paper six HE schemes over  $\mathbb{Z}_p$  are benchmarks against the propose scheme. The following subsections introduce the six cryptosystems.

1) *RSA Cryptosystem*: RSA is a block cipher algorithm over integer finite field which support evaluation function for only homomorphic multiplication computations over ciphertext [69]. In RSA, the plaintext and the ciphertext (which are

TABLE I. MATHEMATICAL NOTATION

Notation	Explanation
$c_i$	a ciphertext
$m_i$	a plaintext
$p$	a large prime number
$q$	a large prime number
$n$	a modulus
$\lambda$	an encryption security parameter
$\mathbb{Z}_n^*$	a set of integer modulo $n$
$\mathbb{Z}_p^*$	a set of integers modulo $p$
$\mathbb{Z}_r^*$	a set of integer modulo $r$
$\mathbb{Z}_T^*$	a set of integer modulo $T$
$Prk$	a private key
$Puk$	a public key
$KeyGen$	a homomorphic $Prk$ and $Puk$ generation
$Dec_{Prk}(c_i)$	a homomorphic decryption of $c_i$ using $Prk$
$Enc_{Puk}(m_i)$	a homomorphic encryption of $m_i$ using $Puk$
$Eval$	a homomorphic function of $m$
$\diamond$	a computation function
$c_r$	a homomorphic computed result in ciphertext
$G$	a cyclic group
$\mathbb{G}$	a multiplicative group

represented as positive integers) are bounded by  $n$ , where  $n$  is defined as  $n < 2^{4096}$  for practical purposes. Following are the four main operations governing the RSA multiplicative-PHE cryptosystem:

- **KeyGen**: The public key  $Pk = \{e, n\}$  and the private key  $Prk = \{d, n\}$  are built upon two large prime numbers  $p, q$  such that  $p \neq q$ , and  $n = p \times q$ . The integer  $e$  is randomly selected such that  $\gcd(\phi(n), e) = 1$ ,  $1 < e < \phi(n)$  and  $d \equiv e^{-1} \pmod{\phi(n)}$ , where  $\phi(n) = (p-1)(q-1)$ .

- **Enc**: The public key  $Pk = \{e, n\}$  is used to encrypt plaintext  $m \in \{0, 1\}^*$  as shown by Equation (2).

$$c = Enc_{Pk}(m) = m^e \pmod{n}. \quad (2)$$

- **Dec**: The ciphertext  $c$  can be decrypted by using private key  $Prk = \{d, n\}$  as shown in Equation (3).

$$m = Dec_{Prk}(c) = c^d \pmod{n}. \quad (3)$$

- **Eval**: RSA cryptosystem satisfies multiplicative homomorphism as shown in Equation (4).

$$\begin{aligned} Enc(m_1) \times Enc(m_2) &= (m_1^e \pmod{n}) \times (m_2^e \pmod{n}), \\ &= (m_1 \times m_2)^e \pmod{n}, \\ &= Enc(m_1 \times m_2). \end{aligned} \quad (4)$$

2) *ElGamal Cryptosystem*: ElGamal proposed a probabilistic cryptography scheme based on public key cryptosystem in 1985 [70]. The scheme is based on Diffie-Hellman key exchange. The security of the scheme is based on the security of the discrete logarithm problem. A simple ElGamal's scheme is as follows:

- **KeyGen**: Key generation process required a cyclic group  $G$  with order  $n$  using generator  $g$ . ( $h = g^y$ ) is calculated based on a randomly chosen  $y \in \mathbb{Z}_n^*$ . The public key and the private keys are defined as  $Pk = \{G, n, g, h\}$  and  $Prk = \{y, n\}$ , respectively.

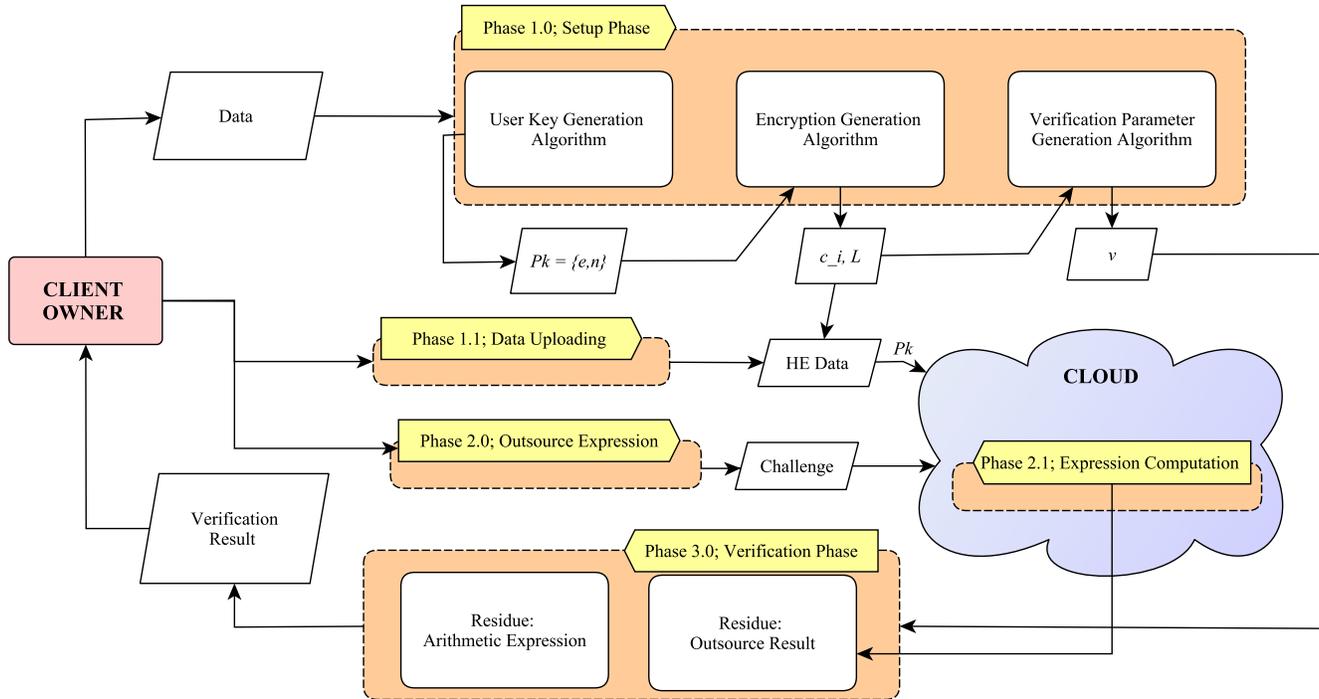


Fig. 1. Proposed Scheme Flow Diagram.

- **Enc:** The encryption of plaintext  $m$  requires a random integer  $r$  to be selected and kept hidden. The result of encrypting plaintext  $m$  is a ciphertext pair  $c = (c_1, c_2)$  which is defined as follows:

$$(c_1, c_2) = Enc_{Pk}(m) = (g^x, mh^x) = (g^x, mg^{xy}) \quad (5)$$

- **Dec:** The decryption is performed by using the private key  $\{y, n\}$  to compute  $s = c_1^y$ , followed by the decryption process itself as shown in the following equation:

$$Dec(c) = c_1 \times s^{-1} = mg^{xy} \times g^{-xy} = m. \quad (6)$$

- **Eval:** ElGamal cryptosystem satisfies multiplicative homomorphism as shown in Equation (7).

$$\begin{aligned} Enc(m_1) \times Enc(m_2) &= (g^{x_1}, m_1 h^{x_1}) \times (g^{x_2}, m_2 h^{x_2}) \\ &= (g^{x_1+x_2}, m_1 \times m_2 h^{x_1+x_2}) \\ &= E(m_1 \times m_2). \end{aligned} \quad (7)$$

3) **Benaloh Cryptosystem:** Benaloh scheme is based on the Goldwasser-Micali (GM) public key cryptosystem [71]. Benaloh scheme enhances the GM scheme by encrypting in blocks of bits rather than encrypting bit by bit. Security assumption of Benaloh scheme is based on the higher residuosity problem which is the generalization of quadratic residuosity problems ( $x^2$ ). Following is the description of the Benaloh additive-PHE cryptosystem:

- **KeyGen:** For a given block size  $r$ , two large primes  $p$  and  $q$  are selected such that  $\gcd(r, (p-1)/r) = 1$  and  $\gcd(r, (q-1)) = 1$ . Subsequently  $n$  and  $\phi(n)$  are calculated as  $n = pq$  and  $\phi(n) = (p-1)(q-1)$ , respectively.  $y \in \mathbb{Z}_n^*$  is selected such that  $(y^{\frac{\phi}{r}}) \equiv 1 \pmod n$ , where  $\mathbb{Z}_n^*$  is the multiplicative subgroup of integers modulo  $n$  which includes all the numbers smaller than  $r$  and relatively prime to  $r$ . The public key is published as  $(y, n)$ , while  $(p, q)$  represents the private key.

- **Enc:** To encrypt a plaintext  $m \in \mathbb{Z}_r$ , where  $\mathbb{Z}_r = \{0, 1, \dots, r-1\}$ , a random  $u \in \mathbb{Z}_r^*$  is selected. The encryption equation is as shown below:

$$c = Enc_{Pk}(m) = (y^m u^r) \pmod n. \quad (8)$$

- **Dec:** The decryption process is done through an exhaustive search for  $i \in \mathbb{Z}_r$ , in which the plaintext  $m$  can be recovered by using Equation (9).

$$m = (y^{-i} c)^{\phi/r} \pmod n. \quad (9)$$

- **Eval:** Benaloh cryptosystem satisfies additive homomorphism as shown in Equation (10).

$$\begin{aligned} Enc(m_1) \times Enc(m_2) &= ((y^{m_1} u_1^r) \pmod n) \\ &\quad \times ((y^{m_2} u_2^r) \pmod n), \\ &= (y^{m_1+m_2} (u_1 \times u_2)^r) \pmod n, \\ &= E((m_1 + m_2) \pmod n). \end{aligned} \quad (10)$$

4) *Okamoto-Uchiyama Cryptosystem*: [73] proposed a new additive cryptosystem which improve the computational performance by defining  $n = p^2q$  within the same domain of  $\mathbb{Z}_n^*$ . The security assumption of OU cryptosystem is based on the  $p$ -subgroup that makes it equivalent to the factorization of  $n$ . Following is the OU cryptosystem:

- **KeyGen**: After determining the value of  $n$ , a random number  $g \in \{2, \dots, n-1\}$  is selected such that  $g^{p-1} \not\equiv 1 \pmod{p^2}$ . Subsequently  $h$  can be calculated as  $h = g^n \pmod{n}$ . The public key and the private key are  $\{n, g, h\}$  and  $\{p, q\}$ , respectively.
- **Enc**: A plaintext  $m < p$  can be encrypted with the public key  $Pk = \{n, g, h\}$  as shown in Equation (11).  $r \in \{1, \dots, n-1\}$  is randomly selected.

$$c = Enc_{Pk}(m) = g^m h^r \pmod{n}. \quad (11)$$

- **Dec**: To recover the plaintext, the private key  $Prk = \{p, q\}$  is used with Equation (12).

$$a = \frac{(c^{p-1} \pmod{p^2}) - 1}{p},$$

$$b = \frac{(g^{p-1} \pmod{p^2}) - 1}{p}, \quad (12)$$

$$b' = b^{-1} \pmod{p},$$

$$Dec_{Prk}(c) = ab' \pmod{p}.$$

- **Eval**: OU cryptosystem satisfies additive homomorphism as shown in Equation (18).

$$Enc(m_1) \times Enc(m_2) = ((g^{m_1} h^{r_1}) \pmod{n})$$

$$\times ((g^{m_2} h^{r_2}) \pmod{n}),$$

$$= (g^{m_1+m_2} h^{r_1+r_2}) \pmod{n},$$

$$= Enc(m_1 + m_2). \quad (13)$$

5) *Paillier Cryptosystem*: Paillier cryptosystem is a probabilistic public key cryptosystem based on higher-order residual classes which support only additive homomorphism computations [72]. Following are the four main operations governing the Paillier additive-PHE cryptosystem:

- **KeyGen**: Paillier cryptosystem has a set of keys.  $p \in \mathbb{Z}_n^*$ ,  $q \in \mathbb{Z}_n^*$ ,  $g \in \mathbb{Z}_{n^2}^*$  are randomly selected such that  $\gcd(L(g^\lambda \pmod{n^2}), n) = 1$ , where  $p, q$  are two large primes,  $n = p \times q$  and functions  $L$  and  $\lambda$  are defined as follows:

$$L(u) = (u-1)/n. \quad (14)$$

$$\lambda = lcm((p-1)(q-1)). \quad (15)$$

- **Enc**: The encryption process utilizes the public key  $Pk = \{n, g\}$  to encrypt an arbitrary plaintext  $m \in \mathbb{Z}_n^*$  with a randomly selected integer  $r \in \mathbb{Z}_n^*$  to produce ciphertext  $c$ .

$$c = Enc_{Pk}(m) = g^m r^n \pmod{n^2}. \quad (16)$$

- **Dec**: The decryption process uses the private key  $Prk = \lambda$  in the decrypting process as shown by Equation (17).

$$Dec_{Prk}(c) = \left( \frac{L(c^\lambda \pmod{n^2})}{L(g^\lambda \pmod{n^2})} \right) \pmod{n} = m. \quad (17)$$

- **Eval**: Paillier cryptosystem satisfies additive homomorphism as shown in Equation (18).

$$Enc(m_1) \times Enc(m_2) = (g^{m_1} r_1^n \pmod{n^2})$$

$$\times (g^{m_2} r_2^n \pmod{n^2}),$$

$$= (g^{(m_1+m_2)} (r_1 \times r_2)^n) \pmod{n^2},$$

$$= Enc(m_1 + m_2). \quad (18)$$

6) *Boneh-Goh-Nissim Cryptosystem*: BGN defined a Paillier-like cryptosystem with an unlimited number of homomorphic additions and a single multiplication on the plaintext [74]. BGN cryptosystem is described as follows:

- **KeyGen**: A two large prime numbers  $q$  and  $r$  are chosen to produce the value of  $n = qr$  and a positive integer  $T < q$  which is selected randomly. Subsequently, two multiplicative groups  $\mathbb{G}, \mathbb{G}_1$  of order  $n$  that support a bilinear pairing  $e: (\mathbb{G} \times \mathbb{G}) \rightarrow \mathbb{G}_1$  are selected. Random generators  $g, u$  are chosen where  $g, u \in \mathbb{G}$ , and  $h = uq$  where  $h$  is a generator of the subgroup of order  $p$ . The public key is composed of  $Pk = \{n, g, h, \mathbb{G}, \mathbb{G}_1, e\}$ , and the private key is  $Prk = \{p, n\}$ .

- **Enc**: For a plaintext  $m \in \mathbb{Z}_T$  a random  $r \in \mathbb{Z}_n$  is selected. The encryption process is as shown by Equation (19).

$$Enc_{Pk}(m) = c = g^m h^r \pmod{n} \quad (19)$$

- **Dec**: Decrypting ciphertext  $c \in \mathbb{G}$  by using private key  $Prk = \{p, n\}$  is shown in Equation (20). Message  $m$  can be recovered in time  $O(\sqrt{T})$  since the message is bounded by  $T$ .

$$c^p \equiv (g^m h^r)^p \pmod{n}$$

$$\equiv (g^m)^p \pmod{n} \quad (20)$$

$$\equiv (g^p)^m \pmod{n}$$

- **Eval**: BGN satisfies unlimited additive homomorphism as shown in Equation (21) and a single multiplicative homomorphism as represented in Equation (22).

$$Enc(m_1) \times Enc(m_2) = ((g^{m_1} h^{r_1}) \pmod{n})$$

$$\times ((g^{m_2} h^{r_2}) \pmod{n})$$

$$= (g^{m_1+m_2} h^{r_1+r_2}) \pmod{n}$$

$$= E(m_1 + m_2) \quad (21)$$

$$Enc(m_1) \times k = c_1^k \pmod{n}$$

$$= (g^{m_1} h^{r_1})^k \pmod{n} \quad (22)$$

$$= (g^{km_1} h^{kr_1}) \pmod{n}$$

$$= E(m_1) \times k$$

HE cryptosystem is malleable, and therefore it is not IND-CCA2 secured by design. Data integrity can still be compromised by CSP and can go undetected. For example, the CSP

can implicitly substitute given ciphertext or the cumulative result with other valid ciphertext without the need to know the content of those substituted data. Different from confidentiality and privacy, once integrity is compromised there is no way to restore the original data. Therefore, data integrity needs to be enforced on such outsource computations.

### B. Proposed Scheme

The verification scheme has three phases: environment setup, computation outsourcing to the CSP by the client, and computation validation of CSP's work by the client, in which the last two phases can be repeated as required (see Table II). The three phases are thoroughly discussed in the subsequent context.

**Phase 1 (Setup):** The client initiates the initialization phase by defining system parameters. The propose scheme consists of two different number systems. The first number system is the finite field  $\mathbb{Z}_p^*$  where the HE calculations take place. The second number system is an  $n$ -bit binary number system, where  $n$  is a positive integer such that  $2^n$  is much smaller than the prime  $p$ . The HE encryption function takes as input a public key  $k_e$  and message  $m$  of index  $i$  and produces a ciphertext  $c_i$  as an output, as shown in Equation (23).

$$c_i = Enc_{k_e}(m_i); m_i, c_i \in \mathbb{Z}_p^*. \quad (23)$$

Subsequently, the client identifies a positive integer  $v < L$  as the secret value, where  $L$  is the largest integer allowed in the implemented system.  $v$  will also serves as the verification parameter.

**Phase 2 (Outsource):** In this phase, the client sends its outsource calculations in a form of an arithmetic equation to the CSP. In return the CSP executes the requested calculations and returns the corresponding result back to the client. From the client's repository, the client sends the arithmetic expression,  $\langle expr \rangle$ , to CSP for evaluation. The expression,  $\langle expr \rangle$ , consists of ciphertexts that had been encrypted by using HE with the corresponding arithmetic operators (e.g. “(101 + 202) × 303”). The syntax of the  $\langle expr \rangle$  follows the following grammar:

$$\begin{aligned} \langle expr \rangle &::= \langle term \rangle \text{ '+' } \langle expr \rangle \mid \langle term \rangle \\ \langle term \rangle &::= \langle factor \rangle \text{ 'x' } \langle term \rangle \mid \langle factor \rangle \\ \langle factor \rangle &::= \text{ '(' } \langle expr \rangle \text{ ')' } \mid \langle const \rangle \\ \langle const \rangle &::= \text{ integer} \end{aligned} \quad (24)$$

In return, CSP calculates the requested arithmetic expression before sending the corresponding result,  $c_r$  (e.g. “91809”), back to the client.

**Phase 3 (Validation):** To verify CSP's calculation(s), the client needs to assure that the value received from CSP,  $c_r$ , is the result of the arithmetic expression outsourced earlier,  $\langle expr \rangle$ .

The equality of a basic arithmetic expression can be validated by evaluating its modular residue. Let  $\langle expr \rangle$  be the outsourced arithmetic expression send by the client to the CSP

and let  $c_r$  be the calculation result received by the client from CSP. Subsequently, the client can validate  $c_r$  by comparing the modular residues of both  $c_r$  and  $\langle expr \rangle$ , as depicted by Equation (25).

$$\begin{aligned} c_r &= \langle expr \rangle. \\ c_r \bmod v &= \langle expr \rangle \bmod v. \end{aligned} \quad (25)$$

To simplify the calculation of the right-hand-side of Equation (25), the expression,  $\langle expr \rangle$ , is further expanded by using the following grammar based on modular arithmetic properties.

$$\begin{aligned} \langle expr \rangle &::= \langle term \rangle \text{ '+' } \langle expr \rangle \mid \langle term \rangle \\ \langle term \rangle &::= \langle factor \rangle \text{ 'x' } \langle term \rangle \mid \langle factor \rangle \\ \langle factor \rangle &::= \text{ '(' } \langle expr \rangle \text{ ')' } \bmod v \mid \\ &\quad \langle const \rangle \bmod v \\ \langle const \rangle &::= \text{ integer} \end{aligned} \quad (26)$$

TABLE II. WORKING EXAMPLES OF THE PROPOSE VERIFIED SCHEME BASED ON THE ARITHMETIC EXPRESSION  $c_r = ((c_1 + c_2) \times c_3)$ : (A) SETUP, (B) OUTSOURCING, (C) VALIDATION

(a) Setup: client determines modulus and identifies ciphertexts.			
Modulus and Ciphertexts	Example 1	Example 2	Example 3
$v$	3 <sub>10</sub>	62 <sub>10</sub>	158 <sub>10</sub>
$c_1$	4 <sub>10</sub>	101 <sub>10</sub>	99999 <sub>10</sub>
$c_2$	7 <sub>10</sub>	202 <sub>10</sub>	88888 <sub>10</sub>
$c_3$	8 <sub>10</sub>	303 <sub>10</sub>	77777 <sub>10</sub>

(b) Outsource: CSP computes the outsourced expression.			
Outsourced Computation	Example 1	Example 2	Example 3
$c_r = ((c_1 + c_2) \times c_3)$	88 <sub>10</sub>	91809 <sub>10</sub>	14691064199 <sub>10</sub>

(c) Validation: client validates result by comparing residues.			
Intermediate Values and Residues	Example 1	Example 2	Example 3
<b>Intermediate Values</b> $c_1 \bmod v$	1 <sub>10</sub>	39 <sub>10</sub>	143 <sub>10</sub>
$c_2 \bmod v$	1 <sub>10</sub>	16 <sub>10</sub>	92 <sub>10</sub>
$c_3 \bmod v$	2 <sub>10</sub>	55 <sub>10</sub>	41 <sub>10</sub>
$((c_1 \bmod v) + (c_2 \bmod v)) \bmod v$	4 <sub>10</sub>	3025 <sub>10</sub>	9635 <sub>10</sub>
<b>Residue: Arithmetic Expression</b> $(((((c_1 \bmod v) + (c_2 \bmod v)) \bmod v) \times (c_3 \bmod v)) \bmod v$	1 <sub>10</sub>	49 <sub>10</sub>	55 <sub>10</sub>
<b>Residue: Out-source result</b> $c_r \bmod v$	1 <sub>10</sub>	49 <sub>10</sub>	155 <sub>10</sub>

## IV. RESULT AND DISCUSSION

In this section, the data storage requirement and computation performance are analyzed when implementing the proposed scheme. The client and the CSP are simulated with different machines capacity to reflect the actual setting of the two domains. Cloud computing enterprises offer different computing instances with different performances as shown in Table III. To reflect such capabilities, an Intel® Core(TM) i7-3770 CPU, 3.40GHz CPU, 12GB RAM machine was used

to emulate the CSP computation environment. On the other hand, the client computations are simulated on a machine with Intel® Core(TM) i5-7500U, 2.70GHz CPU, and 4GB RAM.

On the software side, the proposed verified scheme that is running at CSP was implemented using Numpy [75], a compiled library which is efficient in manipulating big integer calculations for Python. For the client implementation which does not require big integer calculations, a basic C++ compiler was used when implementing the proposed scheme. This paper further assumes the use of the two HE properties; PHE represented by multiplicative homomorphic (RSA, ElGamal) and additive homomorphic (Benaloh, OU, Paillier) and SWHE represented by the BGN's method.

TABLE III. GENERIC CLOUD SERVICE PROVIDER CONFIGURATIONS

CSP	Configuration	CPU	Virtual CPUs	Memory (GiB)
AWS Elastic Cloud Computing™ [76]	Low	Intel Xeon E5-2666 v3	2	3.75
	High	Intel Xeon Platinum	72	192
Azure Virtual Machine™ [77]	Low	Intel Xeon Platinum 8168	2	4
	High	Intel Xeon Platinum 8168	72	144
Google Cloud Compute Engine™ [78]	Low	Intel Xeon Scalable	4	16
	High	Intel Xeon Scalable	60	240

In the following subsections, we present the results of applying the verification scheme to the different ciphertext sizes generated from candidate cryptosystems. The purpose of these calculations is to assess the implementation costs and performance of the proposed scheme for all candidate cryptosystems.

#### A. Storage Analysis

For the storage analysis, it is important to analyze the storage requirement to store the residues of all the encrypted data at the client side against the actual encrypted data stored at the CSP. Storing the residues at the client side is an overhead to the proposed verified scheme, which does not exist in a normal HE implementation. To gauge the CSP's storage requirement, a few assumptions are made. Among the assumptions is the modulus size. NIST recommends 2048-bit as the minimum size for the factoring modulus. While for a more secured applications, factoring modulus of at least 3072-bit is recommended [79]. To simplify calculation while adopting highest modulus value, this paper assumes 4096-bit as the factoring modulus.

Another assumption is the machine word-size. Current CPUs typically operate on 32- or 64-bit data, stacked of 4-bits or 8-bits based on ISO/IEC 2382:2015 standard [80]. The storage requirement for the verified scheme depends on the size of the verifying parameter,  $v$ . In order to simulate primitive encryption, we assume the client operates on 64-bit data which is typical in most modern desktop computers. Thus, the storage requirement at the client side is less than 1.5% of the CSP full storage. To put this result into perspective, for a client who owns petabytes of data stored at the CSP, this scheme will require the client to store only terabytes of the corresponding

TABLE IV. MULTIPLICATIVE HOMOMORPHIC CALCULATIONS: VERIFICATION COST AGAINST THE COST OF PERFORMING THE ACTUAL HOMOMORPHIC CALCULATION

Number of Operations per Verification	CSP: RSA	Client: RSA-Verified Method	
	Actual Multiplicative Homomorphic Calculation* (μsec)	Verification Calculation* (μsec)	Overhead (%)
1	63.83332	0.477777	0.748
10	745.9444	0.833333	0.111
100	88345.34	0.922222	< 0.000
1000	7071374.8	2.5001	< 0.000
10000	1120000000	17.254	< 0.000
Number of Operations per Verification	CSP: ElGamal	Client: ElGamal-Verified Scheme	
	Actual Multiplicative Homomorphic Calculation* (μsec)	Verification Calculation* (μsec)	Overhead (%)
1	115.0222	0.566666	0.49265
10	1592.375	1.622222	0.1018
100	299578.7	2.9785	< 0.000
1000	37347510.18	7.222222	< 0.000
10000	2749672997	33.98888	< 0.000

\* Average of 10 readings.

data at the client side which is feasible on current modern desktop.

#### B. Performance Analysis

It is crucial to analyze the calculation overhead of the proposed verification scheme, that is, it is important to gauge the acceptable number of calculations per verification in order to reduce the calculation overhead in the proposed scheme. The analysis in this section is therefore qualitative in nature and based on how the proposed scheme works in terms of homomorphic operations. In general, the computations performed by the client's machine is slightly faster than the computations performed by the CSP when processing single outsource expression (one expression, one verification). However, a series of expressions (many expressions per verification) can reduce the calculation overhead extremely.

In case of multiplicative-PHE, on verifying one RSA multiplication calculation the client is required to perform one 64-bit multiplication and two 64-bit modular operations on the residues of the two corresponding ciphertexts, while the CSP homomorphically performs one big integer multiplication (4096-bit) operation on the two ciphertexts. Whereas ElGamal cryptosystem needs to double up the RSA computations for one multiplication operation because the nature of the scheme in producing ciphertext pair for each single plaintext. Table IV shows the simulation results in multiplicative-PHE over  $x$  operations. Where Fig. 2 and Fig. 3 show the application of the proposed scheme to RSA and ElGamal cryptosystems, respectively. Both figures demonstrate the requested time variance between the client verification process and the CSP processing the data. Fig. 4 illustrates the corresponding overhead in processing multiplicative-PHE expressions per verification. Both encryption systems converge in the overhead percentage. In which a performing of one verification process per each computation process is less than 0.01%, but it quickly drops further to less than  $1.00E^{-7}\%$  in one verification process per 10000 computations.

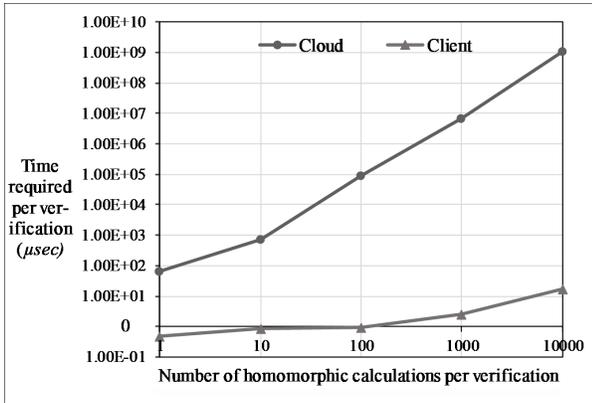


Fig. 2. Verified Scheme over RSA.

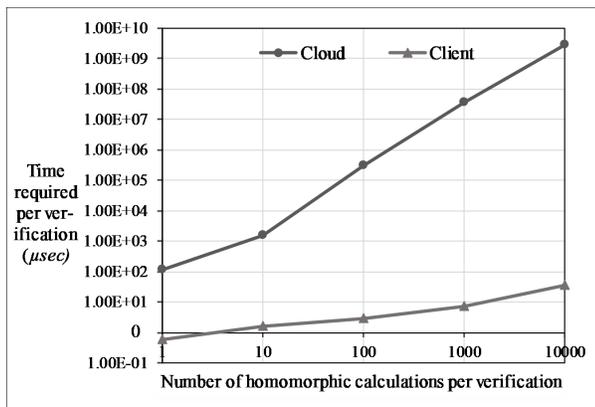


Fig. 3. Verified Scheme over ElGamal.

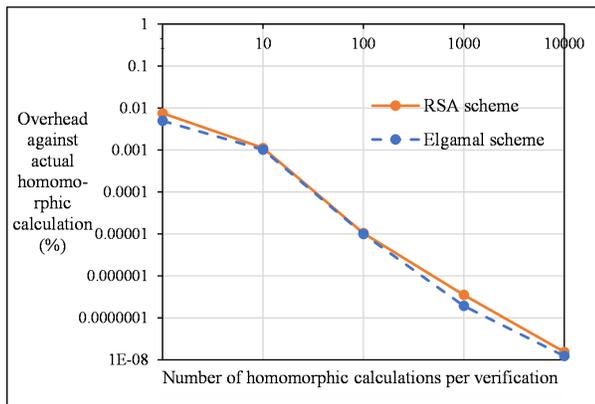


Fig. 4. Cost Overhead for Verifying Multiplicative-PHE Calculation.

The schematic for additive-PHE verification is similar to the multiplicative-PHE. For verifying  $x$  additive Benaloh or OU calculations, the client performs  $x$  multiplications and two modular operations. Whereas in verifying  $x$  additive Paillier calculations, the client performs  $x$  multiplications and two modular  $n^2$  operations, as seen in Section III-A. On the other hand, the CSP homomorphically performs  $x$  big integer multiplications (4096-bit). Table V shows the CSP and client average execution time for the verified scheme in additive-PHE. Fig. 5, Fig. 6 and Fig. 7 display the results of

TABLE V. ADDITIVE HOMOMORPHIC CALCULATIONS: VERIFICATION COST AGAINST THE COST OF PERFORMING THE ACTUAL HOMOMORPHIC CALCULATION

Number of Operations per Verification	CSP: Benaloh		Client: Benaloh-Verified Scheme	
	Actual Additive Homomorphic Calculation* (μsec)	Verification Calculation* (μsec)	Overhead (%)	
1	70.2354	0.5324	0.75802	
10	821.267	0.9924	0.12083	
100	96514.354	1.352	< 0.000	
1000	8075412.25	3.1231	< 0.000	
10000	1750000000	27.564	< 0.000	

Number of Operations per Verification	CSP: OU		Client: OU-Verified Scheme	
	Actual Additive Homomorphic Calculation* (μsec)	Verification Calculation* (μsec)	Overhead (%)	
1	121.733	0.78889	0.6480	
10	1663.42	1.02222	0.06145	
100	154769.59	1.5	< 0.000	
1000	14875365	3.12222	< 0.000	
10000	2394117441	28.9556	< 0.000	

Number of Operations per Verification	CSP: Paillier		Client: Paillier-Verified Scheme	
	Actual Additive Homomorphic Calculation* (μsec)	Verification Calculation* (μsec)	Overhead (%)	
1	86.48889	0.6964	0.80519	
10	1082.333	0.96667	0.08931	
100	139625.84	1.1	< 0.000	
1000	9175365.1	2.88889	< 0.000	
10000	1921808022	29.874	< 0.000	

\* Average of 10 readings.

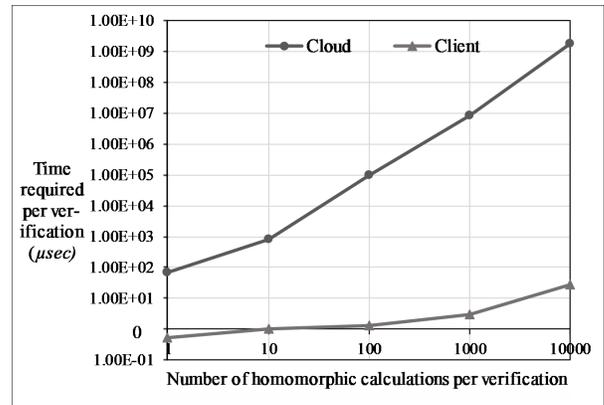


Fig. 5. Verified Scheme over Benaloh.

applying the verification scheme over the selected additive-PHE cryptosystems. Also, Fig. 8 shows the overhead results in processing additive-PHE expressions per verification for the selected cryptosystems. They are at rates less than 0.01% and rapidly decline to be approximately  $1.00E^{-5}\%$  in only 100 applied computations.

The verification for a BGN calculation consists of verifying additive homomorphic and multiplicative homomorphic at the same time. For  $x$  BGN computation, the verification process at the client side involves  $x$  64-bit addition, one 64-bit multiplication and two 64-bit binary operations on the residues of the two respective ciphertexts, while the CSP homomorphically conducts  $x$  big integer addition and one

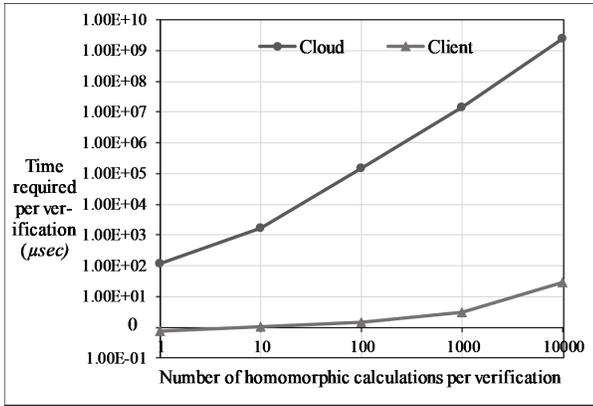


Fig. 6. Verified Scheme over OU.

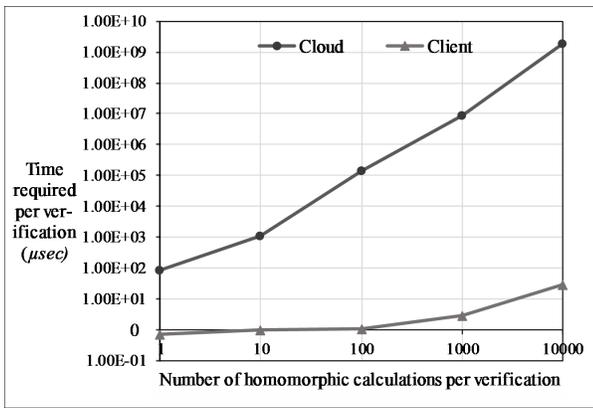


Fig. 7. Verified Scheme over Pailler.

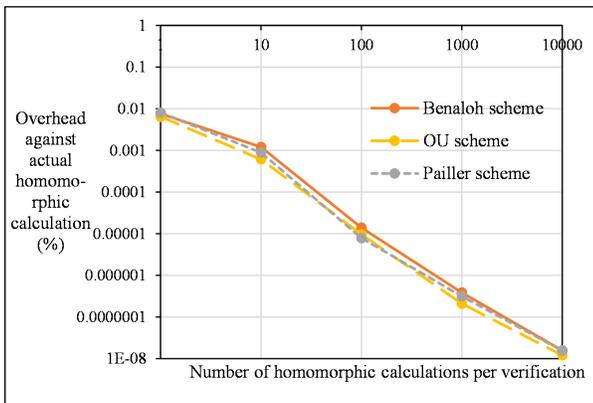


Fig. 8. Cost Overhead for Verifying Additive-PHE Calculation.

TABLE VI. SOMEWHAT HOMOMORPHIC CALCULATIONS: VERIFICATION COST AGAINST THE COST OF PERFORMING THE ACTUAL HOMOMORPHIC CALCULATION

Number of Operations per Verification	CSP: BGN Actual Additive & One Multiplicative Homomorphic Calculation* (μsec)	Client: Verified Scheme	
		Verification Calculation* (μsec)	Overhead (%)
1	128.3111	3.7	2.8836
10	1768.6644	6.87778	0.03889
100	225805.97	8.18889	< 0.000
1000	41472148	11.9333	< 0.000
10000	3168250731	29.77778	< 0.000

\* Average of 10 readings.

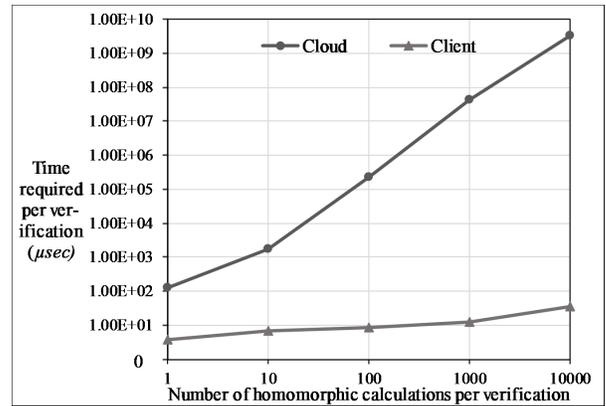


Fig. 9. Verified Scheme over BG.

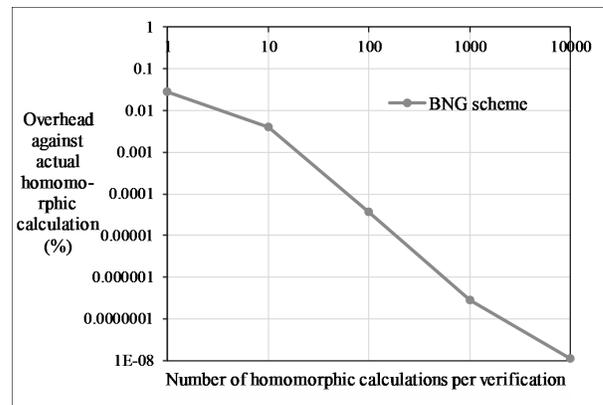


Fig. 10. Cost Overhead for Verifying SWHE Calculation.

big integer multiplication (4096-bit) operations on the two ciphertexts. Simulation result shown in Table VI and Fig. 9. Where Fig. 10 indicates that the verification overhead which is performed by the client is about 2.9% of the computation time needed by the CSP to process the real BGN calculation, moreover, it shows the overhead at the client side decreasing fast, as the number of calculations per verification increases.

### C. Security Analysis

The proposed verification mechanism enhances the security of HE against data tampering. That is, HE cryptosystems with this mechanism are able to provide data integrity, not only confidentiality and privacy. Now the client can infer if any data breach occurred from substitution in ciphertext or change in the query process. In which the verification result does not match the results sent to the client.

### D. Discussion

In general, the overhead of the propose scheme does not varied too much against the homomorphic cryptosystems.

This is because all the mentioned cryptosystems are based on the integer finite field, in which both the multiplicative-PHE and additive-PHE are being designed by manipulating only the multiplication operation on the ciphertexts. Across the board, the overhead is high since the proposed scheme is verifying by invoking calculations within the integer finite field. However, as shown in the previous section, amortization plays an important role in reducing the overhead, that is, one verification calculation is used to verify a batch of outsourced calculations. This is attributed to the increase in the execution time discrepancy between the CSP and the client; that is, the increase in the number of multiplications that CSP applies to the encrypted data against the execution time for verification which changes very slightly on the client machine.

It is also important to note that the increase in the ciphertext size due to the different cryptosystems and the size of the finite field do affect the overall performance of the proposed scheme. It is also important to note that the proposed scheme is less efficient on BGN with SWHE feature. This is due, partly to the high cost of exponential operation that was used to represent a single multiplication operation.

## V. CONCLUSION

This paper addresses the problem of DIV of outsource computation. In the context of outsourcing computation to CSP, HE over  $\mathbb{Z}_p^*$  does provide data confidentiality but lacks in data integrity. This paper presents an efficient DIV scheme for HE over  $\mathbb{Z}_p^*$  by evaluating the modular residue of the outsource calculation. The proposed scheme is flexible and extensible in design, in which the number of modulus that can be used is limited only by the word size of the client's machine. With a 64-bit machine, there are technically  $2^{64}$  possible modules. Subsequently, based on a 64-bit machine the storage requirement on the client's machine is less than 1.5% of the data size stored at the CSP. Across different cryptosystems tested, the worst computational overhead performed by the client is less than 3% of the actual homomorphic calculation performed by the CSP, that is, if one verification is applied to one homomorphic calculation. The worst computational overhead reduces to less than 0.1%, if one verification is performed for every 10 homomorphic calculations. It is also worth noting that the cryptosystems tested are slightly varied in their performances. In general, the proposed verified scheme can be implemented on any homomorphic cryptosystem that operates over the integer finite field  $\mathbb{Z}_p^*$  without much restriction. Although the scheme solves the problem of verifying the integrity of the data computations, it may constitute a burden on the client to provide storage and extra work to achieve the verification phase. Therefore, we aim to shift the verification process to decentralized fog nodes, which communicate through a consensus in future work.

## ACKNOWLEDGMENT

This work was supported by MOHE under the Fundamental Research Grant Scheme with grant number: FRGS/1/2020/ICT07/USM/01/1.

## REFERENCES

- [1] M. Mohammed and F. Abed, "A symmetric-based framework for securing cloud data at rest," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 28, no. 1, pp. 347–361, 2020.
- [2] M. R. Report, "Cloud computing market," <https://www.marketsandmarkets.com/Market-Reports/cloud-computing-market-234.html>, note = Accessed: 2020-05-12, 2019.
- [3] P. K. Senyo, E. Addae, and R. Boateng, "Cloud computing research: A review of research themes, frameworks, methods and future research directions," *International Journal of Information Management*, vol. 38, no. 1, pp. 128–139, 2018.
- [4] R. Awadallah and A. Samsudin, "Using blockchain in cloud computing to enhance relational database security," *IEEE Access*, 2021.
- [5] C. S. Alliance, "Practices for secure development of cloud applications," <https://safecode.org/practices-for-secure-development-of-cloud-applications/>, 2013, accessed: 2021-01-14.
- [6] —, "Top threats research," <https://cloudsecurityalliance.org/group/top-threats/>, 2016, accessed: 2021-01-14.
- [7] —, "Top threats to cloud computing: Egregious eleven," <https://cloudsecurityalliance.org/artifacts/top-threats-to-cloud-computing-egregious-eleven/>, 2020, accessed: 2021-01-14.
- [8] N. Anciaux, M. Benzine, L. Bouganim, P. Pucheral, and D. Shasha, "Ghostdb: querying visible and hidden data without leaks," in *Proceedings of the 2007 ACM SIGMOD international conference on Management of data*, 2007, pp. 677–688.
- [9] S. Pearson and A. Benameur, "Privacy, security and trust issues arising from cloud computing," in *2010 IEEE Second International Conference on Cloud Computing Technology and Science*. IEEE, 2010, pp. 693–702.
- [10] R. Richardson and C. Director, "Csi computer crime and security survey," *Computer security institute*, vol. 1, pp. 1–30, 2008.
- [11] R. Awadallah, A. Samsudin, J. S. Teh, and M. Almazrooe, "An integrated architecture for maintaining security in cloud computing based on blockchain," *IEEE Access*, vol. 9, pp. 69 513–69 526, 2021.
- [12] M. Ibtihal, N. Hassan *et al.*, "Homomorphic encryption as a service for outsourced images in mobile cloud computing environment," in *Cryptography: Breakthroughs in Research and Practice*. IGI Global, 2020, pp. 316–330.
- [13] P. Awasthi, S. Mittal, S. Mukherjee, and T. Limbasiya, "A protected cloud computation algorithm using homomorphic encryption for preserving data integrity," in *Recent Findings in Intelligent Computing Techniques*. Springer, 2019, pp. 509–517.
- [14] R. Awadallah and A. Samsudin, "Homomorphic encryption for cloud computing and its challenges," in *2020 IEEE 7th International Conference on Engineering Technologies and Applied Sciences (ICETAS)*. IEEE, 2020, pp. 1–6.
- [15] Y. Deswarte, J.-J. Quisquater, and A. Saïdane, "Remote integrity checking," in *Working conference on integrity and internal control in information systems*. Springer, 2003, pp. 1–11.
- [16] D. L. Gazzoni Filho and P. S. L. M. Barreto, "Demonstrating data possession and uncheatable data transfer," *IACR Cryptol. ePrint Arch.*, vol. 2006, p. 150, 2006.
- [17] G. Ateniese, S. Kamara, and J. Katz, "Proofs of storage from homomorphic identification protocols," in *International conference on the theory and application of cryptology and information security*. Springer, 2009, pp. 319–333.
- [18] C. Wang, S. S. Chow, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for secure cloud storage," *IEEE Computer Architecture Letters*, vol. 62, no. 02, pp. 362–375, 2013.
- [19] L. Li, Y. Yang, and Z. Wu, "Fmr-pdp: flexible multiple-replica provable data possession in cloud storage," in *2017 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2017, pp. 1115–1121.
- [20] J. Ni, K. Zhang, Y. Yu, and T. Yang, "Identity-based provable data possession from rsa assumption for secure cloud storage," *IEEE Transactions on Dependable and Secure Computing*, 2020.
- [21] J. Zhang, B. Wang, M. R. Ogiela, X. A. Wang, and A. K. Sangaiiah, "New public auditing protocol based on homomorphic tags for secure cloud storage," *Concurrency and Computation: Practice and Experience*, vol. 32, no. 18, p. e5600, 2020.
- [22] S. Hiremath and R. S. Kunte, "Homomorphic authentication scheme for proof of retrievability with public verifiability," in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2020, pp. 1017–1022.

- [23] D. Vasilopoulos, M. Önen, K. Elkhiyaoui, and R. Molva, "Message-locked proofs of retrievability with secure deduplication," in *Proceedings of the 2016 ACM on Cloud Computing Security Workshop*, 2016, pp. 73–83.
- [24] C. B. Tan, M. H. A. Hijazi, Y. Lim, and A. Gani, "A survey on proof of retrievability for cloud data integrity and availability: Cloud storage state-of-the-art, issues, solutions and future trends," *Journal of Network and Computer Applications*, vol. 110, pp. 75–86, 2018.
- [25] J. Yuan and S. Yu, "Proofs of retrievability with public verifiability and constant communication cost in cloud," in *Proceedings of the 2013 international workshop on Security in cloud computing*, 2013, pp. 19–26.
- [26] E. Shi, E. Stefanov, and C. Papamanthou, "Practical dynamic proofs of retrievability," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 325–336.
- [27] K. Omote and T. P. Thao, "Md-por: multisource and direct repair for network coding-based proof of retrievability," *International Journal of Distributed Sensor Networks*, vol. 11, no. 6, p. 586720, 2015.
- [28] Y. Zhu, H. Wang, Z. Hu, G.-J. Ahn, H. Hu, and S. S. Yau, "Efficient provable data possession for hybrid clouds," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 756–758.
- [29] Z. Hao and N. Yu, "A multiple-replica remote data possession checking protocol with public verifiability," in *2010 second international symposium on data, privacy, and E-commerce*. IEEE, 2010, pp. 84–89.
- [30] C. Wang, Q. Wang, K. Ren, N. Cao, and W. Lou, "Toward secure and dependable storage services in cloud computing," *IEEE transactions on Services Computing*, vol. 5, no. 2, pp. 220–232, 2011.
- [31] B. Rakesh, K. Lalitha, M. Ismail, and H. P. Sultana, "Distributed scheme to authenticate data storage security in cloud computing."
- [32] R. Saxena and S. Dey, "Cloud audit: A data integrity verification approach for cloud computing," *Procedia Computer Science*, vol. 89, pp. 142–151, 2016.
- [33] Q. Wang, C. Wang, K. Ren, W. Lou, and J. Li, "Enabling public auditability and data dynamics for storage security in cloud computing," *IEEE transactions on parallel and distributed systems*, vol. 22, no. 5, pp. 847–859, 2010.
- [34] C. Wang, Q. Wang, K. Ren, and W. Lou, "Privacy-preserving public auditing for data storage security in cloud computing," in *2010 proceedings ieee infocom*. Ieee, 2010, pp. 1–9.
- [35] S. E. Arasu, B. Gowri, and S. Ananthi, "Privacy-preserving public auditing in cloud using hmac algorithm," *International Journal of Recent Technology and Engineering*, vol. 2, no. 1, pp. 149–152, 2013.
- [36] M. Kolhar, M. M. Abu-Alhaj, and S. M. Abd El-atty, "Cloud data auditing techniques with a focus on privacy and security," *IEEE Security & Privacy*, vol. 15, no. 1, pp. 42–51, 2017.
- [37] S. H. Abbdal, H. Jin, A. A. Yassin, Z. A. Abduljabbar, M. A. Hussain, Z. A. Hussien, and D. Zou, "An efficient public verifiability and data integrity using multiple tpas in cloud data storage," in *2016 IEEE 2nd International Conference on Big Data Security on Cloud (BigDataSecurity)*, *IEEE International Conference on High Performance and Smart Computing (HPSC)*, and *IEEE International Conference on Intelligent Data and Security (IDS)*. IEEE, 2016, pp. 412–417.
- [38] A. Razaque and S. S. Rizvi, "Triangular data privacy-preserving model for authenticating all key stakeholders in a cloud environment," *Computers & Security*, vol. 62, pp. 328–347, 2016.
- [39] C. Asmuth and J. Bloom, "A modular approach to key safeguarding," *IEEE transactions on information theory*, vol. 29, no. 2, pp. 208–210, 1983.
- [40] M. Backes, D. Fiore, and R. M. Reischuk, "Verifiable delegation of computation on outsourced data," in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, 2013, pp. 863–874.
- [41] X. Chen, J. Li, J. Weng, J. Ma, and W. Lou, "Verifiable computation over large database with incremental updates," *IEEE transactions on Computers*, vol. 65, no. 10, pp. 3184–3195, 2015.
- [42] S. Goldwasser, Y. T. Kalai, and G. N. Rothblum, "Delegating computation: interactive proofs for muggles," *Journal of the ACM (JACM)*, vol. 62, no. 4, pp. 1–64, 2015.
- [43] J. Li, Y. K. Li, X. Chen, P. P. Lee, and W. Lou, "A hybrid cloud approach for secure authorized deduplication," *IEEE Transactions on Parallel and Distributed Systems*, vol. 26, no. 5, pp. 1206–1216, 2014.
- [44] B. Parno, M. Raykova, and V. Vaikuntanathan, "How to delegate and verify in public: Verifiable computation from attribute-based encryption," in *Theory of Cryptography Conference*. Springer, 2012, pp. 422–439.
- [45] P. Renjith and S. Sabitha, "Verifiable el-gamal re-encryption with authenticity in cloud," in *2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT)*. IEEE, 2013, pp. 1–5.
- [46] S. T. Setty, R. McPherson, A. J. Blumberg, and M. Walfish, "Making argument systems for outsourced computation practical (sometimes)," in *NDSS*, vol. 1, no. 9, 2012, p. 17.
- [47] S. Setty, V. Vu, N. Panpalia, B. Braun, A. J. Blumberg, and M. Walfish, "Taking proof-based verified computation a few steps closer to practicality," in *Presented as part of the 21st {USENIX} Security Symposium ({USENIX} Security 12)*, 2012, pp. 253–268.
- [48] Z. Wen, J. Luo, H. Chen, J. Meng, X. Li, and J. Li, "A verifiable data deduplication scheme in cloud computing," in *2014 International Conference on Intelligent Networking and Collaborative Systems*. IEEE, 2014, pp. 85–90.
- [49] X. Yu, Z. Yan, and A. V. Vasilakos, "A survey of verifiable computation," *Mobile Networks and Applications*, vol. 22, no. 3, pp. 438–453, 2017.
- [50] X. Yu, Z. Yan, and R. Zhang, "Verifiable outsourced computation over encrypted data," *Information Sciences*, vol. 479, pp. 372–385, 2019.
- [51] D. Fiore, R. Gennaro, and V. Pastro, "Efficiently verifiable computation on encrypted data," in *Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security*, 2014, pp. 844–855.
- [52] R. Gennaro, C. Gentry, and B. Parno, "Non-interactive verifiable computing: Outsourcing computation to untrusted workers," in *Annual Cryptology Conference*. Springer, 2010, pp. 465–482.
- [53] C. Gentry and S. Halevi, "Implementing gentry's fully-homomorphic encryption scheme," in *Annual international conference on the theory and applications of cryptographic techniques*. Springer, 2011, pp. 129–148.
- [54] T. Li, J. Li, Z. Liu, P. Li, and C. Jia, "Differentially private naive bayes learning over multiple data sources," *Information Sciences*, vol. 444, pp. 89–104, 2018.
- [55] Y. Ding, B. Han, H. Wang, and X. Li, "Ciphertext retrieval via attribute-based fhe in cloud computing," *Soft Computing*, vol. 22, no. 23, pp. 7753–7761, 2018.
- [56] A. Marinho, L. Murta, C. Werner, V. Braganholo, S. M. S. d. Cruz, E. Ogasawara, and M. Mattoso, "Provmanager: a provenance management system for scientific workflows," *Concurrency and Computation: Practice and Experience*, vol. 24, no. 13, pp. 1513–1530, 2012.
- [57] R. Canetti, B. Riva, and G. N. Rothblum, "Two 1-round protocols for delegation of computation," *IACR Cryptol. ePrint Arch.*, vol. 2011, p. 518, 2011.
- [58] P. Chinnasamy and P. Deepalakshmi, "Improved key generation scheme of rsa (ikgsr) algorithm based on offline storage for cloud," in *Advances in big data and cloud computing*. Springer, 2018, pp. 341–350.
- [59] M. Deryabin, M. Babenko, A. Nazarov, N. Kucherov, A. Karachevtsev, A. Glotov, and I. Vashchenko, "Protocol for secure and reliable data transmission in manet based on modular arithmetic," in *2019 International conference on Engineering and Telecommunication (EnT)*. IEEE, 2019, pp. 1–5.
- [60] A. Tchernykh, U. Schwiegelsohn, E.-g. Talbi, and M. Babenko, "Towards understanding uncertainty in cloud computing with risks of confidentiality, integrity, and availability," *Journal of Computational Science*, vol. 36, p. 100581, 2019.
- [61] M. Deryabin, N. Chervyakov, A. Tchernykh, M. Babenko, N. Kucherov, V. Miranda-López, and A. Avetisyan, "Secure verifiable secret short sharing scheme for multi-cloud storage," in *2018 International Conference on High Performance Computing & Simulation (HPCS)*. IEEE, 2018, pp. 700–706.
- [62] N. Chervyakov, M. Babenko, A. Tchernykh, N. Kucherov, V. Miranda-López, and J. M. Cortés-Mendoza, "Ar-rms: Configurable reliable

- distributed data storage systems for internet of things to ensure security,” *Future Generation Computer Systems*, vol. 92, pp. 1080–1092, 2019.
- [63] B. Varghese and R. Buyya, “Next generation cloud computing: New trends and research directions,” *Future Generation Computer Systems*, vol. 79, pp. 849–861, 2018.
- [64] W. Wong and K. Blow, “Design and analysis of an all-optical processor for modular arithmetic,” *Optics communications*, vol. 265, no. 2, pp. 425–433, 2006.
- [65] V. T. Goh and M. U. Siddiqi, “Multiple error detection and correction based on redundant residue number systems,” *IEEE Transactions on Communications*, vol. 56, no. 3, pp. 325–330, 2008.
- [66] C.-H. Chang, A. S. Molahosseini, A. A. E. Zarandi, and T. F. Tay, “Residue number systems: A new paradigm to datapath optimization for low-power and high-performance digital signal processing applications,” *IEEE circuits and systems magazine*, vol. 15, no. 4, pp. 26–44, 2015.
- [67] V. Kuchukov, A. Nazarov, and I. Vashchenko, “Cloud-fog-edge computing model for video surveillance based on modular arithmetic,” in *2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus)*. IEEE, 2020, pp. 374–376.
- [68] A. Acar, H. Aksu, A. S. Uluagac, and M. Conti, “A survey on homomorphic encryption schemes: Theory and implementation. corr abs/1704.03578 (2017),” *arXiv preprint arXiv:1704.03578*, 2017.
- [69] R. L. Rivest, L. Adleman, and M. L. Dertouzos, “On data banks and privacy homomorphisms,” *Foundations of secure computation*, vol. 4, no. 11, pp. 169–180, 1978.
- [70] T. ElGamal, “A public key cryptosystem and a signature scheme based on discrete logarithms,” *IEEE transactions on information theory*, vol. 31, no. 4, pp. 469–472, 1985.
- [71] J. Benaloh, “Dense probabilistic encryption,” in *Proceedings of the workshop on selected areas of cryptography*, 1994, pp. 120–128.
- [72] P. Paillier, “Public-key cryptosystems based on composite degree residuosity classes,” in *International conference on the theory and applications of cryptographic techniques*. Springer, 1999, pp. 223–238.
- [73] T. Okamoto and S. Uchiyama, “A new public-key cryptosystem as secure as factoring,” in *International conference on the theory and applications of cryptographic techniques*. Springer, 1998, pp. 308–318.
- [74] D. Boneh, E.-J. Goh, and K. Nissim, “Evaluating 2-dnf formulas on ciphertexts,” in *Theory of cryptography conference*. Springer, 2005, pp. 325–341.
- [75] S. v. d. Walt, S. C. Colbert, and G. Varoquaux, “The numpy array: a structure for efficient numerical computation,” *Computing in science & engineering*, vol. 13, no. 2, pp. 22–30, 2011.
- [76] Amazon, “Amazon ec2 instance types,” <https://aws.amazon.com/ec2/instance-types/#instance-details>, 2019, accessed: 2020-04-17.
- [77] L. Bruno, “Azure cloud computing user guide,” vol. 53, pp. 1689–1699, 2019.
- [78] Google, “Google cloud compute products,” <https://cloud.google.com/compute/docs/disks/?authuser=3&hl=ru#localssds>, 2019, accessed: 2020-07-28.
- [79] E. Barker, W. Burr, A. Jones, T. Polk, S. Rose, M. Smid, and Q. Dang, “Recommendation for key management part 3: Application-specific key management guidance,” *NIST special publication*, vol. 800, p. 57, 2009.
- [80] S. Trudel and I. Order, “International standard iso/iec information technology—process assessment—requirements for performing process assessment,” 2015.

# Multi-logic Rulesets based Junction-point Movement Controller Framework for Traffic Streamlining in Smart Cities

Sreelatha R<sup>1</sup>

ISE Department

B M S College of Engineering  
Basavanagudi, Bangalore 560091

Roopalakshmi R<sup>2</sup>

CSE Department

Manipal Institute of Technology  
Manipal 576104

**Abstract**—In the internet era, Intelligent Transportation System (ITS) for smart cities is gaining tremendous attention since it offers intelligent smart services for traffic monitoring and management with the help of different technologies such as microelectronics, sensors and IoT. However, in the existing literature, very few attempts are made towards effective traffic monitoring at road junctions in terms of providing faster decision making so that the traffic present in heavily congested urban environments can be dynamically rerouted. In order to tackle this issue, this article proposes a new Controller framework that can be applied at junction-points in order to control the traffic movement. Specifically, the proposed framework utilizes a multi-logic ruleset database to estimate the traffic density dynamically at the first stage followed by the usage of signal-time computation algorithm at the second stage in order to streamline the traffic and achieve faster clearance at the junction-points. The experimental results conducted with the help of test environment using MEMSIC nodes clearly demonstrate the improved efficiency of the proposed framework in terms various performance metrics including move command frequency, ruleset score and fluctuation score.

**Keywords**—Intelligent transportation systems; junction-point traffic monitoring; ruleset database; traffic density estimation

## I. INTRODUCTION

Nowadays, Intelligent Transportation System (ITS) for smart cities is gaining huge attention, which offers smart as well as intelligent services towards traffic management and monitoring with the help of technologies including electronic sensing, data communication, and advanced information management systems [1],[2]. Further, the transportation efficiency can be significantly enhanced with the aid of the proximity cooperation of the user over the road and vehicle targeting towards reducing the congestion of the traffic [3]. Precisely, the prime idea of ITS is to address the all sorts of problems associated with traffic density over the network of the road [4]. In general, ITS system consists of the different sophisticated components such as Advanced Traffic Information Service System (ATIS), Emergency Rescue System (ERS), Freight Management System (FMS), Electronic Public Transport System (EPTS), Advanced Public Transportation System (APTS), Advanced Vehicle Control System (AVCS) and Advanced Traffic Management System (ATMs) and so on [5].

Though enormous amount of research efforts are made towards ITS research domain, yet several serious issues of traffic density control are however remaining unresolved till

now in almost all the major cities in every part of the world. In addition to that, an increase in traffic density gives rise to severe congestion problems and induces pollution and thereby adversely affects economic losses. In the current scenario, the successful deployment of ITS for facilitating effective traffic monitoring is significantly affected by these two limitations: a) To standardize the elementary factors in order to compute and predict the state of deadlock condition of traffic over larger traffic density and b) To ensure the reliability associated with the predictive concept in traffic management along with higher accuracy [6]. The former limitation is addressed up to a certain extent, in the existing literature by means of Vehicular Ad-hoc Networks using forecasting approaches [7]. The latter issue is addressed using infra-structure based approaches by employing GPS data [8]. However, the state-of-the art techniques in both the cases, fail to provide effective performance, due to problems such as inaccurate estimates of traffic, delay and inadequate accuracy in dynamic and large-scale urban traffic environment.

From setup perspective, the existing literature towards ITS traffic monitoring can be broadly classified into two categories namely, infrastructure Vs non-infrastructure-based techniques. The infrastructure-based techniques primarily focus on essential functionalities such as traffic light management, route suggestion, congestion detection, re-routing and speed adjustment whereas non-infrastructure-based approaches primarily concentrate on cooperative congestion identification, congestion avoidance accident detection and warning. However, one of the significant research challenges in the existing literature is, the complexity in design framework due to which only normal classification over test environments can be performed. Further, the traffic density computations are assessed using certain formulated theories without suitable validations with real-world traffic systems, which results in significantly poor performances [9],[10]. Due to these aspects, promising techniques are needed for traffic monitoring in ITS which can effectively make faster decisions for rerouting traffic in heavily congested urban environments. In this article, a novel controller design framework is proposed, which can be deployed at junction-points in order perform effective traffic monitoring and management by formulating a unique multi-logic ruleset. The organization of the article is described as follow: Section 2 discusses the existing literature, Section 3 describes the proposed along with detailed discussion of

system design as well as algorithm. Section 4 details result analysis followed by the illustration of conclusion in Section 5.

## II. RELATED WORK

In the existing literature, a lot of research attempts are made towards incorporating novel features in ITS so that different sorts of traffic monitoring issues can be addressing. For instance, Calabuig et al. [11] presented a novel techniques which is responsible for managing alert message for the remotely positioned vehicle by means of utilizing cluster-head selection strategies of VANETs in ITS. However, it suffers due to huge requirement of resources for unicast communication as well as non-availability of potential broadcasting features incellular networks. Also, recently, Derrouz et al. [12] developed a vehicle type classification framework using both the 3D parameters and 2D features in order to control traffic as well as violations of road code. Specifically, 3D parameters are used to reconstruct complete dimension of given vehicle in terms of height, width and length whereas 2D features are utilized for dimensionality reduction. Though the proposed classification system can accurately detect vehicles from different view angles, yet the performance may get seriously affected due to the errors calibration process used for estimating 3D parameters.

Recently in 2019, Blazek et al. [13] addressed the communication latency problem by presenting a burst-error performance modelling, which utilizes the formulation of the maximum likelihood function to measure the various extensive records based on channel-based parameters. Though, the authors successfully employed the fading information from the target channel and signal noise to investigate the degree of burstiness, yet few of fault-tolerance aspects such as burstiness for stress testing may degrade the performance of the system.

Very recently in 2020, Chavhan et al. [14] proposed a context-aware public transport system based on IoT, which uses both the context information and emergent intelligence, in order to enable public transport services in metropolitan areas. Though, the proposed system provides better results, yet it fails to address towards security issues. Javed et al. [15] addressed the security problems in ITS by developing a mechanism that can detect outliers and un-authenticate the false data and thereby enhance the decision of the traffic. A study towards safety standards in ITS is carried out by Naufal et al. [16], where a control and supervision system is designed for autonomously transport systems. Dotoli et al. [17] introduced have used multi-objective optimization framework in order to perform routing of vehicles by evaluating the user's preference. A similar kind of case study is considered by the adoption of blockchain technology in ITS by the authors in [18]. Szymanski et al. [19] presented a vehicle positioning framework using spatio-temporal features of the delay caused in public transportation systems with the help of GPS. The work carried out by Zhao et al. [20] includes a probabilistic framework in order to study the pattern of flows of passengers over different trains and routes. Calvillo et al. [21] have investigated connecting bridges between all the connected devices in smart cities. The study hypothesizes on distributed energy system, which plays an important role in performance improvement in smart cities.

Recently, Tian et al. [22] developed a recurrent attention framework for identifying the traffic signs by making use of deep neural networks, which suffers due to its computational complexity. Cai et al. [23] introduced a vector-based query processing system, which carries out query processing of ITS. Very recently in 2020, Choy et al. [24] proposed a low power speed monitoring framework with the help of radio frequency as well as neural network architectures. However, the performance of the proposed framework primarily depends on the estimation accuracy and antenna design. Rafter et al. [25] developed an adaptive traffic signal system with multiple modes that integrates position data of linked vehicles with data extracted from a network in a decentralized manner over a single intersection of the road.

To summarize, in the existing literature, huge efforts are made towards introducing the usage of sophisticated mechanisms to perform traffic monitoring, which are not much explored towards compatibility issues. Specifically, every vehicle's practical scenario over the road is given least preference, which on the other way plays a vital role in the realistic traffic situations. More specifically, in most of the existing traffic monitoring systems fail to include the practical constraints such as bi-directional traffic, routing viewpoint and directionality and so on in their decision making process, which may result in slightly less realistic estimations. In addition to that, in existing literature, very few attempts are carried out towards embedding automated decision-making or intelligence within the system to perform traffic monitoring. On the other hand, the adoption of the Global Positioning System (GPS) and sensors are widely popular in the existing literature for controlling navigation and traffic monitoring. However, GPS suffers from outages many times, and they are not always accurate. Usage of the sensor is a good idea, but the sensors are used in a very simplified manner which cannot capture dynamic information about the mobility of the vehicles based on direction in a two-lane system. Furthermore, generally the bottleneck condition of the traffic density is witnessed in intersection points or junctions. When one junction has multiple routes connected, it becomes the most challenging scenario to provide the command for vehicle clearance by executing different commands of the signal light. Unfortunately, most of the existing traffic monitoring systems perform slightly less effective due to manual process in traffic monitoring. Based on these aspects, promising traffic monitoring systems are needed, which can carry out faster decision-making as well as streamlining the traffic based on dynamic traffic events over the peak density conditions on the road.

### A. Motivation and Contributions

In this article, a novel *Junction-point Movement Controller framework, named as JMC Framework* is presented, which makes use of multi-logic ruleset database, in order to estimate the traffic density dynamically and also perform faster clearance at the junction-points. More precisely, the main contributions of the proposed JMC framework are given by,

- ★ *Construction of a new Ruleset Database* consisting of multi-value logic rulesets, which are used to generate aggregated traffic density inferences in the form of vehicle statistics and thereby effectively control the traffic movement.

- ★ Introducing a *novel Traffic Density Estimation and Signal-time Computation Algorithm*, named as *TDM-SC Algorithm*, in order to achieve consistent traffic density estimation followed by effective path determination, so that faster clearance of the vehicles can be ensured at the specified junction-points.

The proposed JMC framework along with construction of rule-set database and TDM-SC algorithm along with the detailed design is illustrated in Section 3.

### III. PROPOSED FRAMEWORK

Fig. 1 describes the overview of proposed JMC framework architecture consists of two stages. In the first stage, the number of inbound and outbound vehicles over the specific route are first inputted into the system. Precisely, the inbound and outbound vehicles are tracked with the help of sensors, which are placed on both the entry as well as exit points of routes, assuming that the multi-routes meet at the junction points. In the second stage, the entire aggregated vehicle movement data is then passed to a controller system hosted over the junction point. The controller processes the aggregated vehicular information and applies a multi-value logic system where different possibilities of ruleset are constructed based on traffic density. The resultant information helps the controller node to understand the degree of traffic density in different routes meeting at the junction. Based on the inferences derived from the ruleset, the controller decides for clearing the vehicles from their routes, by providing three different forms of commands including *MOVE* command, *WAIT FOR* command and *STOP* command, whereas *MOVE* command plays a vital role in clearing the traffic. In this way, the proposed system provides a solution in order to handle the variable traffic density on different routes by means of introducing a faster decision-making system for facilitating traffic monitoring and management in the urban environment. The complete system design including the analytical modelling of the proposed framework is detailed in the forthcoming section.

### IV. SYSTEM DESIGN

In this section, the main concept of the proposed JMC framework design is illustrated in detail, which in turn can be fully automated to optimize the traffic system, especially for any level of traffic density, so that smart traffic monitoring and controlling can be achieved. Specifically, system design modules including assumptions considered, Ruleset Database Formation followed by algorithm design are illustrated.

#### A. Assumptions

The implementation of the proposed JMC system is carried out by considering the following assumptions given by:

- Each vehicle V1 is equipped with a sensing device, which is having the unique identity of the vehicle.
- Every entry and exit points of a road are equipped with a transceiver which performs identification of the vehicles and aggregates the information about several inbound and outbound vehicles.
- A controller system with specific traffic commands tc is assumed to be present in every junction point

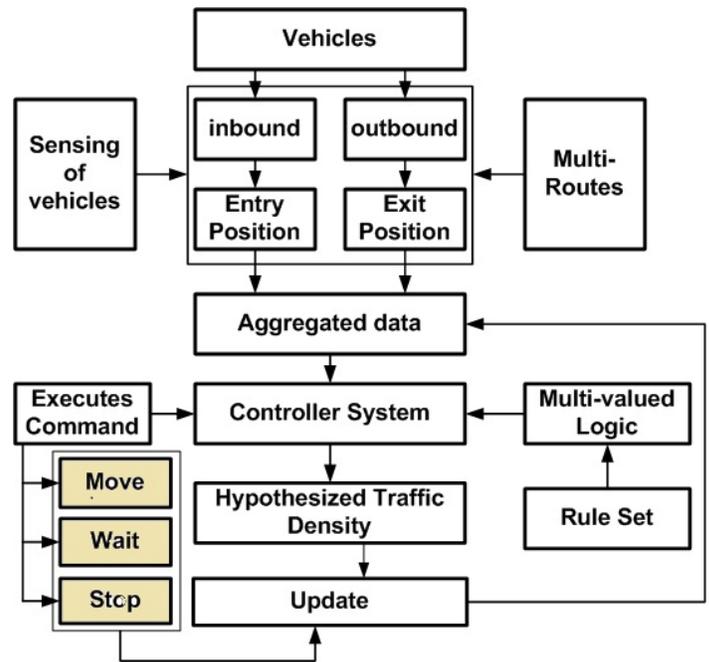


Fig. 1. Overview of the Proposed JMC Framework.

which performs execution of the ruleset in order to implement the automated and intelligent traffic management in the urban region.

- Apart from this, the proposed JMC design also assumes that, any street with a higher capacity is capable of introducing larger number of vehicles within it.
- The proposed framework also assumes that all the sensory devices are powered with a battery of finite lifetime.

#### B. Formation of Ruleset Database

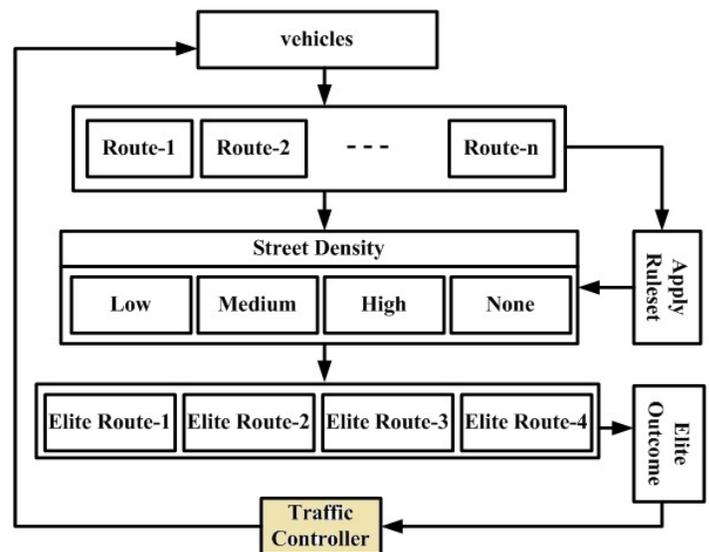


Fig. 2. Formation of Ruleset Database.

The proposed JMC framework, utilizes a Ruleset Database

using which it controls the movement of the traffic by means of employing multi-values logic systems in the form of vehicle statistics from four sample streets. Precisely, Fig. 2 describes the concept of Ruleset Database formation based on the traffic density over the street. More precisely, in the first step, the proposed system uses two primary logical operators, namely, “and” and “then” in order to check the density of all streets and thereby derives the inferences about the traffic density as shown in the top portion of figure. Specifically, a simplified version of a rule in the given ruleset database is given as follows:

$IF(cond1)\&(cond2)\&(Cond3)\&(Cond4)--THEN--Inf1$   
(1)

In the above rule expression, cond1 to Cond4 represent four different street conditions corresponding to its respective traffic density in terms of low, medium, and high traffic. More specifically, cond1 includes {low,medium,high} which represents various combination of street 1 traffic to be low, medium, and high. The similar type of rules are constructed for all combinations of traffic conditions. The inference is the outcome of the combination of these conditions resulting in selection of specific direction of a vehicle to move by choosing an outbound street, and thereby the inferences represent the outbound street. Precisely, in the proposed JMC framework, a complete Ruleset Database consisting of 80+ combinations of rulesets is constructed in order to generate the aggregated traffic density inferences and a snapshot of this database is shown in Fig. 3. After this step, the resultant traffic density

58. If (street1 is high) and (street2 is low) and (street3 is medim) and (street4 is low) then (witch-street is Lstreet1) (1)  
59. If (street1 is high) and (street2 is low) and (street3 is medim) and (street4 is medium) then (witch-street is Lstreet1) (1)  
60. If (street1 is high) and (street2 is low) and (street3 is medim) and (street4 is high) then (witch-street is no-differ) (1)  
61. If (street1 is high) and (street2 is low) and (street3 is high) and (street4 is low) then (witch-street is no-differ) (1)  
62. If (street1 is high) and (street2 is low) and (street3 is high) and (street4 is medium) then (witch-street is no-differ) (1)  
63. If (street1 is high) and (street2 is low) and (street3 is high) and (street4 is high) then (witch-street is no-differ) (1)  
64. If (street1 is high) and (street2 is medium) and (street3 is low) and (street4 is low) then (witch-street is Lstreet1) (1)  
65. If (street1 is high) and (street2 is medium) and (street3 is low) and (street4 is medium) then (witch-street is Lstreet1) (1)  
66. If (street1 is high) and (street2 is medium) and (street3 is low) and (street4 is high) then (witch-street is no-differ) (1)  
67. If (street1 is high) and (street2 is medium) and (street3 is medim) and (street4 is low) then (witch-street is Lstreet1) (1)  
68. If (street1 is high) and (street2 is medium) and (street3 is medim) and (street4 is medium) then (witch-street is Lstreet1) (1)  
69. If (street1 is high) and (street2 is medium) and (street3 is medim) and (street4 is high) then (witch-street is no-differ) (1)  
70. If (street1 is high) and (street2 is medium) and (street3 is high) and (street4 is low) then (witch-street is no-differ) (1)  
71. If (street1 is high) and (street2 is medium) and (street3 is high) and (street4 is medium) then (witch-street is no-differ) (1)  
72. If (street1 is high) and (street2 is medium) and (street3 is high) and (street4 is high) then (witch-street is no-differ) (1)  
73. If (street1 is high) and (street2 is high) and (street3 is low) and (street4 is low) then (witch-street is no-differ) (1)  
74. If (street1 is high) and (street2 is high) and (street3 is low) and (street4 is medium) then (witch-street is no-differ) (1)  
75. If (street1 is high) and (street2 is high) and (street3 is low) and (street4 is high) then (witch-street is no-differ) (1)  
76. If (street1 is high) and (street2 is high) and (street3 is medim) and (street4 is low) then (witch-street is no-differ) (1)

Fig. 3. Snapshot of Ruleset Database.

inferences are fed to the controller, so that it can understand the current traffic data aggregation. Followed by this step, the controller uses similar ruleset to compute the result of go time algorithm based on the traffic density and thereby performs decision-making.

### C. Algorithm Design

The proposed JMC framework presents an algorithm named as, Traffic Density Estimation and Signal-time Computation Algorithm (TDM-SC), which is in short indicated as TDM-SC algorithm for optimizing the traffic density monitoring efficiency in the urban traffic environment. Specifically, in the proposed JMC framework, first traffic density information is calculated with the help of execution of rules in Ruleset database followed by the classification of the traffic density. Then the resultant density estimations are further employed by the Controller in order to compute signal passing time allowed for every vehicle in the specified route. More specifically, the

proposed TDM-SC algorithmic with step-by-step procedure is detailed as given below.

Input: V (vehicles), tc (traffic command), iv (inbound vehicle)

Output:  $\alpha$  (execution of traffic command)

Start

```

1:  For i∈(1: V)
2:      init V, tc, iv
3:      sim→f1(V, tc)
4:      vrand→f2(iv)
5:      V→V + vrand
6:      If V < [max(Vden)]
7:          logrule = f3(V, ruleset)
8:          For m ∈ {(i + 1), mmax}
9:              If logrule ≤ m
10:                 mc(i) = k
11:                 End
12:                 [denmc(i)] = argmax(v)
13:                 gotime(i) = f4(V, mc, iv, et, durcom)
14:                 For j = 1 : gotime(i) + 1
15:                     v(mc(i)) = v(mc(i)) - ov
16:                     V = v + f5(rand, iv, χ)
17:                     If v(mc(i)) < 0
18:                         α=simulate traffic command(V, tc)
19:                     End
20:                 End
21:                 End
22:                 End
23:                 End
End

```

a) *The working of TDM-SC algorithm is illustrated as follows:*

The first initialization step of TDM-SC algorithm is to turn on the controller system for computation of the vehicle’s signal-time calculations. Then, the proposed algorithm takes the inputs namely, input of V (vehicles), tc (traffic command), and iv (inbound vehicle), which after processing yields an outcome of  $\alpha$  (execution of traffic command). Precisely, the algorithm initially considers all the vehicular nodes v as specified in step-1 of Fig. 4 (Line-1). The variable tc (traffic control) represents a controller system that directs the vehicle’s movement using standard signal lights. The variable iv and ov represent the total number of vehicles sensed by sensors over the streets entry and exit points respectively. The proposed study considers four entry points that meet at the junction where the controller system resides. An explicit function f1(x) is implemented which is responsible for simulating the vehicles V and traffic command tc over the junction point as shown in step-3(Line-3). The proposed system considers the junction point as a prominent bottleneck condition of routing within the junction itself in the urban traffic system.

The next part of the implementation focuses on generating the random number of vehicles  $v_{rand}$  by considering the function f2(x), which in turn takes a random number of incoming vehicles iv in step-4 (Line-4). Therefore, the total number of vehicles on each route is the addition of vehicles V and a random number of vehicle  $v_{rand}$  as specified in step-5 (Line-5). In order to depict a realistic traffic scenario, the proposed algorithm takes a fixed number of maximum vehicle density  $v_{den}$  on all of four considered routes as given in step-6 (Line-6). A logical ruleset  $log_{rule}$  is computed by applying a function f3(x) considering the input argument of vehicles

V and ruleset created earlier as specified in step-7 (Line-7). After this step, the function  $f3(x)$  performs the logical ruleset's evaluation by considering the four membership functions of 4 constituent routes meeting at the junction point.

Depending on the deployed environment of vehicular movement on the four test routes, the algorithm compares the value of the ruleset  $log_{rule}$  with the  $m$  variable, representing the output degree of density of the road as shown in step-8 (Line-8). Depending on the degree of road density encountered  $m$ , the algorithm assigns  $k$  to the move command  $mc$  as given in step-9(Line-9).It should be noted that  $k \ll m$ , which means that if the vehicles density is found higher, the number of move command towards every 4 points of streets, is  $k=1, 2, 3, 4$  (Line-10). For example, if the value of the  $log_{rule}$  is found less than 3, it will signal move command  $mc$  to 1st route ( $k=1$ ). If the value of  $log_{rule}$  is found less than 6, it will signal move command  $mc$  to 2nd route ( $k=2$ ). Similarly, if  $log_{rule}$  is found less than 9, it signals move command  $mc$  to 3rd route ( $k=3$ ), and so on as shown in Fig. 4.

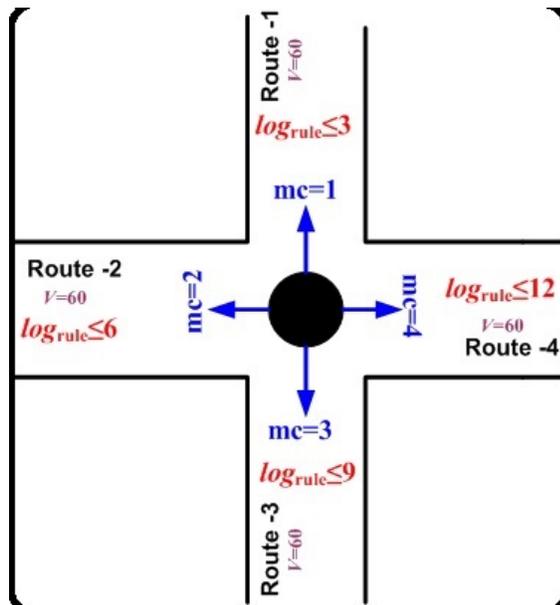


Fig. 4. Signal-Time Computation for Directing Vehicles Through Signals.

## V. RESULT AND DISCUSSION

### A. Experimental Setup:

The experimental setup of the proposed JMC framework including the test environment, deployment scenario as well as simulation nodes are detailed in this section as follows. Precisely, the deployment scenario including the urban traffic for the proposed JMC framework is shown in Fig. 5, in which the simulation environment consisting of inbound and outbound vehicles are visible on the assigned routes connected to respective junction points. More precisely, simulations are carried out with the help of MATLAB and the primary details considered in this setup are illustrated as follow:

- Urban traffic scenario is created by the deployment of Junction-points, that are constructed with 4 orthogonally joined routes.

- All the routes have both inbound and outbound vehicles in terms of 2-lane system with bidirectional traffic is considered.
- The entry and exit point are simulated with standard MEMSIC nodes which are responsible for estimating both inbound and outbound vehicles. Specifically, with one MEMSIC node in each route, the setup is implemented by 4 MEMSIC nodes which can capture from 5 to up to 3000 vehicles in entire simulation rounds.
- The junction point is equipped with the proposed centralized JMC system, which accepts the aggregated data from all the routes and performs the traffic density estimation followed by the signal-time computations by making use of TDM-SC algorithm, as described in the previous section in order to control the traffic density.
- Further, the duration of individual outbound cars is considered as 0.3 seconds. Also, the average number of inbound cars are set as 2 whereas for outbound cars it is 12.
- The simulations are carried out from a lower bound of 50 iterations to 500 iterations, in order to test the efficiency of the proposed framework.
- The simulation is also carried out for sample traffic conditions, where same number of vehicles are allocated in all streets at same time. For an example, all streets have 60 vehicles to be cleared in one signal. This sample scenario is also considered and proposed framework utilizes suitable rulesets in order to make appropriate decisions.

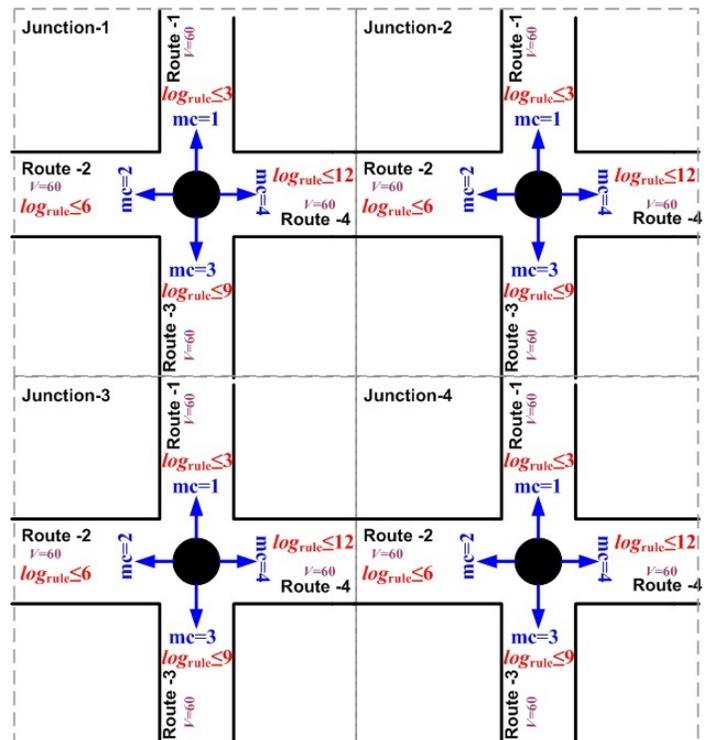


Fig. 5. Simulation Environment for Proposed JMC Framework.

## B. Results and Discussion

The performance of the proposed JMC framework is evaluated in terms of analyzing different parameters, such as no. of vehicles passed and effectiveness multi-value logic set and so on. More specifically, the efficiency of the proposed framework is demonstrated in terms of analyzing the four important parameters as given by,

- a) Analysis of Frequency of MOVE Command and number of vehicles passed.
- b) Analysis of Fluctuation Score.
- c) Analysis of Ruleset score and
- d) Analysis of Command Transition duration.

1) *Analysis of MOVE Command Frequency and number of vehicles passed:* Fig. 6(a) and (b) show the simulation results of move command frequency as well as vehicles passed in terms of bar graphs with respect to the corresponding routes, which are inbound to junction points. Precisely, *move* command frequency is defined as the number of times the controller executes signal for moving the vehicles in order to facilitate clearance to move, which is similar to green light signal. The simulations are carried out up to 500 iterations, in which it exhibits increasing occurrence of vehicle clearance for all four sample routes as shown in Fig. 6(a). Similarly, a number of vehicles that are allowed to pass also exhibit an incremental curve as indicated in Fig. 6(b), which in turn proves the efficiency of the proposed framework.

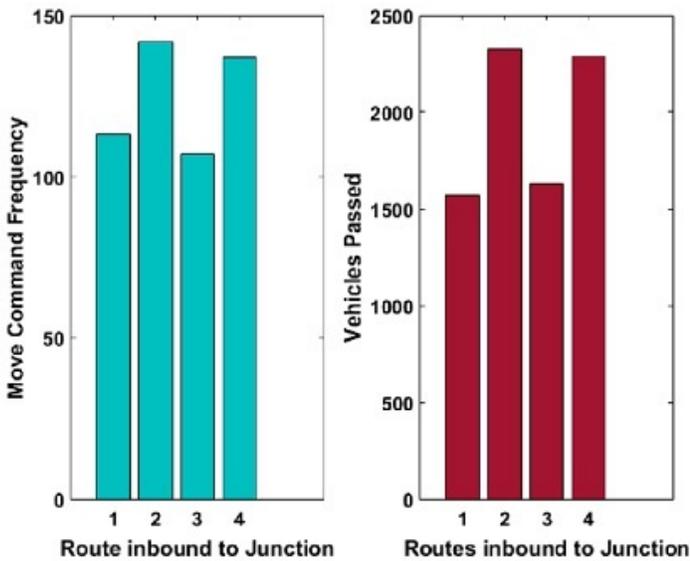


Fig. 6. (a) Analysis of Move Command Frequency (b) No. of Vehicle Passed.

2) *Analysis of Fluctuation Score:* Fig. 7 shows the results of second performance parameter -fluctuation score, which is a dimensionless unit, for a maximum of 500 simulation rounds. Specifically, Fluctuation score is defined as, the degree of execution of the logical ruleset considering three scenarios including lower, medium and higher traffic along with the time for move command is computed. More specifically, the goal is to find differences in the duration of the move command which is needed for vehicle clearance in every defined route. Using ruleset, if the time duration of the move command is found

less than 2 seconds or 5 seconds or more than 5 seconds, then the system automatically allocates scores of value of 0.8, 0.9, and 1 respectively in order to calculate the rate of fluctuation. Fig. 7 clearly indicates that, though different fluctuation rates are shown in the various routes inbound to the junction points, however the fluctuation score is restricted within the maximum of 1-2 units only. In this way, Fig. 7 demonstrates the improved consistency of the proposed JMC framework in terms of lower degree of fluctuations, by means of balancing the complete traffic system without any occurrences of deadlock situations.

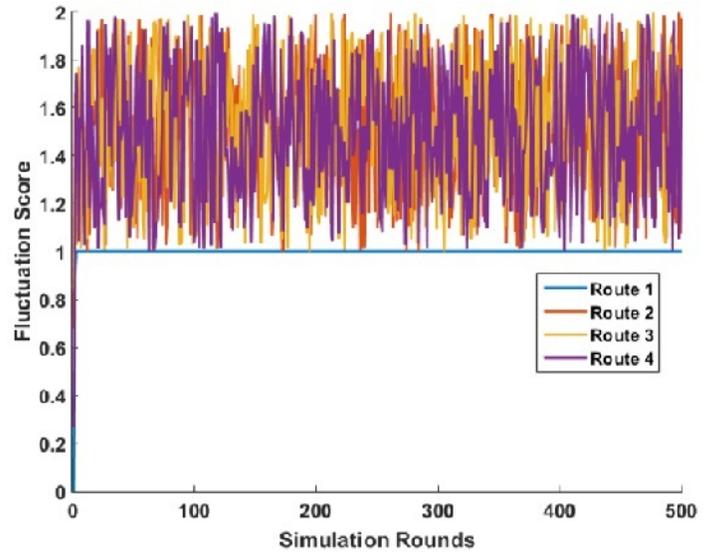


Fig. 7. Analysis of Fluctuation Score.

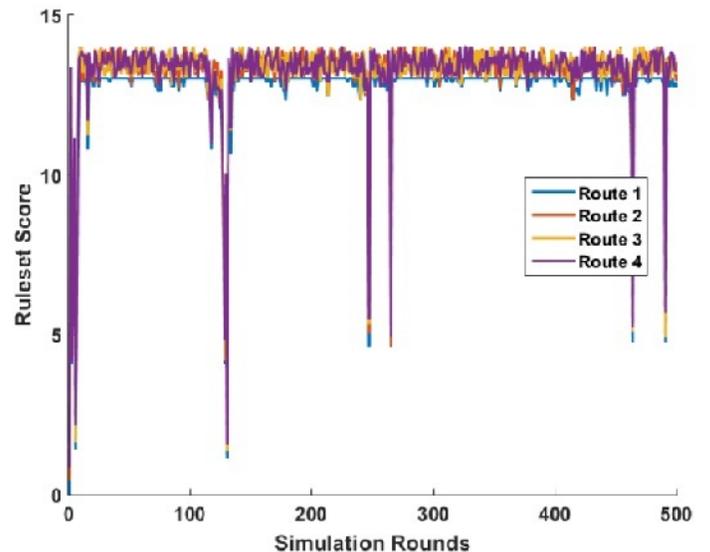


Fig. 8. Analysis of Ruleset Score.

3) *Analysis of Ruleset score:* Fig. 8 illustrates the results of Ruleset score, which is an essential parameter, since it plays a significant role in predicting performance of the proposed JMC framework. Precisely, ruleset score responsible for finding out the actual need of the ruleset on 4 test routes. It is to be noted that, in the proposed system, ruleset database consisting of 81

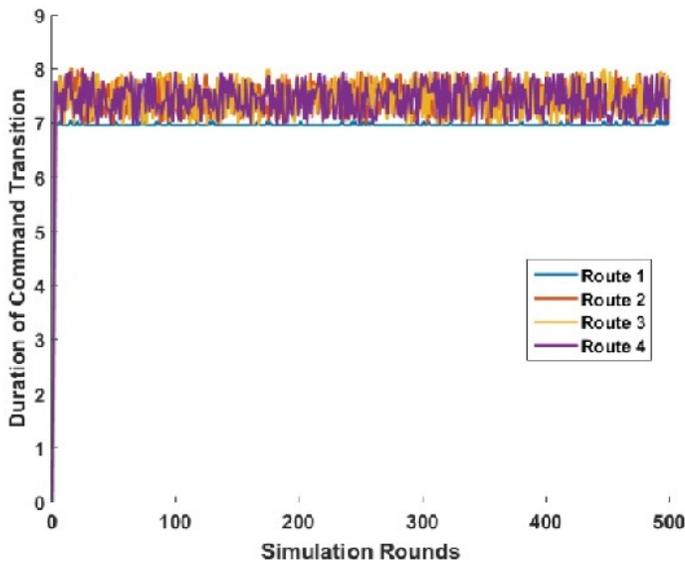


Fig. 9. Analysis of Duration of Command Transition.

rulesets covering all possible cases of traffic density is utilized as described in Section 3. Fig. 8 graph indicates that the rulesets are capable of dynamically controlling the variable rate of traffic density with higher consistency for all four sample routes. It is also observed in Fig. 8 that, though there is an increase in number of simulation rounds, yet there is not much significant divergences in the ruleset scores. Therefore, Fig. 8 results demonstrate the better consistency of ruleset scores and thereby prove the scalability feature support of the proposed JMC framework, even in case of heavy traffic environments.

4) *Analysis of Duration of Command Transition:* Fig. 9. highlights the result graphs of fourth performance parameter - duration of command transition, in terms of simulation rounds vs command transition durations. Precisely, this parameter specifies the duration of command release performed by a controller with respect to move, stop, and wait for signals. From Fig. 9, it can be observed that, a consistent outcome is indicated for all the respective routes, which in turn demonstrates the efficiency of the proposed system in monitoring and managing the traffic system. Though, the number of inbound entries over the junction increase, yet a consistent performance is indicated in the Fig. 9 graphs, which clearly proves the efficiency of the proposed framework.

## VI. CONCLUSION

In this article, a novel junction-point movement controller framework is presented, which can efficiently perform traffic monitoring and management by means of employing multi-logic rulesets. Precisely, the significant features of the proposed system are: i) usage of non-complex mechanism to carry out decision making for the elite route to be selected, ii) inclusion of routes connected at junction point with faster clearance of the vehicles, iii) system capable of counting the both inbound and outbound vehicles and thereby effective path determination and traffic density estimation becomes easier, iv) usage of the non-iterative process to offer cost-effective solution. In future, the proposed framework can be enhanced for inclusion of

security features, adaptive properties and so on, so that it can be reasonably applied in real-world urban traffic situations.

## ACKNOWLEDGMENT

The authors would like to thank the anonymous reviewers for their valuable feedback and suggestions.

## REFERENCES

- [1] Okarma, Krzysztof, Dariusz Andriukaitis, and Reza Malekian, *Sensors in Intelligent Transportation Systems* Hindawi Journal of Advanced Transportation, 1-2, 2019.
- [2] Guerrero-Ibáñez, Juan, Sherali Zeadally, and Juan Contreras-Castillo, *Sensor technologies for intelligent transportation systems* MDPI Journal of Sensors 18, no. 4 ,1212-1224,2018.
- [3] Roozmond, D. A., *Intelligent traffic management and urban traffic control based on autonomous objects* Sixth annual conference on AIS'96, Artificial intelligence, simulation, and planning in high autonomy systems, pp. 23-37. 1996.
- [4] Benalla, M., B. Achchab, and H. Hrimech, *Improving driver assistance in intelligent transportation systems: An agent-based evidential reasoning approach* Journal of Advanced Transportation, vol.20,1-4,2020.
- [5] Ben-Akiva, M, *Intelligent Transportation Systems (ITS) and the Impact of Traveler Information & Emerging Themes in Transportation Economics and Policy* Transportation Systems Analysis: Demand & Economics, USA, 2008.
- [6] Sładkowski, Aleksander, and Wiesław Pamuła, eds, *Intelligent transportation systems-problems and perspectives* Springer international publishing, Vol. 303, 2016.
- [7] Hadiwardoyo, S.A., Patra, S., Calafate, C.T. et al. *An Intelligent Transportation System Application for Smartphones Based on Vehicle Position Advertising and Route Sharing in Vehicular Ad-Hoc Networks* Journal. Comput. Sci. Technol. 33, 249-262,2018.
- [8] Salazar-Cabrera, Ricardo, Álvaro Pachón de la Cruz, and Juan Manuel Madrid Molina. *Sustainable transit vehicle tracking service, using intelligent transportation system services and emerging communication technologies: a review* Journal of Traffic and Transportation Engineering, 1-19,2020.
- [9] Qureshi, Kashif Naseer, and Abdul Hanan Abdullah, *A survey on intelligent transportation systems* Middle-East Journal of Scientific Research 15, no. 5, 629-642,2019.
- [10] Sumalee, Agachai, and Hung Wai Ho, *Smarter and more connected: Future intelligent transportation system* Iatss Research 42, no. 2,67-71,2018.
- [11] D. Calabuig, D. Martín-Sacristán, J. F. Monserrat, M. Botsov and D. Gozálviz, *Distribution of Road Hazard Warning Messages to Distant Vehicles in Intelligent Transport Systems* in IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 4, pp. 1152-1165, 2018, doi: 10.1109/TITS.2017.2718103.
- [12] H. Derrouz, A. Elbouziady, H. Ait Abdelali, R. Oulad Haj Thami, S. El Fkihi, and F. Bourzeix, *Moroccan Video Intelligent Transport System: Vehicle Type Classification Based on Three-Dimensional and Two-Dimensional Features* IEEE Access, vol. 7, pp. 72528-72537, 2019, doi: 10.1109/ACCESS.2019.2920740.
- [13] T. Blazek and C. F. Mecklenbräuker, *Measurement-Based Burst-Error Performance Modeling for Cooperative Intelligent Transport Systems* IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 1, pp. 162-171, Jan. 2019, doi: 10.1109/TITS.2018.2803266.
- [14] S. Chavhan, D. Gupta, B. N. Chandana, A. Khanna and J. J. P. C. Rodrigues, *IoT-Based Context-Aware Intelligent Public Transport System in a Metropolitan Area* IEEE Internet of Things Journal, vol. 7, no. 7, pp. 6023-6034, July 2020, doi: 10.1109/JIOT.2019.2955102.
- [15] M. A. Javed et al., *ODPV: An Efficient Protocol to Mitigate Data Integrity Attacks in Intelligent Transport Systems* IEEE Access, vol. 8, pp. 114733-114740, 2020, doi: 10.1109/ACCESS.2020.3004444.
- [16] J. K. Naufal et al., *A2CPS: A Vehicle-Centric Safety Conceptual Framework for Autonomous Transport Systems* IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 6, pp. 1925-1939, June 2018, doi: 10.1109/TITS.2017.2745678.

- [17] M. Dotoli, H. Zgaya, C. Russo and S. Hammadi, *A Multi-Agent Advanced Traveler Information System for Optimal Trip Planning in a Co-Modal Framework* IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 9, pp. 2397-2412, Sept. 2017, doi: 10.1109/TITS.2016.2645278.
- [18] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, *Blockchain-Based Dynamic Key Management for Heterogeneous Intelligent Transportation Systems* IEEE Internet of Things Journal, vol. 4, no. 6, pp. 1832-1843, Dec. 2017, doi: 10.1109/JIOT.2017.2740569.
- [19] P. Szymański, M. Żołnieruk, P. Oleszczyk, I. Gisterek and T. Kajdanowicz, *Spatio-Temporal Profiling of Public Transport Delays Based on Large-Scale Vehicle Positioning Data From GPS in Wrocław* IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 11, pp. 3652-3661, 2018, doi: 10.1109/TITS.2018.2852845.
- [20] J. Zhao et al., *Estimation of Passenger Route Choice Pattern Using Smart Card Data for Complex Metro Systems* IEEE Transactions on Intelligent Transportation Systems, vol. 18, no. 4, pp. 790-801, April 2017, doi: 10.1109/TITS.2016.2587864.
- [21] C. F. Calvillo, Á. Sánchez-Miralles and J. Villar, *Synergies of Electric Urban Transport Systems and Distributed Energy Resources in Smart Cities* IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 8, pp. 2445-2453, Aug. 2018, doi: 10.1109/TITS.2017.2750401.
- [22] Y. Tian, J. Gelernter, X. Wang, J. Li, and Y. Yu, *Traffic Sign Detection Using a Multi-Scale Recurrent Attention Network* IEEE Transactions on Intelligent Transportation Systems, vol. 20, no. 12, pp. 4466-4475, Dec. 2019, doi: 10.1109/TITS.2018.2886283.
- [23] Z. Cai, F. Ren, J. Chen and Z. Ding, *Vector-Based Trajectory Storage and Query for Intelligent Transport System* IEEE Transactions on Intelligent Transportation Systems, vol. 19, no. 5, pp. 1508-1519, May 2018, doi: 10.1109/TITS.2017.2726103.
- [24] J. L. C. Choy, J. Wu, C. Long and Y. Lin, *Ubiquitous and Low Power Vehicles Speed Monitoring for Intelligent Transport Systems* IEEE Sensors Journal, vol. 20, no. 11, pp. 5656-5665, 2020, doi: 10.1109/JSEN.2020.2974829.
- [25] C. B. Rafter, B. Anvari, S. Box and T. Cherrett, *Augmenting Traffic Signal Control Systems for Urban Road Networks With Connected Vehicles* IEEE Transactions on Intelligent Transportation Systems, vol. 21, no. 4, pp. 1728-1740, 2020, doi: 10.1109/TITS.2020.2971540.

# Employing Video-based Motion Data with Emotion Expression for Retail Product Recognition

Ahmad B. Alkhodre, Abdullah M. Alshanjiti  
Faculty of Computer and Information Systems  
Islamic University of Madinah (IU)  
Madinah 42351, Saudi Arabia

**Abstract**—Mining approaches based on video data can serve in identifying stores' performance by gaining insight into what needs to be proceeded to further enhance customers' experience, leading to increased business profits. To this end, this paper proposes an association rule mining approach, depending on video analytic techniques, for detecting store-items that are likely to be out of demand. Our approach is developed upon motion-tracking and facial emotion expression methods. We used a motion-tracking technique to record information related to customers' regions of interest inside the store and customers' interactions with the on-shelf products. Besides, we have implemented an emotion classification model, trained on recorded video data, to identify customers' emotions towards items. Results of our conducted experiments yielded several scenarios representing customer behavior towards out-of-demand stores' items.

**Keywords**—Shopper Behavior; motion tracking; emotion classification; machine learning; association rule learning

## I. INTRODUCTION

The advancement of Internet retailers and online stores for over two decades has empowered and facilitated consumer experiences. Unlike visiting physical stores, online shoppers can comfortably search for their needs, place them at competitive prices, and then request a home delivery service with ease. To a considerable extent, Internet retailers are highly lucrative as they offer customers the facility to order a universal variety of products from all over the world. However, traditional retail stores necessitate being more competitive with offering services that guarantee customer satisfaction and loyalty. Consequently, marketing specialists and store owners are perpetually attempting to find any intelligent solution that could enhance the customer's shopping experience, using, e.g. sensors equipped with computer vision technologies [1]. Such technologies can aid retail stores in staying competitive and offer the best desirable services [2].

Understanding customer behaviors on one hand and business requirements to success, on the other hand, is essential for the sustainability of e-shopping. There are many traditional methods used by businesses to collect information about the needs of their customers (such as feedback questionnaires). These methods can provide good insight, but they have some significant drawbacks. Therefore, with the advancement of data collection and processing technologies as well as the use of highly accurate sensors, one can collect vast amounts of data about the customers and get many valuable insights [1].

Depending on video analytics, data mining approaches can serve in identifying a store's performance by gaining insight

into what needs to be carried out to further enhance customers' experience, leading to increased business profits [2]. Some helpful information that is obtainable through the use of Big Data analytics such as customers' regions of interest, customer count during a particular time, customer's emotion recognition, general information about the customer like their age and gender, interactions with on-shelf products, purchasing patterns and products that are likely to be bought together. Business owners can leverage this information to achieve great results that help in keeping customers returning to their stores and increase their financial returns.

This paper studies a learning-based solution for predicting the sales of items in retail chains and/or physical stores. In particular, we propose an association rule mining approach, depending on video analytic techniques, for detecting items that are likely to be out of demand. The association rule is a data mining technique that we apply to a store's transactional database to extract information about items (mainly about explicit features). Relying on available video analytic tools, we use a motion-tracking technique to record information related to customers' regions of interest inside the store and customers' interactions with the on-shelf products. Besides, we implement an emotion classification model, trained on recorded video data, to identify customers' emotions towards items. In a nutshell, this paper makes three contributions as follows:

- We propose an association rule-mining approach compounded with video analytic techniques for predicting the sales of items in physical stores, including out-of-demand items.
- We report on seven different scenarios representing customer behavior towards items that are out-of-demand.
- We conclude the paper by giving broad recommendations to tackle the symptoms of out-of-demand items.

The remainder of this paper is organized as follows: Section II represents the related works, shedding light on data analysis, motion-tracking, and emotion detection techniques. In Section III, we introduce a high-level design of our proposed predictor, and then we give a brief description concerning the technical tools used for implementation. Section IV presents and discusses the conducted experiments for assessing our proposal. Last but not least, Section V concludes the paper with suggestions for future research to consider.

## II. RELATED WORK

This section reviews different sorts of related work, described into three aspects: data analysis, motion tracking, and

emotion detection aspects. The original contribution of this paper lies in mixing these three aspects in our proposed solution.

#### A. Literature Related to Data Analysis

The system suggested in [3] mines data from a transaction database of a retail market. It is supposed to be similar to popular mining tools such as Weka and RapidMiner. The data is stored in a MySQL database which is later accessed by simple Java and Python programs to apply a classification algorithm (C4.5) and an association rule mining algorithm (Apriori). Advantages of this system include being simple, user-friendly, and lightweight. In addition, information can be drawn directly from the operational database. The main goal of [4] is to discover the association between items to help store owners figure out the best layout for their stores. A simple Apriori algorithm is used to find the frequent itemsets and then apply the Lift measure for the association between sets to discover the rules between items. Before mining the association rules, the items of the store are divided and then grouped into sub-categories. This is useful because, in many cases, some items are considered substitutes.

Association rule mining in [5] is based on quantitative correlation coefficient (Pearson's correlation coefficient). It allows us to extract linear relations between two item sets. The suggested method starts by grouping transactions by the desired criteria (specific periods, for example), making it worthwhile to discover relevant rules within a given time frame. After the data has been grouped, a quantitative correlation analyzer is used to derive relations between item sets. Results of this implementation show more patterns detected in comparison to traditional association rule mining. In addition to discovering periodic customer demand which helps owners introduce offers and balance the supply and demand for products.

A study described in [6] proposes a model for finding periodically repeated patterns in a database. A pattern-growth algorithm (GPF-growth) was proposed to detect these patterns. A given pattern is considered frequent when it occurs within a defined maximum period, and its support exceeds the user-defined minimum. Thus, when it comes to analyzing data from the customers' transactions finding repeated patterns yields information related to regularly purchased products. The works described in [7], [8] apply the principles of association rule mining algorithms such as Apriori and FP-growth. Nevertheless, unlike these algorithms, the proposed approach focuses on the time of transactions. As a result, a new type of pattern is defined, which is called transitional patterns. The frequency of such patterns changes noticeably over a period of time. First, frequent patterns in the database are discovered by the use of an association rule mining algorithm such as Apriori or FP-growth. After that, an algorithm called TP-mine is introduced for the purpose of transitional mining patterns. With the use of this algorithm, it is possible to extract points in time where a frequency of an item-set has changed negatively or positively.

The aim of a study described in [9] is to introduce a method for analyzing a customer's basket data and deriving relevant association rules between its items. The approach relies on minimum spanning trees (MSTs). Using a minimum spanning tree for representing relations between items allows us to consider those strongly correlated items, which limits the search

space for the association rule mining. Another advantage of this approach is that not only can we extract strong association rules, but also, we can find items that tie other items together. In the study described in [10], an algorithm is proposed for detecting changes and trends in transactions data. It relies on association rule mining and the prediction of rules that may change at a later time. The algorithm works by tracking rules with high confidence, and the result of this algorithm is rules that will have higher confidence in the next period and rules which will have lower confidence. Apriori algorithm is used to mine rules over many time frames, and later each of the rules is given a score for each time frame to help track changes in confidence level over time. The approach provides great insight that could help prepare for upcoming association rules changes and find outlier rules that may apply in few time frames. However, the main disadvantage of this method is that it is heavily skewed based on the manually selected threshold values.

The main point of a study described in [11] is to understand the purpose behind customers' visits to a store. This is done through data mining transactions data and identifies the products in each transaction, and based on these products, the customers' purpose can be understood. The approach uses clustering techniques to segment different visit types, and the purpose behind these visits is later identified based on the types of products they contain. K-means clustering is used to segment visits in this research. The contribution of a study described in [12] is a framework that helps in predicting sales changes based on weather data. Two models are deployed to help with the prediction of the change in product demand. One of them is short-term, and the other is for long-term predictions. A LASSO Poisson regression model was used for predicting the impact of weather on customer demands.

A method for recommending the next purchase for customers is detailed in [13]. They have named the Co-Factorization model over sequential and historical purchase data (CFSH). Transactions data is mined to discover sequential purchasing patterns. From these patterns, two matrices are constructed. One for sequential and one for historical customer behaviors, these two matrices are both factorized to predict the best recommendation for the next customer visit. A study described in [14] suggests a method for segmenting customers based on their lifestyle. The segmentation is done with the help of analyzing a retailer's transactional database. The approach relies on a variable clustering algorithm (VARCLUS), resulting in clusters of related items. The lifestyles for each cluster are identified by looking into the type of items in each cluster. Each customer is then assigned to a lifestyle based on which cluster's item types did they purchase the most.

The contribution of [15] is a framework for product feature characterization and predicting the customer's most preferred specifications by analyzing purchase history data. A trained neural network model was used with the input as a matrix of all possible combinations of a product specification. The output is the predicted customer satisfaction rate. Predicting the customers' preferred characteristics in a product can guide a manufacturer to develop a product based on the customers' needs. A study described in [16] introduces a recommendation system that's based on collaborative filtering and data mining techniques. Customers are segmented based on their values

using the RFM analysis. The used clustering algorithm is K-means. To discover the best recommendation for a customer, the cluster that they belong to is identified first. Then, the Apriori algorithm is applied to transactions that belong to customers in the same cluster to extract the top associated items.

Another study described in [17] proposed a method to discover frequent itemsets with high value to the sellers. Association rule mining is applied on transactional databases considering the FM (frequency, monetary) values for the transactions. The result is association rules which have high revenue potential. These works highlight many important algorithms and techniques in the field of data analysis in order to find helpful information from the customer's transaction data such as products that have more or less sold, compatible products, time statistics, and more information, which we will mention it in the coming sections.

The main advantage of the proposed method in this paper is that it considers user-centric and item-centric recommendations to discover the correlation between customers and products, allowing for better recommendations.

### *B. Literature Related to Motion Tracking*

Work described in [18] describes a computer vision system in real-time; this system is designed for an electronic billboard and recognition and track customers, the provide a piece of demographic information about these people. This information is used to update the current advertisement on current products to fit customer needs. The information provided by this system about customers includes age, the number of customers, how much time customers sets in front of the billboard. Another study described in [19] introduced a new system for monitoring and tracking the number of customers in some open places like a shopping center and museums hall. Two main techniques are used to develop this work first one is the laser scanner, and the second one is a single camera. To combine the information that extracts from these two tracking devices, Bayesian methods are used. The advantage of this approach is that it combines two techniques and uses them in one field of tracking people. However, the disadvantage of this approach is that it is inaccurate information is from the laser scanner. Work described in [20] provides an integrated system based on an RGB-D camera. This system can monitor customer behavior inside the shop environment. In addition, discover the interaction between customer and products through analysis of the recorded videos and classify this interaction into three types: pick up the product, pick up the product, and bring it back to the shelf and no interaction between customer and product.

The study described in [21] provides a system which distinguishes a variety of customer behavior opposite the products: incurious, taking a look, passing the body near shelf, touch the product, take product then return it to a shelf and take it and put into shopping cart, which gives us a hint that the customer has an interest in products. The given system is dependent on the orientation of head and body and arm action, which divided those into eight directions to estimate whether the customer searches to products or looking to the shelf. Then, a semi-supervised learning method was applied to

improve the training dataset and generate the file that contains accurate data. Work described in [22] showcases a system for tracking and identifying customers' interactions with on-shelf products inside a retail store. To accomplish the tasks of this system, an RGB-D camera is installed in a vertical position to capture the area of a store shelf. The Water Filling algorithm is used to recognize customers' interactions. Interactions such as a customer picking up a product off the shelf, putting a product back on the shelf, and customers grouping formation can be evaluated. The data collected from these interactions makes it possible to construct an intensity map on a shelf to show where interactions happened. Some of the most prevalent obstacles that a system like this might face are camera position, person's clothing, occlusion, body pose changes, diversity in product shapes, and constantly changing background. Some key factors make the implementation of this system viable, such as its affordable cost and ease of installation and maintenance. A study described in [23] proposes a framework for people detection in a store environment with the help of essential CCTV (Closed-circuit Television Camera) security cameras. The approach aims to achieve accurate customer detection from video recorded by the store's security cameras. An SVM (Support Vector Machine) binary classifier is used to classify each frame, where it returns positive if a person is detected or negative if not. Detected data is then recorded and mapped with coordinates to signify a customer's location within the video frame. This data is later mapped into a heat map to show the highest traffic areas within the store. The heat map visualization is based on Kernel Density Estimation (KDE). Advantages of this approach are the availability of CCTV cameras in many stores and an unambiguous visual representation of the exciting store regions.

Work described in [24] suggested CREEN system, which is an intelligent mechatronic system for help customers to search or to get the products which they want within the retail environment. This system works to reduce the needing to put helping icons or maps within the storing center. This system's primary function helps people move within the store by forecasting the probability that customers will attract positions that are analyzed in front of a shelf of products. There are installed tools on the cart that include information about the location of elements and a location map for elements, which in turn leads the customer to the product he wants to pick. This system aims to develop a robot that searches for the best location to put the product within the store. Also, it can be used for blind and older adults. A study described in [25] presents the VMBA problem, which is based on set up cameras on store carts and considers three main stages, which include: the interaction, location, and the scene that is taken from the camera. Which in result goal to inference the behavior of customers within the retail environment. Furthermore, by merging these behaviors with information exported from the analysis, the market cart-like (transactions) gives retail store owners the management of areas and shopping strategies. Work described in [25] provides a new methodology for tracking, which is based on the visual attention focusing for customers WVFAO for many persons and which is used on understanding human behavior. This approach is based on capturing the attention of wandering to external ads and considers Bayesian network (HDBN) to discover the number of people in scene, body, head location (Direction), the interactions, and WVFAO

their own. In addition, this research includes the way to design the model WVFOA.

As a result of previous research, we can list many techniques in the field of tracking the motion of people and the study of their behavior. These techniques will provide our work the complete information about customers' behavior within the store, such as information about customers' (age, gender), customer count and region of gathering people, etc. In addition to that, the interactions between customers and products like how much time customers spend in front of a product, if interested or not. This information considers the main thing in our work which we will mention this necessary in the following steps.

### C. Literature Related to Emotion Detection

A study described in [26] explains that a strong structure is a design to recognize the three-dimensional position and local emotional expressions of the face, such as eyelid movements and mouth movements, which given a significant role in explaining the face emotion expression, by using RGB-D camera and the Kalman Extended filters. Advantages of this method include high 3D data with the information of color and density, high accuracy, and full automation. Disadvantages include that it is sensitive to light cases and gets confused by shadows. Another study described in [27] study the face recognition depending on FTFA-DLF. FTFA-DLF can merge deep learning features and handcraft features extracted from the nose, eye, and mouth regions. It used to help deep learning features by adding deep learning and handcraft features to the objective function layer to get better facial recognition performance based on the LFW dataset. Advantages include color information, and the descriptor computation strategy does not affect performance, high accuracy, and is fully automated. Disadvantages include missing pixels and brightness have a harmful effect and data storage.

Work described in [28] study an emotion recognition system depending on a MATLAB environment into a MATLAB Simulink environment that is able to recognize facial expression automatically in real-time. The label and the dataset used in this study build-up from the videos. The facial recognition system built on the programmable array and the camera sensor uses through this study can recognize facial emotion in actual time at a frame rate of 30. Advantages include FPGA devices being updatable, fully automated, high-performance, and FPGA no need cost compared to ASLCS. Disadvantages include Data storage and camera angle. Work described in [29] presents some algorithms for facial expression recognition grin detection. The algorithms depend on deep machine learning a [CNN], the main goal of this network is to select one of the six types of emotions using the [CMN] MultiPie database, by training through this database parallel on a large number of independent flows on [GPU]. Advantages include accuracy in image detection problems and being fully automated. Disadvantages include being very slow to train and needing to use a lot of data and data storage and camera angel training.

A study described in [30] suggests a way for emotion recognition-based facial components. It is complete in extracting the local features of the mouth and eye from each frame using GW with selected orientations and scales. The

express that features on to classifier for detecting of the face scope. From detection, each pixel on through the face. Finally, select and recognize the emotion of the face by using the Adboost algorithm. Advantages include improved performance compared to the current techniques because of its new features and not affected by changes in colors lighting. Work described in [31] applies the concepts of deep learning for detecting facial expression, so they proposed a facial expression monitoring system [PFEMS] in addition to design a convolutional neural network model using TensorFlow into two parts: a) Validation tools and b) Training model for data training after extracts the facial images from the video frames into the facial detector then detecting this image by using CNN to monitor the emotion state from the six universal emotions [angry, disgust, happy, surprise, sad and fear].

A study described in [32] introduces a method for the classification of facial expressions, which is based on a fuzzy logic model. The approach relies on a supervised machine learning method, which uses pre-existing databases that contain images of faces labeled with their respective emotions. A set of fuzzy logic rules are generated from the given data using the FURIA algorithm. These rules are generated based on the cosine values of the essential triangles plotted on the most critical points on a face. Each generated fuzzy rule presents some conditions, which are then used to classify different emotion types. To start the emotion recognition, first, a face must be detected. For this task, the DLIB toolkit was used for real-time face tracking and provide a set of 68 landmarks from the face detected. Some triangles are then overlaid over these points, and the cosine value is calculated for all the vertices of the triangles. The values are later passed to the generated fuzzy rules to recognize the emotions expressed in the image. The main advantages of the proposed method include working with image files, pre-recorded video, and live webcam, and it can classify emotions in real-time and detect multiple faces simultaneously. Limitations of this study include it can only classify six basic emotions, the model used is influenced by the quality of the data used in training it, and the model detects most intensive emotions better than less intensive emotions.

While Cisco has afforded different and promising solutions towards improving the shopper experience using IoT and big data analytical approaches [33], [34] (i.e. depending on monitoring and analyzing the shopping path and their movements), their focus stayed on studying horizontally a massive set of data without paying much attention to specific products. Nevertheless, this paper differs in that our approach focuses on detecting a particular product (i.e. out-of-demand store-items) based on the shopper's interaction with a product vertically.

## III. APPROACH

This section presents our proposed association rule-mining approach, which consists of three main components (i.e., data analysis, motion detection, and emotion detection), illustrated in Figure 1. We explain these components in some detail in the following subsections.

### A. Data Analysis

This component is concerned with analyzing data collected from stores' transactional databases using association rule

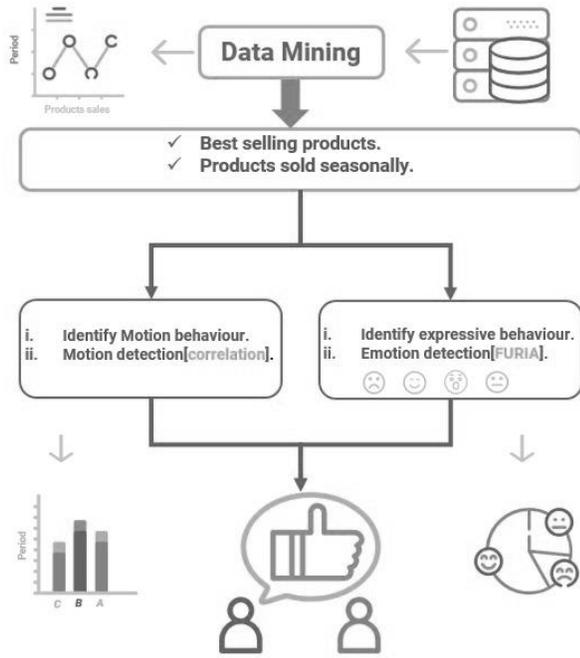


Fig. 1. The Top Level Workflow of our Proposed Approach, Illustrating the Interaction between the three Main Components (i.e. Data Analysis, Motion Detection, and Emotion Detection).

mining. Through this analysis, business owners can discover knowledge pertaining to associated store items that could be bought together, customers’ periodic purchasing patterns, product performance, and other sound patterns. In addition to analyzing the data from the customers’ transactions, this component supports analyzing video data collected from motion and emotion observation tools.

There are different algorithms for association rule mining, but the two widely used are Apriori and FP-Growth. We choose to implement the FP-Growth algorithm as it performs better with larger datasets. In addition, the FP-Growth algorithm relies on the divide-and-conquer approach and only performs two full I/O scans of the database, making it more suitable for more large databases. Concerning the tool used, we have implemented the FP-Growth algorithm using PyFpgrowth<sup>1</sup>.

More in detail, to use PyFpgrowth, one needs to encode data from transactional structures into a 2-dimensional list object, where each sub-list contains the items of a single transaction. To generate the association rules, one also needs to specify the minimum values for support, confidence, and lift. By specifying these values, the best rules can be generated while controlling their size. The output from this algorithm is a set of association rules, each with its specific values for support, confidence, and lift.

Figure 2 describes the results generated from the association rules from a sample dataset used in our experiments using

<sup>1</sup>A Python implementation of the Frequent Pattern Growth algorithm <https://pypi.org/project/pyfpgrowth/>

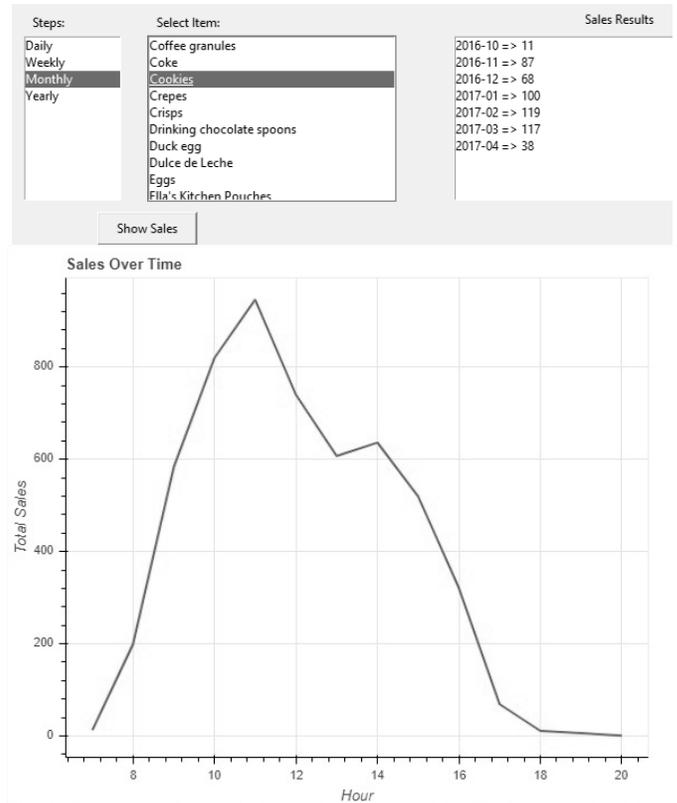


Fig. 2. Examples of Association Rules Generated by FP-Growth Algorithm.

the FP-Growth algorithm with the configurations (Minimum support = 0.05, minimum confidence = 0.2, minimum lift = 0.4). The aim here is to infer the total sales of a selected product in specific periods (weekly, monthly). This is essential to detect the change in customer behavior and their inclination towards some products. By using the same previous dataset of bakery sales, we can view a list of unique products present in the transactions. The next step is to select one of the products from the list and the period steps to show the total sales. The output of choosing the product 'cookies' and choosing the monthly steps shows the total sales of the product for each month recorded in the dataset.

The ability to discover relations between items and to show the change in customer inclination to buy a particular product is helpful for this project as they provide us with critical information about the customers’ behavior. Although sometimes the reasons behind these changes in customer behavior may not be apparent to the business owners. Hence, we suggest that business owners need to further inspect the reasons behind the ambiguous changes using the proposed methods for customer tracking and emotion classification, discussed in the next subsections.

### B. Motion Detection

Store video analytics is an essential technique to understand the customers’ behavior accurately. With the help of this component, we can collect information related to customers’ region of interests (ROIs), customer count, density maps, customer’s interaction with on-shelf products, and general information about the customer such as their age and gender. The system

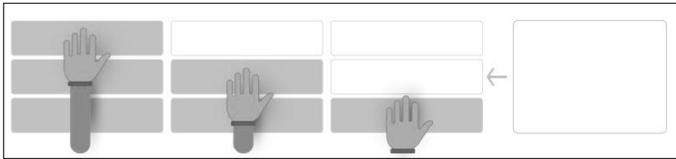


Fig. 3. Classification of Customers' Interest based on Hand Movement.

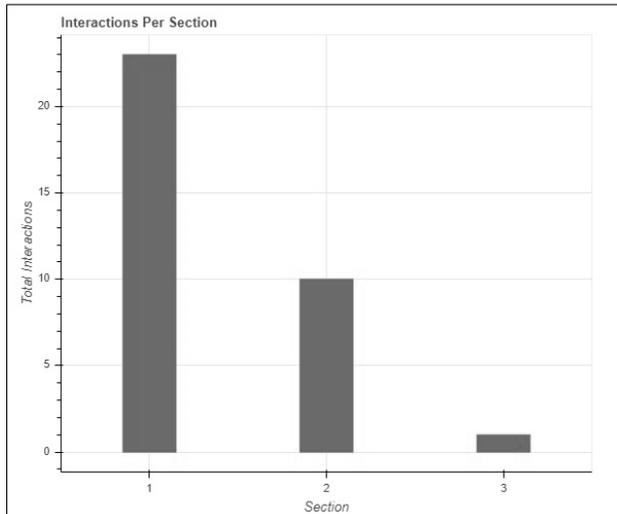


Fig. 4. Result of the Interaction Per Section between the Customer and the Selected Product.

also records data related to the customers' interactions with the products on the shelf; this is done by applying a motion detection algorithm that we implemented. We concluded that the best way to capture the customers' interactions is through a camera that is installed above the shelf. The camera shall only record the area which is very close to the shelf.

The used algorithm works with the real-time video that is captured from the camera and divides every captured video frame into three equal sections, as shown in Fig. 3. The main reason behind this separation is to provide us with a way to classify the customers' interactions based on how close they are to the shelf. The algorithm will then detect the interactions (motion) that happen at each section separately and record the section number and the time when the interaction happened.

This data can help business owners understand the types of interactions that their products get. For example, if we compare the total number of interactions recorded in Section 1 (closest section to the product) and the total sales of that product, we could detect cases where products might get a lot of interaction/interest from customers but a low number of those customers purchasing the product. Thus, we can conclude that there might be something we can improve with that product.

The main goal of the algorithm is to detect and record motion-captured from real-time video. The execution starts by defining a list that contains three objects of the Frame class. The Frame class has a constructor that defines two main properties for each frame. First is the content property, which will be assigned the image captured from a video source. Second is the stoppage frames property that will start as 0

initially but should later be incremented accordingly. Finally, we create a second list that should hold the three corresponding reference frames (background frames) during execution. These frames are only initialized once.

Execution continues by reading the first frame from the video source (camera). The frame will then be split into three equal (in height) frames. Each one of these subframes will be assigned to the three previously declared frame objects. We then iterate over each of the frame objects to detect movement separately for each section. The iteration over a frame object starts by processing the frame to be ready for movement detection. Frame processing includes: (1) converting the frame to grayscale and (2) applying Gaussian blur on the frame.

The next step is to check if the corresponding reference frame is initialized. To determine if there is a movement that occurred between our current frame and its reference frame, we need to:

- 1) Calculate the absolute difference between them and assign it to a new frame.
- 2) Apply threshold on the subtracted image with a chosen threshold value.
- 3) Dilate the threshold image.
- 4) Find contours in the dilated image.
- 5) Calculate the total area of the contours found.

Next, check if the total area of contours exceeds the set minimum. Setting the minimum value depends on how large the object one needs to track (hand in this case). If the minimum is exceeded, we check if the stoppage frames for the current frame if it exceeds a set value (15) that means that an object has entered the frame, and we can record the current time and the section related to the movement and we have to reset the stoppage frames back to 0 because the frame currently has movement.

If the total area of contours did not exceed the minimum value, we could increment the stoppage frames for the object. The execution will then continue for the remaining two frames. After that we begin executing the same steps for the next frame of the video source. Fig. 4 displays the interaction per section between the customer and the selected product.

### C. Emotion Detection

Advancement in the field of deep learning and computer vision allows to capture the facial expressions of a customer and accurately predict their displayed feeling. This can be helpful for getting information about the customers' feelings toward certain products. Understanding how the customer feels opens up many questions about why they feel a certain way in a given moment. Through understanding how the customers feel, we can propose solutions to enhance their shopping experience further. The system analyzes video recordings of people and detects their facial expressions, then record and store that data. The emotions detected from peoples' faces can be helpful in trying to understand their behavior and to evaluate their satisfaction rate. A business must keep the customers' satisfaction to retain their loyalty.

The input is taken from a video camera. At the start, the algorithm splits the video into a list of frames, and each frame constructs an image frame. Then a face must be detected within

the image frame. This is done with the DLIB toolkit. Then cover the face that is discovered with a rectangular shape. The toolkit will also plot some points and form triangles on significant areas in the face (eyes, nose, and mouth) detected and calculate the cosine values for all vertices. Values are then passed to some fuzzy rules to determine the emotion detected from the frame. Testing was done using a video recording of one person. The length of the video was 42 seconds, and the recorded instances in the results were 450. The result is recorded in an Excel file with their respective time stamps and emotion classifications. Then Represent the results in a byte chart to make them more understandable by the client. The recorded result contains 450 instances where each one has a precise time stamp and a value for each emotion recorded as shown in Figure 5.

Data on peoples' expressions could be further analyzed to understand the meaning behind them. For this paper, we found a reliable way to collect such data, but this information is handy to business owners because they need to know the customers' feelings and understand their causes to adapt their business to improve the customers' satisfaction. In our case, we consider that the customer needs to touch the product to know the price.

Time	Msec	Stamp	Happy	Sad	Surprise	Fear	Disgust	Anger	Neutral
00:00:12	967	0.11.967	0.00	0.00	0.00	0.00	0.00	0.00	1.59
00:00:12	0	012.000	0.00	0.00	0.00	0.17	0.00	0.00	1.81
00:00:12	33	0.13.033	0.00	0.00	0.00	0.17	0.00	0.00	1.81
00:00:12	67	012.067	0.00	0.00	0.00	0.17	0.00	0.00	1.81
00:00:12	100	012.100	0.00	0.00	0.00	0.17	0.00	0.00	1.81
00:00:12	133	021.200	0.00	0.00	0.00	0.17	0.00	0.00	1.81
00:00:12	167	012.233	0.00	0.00	0.00	0.17	0.00	0.00	1.81
00:00:12	200	012.267	0.00	0.00	0.00	0.17	0.00	0.00	1.81
00:00:12	233	012.300	0.00	0.00	0.00	0.17	0.00	0.00	1.81
00:00:12	267	012.333	0.00	0.00	0.00	0.17	0.00	0.00	1.81
00:00:12	300	012.367	0.00	0.00	0.00	0.35	0.00	0.00	1.99
00:00:12	333	012.400	0.00	0.00	0.00	0.35	0.00	0.00	1.99
00:00:12	367	012.433	0.00	0.00	0.00	0.35	0.00	0.00	1.99
00:00:12	400	012.467	0.00	0.00	0.00	0.35	0.00	0.00	1.99
00:00:12	333	012.500	0.00	0.00	0.00	0.35	0.00	0.00	1.99
00:00:12	467	012.533	0.00	0.00	0.00	0.35	0.00	0.00	1.99
00:00:13	500	012.567	0.00	0.00	0.00	0.35	0.00	0.00	1.99
00:00:13	533	012.600	0.00	0.00	0.00	0.35	0.00	0.00	1.99
00:00:13	567	012.633	0.00	0.00	0.00	0.35	0.00	0.00	1.99
00:00:13	600	012.667	0.00	0.00	0.00	0.52	0.00	0.00	1.81
00:00:13	633	012.700	0.00	0.00	0.00	0.52	0.00	0.00	1.81
00:00:13	667	012.767	0.00	0.00	0.00	0.52	0.00	0.00	1.81
00:00:13	7000	012.800	0.00	0.00	0.00	0.52	0.00	0.00	1.81
00:00:13	767	012.833	0.00	0.00	0.00	0.52	0.00	0.00	1.81
00:00:13	800	012.867	0.00	0.00	0.00	0.52	0.00	0.00	1.81
00:00:13	833	012.900	0.00	0.00	0.00	0.52	0.00	0.00	1.81
00:00:13	900	012.933	0.00	0.00	0.00	0.52	0.00	0.00	1.81
00:00:13	933	012.967	0.00	0.00	0.00	0.52	0.00	0.00	1.81
00:00:13	967	013.00	0.00	0.00	0.00	0.56	0.00	0.00	1.81
00:00:13	0	013.033	0.00	0.00	0.00	0.56	0.00	0.00	1.81
00:00:13	33	013.067	0.00	0.00	0.00	0.56	0.00	0.00	1.81
00:00:13	67	013.100	0.00	0.00	0.00	0.56	0.00	0.00	1.81
00:00:13	100	013.133	0.00	0.00	0.00	0.56	0.00	0.00	1.81
00:00:13	133	013.167	0.00	0.00	0.00	0.56	0.00	0.00	1.81

Fig. 5. A Screenshot Illustrating the Generated Output from the used Emotion Detector.

#### IV. EXPERIMENT AND DISCUSSION

##### A. Questionnaire

We prepared a questionnaire<sup>2</sup> to identify customers' emotional reactions against the items with exorbitant prices, out-of-date products, and so on. 150 people took the questionnaire

<sup>2</sup>[https://docs.google.com/forms/d/e/1FAIpQLSdSRhmV9esbHdCSZQ6n\CvDMm2e-JK4Q-M\\_FyYQ89VEC7J5xJg/viewform](https://docs.google.com/forms/d/e/1FAIpQLSdSRhmV9esbHdCSZQ6n\CvDMm2e-JK4Q-M_FyYQ89VEC7J5xJg/viewform)

(90 males and 60 females). The mean age of the participants was 22 years. The responses were statistically analyzed to find the customers' emotions against the design and price of the items. Based on the results of the questionnaire, we classified emotions into six categories, which include Happy, Sad, Surprise, Fear, Disgust, and Anger.

##### B. Experimental Setup

We experimented with a grocery store in which some products were facing sales problems, as reasoned from the transaction database of the store. We picked these products for our experiment. We set up the proposed system for 30 days to analyze the behavior of customers towards the product. During the experiment, 3000 customers visited the store in total, with an average 100 customers per day. Out of these, 2500 customers interacted with the products monitored with an average of 83 customers per day.

##### C. Results

TABLE I. SUMMARY OF RESULTS DEPENDING ON BOTH THE PROPOSED PREDICTOR AS WELL AS THE QUESTIONNAIRE RESULTS.

Emotion	Motion		
	Excited (>50%)	Hesitant (>50%)	Careless (>50%)
Happy	Price/Placement	Design	Placement
Sad	Placement	Placement	
Surprise	Price	Design	
Fear	Price	Design	
Disgust	Design	Placement	
Anger	Placement	Placement	

Table I summaries our findings based on the measures from both prediction tasks by our proposal as well as from questionnaires. Moreover, we report on seven different scenarios representing customer behavior towards items that are out-of-demand, as follows:

*Case 1:* This case is an intersection between Excited and Careless. If no motion is recorded, then no emotion can be predicted, and the problem can be addressed by correcting the placement.

*Case 2:* This case represents the emotional happiness for more than 50% of customers towards the selected product and the interaction between customer and product (i.e. excited, hesitant, careless). If the customer feels happy and there is an interaction between the customer and product, but the product's sales are still low, then the problem is in the product price, which needs to be improved.

*Case 3:* This case represents the emotional happiness for more than 50% of customers towards the selected product and the interaction between customer and product (i.e. excited, hesitant, careless). If the customer feels happy and there is no interaction between customer and product, but there are movements in front of the product, the problem is in the product design, which needs to be improved.

*Case 4:* This case represents the emotional sadness for more than 50% of customers towards the selected product and the interaction between customer and product (i.e. excited, hesitant, careless). If the customer feels sad and there is an interaction between customer and product, then the problem is in the product placement, which needs to be corrected.

*Case 5:* This case represents the emotional sadness for more than 50% of customers towards the selected product and the interaction between customer and product (i.e. excited, hesitant, careless). If the customer feels sad and there is no interaction between customer and product, but there are movements in front of the product, then the problem is in the product placement and needs to be corrected.

*Case 6:* This case represents the emotional surprise for more than 50% of customers towards the selected product and the interaction between customer and product (i.e. excited, hesitant, careless). If the customer feels surprised and there is an interaction between customer and product, but the product's sales are still low, then the problem is in the product price, which needs to be improved.

*Case 7:* This case represents the emotional surprise for more than 50% of customers towards the selected product and the interaction between customer and product (i.e. excited, hesitant, careless). If the customer feels surprised and there is no interaction between customer and product, but there are movements in front of the product, then the product design problem needs to be corrected.

## V. CONCLUSION AND FUTURE SCOPE

Mining approaches based on video data can serve in identifying a store's performance and production by gaining insight into what needs to be proceeded to further enhance customers' experience, leading to increased business profits. To this end, we have proposed an association rule mining approach, depending on video analytic techniques, for detecting store-items that are likely to be out of demand. Our approach is developed upon motion-tracking and facial emotion expression methods. Results of our conducted experiments yielded seven different scenarios representing customer behavior towards out-of-demand stores' items.

Regardless of the high computational costs associated with the mining process, challenges to ideally apply our approach require overcoming: illumination conditions, complex people activities, crowded areas, constantly changing backgrounds, occlusion, and ineffective camera placements. We plan to tackle these challenges in the future besides conducting other experiments on a more comprehensive real-world dataset to validate the concept of our approach.

## ACKNOWLEDGMENT

We are grateful to Wasim Ahmad  for his advice on motion-tracking and emotion analysis methods, and their use in association rule-mining..

## REFERENCES

- [1] I. E. Olatunji and C.-H. Cheng, "Video analytics for visual surveillance and applications: An overview and survey," *Machine Learning Paradigms*, pp. 475–515, 2019.
- [2] S. Chandramana, "Retail analytics: Driving success in retail industry with business analytics," vol. Volume 7, 08 2017.
- [3] K. P. Nagwekar, K. S. Chowdhary, G. M. Shejwal, and V. N. Alone, "Data visualization and data mining for retailers," *International Journal for Innovative Research in Science and Technology*, vol. 3, no. 11, 2017.
- [4] K.-I. Ahn, "Effective product assignment based on association rule mining in retail," *Expert Systems with Applications*, vol. 39, p. 12551–12556, 11 2012.

- [5] C. F. Cheung and F. Li, "A quantitative correlation coefficient mining method for business intelligence in small and medium enterprises of trading business," *Expert systems with applications*, vol. 39, no. 7, pp. 6279–6291, 2012.
- [6] K.-C. Lin, I.-E. Liao, T.-P. Chang, and S.-F. Lin, "A frequent itemset mining algorithm based on the principle of inclusion-exclusion and transaction mapping," *Information Sciences*, vol. 276, pp. 278–289, 2014.
- [7] R. U. Kiran, J. Venkatesh, M. Toyoda, M. Kitsuregawa, and P. K. Reddy, "Discovering partial periodic-frequent patterns in a transactional database," *Journal of Systems and Software*, vol. 125, pp. 170–182, 2017.
- [8] Q. Wan and A. An, "Discovering transitional patterns and their significant milestones in transaction databases," *IEEE transactions on knowledge and data engineering*, vol. 21, no. 12, pp. 1692–1707, 2009.
- [9] M. A. Valle, G. A. Ruz, and R. Morrás, "Market basket analysis: Complementing association rules with minimum spanning trees," *Expert Systems with Applications*, vol. 97, pp. 146–162, 2018.
- [10] M. Kaur and S. Kang, "Market basket analysis: Identify the changing trends of market data using association rule mining," *Procedia computer science*, vol. 85, pp. 78–85, 2016.
- [11] A. Griva, C. Bardaki, K. Pramatar, and D. Papakiriakopoulos, "Retail business analytics: Customer visit segmentation using market basket data," *Expert Systems with Applications*, vol. 100, pp. 1–16, 2018.
- [12] G. Verstraete, E.-H. Aghezzaf, and B. Desmet, "A data-driven framework for predicting weather impact on high-volume low-margin retail products," *Journal of Retailing and Consumer Services*, vol. 48, pp. 169–177, 2019.
- [13] P. Wang, J. Chen, and S. Niu, "Cfsh: Factorizing sequential and historical purchase data for basket recommendation," *Plos one*, vol. 13, no. 10, p. e0203191, 2018.
- [14] V. L. Miguéis, A. S. Camanho, and J. F. e Cunha, "Customer data mining for lifestyle segmentation," *Expert Systems with Applications*, vol. 39, no. 10, pp. 9359–9366, 2012.
- [15] J. Zhang, A. Simeone, P. Gu, and B. Hong, "Product features characterization and customers' preferences prediction based on purchasing data," *CIRP Annals*, vol. 67, no. 1, pp. 149–152, 2018.
- [16] F. Rodrigues and B. Ferreira, "Product recommendation based on shared customer's behaviour," *Procedia Computer Science*, vol. 100, pp. 136–146, 2016.
- [17] C.-H. Weng, "Revenue prediction by mining frequent itemsets with customer analysis," *Engineering Applications of Artificial Intelligence*, vol. 63, pp. 85–97, 2017.
- [18] I. Haritaoglu and M. Flickner, "Attentive billboards: Towards to video based customer behavior understanding," in *Sixth IEEE Workshop on Applications of Computer Vision, 2002.(WACV 2002). Proceedings. IEEE*, 2002, pp. 127–131.
- [19] J. Cui, H. Zha, H. Zhao, and R. Shibasaki, "Multi-modal tracking of people using laser scanners and video camera," *Image and vision Computing*, vol. 26, no. 2, pp. 240–252, 2008.
- [20] D. Liciotti, P. Zingaretti, and V. Placidi, "An automatic analysis of shoppers behaviour using a distributed rgb-d cameras system," in *2014 IEEE/ASME 10th International Conference on Mechatronic and Embedded Systems and Applications (MESA)*. IEEE, 2014, pp. 1–6.
- [21] J. Liu, Y. Gu, and S. Kamijo, "Customer behavior classification using surveillance camera for marketing," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6595–6622, 2017.
- [22] E. Frontoni, P. Raspa, A. Mancini, P. Zingaretti, and V. Placidi, "Customers' activity recognition in intelligent retail environments," in *International Conference on Image Analysis and Processing*. Springer (Berlin, Heidelberg), 2013, pp. 509–516.
- [23] T. Katanyukul and J. Ponsawat, "Customer analysis via video analytics: customer detection with multiple cues," *Acta Polytechnica Hungarica*, vol. 14, no. 3, pp. 187–207, 2017.
- [24] M. Paolanti, D. Liciotti, R. Pietrini, A. Mancini, and E. Frontoni, "Modelling and forecasting customer navigation in intelligent retail environments," *Journal of Intelligent & Robotic Systems*, vol. 91, no. 2, pp. 165–180, 2018.

- [25] V. Santarcangelo, G. M. Farinella, A. Furnari, and S. Battiato, "Market basket analysis from egocentric videos," *Pattern Recognition Letters*, vol. 112, pp. 83–90, 2018.
- [26] Y. Dong, Y. Wang, J. Yue, and Z. Hu, "Real time 3d facial movement tracking using a monocular camera," *Sensors*, vol. 16, no. 8, p. 1157, 2016.
- [27] Y. Li, Z. Lu, J. Li, and Y. Deng, "Improving deep learning feature with facial texture feature for face recognition," *Wireless Personal Communications*, vol. 103, no. 2, pp. 1195–1206, 2018.
- [28] S. Turabzadeh, H. Meng, R. M. Swash, M. Pleva, and J. Juhar, "Facial expression emotion detection for real-time embedded systems," *Technologies*, vol. 6, no. 1, p. 17, 2018.
- [29] L. Ivanovsky, V. Khryashchev, A. Lebedev, and I. Kosterin, "Facial expression recognition algorithm based on deep convolution neural network," in *2017 21st Conference of Open Innovations Association (FRUCT)*. IEEE, 2017, pp. 141–147.
- [30] P. I. Rani and K. Muneeswaran, "Emotion recognition based on facial components," *Sādhanā*, vol. 43, no. 3, pp. 1–16, 2018.
- [31] J. Hu, "A personal facial expression monitoring system using deep learning," Ph.D. dissertation, 2019.
- [32] K. Bahreini, W. Van der Vegt, and W. Westera, "A fuzzy logic approach to reliable real-time recognition of facial emotions," *Multimedia Tools and Applications*, vol. 78, no. 14, pp. 18 943–18 966, 2019.
- [33] "Cisco analytics for retail," [https://www.cisco.com/c/dam/en\\_us/solutions/industries/docs/retail/analytics-retail-aag.pdf](https://www.cisco.com/c/dam/en_us/solutions/industries/docs/retail/analytics-retail-aag.pdf), accessed: 2021 November.
- [34] "Retail, digitize and secure your entire retail environment for a more connected experience," <https://www.cisco.com/c/en/us/solutions/industries/retail.html>, accessed: 2021 November.

# Hybrid Model of Quantum Transfer Learning to Classify Face Images with a COVID-19 Mask

Christian Soto-Paredes, Jose Sulla-Torres  
Escuela de Ingeniería de Sistemas  
Universidad Nacional de San Agustín de Arequipa  
Arequipa, Perú

**Abstract**—The problem of the COVID-19 disease has determined that about 219 million people have contracted it, of which 4.55 million died. This importance has led to the implementation of security protocols to prevent the spread of this disease. One of the main protocols is to use protective masks that properly cover the nose and mouth. The objective of this paper was to classify images of faces using protective masks of COVID-19, in the classes identified as correct mask, incorrect mask, and no mask, with a Hybrid model of Quantum Transfer Learning. To do this, the method used has made it possible to gather a data set of 660 people of both sexes (man and woman), with ages ranging from 18 to 86 years old. The classic transfer learning model chosen was ResNet-18; the variational layers of the proposed model were built with the Basic Entangler Layers template for four qubits, and the optimization of the training was carried out with the Stochastic Gradient Descent with Nesterov Momentum. The main finding was the 99.05% accuracy in classifying the correct Protective Masks using the PennyLane quantum simulator in the tests performed. The conclusion reached is that the proposed hybrid model is an excellent option to detect the correct position of the protective mask for COVID-19.

**Keywords**—*hybrid; quantum; classify; face; COVID-19; mask*

## I. INTRODUCTION

According to the COVID-19 Data Repository by the Center for Systems Science and Engineering (CSSE) at Johns Hopkins University [1], which consolidates online information from the World Health Organization, the Chinese Center for Disease Control and Prevention, and the Johns Hopkins University as of September 2021, an estimated 219 million cases of people affected by COVID-19 [2] of which 4.55 million led to death. For this reason, security protocols have been implemented to prevent the spread of this disease. One of the main protocols consists of using protective masks that correctly cover the nose and mouth; even following safety protocols help reduce the incidence of other infectious diseases such as influenza, pneumonia, and mycobacterium tuberculosis [3]. Thus, this research contributes to compliance with the security protocol that establishes the use of protective masks in public places, the global impact is noted since it is not only a requirement demanded in all the cities of Peru, but it is also required in the rest of the countries around the world, in addition, reducing the number of people who dedicate themselves to the task of inspection and monitoring of compliance with this regulation has an impact on reducing costs and increasing the number of people verified. The literature presents Transfer Learning studies that try to solve this problem. A greater incidence in the use of ResNet-18 as a residual network is noted, with

significant results and accuracy greater than or equal to 90%, respectively.

Under this juncture, it was decided to classify the use that people give to masks in 3 classes: correct mask, incorrect mask, and no mask; it was decided to use Transfer Learning with ResNet-18 and enhance it with the use of quantum computing. An innovative hybrid model is born that represents an alternative for improvement to the classical methods of recognition, classification and/or prediction implemented in the literature. It is known that quantum computing helps in the simulation of quantum systems; it is in this subject that it is about simulating objects such as small molecules or macromolecules; quantum computing also supports the field of quantum optimization, helping to solve problems that have a cost that is intended to be minimized; also in stochastic physics, it helps to simulate random processes; It also supports risk analysis or simulation of probability distributions; even in cryptography; and finally in machine learning it allows machines to learn in a faster way since it allows representing multiple states at the same time. An additional motivation for proposing the hybrid model in question is that to date, there have been no Hybrid Quantum Transfer Learning investigations that seek to solve the problem of classifying face images using a COVID-19 protective mask.

A sample of 660 images in resolution of  $1024 \times 1024$  pixels, of people facing the front wearing a protective mask, of both sexes (male and female), aged between 18 to 86 years, was considered, 68% of these images were used for training and the rest 32% for testing, for their use the images were transformed to  $(3 \times 224 \times 224)$ , in the training a resizing and cropping of the images was carried out, to improve the training cases; regarding the quantum simulator, PennyLane was used with four qubits, with an exact number of shots. Regarding the construction of quantum neural networks, these were made up of the embedding layer, the variational layers and the measurement layer; in this sense, 3 types of quantum variational layers were contemplated, those made with the Basic Entangler Layers template, the Strongly Entangling Layers template and a custom construction called Custom Layers, with Basic Entangler Layers being the one that provides the best results; for the optimization tasks of the training of the model as a whole, the performance was compared with the Adam optimizer and with the SGD with Nesterov Momentum, being SGD who provides the best results; to finalize an accuracy of 99.05% in the tests was obtained, which is satisfactory compared to the similar problems of Hybrid Quantum Transfer Learning reviewed in the literature, although it is true that

the accuracy, together with the precision, the recall and the f1-score are essential metrics to validate the relevance of the research, it should be noted that this study focuses on illustrating the innovative proposed method and the particular adaptation of the method by the authors, not on exceeding all existing methods in accuracy, it is in this sense that the development of the research and the techniques used are the most significant contribution left by this study.

After this introduction, this article is organized as follows: The works related to this article are explained in Section II the methodology used in this research in Section III, the experimental results in Section IV, discussions in Section V, conclusions in Section VI, and finally, future works in Section VII.

## II. RELATED WORK

The bibliographic review contemplated various aspects such as Transfer Learning, ResNet, Hybrid Quantum Transfer Learning, and Datasets of images of faces with a mask.

### A. Transfer Learning

Solving a problem involves gathering a large amount of information related to the solution of that problem; Transfer Learning is based on taking advantage of a large amount of data acquired and using it to solve another type of problem that shares certain characteristics. Thus, the author Yadav in [4] proposes a video surveillance system implemented in raspberry pi4, which is developed by Transfer Learning, with MobileNetV2 [5] as a pre-trained neural network and a single Shot Detector (SSD), which provides an 85% to 95% accuracy in detecting people using a protective mask.

There are Transfer Learning researchers that create their own datasets. This is how the authors Wang, Zhao, and Chen [6], propose a two-stage method that uses a Faster RCNN framework with Inception v2; your created dataset consists of 26,403 images of faces using masks; With their proposed model, they achieved 97.32% accuracy in simple scenes and 91.13% in complex scenes.

Transfer Learning modifies patterns already trained in specific characteristics and uses them to recognize similar patterns. Thus, using Inception v3 [7] in Face Mask Detection, the authors Jignesh Chowdary, Punn, Sonbhadra, and Agarwal [8], propose a model of Transfer Learning with the Simulated Masked Face Dataset (SMFD), achieving 99.9% during training and 100% during testing.

### B. ResNet

ResNet [9] is known to allow deep training networks of more than 100 layers; In essence, it is a residual network which is based on the fact that some neurons connect with others in layers that are not necessarily contiguous, that is, jumping intermediate layers, considering this, the authors Loey, Manogaran, Taha and Khalifa [10] propose to use video object recognition to recognize people who use a protective mask, using for this purpose YOLO v2, here a feature extraction process is developed with ResNet-50 [9], achieving an accuracy of 81%.

The authors Addagarla, Kalyan Chakravarthi, and Anitha [11] proposed two models, FMY3 and FMNMobile; the latter uses Resnet SSD300 to tackle the task of recognizing people using masks, obtaining 98% accuracy and 99% recall rate.

The fundamental component of ResNet is the residual blocks; in a residual block, the input  $x$  is added directly to the output of the network by means of the jump connection; thus, the authors Jiang, Fan, and Yan [12], propose a one-stage detector called RetinaFaceMask which implements a Feature Pyramid Network, achieving a prediction in the detection of people with a mask of 82.3% with MobileNet [5] and 93.4% with ResNet-18 [9].

To conclude, the authors Sethi, Kathuria, and Kaushik [13] present a two-stage detector that compares the ResNet-50, AlexNet, and MobileNet models, concluding that ResNet gives better results in the task of classifying faces with a mask in video surveillance, achieving an accuracy of 98.2%.

### C. Hybrid Quantum Transfer Learning

Hybrid neural networks are made up of classical and quantum elements. There is the paradigm by which a pre-trained classical neural network is augmented with a variational quantum circuit [14]; this is how the paradigm called Hybrid Quantum Transfer Learning was born. Based on this approach is that the authors Mari, Bromley, Izaac, Schuld, and Killoran [15], propose to use this method for image recognition and quantum state classification; in their study, they are given the task of classifying images of bees and ants, among their The results obtained are 96.7% accuracy in the Pennylane simulator [16], 95% accuracy in IBM's ibmqx4 quantum hardware [17] and 0.80% in Rigetti's Aspen-4-4Q-A [18]. There are thus four ways to develop Transfer Learning, which are: classical to classical, classical to quantum, quantum to classical, and quantum to quantum; the classical to quantum approach is the one chosen for this research.

The authors Umer, Amin, Sharif, Anjum, Azam, and Shah [19], use Hybrid Quantum Transfer Learning with ResNet-18 and a 4-qubit quantum circuit to classify radiographic images of lungs of 3 types: COVID-19, Normal and Viral Pneumonia, with an accuracy of 99.7% in a quantum computer.

To run a Hybrid Quantum Transfer Learning model with ResNet-18, you can use simulators such as Pennylane [16], Qiskit-Aer [17], and Cirq [20]; you can also use real quantum hardware like the one provided by IBM: ibmq london, ibmq rome, among others, is how the authors Acar and Yilmaz [21] made their proposal in the devices mentioned above; They also used CT images of the lungs of 126 people with COVID and 100 ordinary people, achieving an accuracy of 90% in the simulator and 94% to 100% in quantum computers.

### D. Dataset

The datasets contribute to the task of classifying images of people's faces using masks; so authors such as Cabani, Hammoudi, Benhabiles, and Melkemi [22] created a dataset that they called MaskedFace-Net, which consists of 137,016 images in resolution of 1024x1024 pixels, to which they added masks utilizing image editing [23], that is how they created two groups which they called:

- Correctly Masked Face Dataset (CMFD).
- Incorrectly Masked Face Dataset (IMFD).

To end, in [24], a dataset of more than 250,000 images of faces using masks is provided, it consists of high-quality images 1024x1024 pixels, these images were not edited by computer, so real people are shown as is using masks of 4 different ways, which can be interpreted as follows:

- Correct use of the mask, the one that covers the nose and mouth.
- Incorrect use, which does not cover the nose.
- Incorrect use, which does not cover the nose or mouth.
- Incorrect use, which does not have any mask.

### III. METHODOLOGY

The objective of the study was to classify faces using protective masks from COVID-19 with a hybrid model of Quantum Transfer Learning; taking for this purpose a dataset of 660 people of both sexes (male and female), with ages between 18 to 86 years; in a diverse set of mask types and facial features. The classes identified for classification were 3: correct mask, incorrect mask, and no mask. The methodology used for the classification consists of 4 stages, elaborated under the approach of the Business Process Model and Notation (BPMN) [25] as shown in Fig. 1.

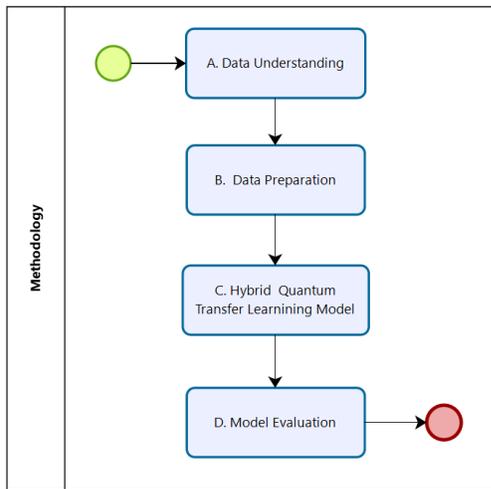


Fig. 1. Proposed Methodology for Classification (BPMN).

#### A. Data Understanding

The original dataset in [24] consists of more than 250,000 images divided into several parts; for the study, only part 2 of this dataset was taken, which consists of 40,000 images. This dataset is accompanied by a .csv file, which contains the detailed list of all the images; this is constituted as shown in Table I; this list is essential because it helped in the identification, understanding, and preparation tasks. Such as the subsequent processing of the sample images.

Explanation of the fields:

TABLE I. STRUCTURE OF THE DATASET LIST

Id	Type	User Id	Gender	Age	Name
Incremental	1-4	Numeric	M—F—N	Numeric	Text

- Type: Represents the four ways in which a person uses a mask, 1-correct mask, 2-incorrect mask (does not cover the nose), 3-incorrect mask (does not cover the nose or mouth), 4-incorrect mask (The person is not wearing the mask).
- User Id: Numerical value with which a person is identified.
- Gender: Male, female, or none.
- Age: Numerical value that is between 18 to 86 years old.
- Name: Sequence of alphanumeric characters with which the .jpg image is labeled.

The dataset organized by gender is shown in Table II, “None” corresponds to people whose gender was not registered; in addition, there is a predominance of people of the male gender 59.58%.

TABLE II. DATASET ORGANIZED BY GENDER

Gender	Number	Percentage (%)
Male	23832	59.58
Female	7012	17.53
None	9156	22.89

The dataset organized by age ranges is shown in Table III. From this, it is observed that the most significant population range is in the range of 18 to 30 years of age and that there are 1,948 people whose age was not registered, approximately 4.87%.

TABLE III. DATASET ORGANIZED BY AGE RANGES

Age	Number	Percentage (%)
18-30	27844	69.61
31-40	7732	19.33
41-50	2416	6.04
51-60	12	0.03
61-70	0	0.00
71-80	44	0.11
81-90	4	0.01
others	1948	4.87

#### B. Data Preparation

As a first step, the number of classes was reduced from 4 to 3, that is, to 30,000 images; since there is no significant difference between not bringing a mask and bringing a mask that does not cover the nose or mouth, the new output classes are:

- Correct Mask: This represents a correct use of the protective mask, which covers the nose and mouth (Fig. 2).

- Incorrect Mask: Representing an incorrect use of the protective mask, which does not cover the nose (Fig. 3).
- No Mask: This represents the absence of a mask that protects the individual (Fig. 4).



Fig. 2. Correct Mask.



Fig. 3. Incorrect Mask.

Second, a representative sample was taken, which is defined in (1), where:

- $n$  Sample size.
- $N$  Population size.
- $p$  Probability of occurrence of the event studied.
- $q$  Probability of non-occurrence of the event studied.
- $Z$  Parameter that depends on the confidence level.
- $e$  Estimation error.

$$n = \frac{N \times Z^2 \times p \times q}{e^2 \times (N - 1) + Z^2 \times p \times q} \quad (1)$$

The 30,000 images considered became the initial population  $N = 30,000$ , in addition, a confidence level of 90% was estimated, that is, a  $Z = 1,645$ , an estimated error of 5.52%,

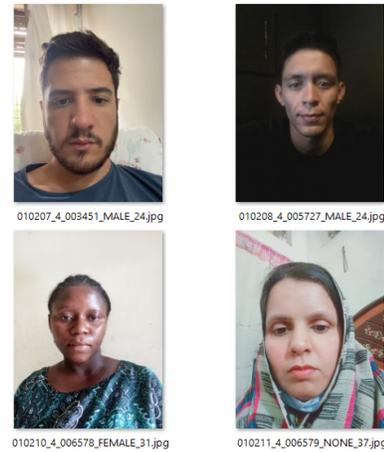


Fig. 4. No Mask.

and the values of  $p$  and  $q$  are calculated to have the same probability of occurrence 50% each. Executing the calculations with (1), it was obtained the selected sample was  $n = 660$  in total, then, the next step was to randomly retrieve the images, considering 68% for training and 32% for testing as well as it's shown in Table IV.

TABLE IV. QUANTITIES FOR TRAINING AND TESTING

Phase	Percentage (%)	Total images	Total per class
training	68	450	150
testing	32	210	70

Then, transformations were made to the sample images; initially, these had a resolution of  $1024 \times 1024$  pixels, but since it was the residual network ResNet-18 it required that they be transformed to the form  $(3 \times 224 \times 224)$ , it was also carry out a normalization with the mean and the standard deviation to  $[0.485, 0.456, 0.406]$  and  $[0.229, 0.224, 0.225]$  respectively, both for training and testing. Additional tasks such as random resizing and clipping were also performed on the training dataset, as well as a random horizontal rotation to improve the training cases. To finish, the data was loaded into a dictionary with the help of the Pytorch DataLoader [26], with a batch size of eight as shown in Fig. 5. and two workers to speed up the loading.

### C. Hybrid Quantum Transfer Learning Model

Here the most critical topics in constructing the proposed hybrid model and its variants are detailed in 9 parts, which give rise to comparisons that trigger the final results.

1) *Number of Qubits*: It took four qubits, a qubit is the basic unit of quantum computers, just like a bit can take the value 0 or 1, however by the superposition principle, it could have a part of 0 and a part of 1, when measuring said qubit it will collapse towards one value or another; in definition, a qubit is a unit modulus vector in a complex two-dimensional vector space, the quantum states are  $|0\rangle$  in (2) and  $|1\rangle$  in (3).



Fig. 5. Transformations Made for Training in a Batch of Images of Size Eight.

$$|0\rangle = \begin{pmatrix} 1 \\ 0 \end{pmatrix} \quad (2)$$

$$|1\rangle = \begin{pmatrix} 0 \\ 1 \end{pmatrix} \quad (3)$$

In addition, the state of a qubit can be represented by the “Bloch Sphere”, this shows in the extreme north the state  $|0\rangle$  and in the extreme south the  $|1\rangle$  the rest of possible states would be represented along the surface of the sphere by  $|\psi\rangle$ , which is a linear combination of the states  $|0\rangle$  and  $|1\rangle$  as in (4), the state of a qubit is more likely to collapse towards  $|0\rangle$  when it is further north and to collapse towards  $|1\rangle$  when it is further south Fig. 6.

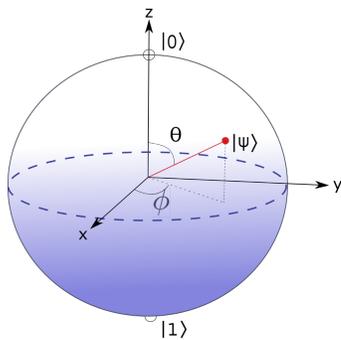


Fig. 6. Graphical Representation of a Qubit as a Bloch Sphere, shows the General States  $|0\rangle$  and  $|1\rangle$  and Arbitrary General States Represented by  $|\psi\rangle$ , where  $\theta$  and  $\phi$  are Real Numbers Such that  $0 \leq \theta \leq \pi$  and  $0 \leq \phi \leq 2\pi$ , any  $|\psi\rangle$  can be Expressed as in (5).

$$|\psi\rangle = \alpha|0\rangle + \beta|1\rangle \quad (4)$$

$$|\psi\rangle = \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\phi} \sin\left(\frac{\theta}{2}\right)|1\rangle \quad (5)$$

2) *Quantum Node and Differentiation Method:* In pennylane [16], quantum computing is represented by objects composed of quantum nodes; a quantum node is used to declare a quantum circuit and relate it to a device that executes said circuit. Regarding the differentiation methods, for the simulation in pennylane [16], they are available: backprop,

adjoint, and reversible, and for real quantum computers: parameter-shift and finite-diff are available. For the present study, “reversible” was chosen because the quantum network will run in a simulator and give better results than the others.

3) *Device and the Number of Shots:* A “device” is the one that allows indicating in which hardware to execute the quantum circuit, for the given case “default.qubit” was chosen, the default local simulator of pennylane [16]; the number of “shots” was established as “exact,” this is only possible because they are simulators, in real quantum computers the number of “shots” is determined by the equation proposed in (6), where:

- $c$  Confidence level.
- $Z$  Parameter that depends on the confidence level.
- $e$  Estimation error.

$$shots = \left(\frac{Z_{1-c}}{2 \times e}\right)^2 \quad (6)$$

For a confidence level of 95%, we have that  $Z = -1.96$ , and if an approximate error of 5% is taken, it is obtained that 384.16 is needed, which rounding would give rise to  $shots = 384$ .

4) *Quantum Neural Network with Basic Entangler Layers:* The proposed quantum neural network is similar to a classical fully connected neural network; it receives a vector of 512 features and has three outputs associated with the correct-mask and incorrect-mask and no-mask classes. The structure is composed of a preprocessing layer of type Linear, an activation function of type hyperbolic tangent, a layered architecture of Basic Entangler layers, and a post-processing layer. The layer mentioned above architecture is built with a variational quantum circuit or variational circuit [27]; this hybrid algorithm combines quantum and classical computing and is designed to be executed in quantum computers. To implement this type of variational circuit, you must first define a node with a quantum function that receives as parameters the number of features and the selected weights; we must resize the weights to the form: number of quantum layers x number of qubits. Then for each wire, you have to place a Hadamard gate ( $H$ ) Fig.7, which operates on a single qubit, this is in charge of transforming the state  $|0\rangle$  in  $|+\rangle$  and the state  $|1\rangle$  in  $|-\rangle$ , its matrix representation is observed in (7) as well as the representations of the  $|+\rangle$  and  $|-\rangle$  in (8) and (9) respectively.

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix} \quad (7)$$

$$|+\rangle = \frac{|0\rangle + |1\rangle}{\sqrt{2}} \quad (8)$$

$$|-\rangle = \frac{|0\rangle - |1\rangle}{\sqrt{2}} \quad (9)$$

Then three types of quantum layers are added, as detailed:

- Embedding layer: Here a layer consisting of single-qubit rotations was inserted, with rotation gates such

as RX (10), RY (11), and RZ (12), where  $\phi$  is the angle of rotation, for this the template “Angle Embedding” was used, The graphic representation of this layer is shown in Fig. 7.

$$R_x(\phi) = \epsilon^{-\frac{i\phi\sigma_x}{2}} = \begin{bmatrix} \cos(\frac{\phi}{2}) & -i \sin(\frac{\phi}{2}) \\ -i \sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{bmatrix} \quad (10)$$

$$R_y(\phi) = \epsilon^{-\frac{i\phi\sigma_y}{2}} = \begin{bmatrix} \cos(\frac{\phi}{2}) & -i \sin(\frac{\phi}{2}) \\ \sin(\frac{\phi}{2}) & \cos(\frac{\phi}{2}) \end{bmatrix} \quad (11)$$

$$R_z(\phi) = \epsilon^{-\frac{i\phi\sigma_z}{2}} = \begin{bmatrix} \epsilon^{-\frac{i\phi}{2}} & 0 \\ 0 & \epsilon^{\frac{i\phi}{2}} \end{bmatrix} \quad (12)$$

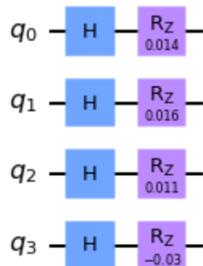


Fig. 7. Embedding Layer for 4 Qubits, with Hadamard Gates and Single Rotation Gates RZ (Graphic Generated with ibm Qiskit).

- Variational layers: Built with the Basic Entangler Layers template, which receives as parameters the weights, a vector of wires, and the axis on which to rotate, this is in charge of building the number of layers specified in the shape of the weights; This template inserts *CNOT* gates (13) and single-qubit rotations (10), (11), and (12), as shown in Fig. 8.

$$CNOT = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix} \quad (13)$$

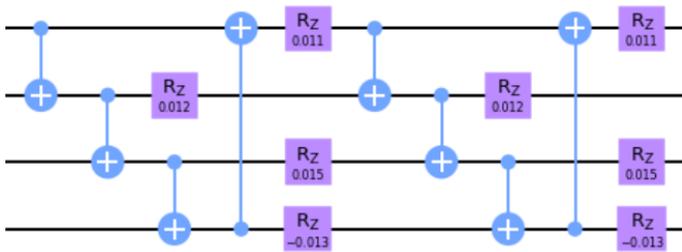


Fig. 8. Variational Layers with Basic Entangler Layers for four Qubits and a Depth of 2 Layers, with CNOT Gates and Single Qubit Rotations Gates RZ, as an Example, only Two Layers are Shown because, for the Evaluation of the Study, a Depth of 10 Variational Layers was Considered (Graphic Generated with ibm Qiskit).

- Measurement layer: This layer contains 4 Pauli *Z* operators (Fig. 9), which allow measuring the state of

the four qubits, which, when observed, will collapse towards one state or another; the matrix that represents it is shown in (14).

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \quad (14)$$

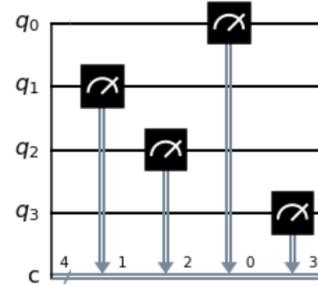


Fig. 9. Measurement Layer with 4 Pauli Z Operators (Graph Generated with ibm Qiskit).

5) *Quantum Neural Network with Strongly Entangling Layers*: In a similar way as in the previous section III-C4, the quantum neural network receives a vector of 512 features and provides three outputs corresponding to correct-mask, incorrect-mask, and no-mask, of Likewise, it consists of a processing layer, a post-processing layer and has a *tanh* activation function, the difference lies in the architecture of the variational circuit that is built with the “Strongly Entangling Layers” template [28], so the embedding layer and the measurement layer are the same as seen in the previous section, Fig. 7 and Fig. 9 respectively, with the same operators seen in (10), (11), (12), (13), and (14).

The “Strongly Entangling Layers” template [28] is based on the circuit-centric classifier design, which is composed of single-qubit rotations interlaced with *CNOT* gates; each single qubit *G* is a  $2 \times 2$  unitary, as shown in (15).

$$G(\alpha, \beta, \gamma, \phi) = \epsilon^{i\phi} \begin{pmatrix} \epsilon^{i\beta} \cos \alpha & \epsilon^{i\gamma} \sin \alpha \\ -\epsilon^{-i\gamma} \sin \alpha & \epsilon^{-i\beta} \cos \alpha \end{pmatrix} \quad (15)$$

“Strongly Entangling Layers” does not support the “reversible” differentiation method, so pennylane [16] automatically selects the best possible method. In Fig. 10, this type of variational circuit is shown with a depth of 2 layers.

6) *Quantum Neural Network with Custom Layers*: Also in a similar way to section III-C4, the quantum neural network is completely connected as described in that section, the difference is that the architecture of the variational layers is based on the examples detailed in [15], this latest layer design proposal is based on interlacing of *CNOT* gates and single-qubit rotations as seen in Fig. 11, the embedding layer is seen in Fig. 7 and the measurement layer in Fig. 9 respectively, also makes use of the operators seen in (10), (11), (12), (13) and (14).

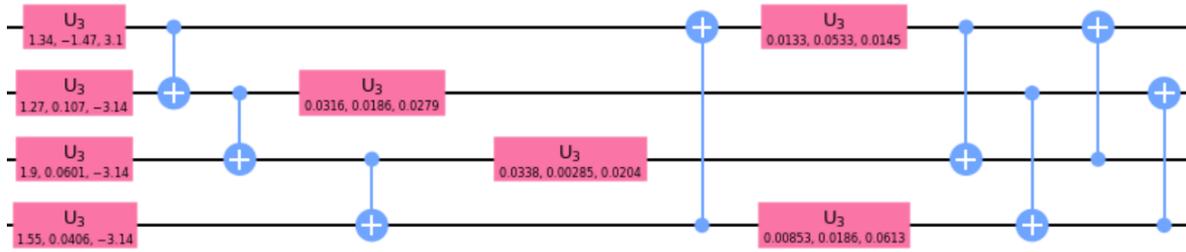


Fig. 10. Variational Layers with the use of the “Strongly Entangling Layers” Template for four Qubits and a Depth of 2 Layers, with CNOT Gates and U<sub>3</sub> Rotations Gates that Represent Three Single-Qubit Rotations R<sub>Z</sub>, R<sub>Y</sub>, and R<sub>Z</sub> Respectively, as an Example only Two are shown Layers because for the Evaluation of the Study a Depth of 10 Variational Layers was Considered (Graph Generated with ibm Qiskit).

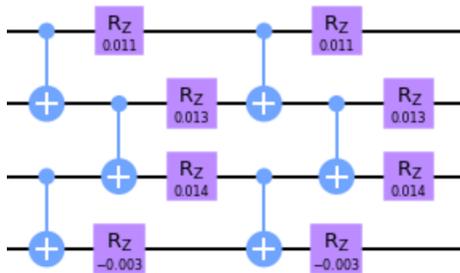


Fig. 11. Variational Layers with Basic Entangler Layers for four Qubits and a Depth of 2 Layers, with CNOT Gates and Single Qubit Rotations Gates R<sub>Z</sub>, as an Example, only Two Layers are shown because, for the Evaluation of the Study, a Depth of 10 Variational Layers was Considered (Graphic Generated with ibm Qiskit).

7) *Hybrid Transfer Learning*: About classic transfer learning, two types are considered: finetuning and feature extraction. In “finetuning,” you start from a pre-trained model and update all the parameters for a new task; essentially, the entire model is completely re-trained. In “feature extraction,” we start from a pre-trained model and only update the final layer’s weights, with which we can now make predictions. Both transfer learning methods follow the following steps:

- Step 1: Initialize the pre-trained model with the selected parameters.
- Step 2: Reshape the final layer.
- Step 3: Define an optimization algorithm.
- Step 4: Carry out the training.

In addition to the above, it should be clarified that hybrid quantum computing receives its name for combining classical computing approaches with quantum computing. So to do hybrid quantum transfer learning, a classical pre-trained network must be taken, for this case, ResNet-18 (Table V), to which the final layer is reshaped to connect it with a quantum neural network whose architecture is based on a variational circuit that will be executed in a quantum computer.

In the present study, “feature extraction” was carried out, and the final layer of ResNet-18 is linked to the quantum neural network with 512 features in the manner described in section III-C4. Furthermore, let  $L$  be a layer,  $n_0 \rightarrow n_1$  represents  $n_0$  inputs and  $n_1$  outputs,  $x$  an input vector and  $y$  an output vector as in (16).

TABLE V. RESNET-18 ARCHITECTURE

Layer Name	Filter Size	Stride	Padding	Number of Filters	Output Feature
Image Input	-	-	-	-	120x240x3
Conv1_x	7x7x3	2	3	64	60x120x64
	3x3	2	1	-	30x60x64
Conv2_x	3x3x64	1	1	64	30x60x64
	3x3x64	1	1	64	
	3x3x64	1	1	64	
	3x3x64	1	1	64	
Conv3_x	3x3x64	2	1	128	15x30x128
	3x3x128	1	1	128	
	1x1x64	2	0	128	
	3x3x128	1	1	128	
	3x3x128	1	1	128	
Conv4_x	3x3x128	2	1	256	8x15x256
	3x3x256	1	1	256	
	1x1x128	2	0	256	
	3x3x256	1	1	256	
	3x3x256	1	1	256	
Conv5_x	3x3x256	2	1	512	4x8x512
	3x3x512	1	1	512	
	1x1x256	2	0	512	
	3x3x512	1	1	512	
	3x3x512	1	1	512	
4x8	-	0	-	-	1x1x512

$$L_{n_0 \rightarrow n_1} : x \rightarrow y \tag{16}$$

Then it is known that  $Q$  is a variational quantum circuit with  $E$  embedding layer and  $M$  measurement layer (17).

$$Q = M \circ Q' \circ E \tag{17}$$

Finally, to apply hybrid quantum transfer learning, the quantum neural network  $\bar{Q}$  [15] has to be created as shown in (18), based on what is formulated in (16) and (17) .

$$\bar{Q} = L_{n_q \rightarrow n_{out}} \circ Q \circ L_{n_{in} \rightarrow n_q} \tag{18}$$

From all the above, it is possible to graphically observe the proposed hybrid quantum transfer learning model Fig. 12.

8) *Optimization*: The optimization process consists of the task of finding the best weights, minimizing the error in each iteration. For this, two methods were used: Adam [29] with a learning rate of 0.0004 and Stochastic Gradient Descent with Nesterov Momentum [30], the implementation of momentum

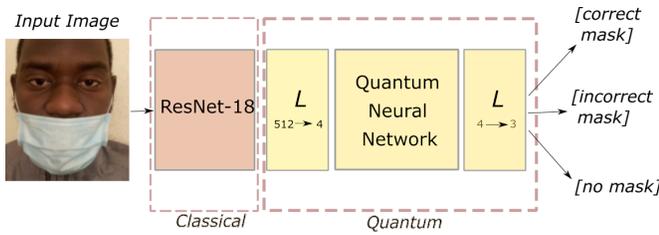


Fig. 12. The Proposed Hybrid Quantum Transfer Learning Model Receives an Image of a Person Wearing a COVID-19 Protective Mask, as Input and as Output a Classification (Correct Mask, Incorrect Mask, and no Mask) is Provided; on the Side of Classical Computing, it is Found ResNet-18 and on the Side of Quantum Computing is the Quantum Neural Network with 512 Features, four Qubits, and Three Outputs, this Quantum Neural Network is based on what is Formulated in (18).

is described in (19) and (20), with a learning rate of 0.001 and a momentum of 0.9.

$$v_{t+1} = \mu * v_t + g_{t+1} \quad (19)$$

$$p_{t+1} = p_t - lr * v_{t+1} \quad (20)$$

Where  $p$  represents the parameters,  $g$  the gradient,  $v$  the velocity and  $\mu$  the momentum.

9) *Training*: Is performed by first defining a training function that receives input parameters such as a model, a dictionary with the information of the loaded images, a loss function, in this case, “cross-validation”, an Adam or SGD optimizer, several epochs to train, and an “is inception” flag which is used to prepare the function to work with Inception v3. It is worth mentioning that this training function was tested in transfer learning with the following classic models: resnet, alexnet, vgg, squeezenet, densenet, inception, and on the quantum side resnet-18 and densenet were implemented. This training function performs 2 phases: one of training itself and another that tests the time in question; with the optimizer, the best weights are chosen to allow the resulting model to classify between correct-mask, incorrect-mask, and no-mask. Finally, the results obtained by executing 10, 20, and 30 epochs were recovered, and each model was tested with the images intended for testing; a sample can be seen in Fig. 13.

#### D. Model Evaluation

To evaluate the model [31], the Precision (21), the Recall (22), and the F1-score (23) were used. For many classes  $C_i$ ,  $fp_i$  represents false positive,  $tp_i$  true positive,  $fn_i$  false-negative, and  $tn_i$  true negative.

$$Precision = \frac{\sum_{i=1}^l \frac{tp_i}{tp_i + fp_i}}{l} \quad (21)$$

$$Recall = \frac{\sum_{i=1}^l \frac{tp_i}{tp_i + fn_i}}{l} \quad (22)$$

$$F1 - score = \frac{(\beta^2 + 1)(Precision)(Recall)}{(\beta^2)(Precision) + Recall} \quad (23)$$



Fig. 13. Composite Model Predictions with Strongly Entangling Layers for 30 Epochs, Optimized with SGD.

The repository where the source code is available, developed by the authors of this research, which allows to recreate the study and obtain the results presented, is available at [32].

## IV. RESULTS

Tables VI and VII show the results of the classification, taking Accuracy and Training time as relevant factors; for 10, 20, and 30 epochs, considering a dataset of 660 images, 450 for training and 150 for testing, on the quantum side, there are four qubits, the number of shots was “exact,” the depth of the variational layers was 10, The differentiation method was “reversible,” and the processor used was the GPU provided by Google Colab [33], the selected simulator was “PennyLane” [16]. From now on, “Basic Entangler Layers” will be used interchangeably as “BEL,” “Strongly Entangling Layers” as “SEL,” and “Custom Layers” as “CL”. The residual network selected for transfer learning was ResNet-18. From now on, all other results tables will work with the same hyperparameters previously described. The results of Tables VI and VII are divided by the type of optimizer used, “Stochastic Gradient Descent with Nesterov Momentum” and “Adam” respectively.

TABLE VI. RESULTS WITH THE STOCHASTIC GRADIENT DESCENT OPTIMIZER WITH NESTEROV MOMENTUM

Variational Layers	Epochs	Testing Accuracy (%)	Training Time (min)
BEL	10	97.14	48
BEL	20	98.57	97
<b>BEL</b>	<b>30</b>	<b>99.05</b>	<b>142</b>
SEL	10	95.71	105
<b>SEL</b>	<b>20</b>	<b>99.05</b>	<b>211</b>
SEL	30	98.57	309
CL	10	97.14	43
<b>CL</b>	<b>20</b>	<b>99.05</b>	<b>85</b>
CL	30	68.10	129

Tables VI and VII show that the best results were for “BEL” at 30 epochs, “SEL” at 20 epochs and “CL” at 20 epochs, the 3 with 99.05% accuracy and the 3 used the SGD as the optimization method. Once the three models with the best accuracy were identified, an analysis was performed based on the Precision, the Recall, and the F1-score to determine the

TABLE VII. RESULTS WITH THE ADAM OPTIMIZER

Variational Layers	Epochs	Testing	Training
		Accuracy (%)	Time (min)
BEL	10	83.81	49
BEL	20	93.33	98
BEL	30	97.14	144
SEL	10	95.24	104
SEL	20	92.38	221
SEL	30	94.29	313
CL	10	87.62	42
CL	20	88.10	80
CL	30	98.57	127

model with the best classification. Tables VIII, IX, and X show the classification reports for the three best models mentioned above.

TABLE VIII. CLASSIFICATION REPORT FOR BASIC ENTANGLER LAYERS WITH STOCHASTIC GRADIENT DESCENT WITH NESTEROV MOMENTUM AT 30 EPOCHS

Class	Precision	Recall	F1-score
Correct Mask	0.96	0.99	<b>0.97</b>
Incorrect Mask	0.97	0.94	<b>0.96</b>
No Mask	0.99	0.99	<b>0.99</b>

TABLE IX. CLASSIFICATION REPORT FOR STRONGLY ENTANGLING LAYERS WITH STOCHASTIC GRADIENT DESCENT WITH NESTEROV MOMENTUM AT 20 EPOCHS

Class	Precision	Recall	F1-score
Correct Mask	0.91	0.87	0.89
Incorrect Mask	0.88	0.84	0.86
No Mask	0.89	0.97	0.93

TABLE X. CLASSIFICATION REPORT FOR CUSTOM LAYERS WITH STOCHASTIC GRADIENT DESCENT WITH NESTEROV MOMENTUM AT 20 EPOCHS

Class	Precision	Recall	F1-score
Correct Mask	0.84	1.00	0.92
Incorrect Mask	0.97	0.80	0.88
No Mask	0.99	0.97	0.98

Still, among the three, it is observed that the best result was for the model that uses variational layers built with the “Basic Entangler Layers” template and whose training optimizer was “Stochastic Gradient Descent with Nesterov Momentum” at 30 epochs, given its accuracy of 99.05% and its F1-score of 97% to classify “Correct Mask,” 96% for “Incorrect Mask” and 99% to rate “No Mask” respectively. Similarly, the confusion matrices Fig. 14, Fig. 15, and Fig. 16 confirm the analysis results mentioned above.

## V. DISCUSSION

Table XI shows a comparison of image classification problems using Hybrid Quantum Transfer Learning models with ResNet-18 and four qubits; it can be seen that the proposed model shows the best accuracy with 99.05% when executed in a simulator, and also it is an encouraging result when compared

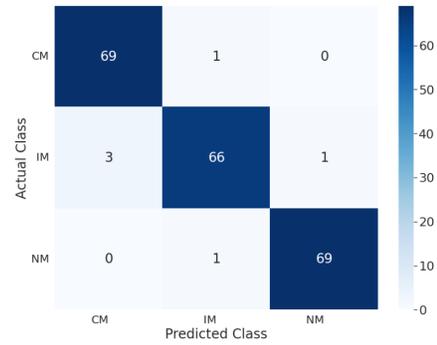


Fig. 14. Confusion Matrix for Basic Entangler Layers with Stochastic Gradient Descent with Nesterov Momentum at 30 Epochs.

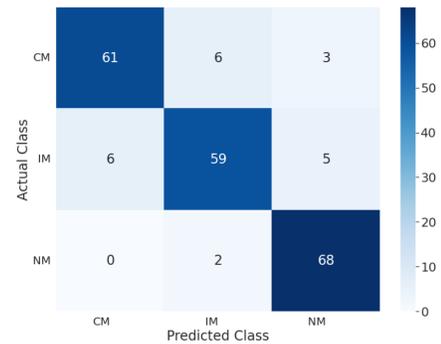


Fig. 15. Confusion Matrix for Strongly Entangling Layers with Stochastic Gradient Descent with Nesterov Momentum at 20 Epochs.

with the other results of real quantum computers. Although indeed, the accuracy, together with the precision, the recall, and the f1-score are essential metrics to validate the relevance of the research, it should be noted that the present study focuses on illustrating the innovative proposed method and the particular adaptation of the method on the part of the authors, not in surpassing in accuracy to all the existing methods, it is in this sense that the development of the investigation and the techniques used are the most significant contribution that the present study leaves.

TABLE XI. COMPARISON OF IMAGE CLASSIFICATION PROBLEMS USING HYBRID MODELS OF QUANTUM TRANSFER LEARNING WITH RESNET-18 AND 4 QUBITS

Autor	Classes	Images	Simulator Acc (%)	QC Acc (%)
[15]	2	ants, bees	96.7	95
[19]	3	lung covid-19	-	98
[21]	2	lung covid-19	90	94 - 100
Proposed	3	masked face covid-19	99.05	-

## VI. CONCLUSION

A hybrid Quantum Transfer Learning model was developed with ResNet-18. Thanks to the inclusion in its quantum neural network of variational layers developed with the Basic Entangler Layers template and Stochastic Gradient Descent with Nesterov Momentum in its optimization, this is how it manages to enhance its performance.

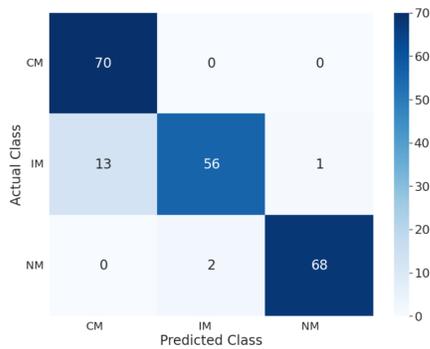


Fig. 16. Confusion Matrix for Custom Class Layers with Stochastic Gradient Descent with Nesterov Momentum at 20 Epochs.

The evaluations carried out in classifying the use of a protective mask (correct mask, incorrect mask, and no mask) of images of 660 people of both sexes between 18 and 86 years old obtained an accuracy of 99.05%. These results are satisfactory when compared with similar hybrid quantum classification problems with ResNet-18 and four qubits in its implementation.

## VII. FUTURE WORK

The models trained with Strongly Entangling Layers at 20 epochs and Custom Layers at 20 epochs also obtained 99.05% in accuracy but decreased in the levels of precision, recall and f1-score, so it is proposed to improve the hyperparameters to enhance their performance and future use. From the consulted literature, it is known that there are other quantum templates that could be more adaptable to the problem of image classification, “CV Neural Net Layers” is one of them, its research and the future proposal are recommended.

## REFERENCES

- [1] E. Dong, H. Du, and L. Gardner, “An interactive web-based dashboard to track covid-19 in real time,” *The Lancet Infectious Diseases*, vol. 20, no. 5, pp. 533–534, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1473309920301201>
- [2] (2021, Sep.) Covid-19 dashboard by the center for systems science and engineering at johns hopkins university. [Online]. Available: <https://www.arcgis.com/apps/dashboards/bda7594740fd40299423467b48e9ecf6>
- [3] O. Dadras, S. A. S. Alinaghi, A. Karimi, M. MohsseniPour, A. Barzegary, F. Vahedi, Z. Pashaei, P. Mirzapour, A. Fakhfour, G. Zargari, S. Saeidi, H. Mojdeganlou, H. Badri, K. Qaderi, F. Behnezhad, and E. Mehraeen, “Effects of covid-19 prevention procedures on other common infections: a systematic review,” *European Journal of Medical Research*, vol. 26, 2021.
- [4] S. Yadav, “Deep learning based safe social distancing and face mask detection in public areas for covid-19 safety guidelines adherence,” *International Journal for Research in Applied Science and Engineering Technology*, vol. 8, pp. 1368–1375, 07 2020.
- [5] M. Sandler, A. Howard, M. Zhu, A. Zhmoginov, and L.-C. Chen, “Mobilenetv2: Inverted residuals and linear bottlenecks,” in *2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2018, pp. 4510–4520.
- [6] B. Wang, Y. Zhao, and C. L. P. Chen, “Hybrid transfer learning and broad learning system for wearing mask detection in the covid-19 era,” *IEEE Transactions on Instrumentation and Measurement*, vol. 70, pp. 1–12, 2021.
- [7] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, “Rethinking the inception architecture for computer vision,” 2015.

- [8] G. Jignesh Chowdary, N. Punn, S. Sonbhadra, and S. Agarwal, “Face mask detection using transfer learning of inceptionv3,” *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12581 LNCS, pp. 81–90, 2020, cited By 10. [Online]. Available: <https://arxiv.org/abs/2009.08369>
- [9] K. He, X. Zhang, S. Ren, and J. Sun, “Deep residual learning for image recognition,” in *2016 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2016, pp. 770–778.
- [10] M. Loey, G. Manogaran, M. H. N. Taha, and N. E. M. Khalifa, “Fighting against covid-19: A novel deep learning model based on yolo-v2 with resnet-50 for medical face mask detection,” *Sustainable Cities and Society*, vol. 65, p. 102600, 2021. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2210670720308179>
- [11] S. Addagarla, G. Kalyan Chakravarthi, and P. Anitha, “Real time multi-scale facial mask detection and classification using deep transfer learning techniques,” *International Journal of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 4, pp. 4402–4408, 2020, cited By 3. [Online]. Available: <https://pesquisa.bvsalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/en/covidwho-820057>
- [12] M. Jiang, X. Fan, and H. Yan, “Retinamask: A face mask detector,” 2020.
- [13] S. Sethi, M. Kathuria, and T. Kaushik, “Face mask detection using deep learning: An approach to reduce risk of coronavirus spread,” *Journal of Biomedical Informatics*, vol. 120, 2021, cited By 0. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S1532046421001775>
- [14] S. Adhikary, S. Dangwal, and D. Bhowmik, “Supervised learning with a quantum classifier using multi-level systems,” *Quantum Information Processing*, vol. 19, no. 3, Jan 2020. [Online]. Available: <http://dx.doi.org/10.1007/s11128-020-2587-9>
- [15] A. Mari, T. R. Bromley, J. Izaac, M. Schuld, and N. Killoran, “Transfer learning in hybrid classical-quantum neural networks,” *Quantum*, vol. 4, p. 340, Oct 2020. [Online]. Available: <http://dx.doi.org/10.22331/q-2020-10-09-340>
- [16] V. Bergholm, J. Izaac, M. Schuld, C. Gogolin, M. S. Alam, S. Ahmed, J. M. Arrazola, C. Blank, A. Delgado, S. Jahangiri, K. McKiernan, J. J. Meyer, Z. Niu, A. Száva, and N. Killoran, “Pennylane: Automatic differentiation of hybrid quantum-classical computations,” 2020.
- [17] (2021, Sep.) Ibm quantum computing. [Online]. Available: <https://quantum-computing.ibm.com/>
- [18] (2021, Sep.) Quantum computing service — amazon braket. [Online]. Available: <https://aws.amazon.com/braket/>
- [19] M. J. Umer, J. Amin, M. Sharif, M. A. Anjum, F. Azam, and J. H. Shah, “An integrated framework for covid-19 classification based on classical and quantum transfer learning from a chest radiograph,” *Concurrency and Computation: Practice and Experience*, p. e6434, 2021. [Online]. Available: <https://onlinelibrary.wiley.com/doi/abs/10.1002/cpe.6434>
- [20] (2021, Sep.) Cirq an open source framework for programming quantum computers. [Online]. Available: <https://quantumai.google/cirq>
- [21] E. Acar and İ. Yilmaz, “Covid-19 detection on ibm quantum computer with classical-quantum transfer learning,” *medRxiv*, 2020. [Online]. Available: <https://www.medrxiv.org/content/early/2020/11/10/2020.11.07.20227306>
- [22] A. Cabani, K. Hammoudi, H. Benhabiles, and M. Melkemi, “Maskedface-net – a dataset of correctly/incorrectly masked face images in the context of covid-19,” *Smart Health*, vol. 19, p. 100144, Mar 2021. [Online]. Available: <http://dx.doi.org/10.1016/j.smhl.2020.100144>
- [23] (2021, Sep.) Maskedface-net. [Online]. Available: <https://github.com/cabani/MaskedFace-Net>
- [24] R. Kucev. (2021, Sep.) 500 gb of images with people wearing masks. [Online]. Available: <https://www.kaggle.com/tapakah68/medical-masks-part2/metadata>
- [25] G. Decker, R. Dijkman, M. Dumas, and L. García-Bañuelos, *The Business Process Modeling Notation*. Springer, 09 2010, pp. 347–368.
- [26] (2021, Sep.) Pytorch: An open source machine learning framework. [Online]. Available: <https://pytorch.org/>

- [27] J. R. McClean, J. Romero, R. Babbush, and A. Aspuru-Guzik, "The theory of variational hybrid quantum-classical algorithms," *New Journal of Physics*, vol. 18, no. 2, Feb 2016. [Online]. Available: <http://dx.doi.org/10.1088/1367-2630/18/2/023023>
- [28] M. Schuld, A. Bocharov, K. M. Svore, and N. Wiebe, "Circuit-centric quantum classifiers," *Physical Review A*, vol. 101, no. 3, Mar 2020. [Online]. Available: <http://dx.doi.org/10.1103/PhysRevA.101.032308>
- [29] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," 2017.
- [30] I. Sutskever, J. Martens, G. Dahl, and G. Hinton, "On the importance of initialization and momentum in deep learning," in *Proceedings of the 30th International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, S. Dasgupta and D. McAllester, Eds., vol. 28, no. 3. Atlanta, Georgia, USA: PMLR, 17–19 Jun 2013, pp. 1139–1147. [Online]. Available: <https://proceedings.mlr.press/v28/sutskever13.html>
- [31] M. Sokolova and G. Lapalme, "A systematic analysis of performance measures for classification tasks," *Information Processing Management*, vol. 45, no. 4, pp. 427–437, 2009. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0306457309000259>
- [32] (2021, Oct.) Hybrid model of quantum transfer learning to classify face images with a covid-19 mask. [Online]. Available: <https://github.com/cjsotopa/Quantum>
- [33] (2021, Sep.) Google colab. [Online]. Available: <https://colab.research.google.com/>

# Code Optimizations for Parallelization of Programs using Data Dependence Identifier

Kavya Alluru<sup>1</sup>

School of Computer Science & Engineering  
Vellore Institute of Technology  
Chennai, India

Jeganathan L<sup>2</sup>

Centre for Advanced Data Science  
Vellore Institute of Technology  
Chennai, India

**Abstract**—In a Parallelizing Compiler, code transformations help to reduce the data dependencies and identify parallelism in a code. In our earlier paper, we proposed a model Data Dependence Identifier (DDI), in which a program  $P$  is represented as graph  $G_P$ . Using  $G_P$ , we could identify data dependencies in a program and also perform transformations like dead code elimination and constant propagation. In this paper, we present algorithms for loop invariant code motion, live range analysis, node splitting and loop fusion code transformations using DDI in polynomial time.

**Keywords**—Automatic parallelization; parallelizing compilers; code optimizations; data dependence; loop invariant code motion; node splitting; live range analysis; loop fusion

## I. INTRODUCTION

Multicore processors have completely replaced single core processors, as a result general purpose computers became parallel systems, this change has thrown lot of challenges to software community in the effective utilization of the former. Though multiprocessing capability of operating systems improves the overall throughput of new hardware still performance of serial programs remains the same even on multicore systems. To enhance the performance of serial programs on multicore systems, instructions in the serial code has to be broken into groups such that each group can be run in parallel. One way to accomplish this task is by manual conversion which is a tedious job. One more way is to use a tool that converts serial program to parallel.

Automating the process of serial to parallel conversion is called as Automatic Parallelization and the compiler which can perform automatic parallelization is typically referred as Parallelizing Compiler. The general process of serial to parallel program conversion is a three step one: 1) perform code transformations in order to detect potential parallelism; 2) check for data dependencies in the code; 3) generate parallel code.

Two instructions  $I_1$  and  $I_2$  in a program are said to be *data dependent* if both the instructions access same memory location. Presence of data dependencies makes parallelism an impossible task. Code transformations help to eliminate some of the data dependencies thereby giving a scope to detect potential parallelism.

In our earlier paper [1], we proposed a model called Data Dependence Identifier(DDI) which can identify data dependencies in scalars, arrays, and pointers in a program. We also

discussed how code optimizations like dead code elimination, constant propagation can be performed using DDI. In this paper, we discussed how code optimizations like loop invariant code motion, live range analysis and node splitting, loop fusion are performed using our model DDI.

## II. RELATED WORKS

Compiler converts source code to Intermediate Representation (IR) to perform code optimizations. This IR may differ from compiler to compiler. Generally, in traditional compilers for uniprocessor systems, instructions in source code are intermediately represented in three address code format and Directed Acyclic Graph (DAG), code optimizations are performed using this Intermediate Representation [3].

Intermediate Representation is crucial for a parallelizing compiler. Here, we will discuss in brief about some of the parallelizing compilers and their Intermediate Representations.

- SUIF (Stanford University Intermediate Format): SUIF is a source to source parallelizing compiler that takes C or FORTRAN serial code as input and produces parallelized code to be run on a multi-processor machine. SUIF intermediate representation is a language-independent abstract syntax tree. Data flow analysis, data dependence analysis, scalar and array privatization, reduction variable analysis are performed using IR [4], [5], [6].
- Cetus: Cetus converts serial program written in C to parallel C program by inserting OpenMP annotations to be run on a multicore system. Cetus intermediate representation is a hierarchical tree based structure implemented in Java. Cetus IR includes a set of iterators that traverses through the IR to get the required information about loops, conditional statements, etc. Data dependence analysis - GCD Test [7] and Range Test [8] are used to identify data dependencies in arrays. Transformation techniques like scalar and array privatization, induction variable substitution, reduction variable recognition are performed using IR to eliminate some of the dependencies [9].
- Pluto: Pluto is a source to source compiler that transforms serial C program to OpenMP C [10]. Intermediate Representation of Pluto is based on polyhedral model. Dependence analysis, loop transformations for parallelism and optimized data locality are performed

using IR [11]. Optimizations based on polyhedral model are integrated in compilers like GCC and LLVM. State-of-art in Pluto includes loop fusion transformation using Fusion Conflict Graphs (FCG) [12] and verified code generation [13].

- Intel compiler [16] automatically identify the loops that can be parallelized and partitions the data accordingly.

Using our proposed model DDI, we have shown how data dependence analysis can be performed. We are broadening the scope of our model by showing how code transformations like loop invariant code motion, live range analysis and node splitting, loop fusion can be applied on DDI.

### III. DATA DEPENDENCE IDENTIFIER

In this section we discuss in brief about our model Data Dependence Identifier(DDI) which we have proposed in our earlier paper [1]. The main objective of DDI model is to represent a program as graph to identify data dependencies in a program. Though many graphical representation of program exists [14], [15], our representation takes a completely different perspective, we consider variables in the program as nodes and the edges between these variables are drawn based on the mode of access of variables from memory. For this purpose, we have categorized the instructions in a program and parameterized program as discussed in sections A and B.

#### A. Categorization of Instructions based on Memory Accessibility

We categorized the instructions in a program broadly into **Memory Access Instruction (MAI)** and **Non Memory Access Instruction (NMAI)** based on the way they access the memory. In MAI, instructions access the memory to perform the required operation. Instructions like arithmetic, conditional fall under this category. In NMAI, instructions do not access the memory at all i.e., instructions like jump, break come under this category.

MA Instructions are further classified into three categories: MA-READ, MA-WRITE, MA-READWRITE. In **MA-READWRITE(MARW)**, instructions access the memory for both read as well as write operations. For example, in Arithmetic instruction: ' $c = a + b$ ', data is read from memory locations  $a$  and  $b$  and written to a memory location  $c$ . In **MA-READ(MAR)**, instructions perform only read operation but no write operation. For example, in conditional instruction: ' $if(a > b)$ ' data is only read from memory locations  $a$  and  $b$  but the output is not written to any variable. Generally in these instructions data is read from memory and send to other Hardware Units(HU) in the computer system like processor or output devices. In **MA-WRITE(MAW)**, instructions perform only write operation but no read operation. For example, in assignment instruction ' $a = 5$ ', a constant value is written to a memory location  $a$ . Here we assume,  $a = 5$  means that the constant 5 is read from the programmer(PR) and written to the location  $a$ .

#### B. Parameterization of Program

A program  $P$  is parameterized with  $I, V, W, HU, PR$ , where:

- Set  $I$ , finite set of instructions  $\{i_1, i_2, \dots, i_n\}$
- Set  $V$ , finite set of memory allocations or variables  $\{v_1, v_2, \dots, v_p\}$
- Set  $MAI$ , finite set of MA instructions where  $MAI \subseteq I$ .  
An instruction  $i \in MAI$  is represented as ordered pair  $[R, W]$  where  $R, W \subseteq V$ .  $R$  is a set that contains all the variables from which the instruction  $i$  reads the data and  $W$  is a set with a single variable to which  $i$  writes the data. For example, instruction ' $c = a + b$ ' is written as pair  $[\{a, b\}, \{c\}]$  where data is read from variables  $a, b$  and output is written to  $c$ .
- $HU$  represents the set of hardware units i.e. input devices, output devices, processor and any other hardware unit in the computer system.
- $PR$  is the set of constant values initialized in the program  $P$  by the programmer.

Therefore, we write  $P$  as  $P(I, V \cup \{HU, PR\}, MAI)$ .

#### C. Directed Graph Representation of a Program

In DDI model, we represent a program as graph. Here, we discuss how a program  $P$  is transformed to an equivalent directed graph called graph of  $P$  written as  $G_P$ .

All instructions in a given program  $P$  are indexed sequentially with the positive integers  $1, 2, \dots, n$ . First instruction in a program is indexed as 1, second instruction as 2 and so on. For  $i_n \in I$ , we call index of  $i_n = n$ . Every instruction  $i_n$  is written as the pair  $[R, W]$ . In other words,  $index[i_n] = index([R, W]) = n$ .

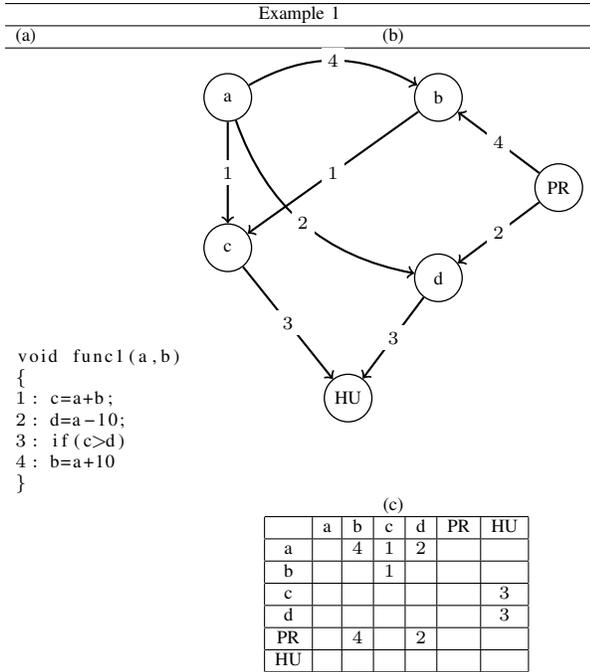
A program  $P = (I, V \cup \{PR, HU\}, MAI)$  is transformed into a directed labeled graph  $G_P = (V \cup \{PR, HU\}, E, L)$  as follows:

- Set of nodes of  $G_P$  are the set of variables  $V \cup \{PR, HU\}$ .
- For every ordered pair of sets  $(R, W) \in MAI$ , we include the edges  $\{(r, w) | \forall r \in R, w \in W\}$ .
- Every edge in  $G_P$  is labeled with elements from label set  $S$  which contains indices of instructions in  $I$ .  $L : E \rightarrow \{1, 2, \dots, n\}$  such that  $L((r, w)) = k$  if  $index([R, W]) = k$  such that  $(r, w) \in E, r \in R, w \in W$ .

We use the notation  $(., .)$  to represent the edges of the graph and  $[\cdot, \cdot]$  indicates the pair of sets  $R, W$  for representing memory access instructions.

In example 1,  $I = \{i_1, i_2, i_3, i_4\}$ ,  $V = \{a, b, c, d\}$  and  $MAI=I$  as all instructions in program  $P$  are memory access instructions. To construct  $G_P$ ,  $V$  acts as nodes  $N$ . For instruction 1 :  $[\{a, b\}, \{c\}]$ , we include the edges  $(a, c)$  and  $(b, c)$  with labels  $L((a, c)) = 1$  and  $L((b, c)) = 1$  are added to  $G_P$ . For instruction 2 :  $[\{a, PR\}, \{d\}]$ , edges  $(a, d)$  and

$(PR, d)$  with labels  $L((a, d)) = 2$  and  $L((PR, d)) = 2$  are added. For instruction 3 :  $\{c, d\}, \{HU\}$ , edges with label  $L((a, HU)) = 3$  and  $L((d, HU)) = 3$  are added. For instruction 4 :  $\{a, PR\}, \{b\}$ , edges with label  $L((a, b)) = 4$  and  $L((PR, b)) = 4$  are added to  $G_P$ . The adjacency matrix



of graph  $G_P$  is shown in example 1(c), rows gives the **read** information about the variables and columns gives the **write** information. Scanning column  $c$  of the matrix tells that variable  $c$  is accessed for 'write' in instruction 1 and row of  $c$  shows variable  $c$  is accessed for 'Read' in instruction 3.

The procedure by which we convert  $P(I, V \cup \{PR, HU\}, W)$  into a simple edge labeled graph  $G_P(N \cup \{PR, HU\}, E, L)$  is discussed in algorithm 1.

**Algorithm 1** Convert Program  $P$  to Directed edge-labeled graph  $G_P$

```

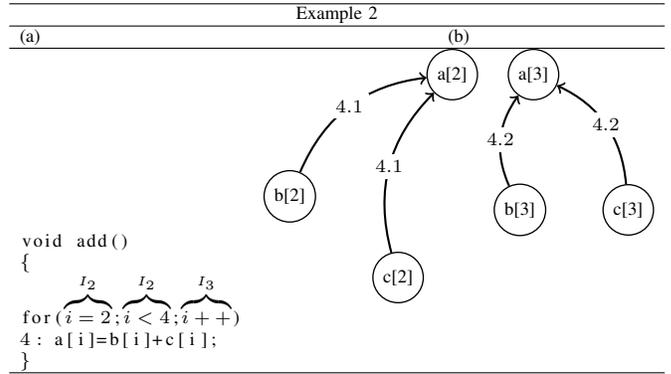
1: procedure PROGRAM TO GRAPH
   Input: Program  $P(I, V \cup \{PR, HU\})$ 
   Output: Graph  $G_P(N \cup \{PR, HU\}, E, L)$ 
2: for each instruction  $[R, W] \in I, index[R, W] = k$  do
3:   if MAI-verification() then
4:     for every  $r \in R$  and  $w \in W$  do
5:        $E = E \cup \{(r, w)\}$ 
6:        $L([r, w]) = k$ 
                
```

**Loop representation in DDI:**

The statements within the loop are denoted as  $i.k$ , where  $i.k$  represents instruction  $i$  when the loop is executed  $k^{th}$  time.

**Nested loop representation in DDI:**

Consider nested loops  $L_1$  and  $L_2$ , where  $L_1$  is the outer loop and  $L_2$  is the inner loop. The statements within the nested loop are denoted as  $m.x.p$ , where  $m.x.p$  represents  $m^{th}$  instruction when the loop is executed  $x^{th}$  iteration in  $L_1$  loop and  $p^{th}$  iteration in  $L_2$  loop.



Consider the nested sequence of loops  $L_1, L_2, L_3, \dots, L_n$ , where  $L_1$  is the outermost loop and  $L_n$  is the innermost loop. The statements within this nested loop are denoted as  $m.x_1.x_2 \dots x_n$ , where  $m$  represents the instruction number and  $x_1$  represents the instance of iteration of outermost loop  $L_1$ ,  $x_2$  represents the instance of iteration of loop  $L_2$ , and  $x_n$  represents the instance of execution of innermost loop  $L_n$ .

**IV. APPLICATIONS OF DDI**

In our earlier paper [1], we proposed how compiler optimizations like constant propagation, dead code elimination and induction variable detection can be performed using our DDI model. In this section, we will discuss how optimizations like loop invariant code motion, live range analysis, loop fusion, scalar privatization can be performed using our DDI model.

**A. Loop Invariant Code Motion**

A set of statement(s) within a loop is called as Loop Invariant Code if the semantics of the program is not affected when the statements are moved out of the loop. Identifying and removing invariant code loop reduces the number of statements within the loop, thereby enhancing the performance of the parallel loop. Code Motion is the process of moving the loop invariant code outside the loop. In the program given in example 3(a), value of  $x$  in instruction 5 remains unchanged through out the execution of loop. Even if instruction 5 is moved above the loop, value of  $x$  remains the same.

Following observation is made to identify loop invariant code:

- For an instruction  $i : [R, W]$ , the value of the variable 'W' will get updated during the loop iteration if atleast one of the values of variables in 'R' is changing during the execution of the loop. In example 3(a), in instruction 5 :  $\{t, PR\}, \{x\}$ , input variables are  $\{t, PR\}$ ,  $t$  is the only input variable here as  $PR$  is a constant value and variable  $t$  never gets updated in the loop. As  $t$  value never changes during the execution of the loop, consequently there is no change in  $x$ . We call statement 5 as 'Loop Invariant Code'.

**Theorem 1.** Given a loop  $l$  with statements  $\{i_1, i_2, \dots, i_s\}$  and  $G_l$  be the graph that corresponds to the loop  $l$ . A statement  $l_k \in l$  is said to be **Loop Invariant Code** if

1. There exists a node  $u \in N.G_l$  such that  $L((u', u)) = [i_k.1, i_k.2, \dots, i_k.m]$  where  $m$  is the number of iterations of the loop.

2. There is no edge  $(v, u')$  for every  $u \in N.G_l$ .

*Proof:*  $i_k$  is 'Loop Invariant Code'

$\implies$  If  $i_k : [R, W]$ , then  $\exists u \in W$  where the value of  $u$  does not change through out the loop.

$\implies u \in W$  implies that there exists  $u_k \in R$  such that value of  $u_k$  is written in  $u$  and there is no change in  $u_k$  through out the loop.

$\implies$  By algorithm,  $G_l$  will have the edges  $(u_k, u)$  and there will not be any edge of the form  $(v, u_k)$  where  $u, u_k \in N.G_l$ , since the nodes of  $G_l$  pertains to the variable inside the loop. ■

Algorithm illustrates the process of loop invariant code detection. Line 3-6 of the algorithm examines if node  $u$  have

**Algorithm 2** Loop invariant code detection

```

1: procedure LOOP INVARIANT CODE DETECTION
   Input: Graph  $G_p(N, E, L)$ 
2:   edgelabels=FALSE, invariant=TRUE
3:   LS={ $i_1, i_2, \dots, i_s$ }
4:   for every  $u \in N.G$  do
5:     if  $L((u_i, u)) == [n.1, n.2, \dots, n.m]$  then
6:       if  $L((v_i, u_i)) \in LS$  then
7:         invariant=FALSE
8:       if invariant==TRUE then  $\triangleright$  perform Code Motion
9:         delete edges  $L((u_i, u)) = [n.1, n.2, \dots, n.m]$ 
10:        add edge  $L((u_i, u)) = p, p < l_1$ 

```

any incoming edges from nodes  $u, u_1, u_2, \dots, u_k$  with labels matching the pattern  $[n.1, n.2, \dots, n.m]$ . If so, then line 8-10 checks if there are any incoming edges to nodes  $u, u_1, u_2, \dots, u_k$  with label  $l$  where  $l \in LS$ , LS contains loop statement labels. If no such edges exist, instruction  $n$  is considered as loop invariant code, move instruction  $n$  above the loop in the program. Line 8-10, perform code motion. Example 3(b) shows the program and graph after code motion.

**B. Live Range Analysis**

For parallelizing a program, statements in the program has to be grouped in such a way that the statements in these groups can be executed in parallel and gives the same output as sequential execution. one way to accomplish this task is using the live range information of variables in the program. We define the *live range* of a variable in a program as follows:

**Definition IV.1.** A variable  $u$  is said to *live* in statement  $k$  of program  $P$  if either *Read* or *Write* operation is performed on  $u$ .

Consider the program in example 5,  $y$  is *live* in statement 2 and *not live* in statements 1,3,4.

**Definition IV.2.** Live Range Analysis of a program  $P$  is a description which provides an information on the nature of the variable, whether live or not, in each of the instruction of program  $P$ .

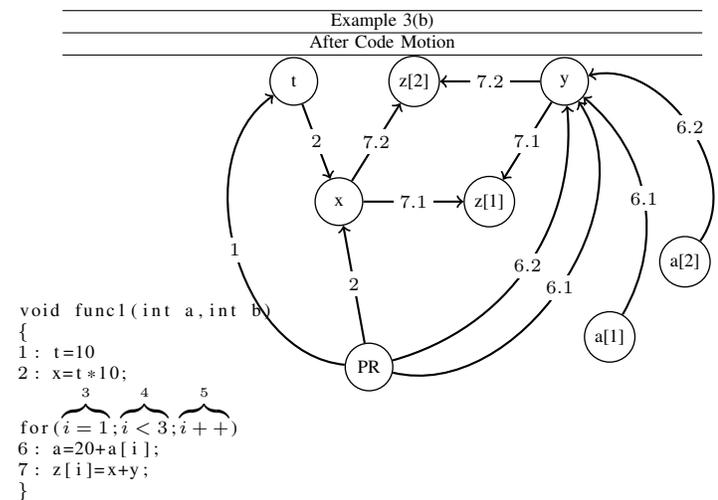
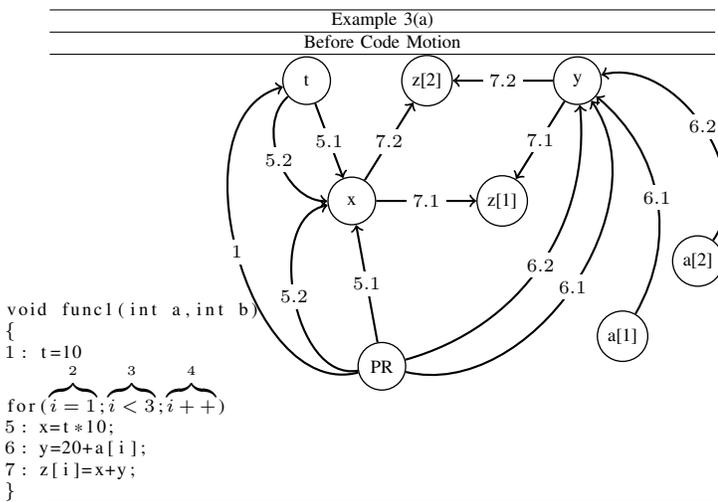
In example 4(a),  $x$  is live in statements 1,2,3,4.  $y$  is live in statement 2.  $k$  is live in statement 1.  $a$  is live in statement 4. This information is represented in the form:  $x : \{1, 2, 3, 4\}$ ,  $y : \{2\}$ ,  $k : \{1\}$ ,  $z : \{3\}$ ,  $a : \{4\}$ , which is usually referred as live range analysis of P.

Now, we propose a method to compute live range of variables in a program using our DDI model.

**Theorem 2.** Given a program  $P$  and the corresponding graph  $G_p$ . If node  $u \in G_p$  have either incoming and outgoing edges with labels  $i_k$  then variable  $u$  is said to be *live* in statements  $i_k$  of program  $P$ .

*Proof:*  $u$  is live in instruction  $i_k$ .

$\implies$  By definition IV.1, either *Read* or *Write* operation is performed on  $u$  in  $i_k$ .  $\implies$  By algorithm 1, there will be



In example 4(a), Loop Statements(LS)={5,6,7} for node  $x$ ,  $L((t, x)) = [5.1, 5.2]$  and  $L((PR, x)) = [5.1, 5.2]$ , there exists no other edges to node  $x$  with label 5. Only source of input to node  $x$  with label 5 is from nodes  $t$  and  $PR$ . As  $PR$  is constant value, only input is node  $t$ . Incoming edge to node  $t$  is  $L((PR, t)) = 1, 1 \notin LS$ . Therefore, we conclude statement 5 is loop invariant code.

an outgoing edge with label  $i_k$  from  $u$  (if Write operation is performed over  $u$  in  $i_k$ ) or there will be an incoming edge with label  $i_k$  to  $u$  (if Read operation is performed over  $u$  in  $i_k$ ).

⇒ There is an edge incident on  $u$  with label  $i_k$ . ■

Based on the above theorem, we propose an algorithm to compute live range of variables in a program.

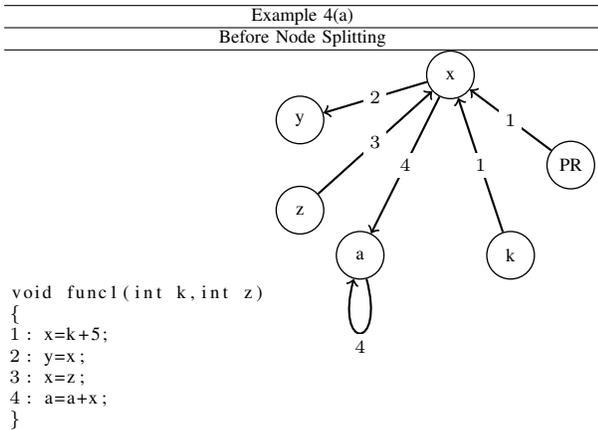
In Line 2 of algorithm 3, A is initialized as an empty two

**Algorithm 3** Live Range Analysis

```

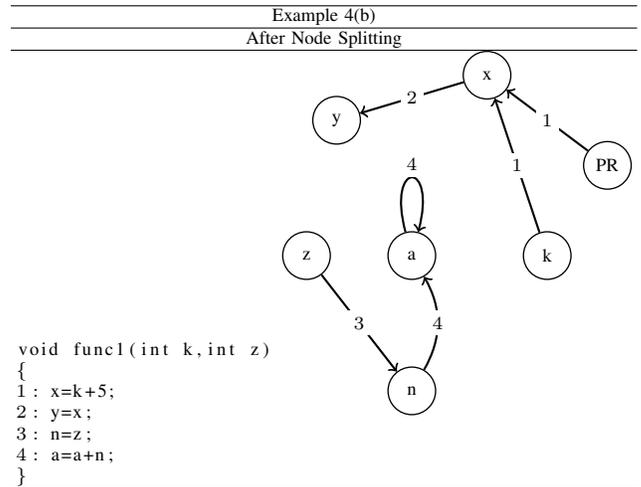
1: procedure LIVE RANGE ANALYSIS
   Input: Graph  $G_p(N, E, L)$ 
2:   A=[ ]
3:   i=0
4:   for every  $u \in N.G$  do
5:     A[i].append( $u, L((v, u)), L((u, u'))$ )
6:     i=i+1
7:   return A
    
```

dimensional array. The for loop in lines 4-6 examines all the incoming and outgoing edge labels of each node and assigns this information to A. Each row of array A have node label  $u$ , the incoming and outgoing edge labels of node  $u$ . With assumption the graph is represented using adjacency matrix, the running time of this algorithm is  $O(n^2)$ , where  $n$  is the number of nodes in the graph. The for loop requires scanning the row and column of each and every node, therefore the complexity  $O(n^2)$ .



**C. Node Splitting**

If a variable is *live* through out the program means there exists data dependence among the statements. The data dependence has to be broken in order to group the statements such that each group can execute in parallel. One approach to break the data dependence cycle is using **Node Splitting**. Node splitting creates one more copy of a node(duplicate node) in the graph and divides the edges between two nodes to produce an analogous graph. This transformation limits the live range of a variable to a section in the code hence producing a code more feasible for parallelization. Consider the program in example 4, variable  $x$  is live in instructions  $\{1, 2, 3, 4\}$ , after splitting  $x$  as  $x$  and  $n$ ,  $x$  is live in instructions  $\{1, 2\}$  and  $n$  in  $\{3, 4\}$ .



Given a variable  $v$ , the possible sequence of *Read*(R) and *Write*(W) operations on  $v$  are 1.  $\{W, R, R, R..R\}$  - value assigned to  $v$  is only *Read* through out the program. 2.  $\{W, R, W, R..R\}$  - variable  $v$  is updated multiple times in the program. Based on this observation, we define the scope of node splitting as follows:

**Definition IV.3.** A node  $u \in V.G_P$  is said to be a splitting node if the sub-graph that involves  $u$  can be split into two sub-graphs  $G_{P_1}$  and  $G_{P_2}$  such that functionality of both the programs  $P_1$  and  $P_2$  is equivalent to the functionality of  $P$ .

**Theorem 3.** Let  $P$  be a program,  $G_P$  be the graph that corresponds to  $P$ . A node  $u \in V.G_P$  is a splitting node of  $G_P$  if and only if  $\exists$  a sub-graph  $G_P^u$  that involves the node  $u$  as follows.

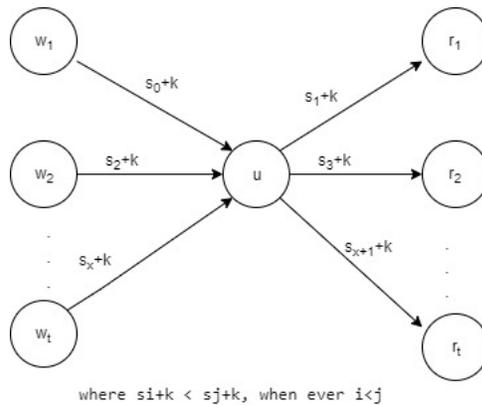


Fig. 1.  $u$  is Splitting Node of  $G_P$ .

*Proof:*  
Hypothesis:  $u$  is a splitting node of  $G_P$ .

Claim:  $\exists$  a sub-graph  $G_P^u$  of  $G_P$  as shown in fig1.

Hypothesis:  $G_P^u$  can be split into two sub-graphs  $G_{P_1}^u$  and  $G_{P_2}^u$  such that the functionality of  $P_1$  and  $P_2$  is equivalent to  $P$ .

$\implies \exists$  a program  $P$  in which variable  $u$  is used more than once ( $t_1$  times) for writing and  $u$  is used more than once ( $t_2$  times) such that  $t_1 \geq t_2$ .

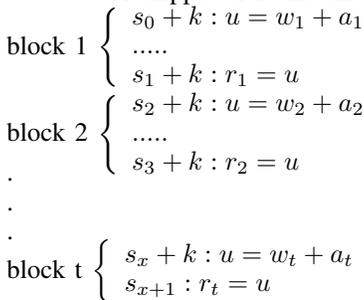
without loosing any generality, assume  $t_1 = t_2 = t$

$\implies u$  is used  $t$  times for writing and  $u$  is used  $t$  times for reading purpose.

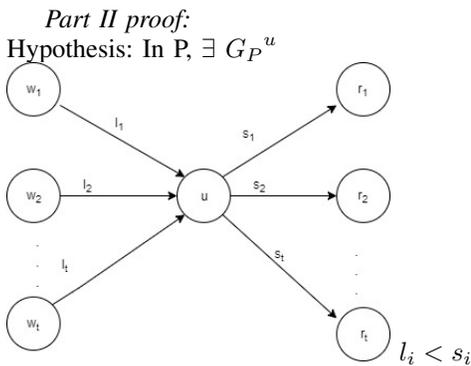
$\implies$  Again, without loss of any generality, for every writing to  $u$ , we have a reading from  $u$ .

$\implies$  Since  $u$  is a splitting node, we have a sequence of  $t$  blocks in  $P$  such that in each block,  $u$  is written first and then  $u$  is read.

$\implies$  A snippet of  $P$  that involves  $u$  will look as follows:



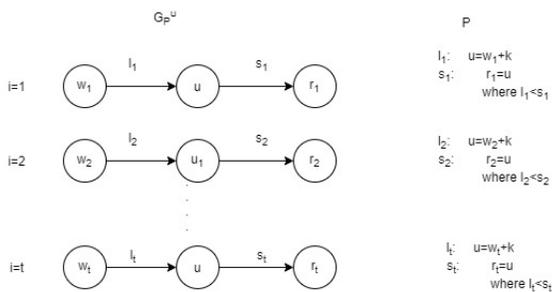
Corresponding  $G_P$  will be as shown in fig.1, hence the claim.



Claim:  $u$  is a splitting node.

Hypothesis:  $P$  has a sequence of  $t$  blocks and in each block, value is read from  $u$  after a value is written to  $u$ .

$\implies G_P^u$  can be split as follows



In each  $P_i$ , a value is written to  $u$  first and then  $u$  is read.

$\implies$  From  $G_P^u$ , we infer that in  $P$ , value is written first and then read next.

$\implies$  By sheer observations, we infer that the total functionality of the snippets  $P_i (i = 1 \text{ to } t)$  is same as

the functionality of  $P$ . The functionality of other statements (which does not involve  $u$ ) in  $P$  remains as such in  $P_i$  also.

$\implies$  We have a node  $u$  in  $G_P^u$  which can be split into a sequence of sub-graphs  $G_P^u, i = 1, 2, \dots, t$  such that the total functionality of  $P_i, i = 1, 2, \dots, t$  is equivalent to the functionality of  $P$ .

$\implies u$  is a splitting node of  $G_P$ . ■

**Corollary 3.1.** Let  $P$  be a program. Let  $G_P$  be the graph that corresponds to  $P$ .  $P$  is parallelizable if and only if  $G_P$  has atleast one splitting node.

**Algorithm 4** Node Splitting

```

1: procedure NODE SPLITTING
   Input: Graph  $G_P(N, E, L)$ 
2: for every  $u \in N.G$  do
3:   if  $L((u', u)) = m$  and  $L((u', u)) = n$  and  $n > m$ 
      then
4:     add node  $w$ 
5:     delete edge  $L((u', u)) = n$ 
6:     add edge  $L((u', w)) = n$ 
7:     for every edge  $(L((u, v)) > n)$  do
8:       delete  $L((u, v))$  and add  $L((w, v))$ 

```

Let  $M$  be the adjacency matrix representation of  $G_P$ . In algorithm, line 2 requires scanning each and every column of  $M$  to check if there exists any node  $u$  which satisfies the condition in line 3. Lines 4-6 i.e. adding a new node and edges takes constant time. In line 3, if a node  $u$  meet the condition then in lines 7-8 the entire row of the node  $u$  has to be examined. Let's say if there are  $n$  nodes among which  $m$  nodes satisfy the condition in line 3, then the complexity is  $O(mn)$ .

**D. Loop Fusion**

Loop fusion is a technique in which two loops are merged or fused to form a single loop. Generally, a loop iterates through the same set of instructions to perform a task. Two loops  $L1$  and  $L2$  can be fused if number of iterations, terminating conditions of both the loops match and the semantics of the code be intact after merging. Fusing of loops reduces the number of loops present in a program thereby mitigating the overhead involved in parallelization of many loops.

**Definition IV.4. Loop Fusion:** is a technique by which statements of multiple loops are merged into a single loop such that semantics of the code is intact.

Consider  $L1$  be the first loop and  $L2$  be the second loop in sequence, then  $L1$  and  $L2$  can be fused if the following conditions are satisfied:

- Loops  $L1$  and  $L2$  should have same looping conditions and should iterate for same number of times.
- Dependencies that exist between statements of loop  $L1$  and  $L2$  does not change the semantics of the code.

So, concept of fusion depends on the dependencies that exist between the loops. Hence, first we discuss different dependencies that exist between the loops. Two loops  $L1$  and  $L2$

are said to be data dependent if dependence exists between any statement of  $L1$  and any statement of  $L2$ . Let statements  $S_i \in L1$  and  $S_j \in L2$ . The following dependencies may exist between  $S_i$  and  $S_j$ :

**Definition IV.5. No dependence:**  $L1$  and  $L2$  are said to have no dependence if the statements  $S_i$  and  $S_j$  do not access any common memory location.

**Definition IV.6. Flow dependence:** If memory location  $M$  is accessed for 'Write' operation in statement  $S_i$  and the same location  $M$  is accessed for 'Read' in statement  $S_j$ . Then, flow dependence exist between statements  $S_i$  and  $S_j$ .

In example 6(case i), 'Write' operation is performed on an index location in array  $A$  in first loop and is 'Read' from the same index location in array  $A$  in second loop. So, there exist flow dependence between loops  $L1$  and  $L2$ .

**Definition IV.7. Anti dependence:** If memory location  $M$  is accessed for 'Read' operation in statement  $S_i$  and the same location  $M$  is accessed for 'Write' in statement  $S_j$ . Then, anti dependence exist between statements  $S_i$  and  $S_j$ .

In example 7(case i), 'Read' operation is performed on an index location in array  $x$  in first loop and 'Write' operation on the same index location of array  $x$  in second loop, there exist Anti dependence between loops  $L1$  and  $L2$ .

**Definition IV.8. Loop carried forward dependence:** If memory location  $M$  is accessed by an iteration of statement  $S_i$  and then the same location  $M$  is accessed in later iterations of statement  $S_j$ . Then, loop carried forward dependence exists between statements  $S_i$  and  $S_j$ .

In example 8,  $A[1]$  value computed in first iteration of first loop is read in the second iteration of second loop, shows existence of loop carried forward dependence between  $L1$  and  $L2$ .

**Definition IV.9. Loop carried backward dependence:** If memory location  $M$  is accessed in an iteration of statement  $S_j$  and then the same location  $M$  is accessed in later iterations of statement  $S_i$ . Then, loop carried backward dependence exists between statements  $S_i$  and  $S_j$ . In example 9,  $A[2]$  value computed in second iteration of first loop is read in the first iteration of second loop, shows presence of loop carried backward dependence.

#### Identification of data dependencies using DDI and feasibility of fusion

So far we have discussed the dependencies that exist between the loops. Here, we will discuss the type of dependencies between  $L1$  and  $L2$  which does not affect the fusion of  $L1$  and  $L2$ . We propose four theorems with which we can identify the type of dependence that exist between  $L1$  and  $L2$  using our DDI and the feasibility of fusing them.

**Theorem 4.** Given program  $P$  with loops  $L1$  with statements  $\{i_{r_1}, i_{r_2}, \dots, i_{r_n}\}$  and loop  $L2$  with statements  $\{i_{s_1}, i_{s_2}, \dots, i_{s_m}\}$ . Let  $G_P$  be the corresponding graph of  $P$ , with  $G_{L1}$  and  $G_{L2}$  as the sub-graphs of  $G_P$  that corresponds to loops  $L1$  and  $L2$  respectively.  $L1$  and  $L2$  is said to have **no dependence** if there exists no edge  $(u, v)$ ,  $\forall u \in G_{L1}$  and  $\forall v \in G_{L2}$ . Such

loops  $L1$  and  $L2$  can be fused.

*Proof:* Assume that there exists an edge  $(u, v)$  where  $u \in V(G_{L1})$ ,  $v \in V(G_{L2})$ .

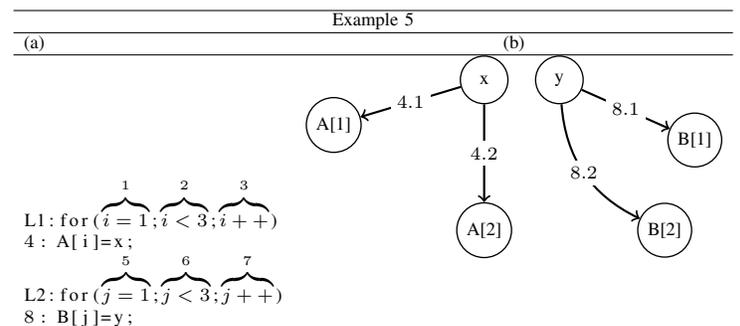
$\implies$  An edge  $(u, v)$  in  $G_{L1}$  means that a value is Read from variable  $u$  in some statement  $i_{r_j}$  (say) and Written to variable  $v$ . As  $v \in G_{L2}$ ,  $v$  is accessed by some statement  $i_{s_k}$  (say) in  $L2$ .

$\implies$  By Algorithm 1, there exists a statement  $i_{r_j}$  in  $L1$  which Read's a value from variable  $u$  and that value is Written to a variable  $v$  in statement  $i_{s_k}$  in  $L2$ .

$\implies$  Thus, we have proved that if there exists an edge  $(u, v)$  with label  $i_{r_j}$  then there exists a statement  $i_{r_j}$  which accesses the variables  $u$  and  $v$ .

$\implies$  By considering contrapositive statement of above proposition i.e, if there does not exist a statement  $i_{r_j}$  which accesses the variables  $u$  and  $v$  then there does not exist edge  $(u, v)$ .  $\implies$  There exists no common variable accessed by statements of  $L1$  and  $L2$ . Therefore, by Definition 4.5, if statements of  $L1$  and  $L2$  do not access common memory location then there exists no dependence between statement of loops  $L1$  and  $L2$ .

■



In Example 5, nodes  $\{x, A[1], A[2]\} \in L1$  and nodes  $\{y, B[1], B[2]\} \in L2$ , there exists no common nodes among  $L1$  and  $L2$ , no edges between nodes of  $L1$  and  $L2$ . Therefore, no dependence exist between the two loops, in which case merging of loops is possible.

**Theorem 5.** Given program  $P$  with loops  $L1$  with statements  $\{i_{r_1}, i_{r_2}, \dots, i_{r_n}\}$  and  $L2$  with statements  $\{i_{s_1}, i_{s_2}, \dots, i_{s_m}\}$ .  $G_P$  be the corresponding graph of  $P$ ,  $G_{L1}$  and  $G_{L2}$  are the sub-graphs of  $G_P$  that corresponds to loops  $L1$  and  $L2$  respectively. Let there exist edges  $L((u, v)) = i_{r_j}.n$  and  $L((v, w)) = i_{s_k}.m$  such that  $i_{r_j} \in L1$ ,  $i_{s_k} \in L2$ . i

- 1)  $L1$  and  $L2$  is said to have **flow dependence** if  $i_{s_k} > i_{r_j}$ .
- 2)  $L1$  and  $L2$  can be fused if  $m \geq n$  and  $i_{s_k} > i_{r_j}$ .
- 3)  $L1$  and  $L2$  can not be fused if  $n > m$ .

*Proof:* Let  $G_{L1}$  and  $G_{L2}$  be the sub-graphs of  $G_P$  that corresponds to loops  $L1$  and  $L2$  in  $P$  and there exist edges  $L((u, v)) = i_{r_j}.n$  and  $L((v, w)) = i_{s_k}.m$  in  $G_P$ .

Hypothesis 1: There is a flow dependence if  $i_{s_k} > i_{r_j}$ .

⇒ An incoming edge with label  $i_{r_j}.n$  to node  $v$  means variable  $v$  is Written in  $n$ th iteration of instruction  $i_{r_j}$ . An outgoing edge with label  $i_{s_k}.m$  to node  $v$  means variable  $v$  is Read in  $m$ th iteration of instruction  $i_{s_k}$ .

⇒ The condition  $i_{s_k} > i_{r_j}$  means that first a value is Written to  $v$  in  $n$ th iteration of instruction  $i_{r_j}$  and then Read from  $v$  in  $m$ th iteration of instruction  $i_{s_k}$ .

⇒ By Definition IV.6, there exists flow dependence between statements  $i_{s_k}$  and  $i_{r_j}$  if Read operation succeeds Write operation.

Hypothesis 2:  $L1$  and  $L2$  can be fused if  $m \geq n$  and  $i_{s_k} > i_{r_j}$ .

⇒ As  $m \geq n$  and  $i_{s_k} > i_{r_j}$ , even after fusing the statements  $i_{s_k}$  and  $i_{r_j}$  as Read operation succeeds Write operation on variable  $v$ , semantics of code is unchanged.

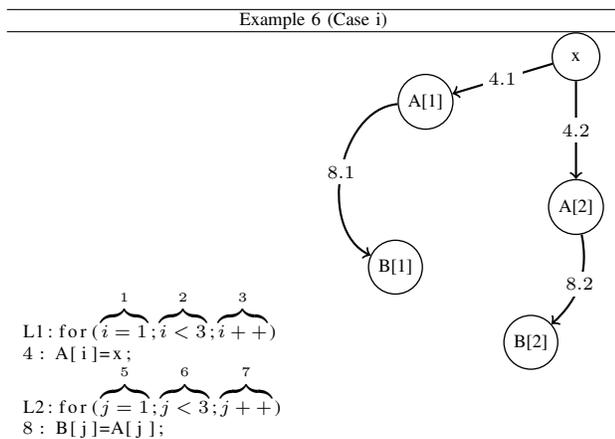
⇒ By definition IV.4, statements of loops  $L1$  and  $L2$  can be fused if the semantics of the code is intact.

Hypothesis 3:  $L1$  and  $L2$  can not be fused if  $n > m$ .

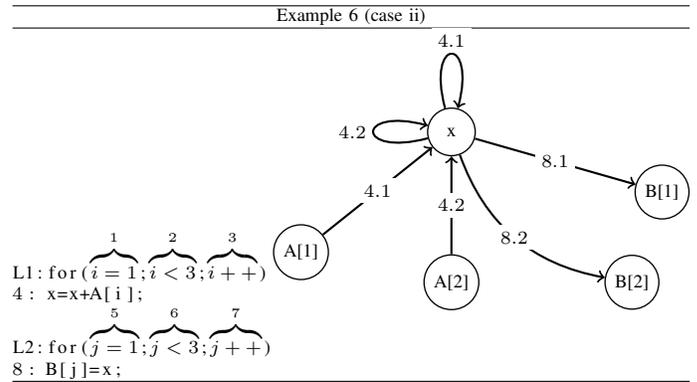
⇒ Before fusing, in loop  $L1$  write operation is performed on variable  $v$  in  $n$ th iteration of instruction  $i_{r_j}$ . In loop  $L2$  variable  $v$  is Read in  $m$ th iteration of instruction  $i_{s_k}$ .

⇒ If  $L1$  and  $L2$  are fused, as  $n > m$ , variable  $v$  is read in  $m$ th iteration of instruction  $i_{s_k}$  even before  $v$  is written in  $n$ th iteration of instruction  $i_{r_j}$  i.e., older value of variable  $v$  is read not the updated.

⇒ As semantics of code changes, loop fusion is not possible if  $n > m$ . ■



If flow dependence exists between loops  $L1$  and  $L2$  i.e., if an instruction in  $L1$  access a memory location  $M$  for ‘Write’ and the same location is accessed by an instruction in loop  $L2$  for ‘Read’ then merging of loops is possible if  $M$  is accessed for ‘Write’ and then for ‘Read’ even after fusion. In example 6(case i),  $L((x, A[1])) = 4.1$  and  $L((A[1], B[1])) = 8.1$  says  $A[1]$  is updated in iteration 1 of instruction 4 and read in iteration 1 of instruction 8. As a value is updated in first loop and read in second loop in the same iteration, merging of loops will not change the semantics of code. Therefore edges  $L((u, v)) = n.i$  and  $L((v, w)) = m.j$  where  $n \in L1$ ,  $m \in L2$



and  $j \geq i$  in the graph represents flow dependence where merging of loops is possible.

If flow dependence exists between loops  $L1$  and  $L2$  merging of loops is *not* possible if on fusing of loops ‘Write’ operation succeeds ‘Read’ on memory location  $M$ , which changes the semantics of the code. In example 6(case ii),  $x$  is accessed for ‘Write’ in first loop and for ‘Read’ in second loop, which shows flow dependence.  $L((A[2], x)) = 4.2$  and  $L((x, B[1])) = 8.1$  says, value of variable  $x$  to be written in iteration 2 of instruction 4 is read in iteration 1 of instruction 8 i.e., value of  $x$  is read even before write operation. Therefore, merging of loops  $L1$  and  $L2$  changes the semantics of the code.

**Theorem 6.** Given program  $P$  with loops  $L1$  with statements  $\{i_{r_1}, i_{r_2}, \dots, i_{r_n}\}$  and loop  $L2$  with statements  $\{i_{s_1}, i_{s_2}, \dots, i_{s_m}\}$ .  $G_P$  be the corresponding graph of  $P$ ,  $G_{L1}$  and  $G_{L2}$  are the sub-graphs of  $G_P$  that corresponds to loops  $L1$  and  $L2$  respectively. Let there exist edges  $L((u, v)) = i_{r_j}.n$  and  $L((w, u)) = i_{s_k}.m$  such that  $i_{r_j} \in L1$ ,  $i_{s_k} \in L2$ . i

- 1)  $L1$  and  $L2$  is said to have **Anti dependence** if  $i_{s_k} > i_{r_j}$ .
- 2)  $L1$  and  $L2$  can be fused if  $m \geq n$  and  $i_{s_k} > i_{r_j}$ .
- 3)  $L1$  and  $L2$  can not be fused if  $n \geq m$ , i.e., an outgoing edge from  $u$  of  $L1$  have iteration number greater than an incoming edge to  $u$ .

*Proof:* Let  $G_{L1}$  and  $G_{L2}$  be the sub-graphs of  $G_P$  that corresponds to loops  $L1$  and  $L2$  in  $P$  and there exist edges  $L((u, v)) = i_{r_j}.n$  and  $L((w, u)) = i_{s_k}.m$  in  $G_P$ .

Hypothesis 1: There is an anti dependence if  $i_{s_k} > i_{r_j}$ .

⇒ An incoming edge with label  $i_{r_j}.n$  to node  $v$  means variable  $v$  is Written in  $n$ th iteration of instruction  $i_{r_j}$ . An outgoing edge with label  $i_{s_k}.m$  from node  $w$  to node  $u$  means variable  $u$  is Written in  $m$ th iteration of instruction  $i_{s_k}$ .

⇒ The condition  $i_{s_k} > i_{r_j}$  means that first a value is Read from  $u$  in  $n$ th iteration of instruction  $i_{r_j}$  and then Written from  $w$  to  $u$  in  $m$ th iteration of instruction  $i_{s_k}$ .

⇒ By Definition IV.7, there exists anti dependence between statements  $i_{s_k}$  and  $i_{r_j}$  if Write operation succeeds Read operation.

Hypothesis 2:  $L1$  and  $L2$  can be fused if  $m \geq n$  and  $i_{s_k} > i_{r_j}$ .

$\Rightarrow$  As  $m \geq n$  and  $i_{s_k} > i_{r_j}$ , even after fusing the statements  $i_{s_k}$  and  $i_{r_j}$  as Write operation succeeds Read operation on variable  $u$ , semantics of code is unchanged.

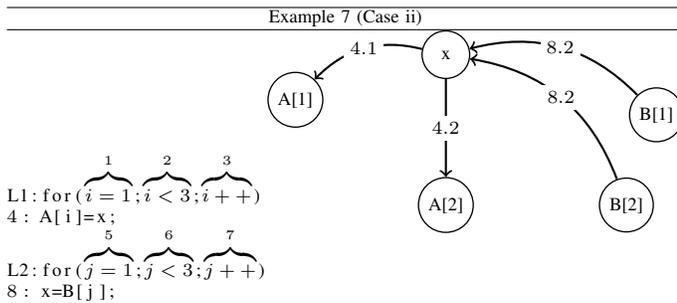
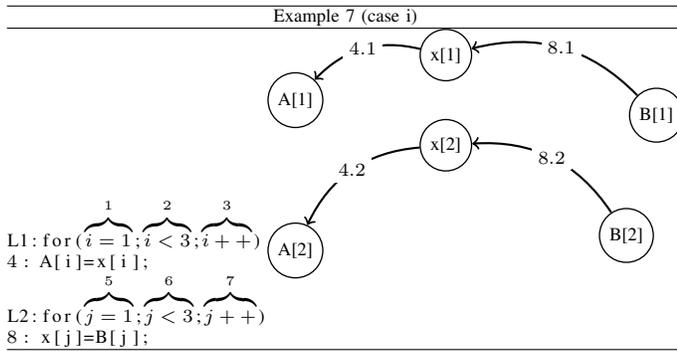
$\Rightarrow$  By definition IV.4, statements of loops  $L1$  and  $L2$  can be fused if the semantics of the code is intact.

Hypothesis 3:  $L1$  and  $L2$  can not be fused if  $n > m$ .

$\Rightarrow$  Before fusing, in loop  $L1$  Read operation is performed on variable  $u$  in  $n$ th iteration of instruction  $i_{r_j}$ . In loop  $L2$  variable  $u$  is Written in  $m$ th iteration of instruction  $i_{s_k}$ .

$\Rightarrow$  If  $L1$  and  $L2$  are fused, as  $n > m$ , variable  $u$  is Written in  $m$ th iteration of instruction  $i_{s_k}$  even before  $u$  is Read in  $n$ th iteration of instruction  $i_{r_j}$  i.e., a new value is written to  $u$  even before older value is Read.

$\Rightarrow$  As semantics of code changes, loop fusion is not possible if  $n > m$ . ■

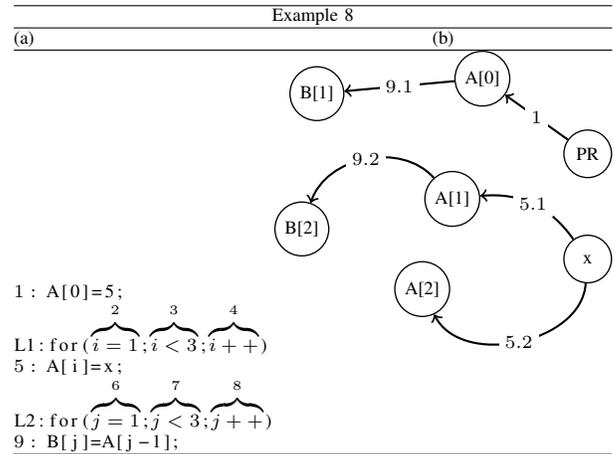


If anti dependence exists between loops  $L1$  and  $L2$  i.e. if an instruction in  $L1$  access an memory location  $M$  for Read and the same location is accessed by an instruction in loop  $L2$  for Write, merging of loops is possible if  $M$  is accessed for Read first and then for Write even after fusing. In example 7(case i),  $L((x[2], A[4])) = 4.2$  and  $L((B[2], x[2])) = 8.2$  says  $x[2]$  is read in iteration 2 of instruction 4 and written in iteration 1 of instruction 8. As the value is 'Read' in first loop and 'written' in second loop in the same iteration, merging of loops will not change the semantics of code. Therefore edges  $L((u, v)) = n.i$  and  $L((w, u)) = m.j$  where  $n \in L1$ ,  $m \in L2$  and  $j \geq i$  in the graph represents anti dependence where merging is possible.

If anti dependence exists between loops  $L1$  and  $L2$  merging of loops is not possible if a memory location  $M$  which is accessed for 'Read' in  $L1$  and then for 'Write' in  $L2$  is not preserved after fusing. Example 7(case ii) shows the anti

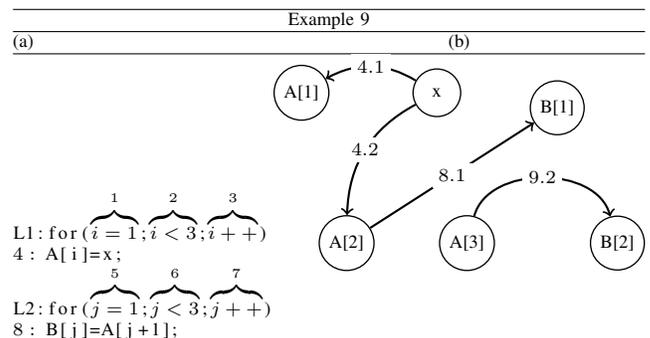
dependence where memory location  $x$  is accessed for 'Write' many times in first loop and for 'Read' in second loop, merging of loops is not possible.

If **Loop carried forward dependence** exists between loops  $L1$  and  $L2$  merging of loops is possible. In Example 8,  $L((x, A[1])) = 5.1$  and  $L((A[1], B[2])) = 9.2$  says memory location  $A[1]$  is written in iteration 1 of instruction 5 and is read in iteration 2 of instruction 9. As a value computed in iteration  $i$  of first loop is accessed in iteration  $j$  of second loop where  $j \geq i$ , merging of loops will not change the semantics of the code.



If **Loop carried backward dependence** exists between loops  $L1$  and  $L2$  merging of loops is not possible. If a memory location is accessed by an iteration of a statement  $S_i$  in loop  $L1$  and the same location is accessed by previous iterations of statement  $S_j$  in loop  $L2$ , when such statements are merged  $S_j$  in  $L2$  will access the memory location first and then  $S_i$  which will change the order of execution. As semantics of code will change, fusing of loops is not possible if *loop carried backward dependence* is present between  $L1$  and  $L2$ .

In Example 9,  $L((x, A[2])) = 4.2$  and  $L((A[2], B[1])) = 8.1$  says memory location  $A[2]$  is written in iteration 2 of instruction 4 and is read in iteration 1 of instruction 8 i.e., memory location  $A[2]$  is read even before it is updated. As a value computed in iteration  $i$  of first loop is accessed in iteration  $j$  of second loop where  $j < i$ , merging of loops can change the semantics of the code.



Thus, we conclude that fusion of two loops  $L1$  and  $L2$  is possible though the above discussed dependencies such

as flow dependence(case i), loop carried dependence, anti dependence(case i) exists between the statements of the loops.

## V. CONCLUSION AND FUTURE WORK

In this paper, we have introduced a model to perform various optimizations like loop invariant code motion, live range analysis, node splitting and loop fusion through a graphical representation of the program called as Data Dependence Identifier (DDI). For each of the optimization we have investigated on the condition that has to be satisfied by DDI (graphical representation of the program  $P$ ) so that optimizations can be performed which leads to an effective parallelization of  $P$ .

All the optimizations that were discussed are justified as well as validated conceptually with a sequence of rigorous theorems. These theoretical proofs also serve the purpose of the *correctness of proposed algorithms* with which one could easily perform the optimizations of a program.

**Salient Features:** Though there are many graphical representations for a program, our graphical representation referred as DDI is a unique graphical representation in the state that the variables of  $P$  are used as nodes and the edges between the nodes reflect the nature of access (read/write) of the variables from the memory.

Thus, salient features of our work are:

- a novel graphical representation of a program.
- performing almost all the optimizations with one model DDI.

**Future Work:** The optimization procedures are the main components of parallelization process. With our DDI model, in this paper we have just established the performance of various optimization procedures. Validating the optimization procedures with the benchmarked programs may not yield any significant insight on the performance of optimization procedures with DDI. The reason being that, performance of the various components of a machine may not yield any useful information on the performance of the machine built with those components. For this reason, experimental validation of a full DDI based parallelizer is proposed as future work and to be taken as separate work.

Further, one can initiate investigating DDI for extending the DDI as an optimizer, to as parallelizer. Extension of the DDI as a full fledged parallelizer and the empirical comparison of

the DDI based parallelizer with the contemporary parallelizers are the two major works worthful to be considered as future works in the direction of the present paper.

## REFERENCES

- [1] Kavya Alluru, Jeganathan L. Graph based Data Dependence Identifier for Parallelization of Programs. <https://arxiv.org/abs/2102.09317>.
- [2] Michael Wolfe. Parallelizing Compilers. ACM Computing Surveys, Vol.28, No.1, March 1996.
- [3] A.Aho, R.Sethi, and J.Ullman. Compilers: Principles, Techniques, and Tools. Addison-Wesley.
- [4] M.W. Hall, J.M. Anderson, S.P. Amarasinghe, B.R. Murphy, Shih-Wei Liao, E. Bugnion, M.S Lam. Maximizing multiprocessor performance with the SUIF compiler. Computer, Volume 29, Issue 12, 1996.
- [5] <https://suif.stanford.edu/>
- [6] Robert R Wilson, Robert S. French, Christopher S. Wilson, Saman R Amarasinghe, Jennifer M. Anderson, Steve W. K. Tjiang, Shih-Wei Liao, Chau-Wen Tseng, Mary W. Hall, Monica S. Lain, and John L. Hennessy. SUIF: An Infrastructure for Research on Parallelizing and Optimizing Compilers. ACM SIGPLAN Notices, Volume 29, No. 12, December 1994.
- [7] Uptal Banerjee, Rudolf Eigenmann, Alexandru Nicolau, and David A.Padua. Automatic Program Parallelization. Proceedings of the IEEE, Volume 81, Issue 2, Feb 1993.
- [8] W. Blume, R. Eigenmann. The range test: a dependence test for symbolic, non-linear expressions. Proceedings of the 1994 ACM/IEEE Conference on Supercomputing.
- [9] Chirag Dave, Hansang Bae, Seung-Jai Min, Seyong Lee, Rudolf Eigenmann, Samuel Midkiff. Cetus: A Source-to-Source Compiler Infrastructure for Multicores. Computer, Volume 42, Issue 12, 2009.
- [10] <http://pluto-compiler.sourceforge.net/>
- [11] Bondhugula, A. Hartono, J. Ramanujam, and P. Sadayappan. A Practical and Automatic Polyhedral Program Optimization System. Proc. ACM SIGPLAN 2008 Conference on Programming Language Design and Implementation (PLDI 08), Tucson, June 2008.
- [12] Aravind Acharya and Uay Bondhugula. Effective Loop Fusion in Polyhedral Compilation Using Fusion Conflict Graphs. ACM Transactions on Architecture and Code Optimization, Vol. 17, No. 4, Article 26, September 2020.
- [13] Nathanaël Courant, Xavier Leroy. Verified Code Generation for the Polyhedral Model. Proceeding of the ACM on Programming Languages, ACM, 2021, 5 (POPL), pp.40:1-40:24.
- [14] D. J. Kuck, R. H. Kuhn, D. A. Padua, B. Leasure, and M. Wolfe. Dependence Graphs and Compiler Optimizations. Proceedings of the 8th ACM SIGPLAN-SIGACT symposium on Principles of programming languages,1981.
- [15] J. Ferrante (IBM), K. J. Ottenstein (Michigan Technological University) and Joe D. Warren (Rice University), 1987. The Program Dependence Graph and Its Use in Optimization.
- [16] <https://software.intel.com/en-us/fortran-compiler-developer-guide-and-reference-automatic-parallelization>, 2019.

# A Novel Deep Learning-based Online Proctoring System using Face Recognition, Eye Blinking, and Object Detection Techniques

Istiaq Ahmad<sup>1</sup>, Fahad AlQurashi<sup>2</sup>, Ehab Abozinadah<sup>3</sup>, Rashid Mehmood<sup>4</sup>

Department of Computer Science, Faculty of Computing and Information Technology<sup>1,2</sup>

Department of Information Systems, Faculty of Computing and Information Technology<sup>3</sup>

High Performance Computing Center<sup>4</sup>

King Abdulaziz University, Jeddah 21589, Saudi Arabia

**Abstract**—Distance and online learning (or e-learning) has become a norm in training and education due to a variety of benefits such as efficiency, flexibility, affordability, and usability. Moreover, the COVID-19 pandemic has made online learning the only option due to its physical isolation requirements. However, monitoring of attendees and students during classes, particularly during exams, is a major challenge for online systems due to the lack of physical presence. There is a need to develop methods and technologies that provide robust instruments to detect unfair, unethical, and illegal behaviour during classes and exams. We propose in this paper a novel online proctoring system that uses deep learning to continually proctor physical places without the need for a physical proctor. The system employs biometric approaches such as face recognition using the HOG (Histogram of Oriented Gradients) face detector and the OpenCV face recognition algorithm. Also, the system incorporates eye blinking detection to detect stationary pictures. Moreover, to enforce fairness during exams, the system is able to detect gadgets including mobile phones, laptops, iPads, and books. The system is implemented as a software system and evaluated using the Fddb and LFW datasets. We achieved up to 97% and 99.3% accuracies for face detection and face recognition, respectively.

**Keywords**—Online learning; online proctor; student authentication; face detection; face recognition; eye blinking detection; object detection; distance learning; e-learning

## I. INTRODUCTION

Most schools and universities provide educational courses and training physically, i.e., requiring the attendance of lectures, entrance examinations, semester exams, and other activities in physical classrooms and spaces. Teaching and learning in physical spaces have many disadvantages such as inflexibility for students, teachers, and other staff, requiring physical spaces with stringent requirements, accessibility-related challenges for the students and staff in terms of space and time, challenges related to human disabilities, higher financial costs, transportation-related challenges and harms to people and environment, and many more. Online teaching and learning have been known to have many advantages including the flexibility and accessibility for people to attend classes from homes, at their convenience both in time and space, lower costs, a much smaller impact on the planet environment, and many more. Indeed, all the disadvantages of in-class teaching mentioned above could be overcome or abated by online learning.

Despite the many benefits of online learning, in-class learning has remained the mainstream choice for teaching and learning. Massive open online courses (MOOCs) that are offered online have motivated many to attend and complete courses and degrees online [1]. Many of the top schools and universities worldwide provide students with online courses as well as certificates upon completion of the courses. However, these MOOCs are mainly used to upskill knowledge rather than replace school and university education. This trend of moving towards MOOCs had been on the rise and is expected to take an increasingly larger share of in-class education.

The COVID-19 pandemic has caused disruption in many spheres of our lives. Physical interaction for education, work, and leisure has been regulated by governments around the world to minimise human infection rates [2]. This situation has forced education and many other physical activities and businesses to move from physical to online spaces [3]. School, university, and other education and training around the world have moved to online learning. However, many challenges are prohibiting its wide adoption by the governments and public. For example, monitoring of attendees and students during classes, particularly during exams, is a major challenge for online systems due to the lack of physical presence. There is a need to develop methods and technologies that provide robust instruments to detect unfair, unethical, and illegal behaviour during classes and exams. Current literature in this respect is limited with most of the software available from commercial entities that provide limited and “non-open” software tools. Many open-source tools and efforts are needed to bring innovation, variety, and richness to this online learning software systems domain.

Artificial intelligence (AI) has revolutionized our world and environments by providing smartness to many of our daily life activities [4], [5], [6], albeit with several challenges [7], [8]. Particularly, machine and deep learning has accelerated innovation in many fields such as education [1], healthcare [9], [10], transportation [11], [12], communication networks [13], disaster management [14], smart cities [15], and many more. With no exception, AI has the capacity to revolutionise online learning and proctoring.

This paper proposes a novel online proctoring system that uses deep learning to continually proctor physical places without the need for the presence of a physical proctor.

The system employs biometric approaches including face recognition using the HOG face detector and the OpenCV face recognition algorithm. Also, the system incorporates an eye blinking detection method to detect stationary pictures. Moreover, to enforce fairness during exams, the system is able to detect gadgets including mobile phones, laptops, iPads, and books. The system is implemented as a software system and evaluated using the Fddb (Face Detection Data Set and Benchmark) and LFW (Labeled Faces in the Wild) datasets.

The rest of the paper is structured as follows. Section II discusses the research related to online proctoring systems. Section III describes the methodology and design of the proposed system. Section IV provides system evaluation. Section V concludes and discusses future work.

## II. LITERATURE REVIEW

An overview of the relevant research is presented in this section. In the online proctoring system, Section II-A analyzes the literature in the academic realm, and Section II-B reviews the literature in the commercial sector.

### A. Academic Research

The online exam is facing immense challenges throughout the exam. Sarrayrih et al. [16] discussed the several challenges presented by the online exam, as well as providing a solution by grouping the hostnames or IPs of clients for a specific location and time, with a biometric solution like face recognition and fingerprints. In [17], a profile-based authentication framework is proposed for the online exam based on different challenging questions, including the favourite questions, personal questions, and an academic question. Fenu et al. [18] proposed a multi bio-metric continuous authentication system including face recognition, voice recognition, touch recognition, mouse, and keystroke in 2018. Selvi et al. [19] designs and implements a firewall security system using different firewall technologies, including Network Address Translation, Demilitarized Zone, and Virtual Protocol Network, which are used for intrusion detection. Wei et al. [20] proposed fingerprint-based solution. Garg et al. [21] proposed a face recognition and detection solution for the secured online exam using deep learning. Another online proctoring system was proposed by Atoum et al. [22], which continuously estimates six components, including voice, phone, text, and active window detection, gaze estimation, and user verification. A fingerprint and eye tracker-based online test management system was proposed by Bawarith et al. [23]. Cheating and not cheating are used as student status to evaluate their proposed methodology.

### B. Commercial Systems

Recently, the online proctoring system has become a challenge for researchers and developers. Due to the coronavirus situation, the demand and challenges for the online proctoring system are enormously increasing day by day. Several industrial companies developed the proctoring system commercially with the paid version. For example, Mettl [24], Proctortrack [25], Proctoredu [26], Proctoru [27], Comprobo [28], and so on.

**Mettl:** Mettl created web-based online proctoring software that divides their system into four major components: candidate authentication using a picture, OTP and ID affirmation, human-based proctoring using real-time recording in the classroom, secure browser-based proctoring using disables the following features: opening new browsers and data transferring media, and AI-based proctoring using facial, mobile phone, candidate distraction, and multiple person detection. To use this software, the examiners have to pay.

**Proctortrack:** Proctortrack built a web-based multi-level proctoring system through four levels of security. Level 1 is called ProctorLock, and it has automated identity verification, including audio, video, and desktop data recording. The real-time video data is available up to 2-3 hours for the proctor. Level 2 is named ProctorAuto, and it includes level 1 features with automated data analysis. Level 3 is called ProctorTrackQA, which is a robust version of level 2. It analyzes the results from level-2 using a manual QA review process. Finally, level 4, called ProctorLive AI, includes AI-based auto proctoring intervention capabilities in cases of suspicious reactions, cheating, or aiding a student. Testing sincerity results are additionally analyzed with AI.

**Proctoredu:** Proctoredu is a web-based online proctoring system which includes features like online supervision and video recording, additional camera, face and voice detection, passport recognition, face bio-metric, focus, and online status tracking, locking a parallel login, content copy protection, screen recording, and determining a second monitor. For PC Chrome and Firefox, all features are available. For Android, Chrome and IOS Safari supported all the features except screen recording and second monitor determination.

**Proctoru:** Proctoru promoted a web-based online proctoring system including live proctor monitoring, flagging, and intervention. Admins can observe the session in real-time and perform AI-based behavior analysis.

**Comprobo:** Comprobo solutions developed an online automated invigilation system on the web-based platform including features such as capturing the user's photographic ID against each assignment and verifying the reference photo, substitution check, restriction of using other applications or browsers, recording the IP address of the device, remote ID verification, biometric monitoring, and recording the full working environment.

Motivated by the challenges in the area of online learning systems, we propose and implement an online proctoring system that provides solutions to mitigate problems including fraud and multiple student attendance, cheating using still images, and unauthorised use of devices during class or exam time.

## III. METHODOLOGY AND DESIGN

### A. The Proposed Framework

The proposed web-based online proctoring system is distributed into two modules. Firstly, the online registration part, and secondly, the online proctoring part. Fig. 1 describes the proposed architecture for the online proctoring system.

1) *Online Registration:* For registering students' faces, we accessed the student's web-camera through HTTPS protocol

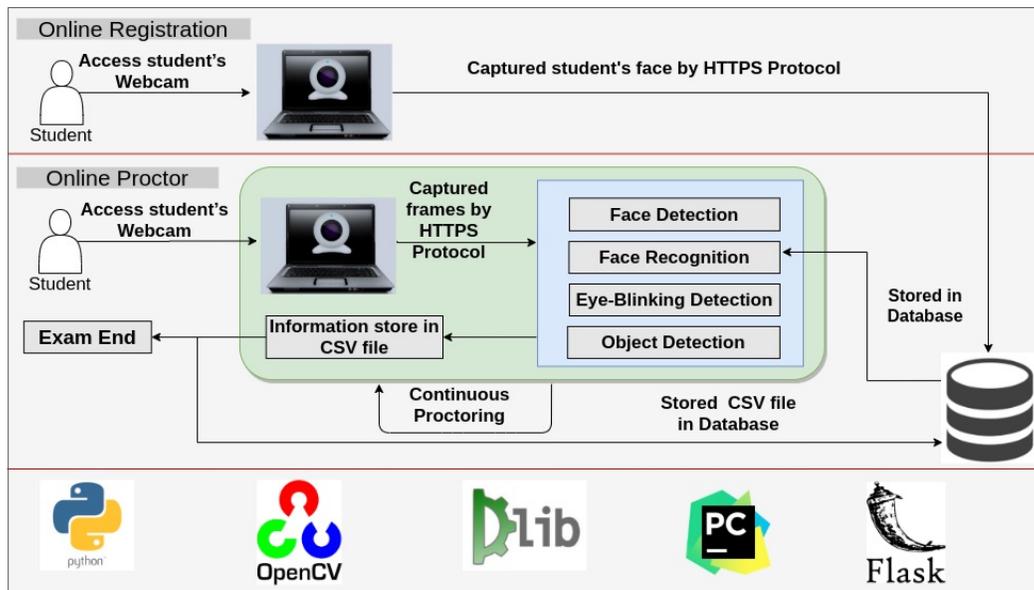


Fig. 1. Proposed Architecture.

during registration and captured the students' faces, storing the face information in the database. We used a flask micro-framework for web development.

The primary challenge in this module was accessing the client-side camera to capture the students' faces. To get around this, we utilized the HTTPS (HyperText Transfer Protocol Secure) protocol to access the students' webcams, which encrypts all conversations between the browser and the server. When using the HTTPS protocol to host a website, SSL certificates are also required. We used a self-signed SSL certificate to run the server.

2) *Online Proctoring*: During online exam sessions, there are some challenges to conducting the exam. Challenges are:

- An unauthorized student may participate in the exam.
- Multiple students may participate together for the exam.
- The student may use his still picture for face recognition.
- The student may use a device such as a mobile, laptop, or iPad to run a video for face recognition.
- The student may use books during the exam.

Our main goal is to mitigate those challenges. In the online proctoring module, we use biometric methods like face detection and recognition with eye-blinking detection. The suggested system's algorithm is detailed in Algorithm 1. In the face-recognition part, we detect and recognize students' faces and detect multiple faces in front of the camera. There is a chance that students can use their still pictures in front of the web-camera. As a result, the face-recognition algorithm recognizes the student as a real face. To avoid the recognition of still pictures, we use eye-blinking methods. If the number of eye-blinking is not more than 30, then we can confirm that the picture in front of the camera is still. There is another possibility that students can hold a device in front of the

web camera by playing his face video. In this case, face recognition and eye-blinking algorithms will detect the image as real and authenticate. So, we use object detection methods like YOLOv3, which also serve to prevent cheating in the exam using devices. We also detected the book using the same YOLOv3 model as the fare and secure exam.

**Algorithm 1** Master Algorithm

```

1: procedure onlineProctor
2:   while True do
3:     frame ← captureFrameFromWebCamera
4:     faceDetect ← faceDetection(method = "HOG")
5:     faceCount ← detectFaceCountForCurrentFrame
6:     if faceCount == 0 then
7:       Exam cancel: no face found
8:     else if facecount == 1 then
9:       Exam continue
10:    else if facecount > 1 then
11:      Exam cancel: multiple face found
12:    end if
13:    faceMatch ← faceRecognition()
14:    if faceMatch == False then
15:      Exam cancel: Unauthorized face found
16:    end if
17:    blinkingRatio ← eyeBlinkingDetection()
18:    if blinkingRatio > 4.5 then
19:      noBlinking ← noBlinking + 1
20:    end if
21:    if noBlinking > 30 then
22:      Exam cancel: still image found
23:    end if
24:    object ← objectDetection()
25:    if object == list of target objects then
26:      Exam cancel: object found
27:    end if
28:  end while
29: end procedure

```

## B. Datasets

We have used FDDB data sets for face detection which contain 5171 face annotation from 2845 images collected from Faces in the wild data sets. We divide the data sets into two parts, including faces and without faces, and implement face detection algorithms to evaluate our proposed system. The resolution of each image in the data set is 86 x 86 pixels. To evaluate face recognition algorithms, we used LFW dataset which contain 5749 people's 13233 images, where 1680 people's had two or more images. As our face recognition algorithm needs a single image for face recognition, we divided the data sets into ten sections based on the number of images available of the people in each data set. In the data set, every 3180 people have one image, every 775 and 290 people have two and three images consecutively, and so on. Each of the image resolutions is 250 x 250 pixels.

## C. Face Detection

In our proposed system, we used the HOG (Histograms of Oriented Gradients) method to detect the faces that were proposed by Navneet and Dalal [29]. In the initial stage of face detection, we convert our input image into grayscale because we don't need an RGB image to find faces. After that, we process every single pixel and the directly surrounding pixels of the image at a moment. We would like to determine the darkness of the current pixel is in contrast to the pixels around it. To show in which direction the image is becoming darker, we draw an arrow. If we replicate such a method for each and every pixel in the image, then we discover that every pixel is followed by an arrow. Gradients are the arrows, which determine the overall image's movement from brightness to darkness. Following that, we can see the image's fundamental pattern. To conduct the function, we divided all of the images into 16x16 pixel squares. Then we count gradient points in each major direction of each square and replace the square image with the strongest single gradient direction. The process's output will convert the original picture into the face's fundamental structure, which seems to be the most similar to the HOG pattern derived from training images. We used the HOG frontal face detector using dlib and the OpenCV library for face detection.

## D. Face Recognition

Face recognition is the most popular biometric solution for the online authentication system. OpenCV is a famous computer vision library that was started by Intel in 1999. OpenCV implements three face recognition algorithms, including Eigenface, Fisherface, and LBPH (Local Binary Patterns Histograms) face recognition. To detect faces, these algorithms employ the Haar cascade classifier technique, introduced by Paul and Michael [30].

In our proposed methodology, we snap a picture of a student as input and use HOG techniques to recognize faces in the image. Then, for the identified picture, estimate the 68 landmarks. Faces that are oriented differently and seem differently to a computer may all belong to the same person, and these signs can be used to easily identify them. Finally, the identified photos are directly compared to previously learnt and saved faces in our database. The pseudo code for facial recognition is shown in the Algorithm 2.

We match a known face from our database to unknown faces using a deep neural network. We train a classifier to determine which known student is the closest match based on measures from a new test image. The classifier's output would be the name of a student. The number of faces in the photograph is also counted.

---

### Algorithm 2 Face Recognition

---

```
1: procedure Face Recognition (studentId, studentName)
2:   while True do
3:     Grab current frame from student's Webcam
4:     frame ← currentFrame
5:     faceLocations ← get all faces on frame
6:     faceEncoding ← get all faceEncodings on frame
7:     faceMatch ← compare studentFace with all faces
8:     if faceMatch == True then
9:       Face Recognized
10:    else
11:      Face Unrecognized
12:    end if
13:  end while
14: end procedure
```

---

1) *Facial Landmark Estimation*: To a computer, the split faces rotated in various orientations appear to be different. To address this issue, we apply the face landmark estimation algorithm [31], which aids in the localization and representation of important facial features including the right and left eye, nose, jawline, mouth, and right and left eyebrow. The HELEN dataset is being utilized to find 194 landmarks on the face from a single image in a millisecond using this approach, which gives an ensemble of randomized regression trees. The method below can help determine whether two faces facing different directions and appearing differently from a computer's perspective are actually the same person.

Based on the fundamental concept of 68 distinct places on an image, we will train the system to recognize any 68 specific landmarks from the target image. We can center the eyes and lips no matter how the faces are rotated after using this method. The landmark boundary of the face is shown in Fig. 3(a), and the face landmark with 64 points is shown in Fig. 3(b).

2) *Encode the Faces*: The most basic concept in facial recognition is matching a recognized face to an unknown one. We identify a previously tagged face that appears to be frighteningly similar to an unknown face as belonging to the same individual. If there are thousands of students, it will take a long time to recognize everyone. As a result, we will need a technique for extracting a few basic measures from each face so that we can measure our unknown face and find the closest known face. We may, for example, measure the distance between the eyes and eyebrows, the length of the nose and mouth, and the size of each ear.

## E. Eye Blinking Detection

To identify a still image, the eye blinking method is utilized. Each eye is represented by 6 (x, y)-coordinates, which begin in the upper left corner and work clockwise around the rest of the area.

---

**Algorithm 3** Eye Blinking Detection

---

```

1: procedure Blinking Detection(studentId, studentName)
2:   eyeModel ← load shape-predictor-68-face-landmarks
3:   while True do
4:     frame ← Grab current frame from Webcam
5:     # get Blinking Ratio
6:     function bRatio( EyePoint, landmark)
7:       leftPoint ← left eye point
8:       rightPoint ← right eye point
9:       centerTop ← center top eye point
10:      centerBottom ← center bottom eye point
11:      horLineLenght ← horizontal line of eye point
12:      verLineLenght ← vertical line of eye point
13:      ratio ← horLineLenght / verLineLenght
14:      return ratio
15:   end function
16:   faces ← dlibFrontalFaceDetector (Frame)
17:   for face ← faces do
18:     # facial landmark (lm)
19:     lm ← eyeModel(grayFrame, faces)
20:     # Left Eye Ratio
21:     ler ← bRatio ([37,38,39,40, 41,42], lm)
22:     # Right Eye Ratio
23:     rer ← bRatio([43,44,45,46, 47,48], lm)
24:     bliningRatio ← (ler + rer)/2
25:   end for
26: end while
27: end procedure

```

---

From Fig. 2 image, we can get the key point to find the relation between height and width.

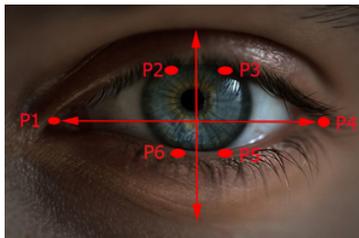


Fig. 2. Eye Blink Detection Landmarks.

In 2016, soukuter and cechj[32] proposed a method for real-time eye detection using facial landmarks. According to their research, we use an eye aspect ratio (EAR) equation that represents this connection, where 2D facial landmark positions are p1,..., p6. We utilize dlib and OpenCV to create eye blinking detection using facial landmarks and a frontal face detector.

#### F. Object Detection

Object recognition refers to identifying objects from digital images. Object classification can be divided into three tasks: object localization, image classification, and object detection. Object segmentation is the final task for object recognition. R-CNN, YOLO, SSD, RetinaNet, and ImageNet are popular deep learning-based object recognition models. The improved versions of the R-CNN model are Faster R-CNN, and Fast R-CNN, which are demonstrated and designed

for object recognition, and object localization. The acronym YOLO stands for ‘You Only Look Once’. YOLO model versions are YOLOv2 and YOLOv3 [33].

The R-CNN family of models delivers excellent object identification accuracy, but its processing speed is a key drawback. The processing speed is just 5 frames per second on a GPU, but the YOLO model is significantly quicker than R-CNN since a single-layer neural network is applied to the entire image. The YOLOv3 model is 100 times quicker than fast R-CNN, and 1000 times quicker than R-CNN. For training, the YOLO model is linked to a single neural network. It takes pictures and divides them into a grid of cells, with the cells anticipating bounding boxes and class labels. The predicted accuracy rate for this model is lower. ‘YOLO9000: better, faster, stronger’ is how YOLOv2 is known. This model can predict 9000 object classes after being trained on two object identification datasets in parallel. The model is trained using high-resolution input pictures and batch normalization. Darknet-19, a proprietary deep architecture with a 19-layer neural network augmented with an additional 11 layers to identify the objects, was utilized by YOLOv2. YOLOv2’s 30-layer design made it difficult to detect tiny objects, but it’s primarily utilized in real-time object identification when precision isn’t required.

YOLOv3 is better than YOLOv2 in terms of speed and strength. It implements the darknet-53 proprietary deep architecture, which includes a 53 network and additional layers for object identification trained on ImageNet. As a result, it has a fully convolutional underlying architecture with 106 layers. The YOLOv3 model was employed in our suggested approach. This model was trained on pictures from the COCO dataset with different sizes: 608 x 608 (less speed, high accuracy), 416 x 416 (moderate speed, moderate accuracy), and 320 x 320 (high speed, low accuracy), and includes 80 labels such as laptop, mobile phone, and book.

---

**Algorithm 4** Object Detection Algorithm

---

```

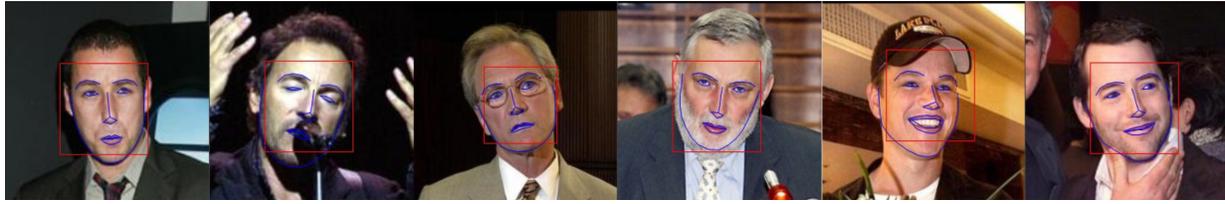
1: procedure ObjectDetection (studentId, studentName)
2:   while True do
3:     Grab current frame from student’s Webcam
4:     frame ← currentFrame
5:     height, width, channels ← frame.shape
6:     blob ← blobFromImage(frame, scale)
7:     set the blob in network as input
8:     outputs ← forward pass to get Outputlayer
9:     for out ← outputs do
10:      for detection ← output do
11:        #scan outputs to get max confidence score
12:        confidence ← max scores
13:        if confidence > 0.7 then
14:          Object detected
15:        end if
16:      end for
17:    end for
18:  end while
19: end procedure

```

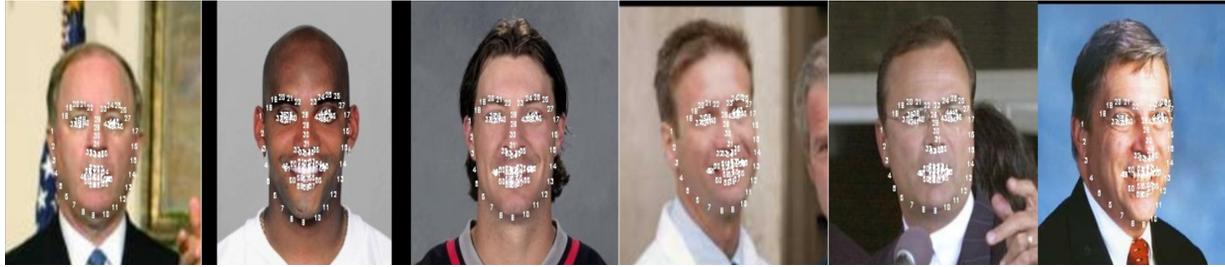
---

## IV. SYSTEM EVALUATION

To implement our proposed system, we use OpenCV for image processing, the dlib package for machine learning and



(a) Face landmark boundary



(b) Face landmark with 64 points

Fig. 3. Facial Landmarks.

Python, etc. We continuously proctor the exam system and concurrently implement each of the methods. Several experiments have been carried out to determine its efficiency, and the results are presented below.

We used the confusion matrix, which is a technique for summarizing the performance of a classification algorithm. There are some key terms for evaluating the confusion matrix, including TP, TN, FP, FN, accuracy, precision, recall, etc.

**True Positive (TP):** The number of positive samples that are accurately labelled.

**True Negative (TN):** The number of negative samples that are accurately labelled.

**False Positive (FP):** The number of negative samples that are mislabelled as positive.

**False Negative (FN):** The number of positive samples that are mislabelled as negative.

**Accuracy:** The percentage of classes are properly anticipated across all classes.

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100$$

**Precision:** The percentage of positive classes that are accurately predicted and truly positive.

$$Precision = \frac{TP}{TP + FP} \times 100$$

**Recall:** The percentage of classes are properly anticipated across all positive classes.

$$Recall = \frac{TP}{TP + FN} \times 100$$

### A. Face Detection

The face detection results are shown in Fig. 4 and 5. We have used the “HOG” method for face detection. In our test image dataset, we have a total of 4305 images with faces from the Fddb dataset. After implementing the face detection method, we got 97.21% accuracy, 100% precision, 97.18% recall, and 98.57% F1-score. Additionally, we obtained 4141, 0, 44, and 120 TP, FP, TN, and FN from the confusion matrix, correspondingly.

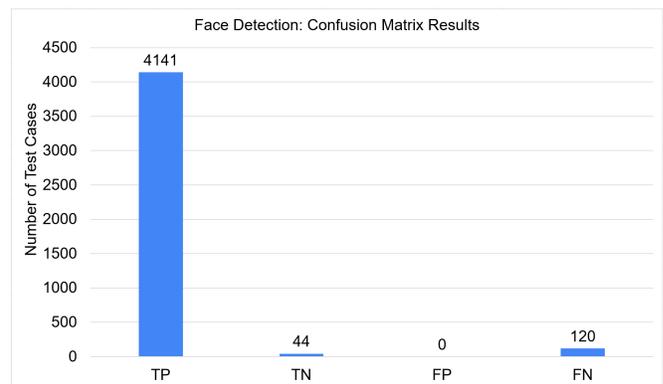


Fig. 4. Face Detection Result (TP, TN, FP, FN).

### B. Face Recognition

The experimental result for face recognition is shown in Table I, and II. We used the LFW face dataset to experiment with the results of the face recognition algorithm. In our proposed system, we need a single image per person for the proposed algorithm. So, we use one image per person in the training image, whereas in the test image set, we use the corresponding person images in identical or different backgrounds or poses, as well as unknown person mages. Table I shows the confusion matrix number of correctly and

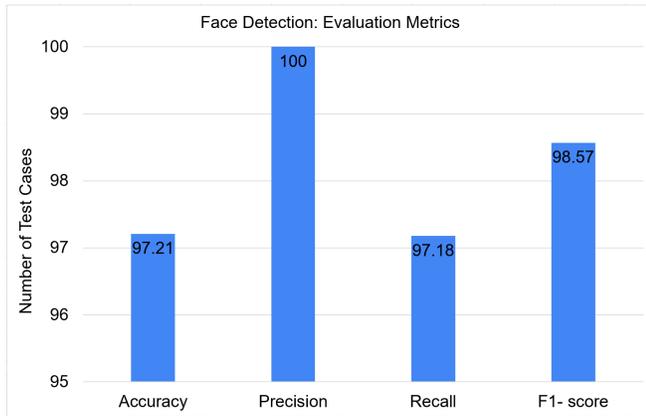


Fig. 5. Face Detection Results (Accuracy, Precision, Recall, F1-Score).

incorrectly predicted images for several users and test images using TP, TN, FP, and FN. We achieved reasonable results with the proposed algorithm.

TABLE I. FACE RECOGNITION RESULT (TP, TN, FP, AND FN)

No. of Users	No. of Test Cases	TP	TN	FP	FN
3810	5256	3808	0	1410	38
143	3897	3824	0	52	21
775	1431	1401	0	28	2
290	808	779	0	24	5
187	695	675	0	11	9
112	525	508	0	12	5
55	304	298	0	3	3
39	253	249	0	2	2
33	247	245	0	2	0
26	221	212	0	7	2
15	144	143	0	1	0

We perceive from Table II that the accuracy of the algorithm is almost near to 99% for around 1000 people, but if the number of people is increased, then the accuracy decreases slowly. For example, if we train 15 to 775 people’s faces, then the accuracy is near to 99% and for 143 people’s faces, we used a large image set for testing where we achieved a better accuracy of about 98%. For training 3810 people’s faces, we got a low accuracy result of about 72%. Based on the aforementioned findings, we may conclude that the suggested algorithm performs significantly better with a smaller number of students.

TABLE II. FACE RECOGNITION RESULTS

No. of Users	No. of Test Cases	Accuracy	Precision	Recall	F1 Score	Time (S)
3810	5256	72.45	72.98	99.01	84.02	2373.03
143	3897	98.12	98.66	99.45	99.05	1096.74
775	1431	97.90	98.04	99.86	98.94	587.42
290	808	96.41	97.01	99.36	98.17	304.15
187	695	97.12	98.39	98.68	98.54	268.46
112	525	96.76	97.69	99.02	98.35	173.27
55	304	98.03	99.00	99.00	99.00	97.44
39	253	98.42	99.20	99.20	99.20	76.49
33	247	99.19	99.19	100.0	99.59	83.38
26	221	95.93	96.80	99.07	97.92	67.48
15	144	99.30	99.30	100.0	99.65	41.06

### C. Object Detection

As we mentioned earlier, we implemented the Yolov3 object detection model for our proposed system that was proposed by Joseph and Ali [33], and the model was assessed on the COCO dataset. They compared YOLOv3 with RetinaNet and found that YOLOv3 has a similar mean average precision (mAP) with a considerably quicker inference time. For example, YOLOv3-608 achieved 57.9% mAP in 51 milliseconds, while RetinaNet-101-800 achieved 57.5% mAP in 198 milliseconds, a 3.8 milliseconds faster.

## V. CONCLUSION AND FUTURE WORK

Face recognition and object identification techniques are utilized in this study to give comprehensive knowledge for online tests. Our proposed method will aid in reducing inequity during the online exam. Human-induced detection is very important when conducting an online proctoring system, as it will aid in detecting students’ suspicious behavior throughout the test. We do not incorporate human activity detection in our suggested model, instead of relying on a single biometric solution and object recognition approaches for the online proctoring system.

In the future, we hope to apply and investigate various human behaviors such as gazing out the window, conversing with people, focusing on other directions, moving about, and so on. We only utilize the YOLOv3 model because of its quicker object detection algorithms, although there are several other object detection approaches available. In the next study, we will focus on such approaches and compare them to our current suggested system.

We have evaluated our proposed system using two datasets. However, the system has not been tested in a real-life deployment with a large number of users. Future work will look into further testing and development of the system in real-life environments. The current proctoring systems are commercial and their designs and sources are not available openly. This work is an effort to develop open systems so the community can learn from each other leading to faster innovations in the field under open-source developments.

### ACKNOWLEDGMENT

The work reported in this paper is supported by the High Performance Computing Centre at King Abdulaziz University, Saudi Arabia. The experiments reported in this paper were performed on the Aziz supercomputer at King Abdulaziz University.

### REFERENCES

- [1] R. Mehmood, F. Alam, N. N. Albogami, I. Katib, A. Albeshri, and S. M. Altowaijri, “UTiLearn: A Personalised Ubiquitous Teaching and Learning System for Smart Societies,” *IEEE Access*, vol. 5, pp. 2615–2635, 2017.
- [2] E. Alomari, I. Katib, A. Albeshri, and R. Mehmood, “COVID-19: Detecting Government Pandemic Measures and Public Concerns from Twitter Arabic Data Using Distributed Machine Learning,” *International Journal of Environmental Research and Public Health*, vol. 18, no. 1, p. 282, jan 2021. [Online]. Available: <https://www.mdpi.com/1660-4601/18/1/282>

- [3] F. Alam, A. Almaghthawi, I. Katib, A. Albeshri, and R. Mehmood, "iResponse: An AI and IoT-Enabled Framework for Autonomous COVID-19 Pandemic Management," *Sustainability*, vol. 13, no. 7, p. 3797, mar 2021. [Online]. Available: <https://www.mdpi.com/2071-1050/13/7/3797>
- [4] T. Yigitcanlar, N. Kankanamge, M. Regona, A. Maldonado, B. Rowan, A. Ryu, K. C. Desouza, J. M. Corchado, R. Mehmood, and R. Y. M. Li, "Artificial Intelligence Technologies and Related Urban Planning and Development Concepts: How Are They Perceived and Utilized in Australia?" *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 6, no. 4, p. 187, dec 2020. [Online]. Available: <https://www.mdpi.com/2199-8531/6/4/187>
- [5] T. Yigitcanlar, L. Butler, E. Windle, K. C. Desouza, R. Mehmood, and J. M. Corchado, "Can Building "Artificially Intelligent Cities" Safeguard Humanity from Natural Disasters, Pandemics, and Other Catastrophes? An Urban Scholar's Perspective," *Sensors*, vol. 20, no. 10, p. 2988, may 2020. [Online]. Available: <https://www.mdpi.com/1424-8220/20/10/2988>
- [6] N. Janbi, I. Katib, A. Albeshri, and R. Mehmood, "Distributed Artificial Intelligence-as-a-Service (DAIaaS) for Smarter IoE and 6G Environments," *Sensors*, vol. 20, no. 20, p. 5796, oct 2020. [Online]. Available: <https://www.mdpi.com/1424-8220/20/20/5796>
- [7] T. Yigitcanlar, J. M. Corchado, R. Mehmood, R. Y. M. Li, K. Mossberger, and K. Desouza, "Responsible Urban Innovation with Local Government Artificial Intelligence (AI): A Conceptual Framework and Research Agenda," *Journal of Open Innovation: Technology, Market, and Complexity*, vol. 7, no. 1, p. 71, feb 2021. [Online]. Available: <https://www.mdpi.com/2199-8531/7/1/71>
- [8] T. Yigitcanlar, R. Mehmood, and J. M. Corchado, "Green Artificial Intelligence: Towards an Efficient, Sustainable and Equitable Technology for Smart Cities and Futures," *Sustainability 2021*, Vol. 13, Page 8952, vol. 13, no. 16, p. 8952, aug 2021. [Online]. Available: <https://www.mdpi.com/2071-1050/13/16/8952>
- [9] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, "UbeHealth: A personalized ubiquitous cloud and edge-enabled networked healthcare system for smart cities," *IEEE Access*, vol. 6, pp. 32 258–32 285, 2018.
- [10] S. Alotaibi, R. Mehmood, I. Katib, O. Rana, and A. Albeshri, "Sehaa: A Big Data Analytics Tool for Healthcare Symptoms and Diseases Detection Using Twitter, Apache Spark, and Machine Learning," *Applied Sciences*, vol. 10, no. 4, p. 1398, feb 2020. [Online]. Available: <https://www.mdpi.com/2076-3417/10/4/1398>
- [11] E. Alomari, R. Mehmood, and I. Katib, "Road Traffic Event Detection Using Twitter Data, Machine Learning, and Apache Spark," in *2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovation (SmartWorld/SCALCOM/UIC/ATC/CBDCOM/IOP/SCI)*. Leicester, UK: IEEE, aug 2019, pp. 1888–1895. [Online]. Available: <https://ieeexplore.ieee.org/document/9060213/>
- [12] M. Aqib, R. Mehmood, A. Alzahrani, I. Katib, A. Albeshri, and S. Altowajri, "Smarter traffic prediction using big data, in-memory computing, deep learning and gpus," *Sensors (Switzerland)*, vol. 19, no. 9, 2019.
- [13] T. Mohammed, A. Albeshri, I. Katib, and R. Mehmood, "UbiPriSEQ—Deep reinforcement learning to manage privacy, security, energy, and QoS in 5G IoT hetnets," *Applied Sciences (Switzerland)*, vol. 10, no. 20, 2020.
- [14] M. Aqib, R. Mehmood, A. Albeshri, and A. Alzahrani, "Disaster management in smart cities by forecasting traffic plan using deep learning and GPUs," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNCS*, vol. 224. Springer, Cham, nov 2018, pp. 139–154. [Online]. Available: [http://link.springer.com/10.1007/978-3-319-94180-6\\_15](http://link.springer.com/10.1007/978-3-319-94180-6_15)
- [15] R. Mehmood, S. See, I. Katib, and I. Chlamtac, *Smart Infrastructure and Applications: foundations for smarter cities and societies*, R. Mehmood, S. See, I. Katib, and I. Chlamtac, Eds. Springer International Publishing, Springer Nature Switzerland AG, 2020.
- [16] M. A. Sarayrih and M. Ilyas, "Challenges of online exam, performances and problems for online university exam," *International Journal of Computer Science Issues (IJCSI)*, vol. 10, no. 1, p. 439, 2013.
- [17] A. Ullah, H. Xiao, M. Lilley, and T. Barker, "Privacy and usability of image and text based challenge questions authentication in online examination," in *2014 International Conference on Education Technologies and Computers (ICETC)*. IEEE, 2014, pp. 24–29.
- [18] G. Fenu, M. Marras, and L. Boratto, "A multi-biometric system for continuous student authentication in e-learning platforms," *Pattern Recognition Letters*, vol. 113, pp. 83–92, 2018.
- [19] V. Selvi, R. Sankar, and R. Umarani, "The design and implementation of on-line examination using firewall security," *IOSR Journal of Computer Engineering*, vol. 16, no. 6, pp. 20–24, 2014.
- [20] L. Wei, Z. Cong, and Y. Zhiwei, "Fingerprint based identity authentication for online examination system," in *2010 Second International Workshop on Education Technology and Computer Science*, vol. 3. IEEE, 2010, pp. 307–310.
- [21] K. Garg, K. Verma, K. Patidar, and N. Tejra, "Convolutional neural network based virtual exam controller," in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*. IEEE, 2020, pp. 895–899.
- [22] Y. Atoum, L. Chen, A. X. Liu, S. D. Hsu, and X. Liu, "Automated online exam proctoring," *IEEE Transactions on Multimedia*, vol. 19, no. 7, pp. 1609–1624, 2017.
- [23] R. Bawarith, D. Abdullah, D. Anas, and P. Dr., "E-exam Cheating Detection System," *International Journal of Advanced Computer Science and Applications*, vol. 8, no. 4, pp. 176–181, 2017.
- [24] Mettl. "Conduct secure online exams with our examination systems," [https://mettl.com/en/computer-based-tests/online-exam-software?utm\\_source=www.google.com&utm\\_medium=website&](https://mettl.com/en/computer-based-tests/online-exam-software?utm_source=www.google.com&utm_medium=website&), accessed October 04, 2020.
- [25] Proctortrack, "Proctortrack leverages automation and live online remote proctoring using ai to deliver innovation, quality and price leadership at scale." <https://www.proctortrack.com/>, accessed October 04, 2020.
- [26] Proctoredu, "Conduct credible online tests anywhere, anytime." <https://www.proctoredu.com/>, accessed October 04, 2020.
- [27] Proctoru, "Protect any online exam," <https://www.proctoru.com/>, accessed October 04, 2020.
- [28] Comprobo, "Online automated invigilation or proctoring," <https://comprobo.co.uk>, accessed October 04, 2020.
- [29] N. Dalal and B. Triggs, "Histograms of oriented gradients for human detection," in *2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05)*, vol. 1. IEEE, 2005, pp. 886–893.
- [30] P. Viola and M. Jones, "Rapid object detection using a boosted cascade of simple features," in *Proceedings of the 2001 IEEE computer society conference on computer vision and pattern recognition. CVPR 2001*, vol. 1. IEEE, 2001, pp. 1–I.
- [31] V. Kazemi and J. Sullivan, "One millisecond face alignment with an ensemble of regression trees," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2014, pp. 1867–1874.
- [32] T. Soukupová and J. Cech, "Eye blink detection using facial landmarks," in *21st computer vision winter workshop, Rimske Toplice, Slovenia*, 2016.
- [33] J. Redmon and A. Farhadi, "Yolov3: An incremental improvement. arxiv 2018," *arXiv preprint arXiv:1804.02767*, pp. 1–6, 2018.

# Faculty e-Learning Adoption During the COVID-19 Pandemic: A Case Study of Shaqra University

Asma Hassan Alshehri<sup>1</sup>

Durma College of Science and Humanities  
Shaqra University, Shaqra 11961, Saudi Arabia

Saad Ali Alahmari<sup>2</sup>

Department of Computer Science  
Shaqra University, Saudi Arabia

**Abstract**—e-Learning can generally be applied by employing learning management system (LMS) platforms designed to support an instructor to develop, manage, and provide online courses to learners. During the COVID-19 pandemic, several LMS platforms were adopted in Saudi Arabian institutions, such as Moodle and Blackboard. However, in order to adopt e-learning and operate LMS platforms, there is a need to investigate factors that influence the capability of faculty to utilize e-learning and its perceived benefits on students. This paper examines how training support and LMS readiness factors influence the capability of faculty to adopt e-learning and student perceived benefits. A quantitative research method was conducted using an online questionnaire survey method. Research data was collected from 274 faculty members, who used Moodle as a main LMS platform, at Shaqra University in the Kingdom of Saudi Arabia (KSA). The results reveal that training support and LMS readiness have a positive influence on the faculty's capability to adopt e-learning, which leads to enhancing students' perceived benefits. By identifying the factors that influence e-learning adoption, universities can provide enhanced e-learning services to students and support faculty through providing adequate training and powerful e-learning platform.

**Keywords**—e-Learning; Learning Management System (LMS); distance learning; LMS readiness; training

## I. INTRODUCTION

The COVID-19 pandemic has affected education worldwide [1]. Universities have adopted e-learning as an alternative to conventional ways of learning as its relevance have never been as significant as during this pandemic. E-learning can generally be implemented by using a learning management system (LMS), which is a web platform to manage all online e-learning processes and course materials for students and faculty [2]. Most of the Saudi universities provide Blackboard LMS for their teaching and learning activities [3], [4], while several other Saudi universities, such as Shaqra University, use open source LMS like Moodle platform.

Given LMS' enormous benefits in education during the COVID-19 pandemic, many researchers have examined the adoption of e-learning systems and investigated the key factors that can increase its adoption at their institutions. These studies focus on varied e-learning perspectives such as student adoption's evaluation. Reference [5] explores a small interpretive case study that finds students realistic and social perceptions. That have impacted positively by habitual activities. It recommends that faculty should engage informal social platforms such as Facebook and WhatsApp in e-learning approaches. Meanwhile, Reference [6] evaluates the student academic performance using organizational aspects and finds

that there are positive relationships between organizational aspects and student's performance during the emergent remote teaching. Reference [7] propose a new adoption framework for e-learning, grouping various characteristics from information system success and diffusion of innovation (DOI). Applying the framework on students' data results in a significant relationship of these characteristics with e-learning adoption. Reference [8] examines four factors from the perspective of students such as ease of use and technical usage of LMS in order to investigate the student's behavior toward using the LMS.

To reach success factors that can affect the e-learning activities, various approaches were used. Theoretical frameworks can be used to analyze the challenges facing e-learning adoption. For example, unified theory of acceptance and use of technology (UTAUT) and diffusion of innovation theory (DOI) are employed to rationalize challenges in e-learning activities [9]. Researchers extend the technology acceptance model (TAM) with factors of knowledge sharing and acquisition, building a new model to assess e-learning adoption [10]. Advanced techniques in artificial intelligence (AI) have also been used to examine the significance of selected factors [11]. Nevertheless, there is limited research investigating several factors, e.g. technical support, relevant to increase the faculty productivity of the LMS benefits [12].

In order to adopt e-learning and operate LMS platforms, it is important to realize the user's perspective toward e-learning adoption [13], so faculty members certainly have major roles in the execution of e-learning activities. There is a need to examine factors that influence the capability of faculty to adopt e-learning and its perceived benefits on students. Thus, this study fills the literature gap by investigating the relationship among faculty training support, LMS readiness, the capability of faculty to adopt e-learning, and students' perceived benefits in the context of one university in Saudi Arabia: Shaqra University.

This paper is organized as follows. Section II provides a literature review, Section III describes a research model, Section IV presents the research methodology, Section V shows the research results, Section VI offers a discussion, and, finally, Section VII concludes the paper.

## II. LITERATURE REVIEW

This research reviews four key research areas: training support, readiness of the LMS, capability to adopt e-learning, and students' perceived benefits. These research areas are used

to develop the theoretical base for the research's hypotheses and model in the following subsections.

#### A. Training Support

Training support that is provided by institutions, such as readable guides and training videos, definitely enhance faculty's capability to interact with e-learning tools and apply course design standards. Researchers have found the importance of supporting faculty in teaching online by, for example, providing online education resources and training, especially on ICT skills, e-learning tools, and course design abilities.

Authors in [14] identify the lack of technical support systems as one of the main barriers an instructor may experience. Teo and others [15] also show that the quality and the accessibility of online education resources have shaped the effectiveness of e-learning, which encourage users to adopt and utilize e-learning systems. Furthermore, researchers on [12] found that the more the institution provides support, the higher the confidence and capability of faculty is in using LMS to accomplish their work. March and Lee in [16] find that a university faculty have gained technical knowledge after going through a training program. The LMS capability test, for instance, shows that post-test correct responses have increased nearly 160% than pre-test. Adequate training from institution as well as institutional encouragement and support have been suggested in [17] as a factor to raise faculty motivation towards the use of e-learning systems.

#### B. Readiness of the LMS

The LMS readiness presents the readiness of all aspects that are part of the e-learning environment. There are number of factors might affect the readiness of LMS adoption in various dimensions e.g. technology, user proficiency, motivations, organization support. Factors can be based on behavioral patterns studying multiple constructors of readiness to accept changes, to change beliefs and to resist changing [18]. Successfully preparing the technological requirements of LMS is essential in increasing its adoption [19]. Researchers have discussed the technical factors from different perspectives. A theoretical base based on the technology acceptance model (TAM) in [20], [21], where others from analyzing perceptive such as [19] focusing on the importance of user-support technical. Several characteristics can be considered to measure the quality of readiness software systems, especially in open-source systems such as the LMS Moodle system used for this case study [22]. However, we found that the usability characteristic as defined by [22] covers several important factors such as learnability, operability, accessibility, and user interface. Thus, we tailored our survey specifically to the usability factors that match our requirements.

#### C. Capability to Adopt e-Learning

Many studies discuss how the desire and technical capability of faculty members impact their successful adoption of e-learning. [14] identified faculty resistance to change, lack of time to develop e-courses, lack of e-learning knowledge, and lack of motivation as main barriers in adopting e-learning. Also, the acceptance to change and the adoption of Blackboard platform in [18] is affected by various variable, such as

resistance to change and individual differences. Moreover, [12] identified the ability to use LMS for teaching as LMS self-efficacy. The paper showed that the higher LMS self-efficacy the higher faculty perceived benefits. [23] also reveal that unwillingness, disinterest, and demotivation are main internal challenges that hinder e-learning uptake.

Adopting LMS and e-learning tools has a positive influence on students' perceived benefits and satisfaction. Engaging students with e-learning tools has a positive impact on their performance and score [24], [25]. [26] revealed the positive impact of adopting blogs for learning on students perceived satisfaction. Also, providing students with supported e-learning apps through their own tablet devices found to be useful for students in the learning scenario [27].

The level of development of e-learning in an educational institution helps overcome faculty challenges in adopting e-learning. Al Gamdi and Samarji [28] found that the most-cited barriers in adopting e-learning is the external barriers such as lack of technical support in the university, training on e-learning, institutional policy for e-learning, and Internet access in universities. The author in [29] evaluated e-learning readiness and showed that improvement in the field of e-learning, like arranging workshops and resetting the infrastructure of the organization create a positive attitude towards adopting e-learning.

#### D. Students' Perceived Benefits

1) *Cognitive Skills*: Cognitive skills (CS) is an important concept, which refers to the level of the knowledge a student gains [30]. The level of the gained knowledge indicates the improvement of a student's skills and the effectiveness of the teaching methods used. Researchers have considered a number of factors affecting CN. These factors varied from basic factors e.g. student's learning behaviors [31], students' duties [32] to advance factors, e.g. travel schedule and outing schedule [30]. Current research in the field of CN that studies e-learning adoption shows adequate contributions. However, we believe that there are more CN factors to be investigated. In our research, we focus on four CN factors: student's IT skills, student's self-learning, student's effective communication with faculty, and student's effective communication with classmates.

Relative research has defined the concept of student's IT skills and self-learning under the term self-efficacy, which refers broadly to the efforts and capabilities of a student toward executing and organizing successfully required course tasks [12], [33], [34], [35]. In this research, student's IT skills (SITS) factor refers to the student's technical ability to use the LMS software effectively. The student's self-learning (SSL) factor represents the motivation of the student in using the course 's learning resource' to learn from the faculty's perspective. Effective communication is the volume of two-way electronic communication between one or more parties. Lastly, student's effective communication with faculty (SECF) refers to announcements, audio/video message and comments, online discussions, and e-mail exchanged between students and faculty [36].

There are several studies in the field of exploring students' adoption of e-learning systems. These studies have investigated

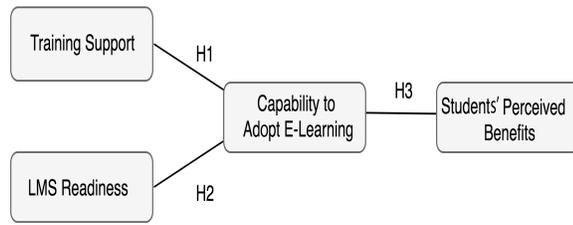


Fig. 1. Research Model.

students' adoption from different perspectives such as knowledge sharing [10], [37], [19] qualitative [19], and quantitative [36], [38]. [10] studies the results of acquisition and sharing of the knowledge on the students' behavioral intention to adopt e-learning systems. It employs the acquisition and sharing of the knowledge as extensions of the technology acceptance model (TAM). The results show that the factors considered on the studies have significant effects on the student's e-learning adoption. [38] focus on studying students' intention to use LMS and the element of attitude strength.

These studies have applied their experiments and surveys on data sets that have been collected from students' feedback. In contrast, in this research, we have evaluated the students based on specific factors collected from faculty's perspective.

2) *Academic Achievements*: The factors that might measure the student academic achievements (SAA) are classified into three domains: traditional, psychological, and students' demographic characteristics [31]. In this research, we define three traditional and two psychological factors: student's remote attendance (SRA), student's completed assignments (SCA), student's grade-average (SGA), student's e-interactions with lectures (SEIL), and student's e-interactions with resources (SEIR). This research has derived these factors as the most frequently used factors in recent literature [39], [40]. Although the traditional factors are numerically accurate, we adopt a scale-base in order to unify measurements.

The SRA presents actual attendance of registered students in a course from the point of view of the faculty at scale base. The SCA is the total of completed assignments in a specific due date for all registered students in a course. The SGA refers to the average final grade achieved by students in a course. The SEIL is the communications among registered students and course's faculty, while the SEIR is registered students' utilization of the online resources of a course.

### III. RESEARCH MODEL

The proposed research model examines the impact of training support and faculty LMS readiness on the capability of faculty to adopt LMS. It also examines students' perceived benefits, as described in Fig. 1.

Training support is defined as the training provided to faculty by organization, which includes technical, instructional, and pedagogical training. Many educational institutions provide various training programs, digital guides, and awareness publications to, for example, support the capability of faculty to deal with e-learning tools, course design, and teaching strategies.

Although LMS is widely considered in institutions, some educational institutions, especially before the COVID-19 pandemic, did not offer enough training programs and instructions on using LMS tools and course design. However, faculty members who utilize e-learning tools depend significantly on the support from technicians in employing different e-learning tools and course design [12], [16]. The faculty's capability to adopt e-learning is defined as the extent to which faculty members believe that they have enough efficiency and intention to adopt e-learning and its technical tools in education. Accordingly, a sufficient training support provided by an organization can better aid the faculty members capability and aspiration to adopt e-learning in education. Thus, the following hypothesis is proposed:

**Hypothesis 1 (H1).** Training support provided by an institution has a positive effect on faculty capability to adopt e-learning.

LMS readiness is defined as the extent to which faculty members believe that the LMS in their institution is sufficiently prepared, accessible, effective, and has a friendly interface to support future use. In other words, the higher quality of LMS in terms of availability, system efficiency, and ease of use is a main motivation for faculty to adopt e-learning. It has been identified that quality of system services have a positive influence on users perceived value, which also has a positive influence on users intention and adoption of e-learning [41]. This study is intended to examine the effect of LMS readiness on the capability of faculty members to adopt e-learning. Thus, the following hypothesis is proposed:

**Hypothesis 2 (H2).** The LMS readiness has a positive effect on faculty capability to adopt e-learning.

Authors in [42] have found that engaging students in the e-learning process with developed e-learning teaching strategies is has a statistically significant impact on students' performance and satisfaction by comparing with traditional learning. Students' perceived benefits is defined as the extent to which a student is expected to benefit from the faculty's capability to apply e-learning regarding academic achievement and cognitive skills. This study is intended to examine the capability of faculty members to adopt e-learning on students' perceived benefits from the point of view of faculty members. Thus, the following hypothesis is proposed:

**Hypothesis 3 (H3).** The faculty capability to adopt e-learning has a positive effect on students' perceived benefits from the point of view of faculty members.

### IV. RESEARCH METHODOLOGY

This paper shows how training support and LMS readiness influence the capability of faculty to adopt e-learning, which influence the students' perceived benefits. This study was carried out to measure the variables and test the hypothesis. The survey structure and its constructs will be presented in Section IV-A, then data collection and the demographic factors of the survey respondents will be discussed in Section IV-B.

TABLE I. RESULTS OF THE DESCRIPTIVE STATISTICS OF ALL ITEMS IN THE CONSTRUCTS (N = 274).

Construct	Item	Mean	Std.Dev
Training Support (TS)	What is your assessment of training support in terms of:		
	- TS1: Your knowledge of accessing it	3.34	1.09
	- TS2: Your Knowledge of it	3.61	1.08
	- TS3: Its Quality	3.37	1.10
	- TS4: Its Diversity	3.38	1.16
LMS Readiness (LMS-R)	How do you evaluate LMS in terms of:		
	- LMS-R1: Accessibility	3.79	1.05
	- LMS-R2: Efficiency	3.85	0.98
	- LMS-R3: Friendly interface	3.62	1.06
	- LMS-R4: Continuous use	3.61	1.02
Capability to adopt e-learning (CA-EL)	How do you rate e-learning in terms of your:		
	- CA-EL1: Satisfaction level	3.53	0.99
	- CA-EL2: Desire to use	3.87	1.08
	- CA-EL3: Technical capability	4.09	0.92
	- CA-EL4: Level of development	3.78	1.05
Students' Perceived Benefits (SPB)	How would you evaluate e-learning in terms of supporting students in the following:		
	- SPB1: Self-learning	3.38	1.04
	- SPB2: Communication with classmates	3.62	1.03
	- SPB3: Communication with faculty	3.68	1.04
	- SPB4: Technical capability	3.18	1.09
	How do you rate students' discipline when applying e-learning in terms of:		
	- SPB5: Commitment to attend	3.70	0.94
	- SPB6: Interaction in lectures	3.14	0.99
	- SPB7: Interaction with e-resources	3.15	1.04
	- SPB8: Completion of assignments	3.66	0.90
- SPB9: Students' grade	3.80	0.91	

### A. Survey Structure

An online questionnaire survey has been prepared and distributed among Shaqra University faculty members. The first part of the survey collected some personal data from the participants, such as their gender, department, and college. The second section of the online survey contains four constructs that are broken down by items and is shown in Table I.

The first construct has four items to assess the level of training support from the university to faculty. The second construct has four items that allow faculty to evaluate LMS readiness. The third structure also contains four components that give the opportunity for faculty members to assess e-learning. Finally, the fourth construct has four items that faculty members answer to assess the extent to which a student is expected to benefit from the faculty's capability to adopt e-learning. The survey consists of a five-point Likert scale with very satisfied (5), satisfied (4), moderately satisfied (3), dissatisfied (2), and very dissatisfied (1).

### B. Data Collection

The questionnaire was administered to faculty members of Shaqra University. First, a cross-sectional online questionnaire was distributed among all faculty members of Shaqra University on January 2021 through their formal emails. Shaqra University has only provided Moodle as the main LMS since the beginning of 2019 and did not provide any other LMS, such as blackboard, before it. The study was conducted on faculty members who completed the online questionnaire also on January 2021. The faculty members officially used Moodle as the main LMS during the first year of the COVID-19 pandemic. They used it to manage virtual classes, discussions, assignments, and exams among others. The Moodle LMS has

been used at Shaqra University limitedly before the COVID-19 pandemic, but the number of users increased remarkably right when the COVID-19 pandemic started. As a result, the questionnaire was distributed after a year of using e-learning in the university. All survey respondents were considered because they were able to finish the questionnaire successfully.

## V. RESULTS

In this section, the frequency of respondents and a descriptive statistics is explained to show if variables are normally distributed and have adequate reliability.

The study collected data from faculty members of Shaqra University. The collected data was analyzed and examined using statistical analysis system (SAS) program. Among 274 faculty members that participated, 151 (55.1%) were males and 123 (44.9%) were females. Table II shows the demographic for respondents based on their professional fields. The table shows that most of the respondents, 98 (35.8%), were from science and engineering fields, and among respondents in these fields, 53 (54.1%) were males and 45 (45.9%) were females.

Table I shows the mean and standard deviation of all constructs' items. Among the four items of the training support assessments, faculty knowledge about training support materials gained the highest mean among assessment items of training support (3.61  $\pm$ 1.08), while the knowledge of how to access materials gained the lowest mean (3.34  $\pm$  1.09). The last three items have very close means. Among items related to LMS readiness, efficiency of LMS Moodle (3.85  $\pm$ 0.98) and accessibility (3.79  $\pm$ 1.05) rated as the most important factors determining LMS readiness, according to faculty members, while the friendly interface (3.62  $\pm$ 1.06) and continues use items(3.61  $\pm$ 1.02) were rated as the lowest

TABLE II. DEMOGRAPHIC DATA OF RESPONDENTS' PROFESSIONAL FIELDS

Fields	Female	Male	Total
Science and Engineering	45 45.9%	53 54.1%	98 35.8%
Humanities	27 48.2%	29 51.8%	56 20.4%
Business Administration	21 38.2%	34 61.8%	55 20.1%
Medicine and Applied Medicine	11 33.3%	22 66.7%	33 12%
Others	19 59.4%	13 40.6%	32 11.7%
Total	123 44.9%	151 55.1%	274 100%

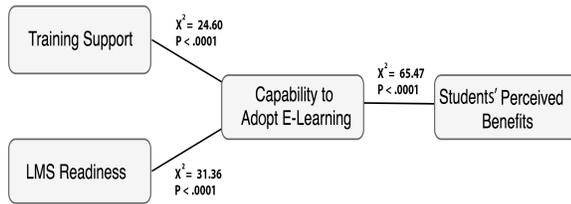


Fig. 2. The Research Model with Significant Results.

factors for LMS readiness. The technical capability item within the faculty capability to adopt e-learning construct was rated as the highest value among all items in the survey (3.09 ±0.92), while satisfaction level is the lowest within the construct (3.53 ±0.99). Finally, the students' grade items of the students' perceived benefits construct had the highest mean value from the faculty's point of view (3.80 ±0.91) in the academic achievement category, while communication with faculty had the highest mean value in the cognitive skills category (3.68 ±1.04).

The results of the descriptive analysis of the four constructs, including the constructs' mean and standard deviation, are shown in Table III. The mean values of the four variables are from 3.42 to 3.82, where the highest value is the mean of the capability to adopt e-learning. Also, the standard deviations of the four variables range from 0.76 to 0.95, where the highest value is the standard deviations of training support. The statistics together indicate that all variables are normally distributed.

The reliability and validity test in Table III reports the values of Cronbach Alpha  $\alpha$  and Pearson's correlation coefficient (Corr). A Cronbach Alpha value of 0.70 or higher suggests that the measurement scale performs consistently when it is tested repeatedly [43]. Thus, the measurement scale is viewed as reliable. The  $\alpha$  value of all four variables ranged from 0.81 and 0.83, implying that their measurement scales have suitable reliability. Pearson correlation showed a positive correlation among all variables[44]. These correlations were separated into strong and moderate correlations. The strong positive correlations were found between training support and LMS readiness and between capability to adopt e-learning and student perceived benefits (> 0.70). While moderate positive correlation was found between all the remaining variables (>0.5).

Table IV showed the result of the study logistic regression analysis, which examined the study hypothesis. First, the logistic regression significantly rejects the first null hypothesis and conclude there was a statistically significant association between an exogenous variable training support and an endogenous variable capability to adopt e-learning ( $\chi^2 = 24.60$  and  $p < .0001$  as shown in Fig. 2). As the score of training support increased by one unit, the odds ratio of faculty capability to adopt e-learning increased by 7.87 (OR = 7.87, 95% CI = 3.36 – 18.42,  $p < 0.0001$ ), supporting hypothesis H1 (Training support provided by institution has a positive effect on faculty capability to adopt e-learning).

Next, the logistic regression significantly rejects the second null hypothesis and concludes that there was a statistically significant association between LMS readiness and the faculty's capability to adopt e-learning ( $\chi^2 = 31.36$  and  $p < .0001$  as shown in Fig. 2). The score for LMS readiness increased by one unit and the odds of faculty's capability to adopt e-learning increased by 11.78 (OR = 11.78, 95% CI = 5.01 – 27.72,  $p < 0.0001$ ), suggesting that hypothesis H2 (The LMS readiness has a positive effect on faculty capability to adopt e-learning) is supported.

Finally, the logistic regression significantly rejects the third null hypothesis and conclude that there was a statistically significant association between an endogenous variable capability to adopt e-learning and another endogenous variable students' perceived benefits ( $\chi^2 = 65.47$  and  $p < .0001$  as shown in Fig. 2). The score for faculty capability to adopt e-learning increased by one unit and the odds of students' perceived benefits increased by 41.61 (OR = 41.61, 95% CI = 13.53 – 127.98,  $p < 0.0001$ ), which supports hypothesis H3 (The faculty capability to adopt e-learning has a positive effect on Students' Perceived Benefits from faculty point of view).

## VI. DISCUSSION

This research examined factors influencing the adoption of e-learning and student perceived benefits from the perspective of faculty members at Shaqra University, Saudi Arabia. By applying simple and multivariate logistic regression analyses, the findings indicate that the proposed research model demonstrates the significance of selected factors on e-learning adoption. The results evidently support positive effects for our hypotheses (H1, H2, and H3).

The study size is similar to comparable studies, but the study sample socio-demographics are slightly different. The proportion of female to male participants was approximately half the proportion of female to male participants in a similar study [12] and different from what was found in earlier Saudi studies [28], [14], [45]. More than third of the participants in our survey were from science and engineering fields, most likely because of their strong e-learning knowledge and ICT background. Also, the fewest respondents in the survey came from the Other category, such as Arabic language sciences and Islamic studies sciences, most likely because of their lack of e-learning knowledge and ICT backgrounds [14], [45], [46].

The findings of this study show a positive association between training support and the faculty's capability to adopt e-learning. Previous studies validated our results by finding that a lack of e-learning knowledge and skills will impact its

TABLE III. DESCRIPTIVE STATISTICS, RELIABILITY, AND DISCRIMINANT VALIDITY TEST (N = 274)

Construct	Mean	Std.Dev	Cronbach's Alpha ( $\alpha$ )	Pearson correlation coefficient (Corr)			
				1	2	3	4
Training Support (TS)	3.42	0.95	0.84	1	0.71565	0.63197	0.54697
LMS Readiness (LMS-R)	3.72	0.92	0.83	0.71565	1	0.60942	0.57849
Capability to Adopt e-learning (CA-EL)	3.82	0.87	0.82	0.63197	0.60942	1	0.70880
Students' Perceived Benefits (SPB)	3.48	0.77	0.81	0.54697	0.57849	0.70880	1

TABLE IV. RESULTS OF RESEARCH MODEL

Independent Variables	P-Value <sup>a</sup>	Odds Ratio (OR)	95% Confidence Interval (CI)
First Hypothesis (Dependent variable = Capability to Adopt E-learning (CA-EL)) <sup>b</sup>			
Training Support (TS)	<0.0001	7.87	3.36 – 18.42
Second Hypothesis (Dependent variable = Capability to Adopt E-learning (CA-EL)) <sup>c</sup>			
LMS Readiness (LMS-R)	<0.0001	11.79	5.01 -27.72
Third Hypothesis (Dependent variable = Students' Perceived Benefits (SPB)) <sup>d</sup>			
Capability to Adopt E-learning (CA-EL)	<0.0001	41.61	13.53-127.98

<sup>a</sup> Significant at  $p < 0.05$

<sup>b</sup> Model  $\chi^2 = 24.60$ ,  $df = 1$ ,  $p < 0.001$

<sup>c</sup> Model  $\chi^2 = 31.36$ ,  $df = 1$ ,  $p < 0.001$

<sup>d</sup> Model  $\chi^2 = 65.47$ ,  $df = 1$ ,  $p < 0.001$

successful implementation in Saudi Arabia, Iraq, and Libya [14], [23], [46]. Shaqra University is an emerging university in Saudi Arabia that had limited training support before the COVID-19 pandemic and intense training support after it. Training support is a necessary factor for all universities regardless of their rank, size, or country. [23], who conducted a survey on four medium-size universities in the United States, found that the higher the organizational support, through training programs, the higher the faculty member's confidence in adopting LMS, which is also emphasizes the importance of the training support factor.

As shown in Table IV, the faculty's capability to adopt e-learning has the strongest association with the e-learning adoption (OR = 41.61) as compared to the association between training support and capability to adopt e-learning (OR = 7.87) and between LMS readiness and capability to adopt e-learning (OR = 11.787). Interestingly, this association is uncertain with a wider interval (13.53-172.98), which might indicate the need to study further the capability to adopt the e-learning factor and consider more sub-factors. Unlike some previous studies, such as [10], [19], [38], this study was conducted in the context of a pandemic, traditional learning was necessarily replaced by e-learning methods. Therefore, it is recommended to reconduct this study in more regular circumstances and compare results to better comprehend e-learning adoption.

It is worth mentioning that Shaqra University is only providing Moodle system, unlike most other Saudi government universities that use officially Blackboard system. As result, the LMS readiness findings could be slightly different if they are applied in other universities that use different LMS platforms, such as Blackboard or Canvas. It is advisable to apply our research model with faculty from different universities who use different LMS platforms. This will help in revealing the suitable LMS platform and e-learning tools that fit e-learning environment. Also, it might consequently change the significant association with other factors such as the capability to adapt e-learning.

## VII. CONCLUSION

In the current study, the proposed research model describes a set of constructors that could impact e-learning adoption from faculty's perspective. The selected constructors are defined from four relevant factors based on the available literature, i.e. training support, readiness of the LMS, capability to Adopt e-learning, and students perceived benefits. These factors basically present the essential dimensions of the e-learning processes.

The findings demonstrate the statistical significance association among the selected constructs in the space problem, supporting our hypotheses. The results reveal the importance of providing the adequate training to faculty and LMS readiness in order to increase e-learning adoption. It confirms that the faculty's capabilities play a major role not only in provoking students' perceived benefits but also in overcoming challenges in LMS readiness. Although faculty members' capabilities were an essential factor that significantly affects all e-learning processes, some statistical uncertainties were found that might affect the reliability of the results. Indeed, the results of this study can be used to increase e-learning adoption specifically in Shaqra University and other universities in the region. For future work, further detailed and reliable analysis, such as sensitive analysis, is required to understand faculty's capabilities.

## VIII. ACKNOWLEDGMENT

The authors are grateful and thankful for Shaqra University for all the support. They would also like to thank all participants in this research for their valuable comments.

## REFERENCES

- [1] Eugene Adu Henaku. Covid-19 online learning experience of college students: The case of Ghana. *International Journal of Multidisciplinary Sciences and Advanced Technology*, 1(2):54–62, 2020.

- [2] Dina Fitri Murad, Yaya Heryadi, Bambang Dwi Wijanarko, Sani Muhamad Isa, and Widodo Budiharto. Recommendation system for smart lms using machine learning: a literature review. In *2018 International Conference on Computing, Engineering, and Design (ICCED)*, pages 113–118. IEEE, 2018.
- [3] Abdulaziz Aldiab, Harun Chowdhury, Alex Kootsookos, Firoz Alam, and Hamed Allhibi. Utilization of learning management systems (lms) in higher education system: A case review for saudi arabia. *Energy Procedia*, 160:731–737, 2019.
- [4] Rayed AlGhamdi and Adel Bahadad. Assessing the usages of lms at kau and proposing force strategy for the diffusion. *arXiv preprint arXiv:1902.00953*, 2019.
- [5] MA Makumane. Students’ perceptions on the use of lms at a lesotho university amidst the covid-19 pandemic. *African Identities*, pages 1–18, 2021.
- [6] Santiago Iglesias-Pradas, Ángel Hernández-García, Julián Chaparro-Peláez, and José Luis Prieto. Emergency remote teaching and students’ academic performance in higher education during the covid-19 pandemic: A case study. *Computers in Human Behavior*, 119:106713, 2021.
- [7] Saleem Issa Al Zoubi and Ahmad Issa Alzoubi. E-learning benchmarking adoption: A case study of sur university college. *E-learning*, 10(11):463–470, 2019.
- [8] Zhumagul Nurakun Kyzy, Rita Ismailova, and Hakan Dündar. Learning management system implementation: a case study in the kyrgyz republic. *Interactive Learning Environments*, 26(8):1010–1022, 2018.
- [9] Bongani T Gamede, Oluwatoyin Ayodele Ajani, and Olufemi Sunday Afolabi. Exploring the adoption and usage of learning management system as alternative for curriculum delivery in south african higher education institutions during covid-19 lockdown. *International Journal of Higher Education*, 11(1), 2022.
- [10] Mostafa Al-Emran and Timothy Teo. Do knowledge acquisition and knowledge sharing really affect e-learning adoption? an empirical study. *Education and Information Technologies*, 25(3):1983–1998, 2020.
- [11] Nadire Cavus, Yakubu Bala Mohammed, and Mohammed Nasiru Yakubu. Determinants of learning management systems during covid-19 pandemic for sustainable education. *Sustainability*, 13(9):5189, 2021.
- [12] Yun Zheng, Jianfeng Wang, William Doll, Xiaodong Deng, and Melvin Williams. The impact of organisational support, technical support, and self-efficacy on faculty perceived benefits of using learning management system. *Behaviour & Information Technology*, 37(4):311–319, 2018.
- [13] Darrell S Walker, James R Lindner, Theresa Pesi Murphrey, and Kim Dooley. Learning management system usage. *Quarterly Review of Distance Education*, 17(2):41–50, 2016.
- [14] Quadri Noorulhasan Naveed, AbulHafeez Muhammed, Sumaya Sanober, Mohamed Rafik N Qureshi, and Asadullah Shah. Barriers effecting successful implementation of e-learning in saudi arabian universities. *International Journal of Emerging Technologies in Learning*, 12(6), 2017.
- [15] Thompson SH Teo, Sojung Lucia Kim, and Li Jiang. E-learning implementation in south korea: Integrating effectiveness and legitimacy perspectives. *Information Systems Frontiers*, 22(2):511–528, 2020.
- [16] Laura March and James Lee. Teaching teachers to teach online: How to implement an evidence-based approach to training faculty. In *Society for Information Technology & Teacher Education International Conference*, pages 714–720. Association for the Advancement of Computing in Education (AACE), 2016.
- [17] Chin Fei Goh, Puong Koh Hii, Owee Kowang Tan, and Amran Rasli. Why do university teachers use e-learning systems? *The International Review of Research in Open and Distributed Learning*, 21(2):136–155, 2020.
- [18] Mohammed Ilyas. Investigating readiness for acceptance of change for the adoption of blackboard lms at prince sattam bin abdulaziz university, saudi arabia. *International Journal of Education and Practice*, 6(4):216–226, 2018.
- [19] Fezile Ozdamli and Nadire Cavus. Knowledge sharing technologies in higher education: Preferences of cis students in cyprus. *Education and Information Technologies*, 26(2):1833–1846, 2021.
- [20] Muyesser Eraslan Yalcin and Birgul Kutlu. Examination of students’ acceptance of and intention to use learning management systems using extended tam. *British Journal of Educational Technology*, 50(5):2414–2432, 2019.
- [21] Shamsul Anuar Mokhtar, Hamidon Katan, and Imdadullah Hidayat-ur Rehman. Instructors’ behavioural intention to use learning management system: an integrated tam perspective. *TEM Journal*, 7(3):513, 2018.
- [22] Mohamed Sarrab and Osama M Hussain Rehman. Empirical study of open source software selection for adoption, based on software quality characteristics. *Advances in Engineering Software*, 69:1–11, 2014.
- [23] Ahmed Al-Azawei, Patrick Parslow, and Karsten Lundqvist. Barriers and opportunities of e-learning implementation in iraq: A case of public universities. *The International Review of Research in Open and Distributed Learning*, 17(5), 2016.
- [24] Mushtaq Hussain, Wenhao Zhu, Wu Zhang, and Syed Muhammad Raza Abidi. Student engagement predictions in an e-learning system and their impact on student course assessment scores. *Computational intelligence and neuroscience*, 2018, 2018.
- [25] Nenagh Kemp. University students’ perceived effort and learning in face-to-face and online classes. *Journal of Applied Learning and Teaching*, 3(1):69–77, 2020.
- [26] Princely Ifinedo. Students’ perceived impact of learning and satisfaction with blogs. *The International Journal of Information and Learning Technology*, 2017.
- [27] Neil P Morris, J Lambe, J Ciccone, and Bronwen Swinnerton. Mobile technology: students perceived benefits of apps for learning neuroanatomy. *Journal of Computer Assisted Learning*, 32(5):430–442, 2016.
- [28] MA Al Gamdi and A Samarji. Perceived barriers towards e-learning by faculty members at a recently established university in saudi arabia. *International Journal of Information and Education Technology*, 6(1):23, 2016.
- [29] Yogita Navani and MA Ansari. Assessing e-learning readiness of university faculty in india. *Advances in Computer Science and Information Technology (ACSIT)*, 4(3):209–214, 2017.
- [30] Sadique Ahmad, Kan Li, Adnan Amin, Muhammad Shahid Anwar, and Wahab Khan. A multilayer prediction approach for the student cognitive skills measurement. *IEEE Access*, 6:57470–57484, 2018.
- [31] Amin Zollanvari, Refik Caglar Kizilirmak, Yau Hee Kho, and Daniel Hernández-Torrano. Predicting students’ gpa and developing intervention strategies based on self-regulatory learning behaviors. *IEEE Access*, 5:23792–23802, 2017.
- [32] Robert V Lindsey, Mohammad Khajah, and Michael C Mozer. Automatic discovery of cognitive skills to improve the prediction of student learning. In *Advances in neural information processing systems*, pages 1386–1394. Citeseer, 2014.
- [33] Demei Shen, Moon-Heum Cho, Chia-Lin Tsai, and Rose Marra. Unpacking online learning experiences: Online learning self-efficacy and learning satisfaction. *The Internet and Higher Education*, 19:10–17, 2013.
- [34] Rezart Prifti. Self-efficacy and student satisfaction in the context of blended learning courses. *Open Learning: The Journal of Open, Distance and e-Learning*, pages 1–15, 2020.
- [35] Emtinan Alqurashi et al. Self-efficacy in online learning environments: A literature review. *Contemporary Issues in Education Research (CIER)*, 9(1):45–52, 2016.
- [36] Hungwei Tseng. An exploratory study of students’ perceptions of learning management system utilisation and learning community. *Research in Learning Technology*, 28, 2020.
- [37] Sharmila Gamlath and Therese Wilson. Dimensions of student-to-student knowledge sharing in universities. *Knowledge Management Research & Practice*, pages 1–15, 2020.
- [38] Nicolae Nistor, Dorin Stanciu, Thomas Lerche, and Ewald Kiel. “i am fine with any technology, as long as it doesn’t make trouble, so that i can concentrate on my study”: A case study of university students’ attitude strength related to educational technology acceptance. *British Journal of Educational Technology*, 50(5):2557–2571, 2019.
- [39] Ritanjali Panigrahi, Praveen Ranjan Srivastava, and Dheeraj Sharma. Online learning: Adoption, continuance, and learning outcome—a review of literature. *International Journal of Information Management*, 43:1–14, 2018.

- [40] Renu Sabharwal, Ritesh Chugh, Md Rahat Hossain, and Marilyn Wells. Learning management systems in the workplace: A literature review. In *2018 IEEE International Conference on Teaching, Assessment, and Learning for Engineering (TALE)*, pages 387–393. IEEE, 2018.
- [41] KM Faqih. Which is more important in e-learning adoption, perceived value or perceived usefulness? examining the moderating influence of perceived compatibility. In *4th Global Summit on Education GSE. Kuala Lumpur. World Conferences*, 2016.
- [42] Nahid Khalil Elfaki, Itedal Abdulraheem, and Rashida Abdulrahim. Impact of e-learning vs traditional learning on student's performance and attitude. *International Journal of Medical Research & Health Sciences*, 8(10):76–82, 2019.
- [43] Keith S Taber. The use of cronbach's alpha when developing and reporting research instruments in science education. *Research in science education*, 48(6):1273–1296, 2018.
- [44] Patrick Schober, Christa Boer, and Lothar A Schwarte. Correlation coefficients: appropriate use and interpretation. *Anesthesia & Analgesia*, 126(5):1763–1768, 2018.
- [45] Muhammad Arshad, Ahmad Almufarreh, Khaled MG Noaman, and Muhammad Noman Saeed. Academic semester activities by learning management system during covid-19 pandemic: A case of jazan university. *International Journal on Emerging Technologies*, 11(5):213–219, 2020.
- [46] Thuraya Kenan, Crinela Pislaru, and Abdussalam Elzawi. Trends and policy issues for the e-learning implementation in libyan universities. *International Journal of Trade, Economics and Finance*, 5(1):105–109, 2014.

# Joint Deep Clustering: Classification and Review

Arwa Alturki, Ouiem Bchir, Mohamed Maher Ben Ismail  
Department of Computer Science  
King Saud University, Riyadh  
Saudi Arabia

**Abstract**—Clustering is a fundamental problem in machine learning. To address this, a large number of algorithms have been developed. Some of these algorithms, such as K-means, handle the original data directly, while others, such as spectral clustering, apply linear transformation to the data. Still others, such as kernel-based algorithms, use nonlinear transformation. Since the performance of the clustering depends strongly on the quality of the data representation, representation learning approaches have been extensively researched. With the recent advances in deep learning, deep neural networks are being increasingly utilized to learn clustering-friendly representation. We provide here a review of existing algorithms that are being used to jointly optimize deep neural networks and clustering methods.

**Keywords**—Clustering; deep learning; deep neural network; representation learning; clustering loss; reconstruction loss

## I. INTRODUCTION

Clustering is a challenging problem in machine learning, as its purpose is to categorize objects into groups according to similarity measures. To achieve this, many clustering algorithms have been published in the literature [1]. These algorithms can be classified into two groups: hierarchical and partitional approaches. In hierarchical clustering, the data are organized into nested clusters that are merged into larger ones or divided into smaller ones. This yields a hierarchy of clusters called a dendrogram. Conversely, partitional clustering is based on the optimization of a specific cost function that allows separation between clusters. The performance of these different clustering algorithms depends on their accurate representation of the data. Hence, data representation learning is a critical step in the clustering process.

Over the past several decades, many traditional representation learning techniques have been proposed. Some of these techniques are designed to learn low-dimensional data representation with linear projections, such as unsupervised principal component analysis (PCA) [2], supervised linear discriminant analysis (LDA) [3], kernel-based PCA [4], and generalized discriminant analysis (GDA) [5]. To discover the intrinsic structure of high-dimensional data, manifold learning algorithms that are based on locality were introduced, such as isometric feature mapping (Isomap) [6] and locally linear embedding (LLE) [7]. In 2006, Hinton et al. [8, 9] introduced the concept of deep learning by utilizing artificial neural networks (ANNs) for dimensionality reduction. Specifically, they introduced a greedy layer-wise pretraining process and a finetuning framework for deep neural network (DNN) learning. The resulting performance was better than that of state-of-the-art algorithms on MNIST [9] handwritten digit recognition and

document retrieval tasks. Following this groundbreaking work, a considerable number of deep representation learning algorithms were developed.

Recently, frameworks that perform deep representation learning and clustering procedures have attracted much attention. These frameworks are referred to as deep clustering algorithms, and they can be divided into (1) separated deep clustering and (2) combined deep clustering methods. In separated deep clustering, the deep representation is learned first, and then fed into a clustering algorithm. However, because these two tasks are optimized separately, the learned representation may not be suitable or sufficient for the clustering. In combined deep clustering, the deep representation learning and clustering are jointly optimized. This implies that the clustering assignments and network parameters are reciprocally affected in every learning iteration. Such an approach yields a representation that is more suitable for clustering. Two approaches to achieve combined optimization exist: the pretraining and finetuning approach, and the joint training approach. In the pretraining and finetuning approach, the DNN is pre-trained with nonclustering loss (network loss) to initialize the network parameters and learn initial representation. Then, the clustering loss is used to train (finetune) the initialized network and output clusters. In contrast, in the joint training approach, the network is trained with a joint loss function that integrates the clustering loss with a nonclustering loss (network loss). In this review, we survey joint deep clustering algorithms by examining different network structures and analyzing the building blocks of these algorithms.

In Section 2, we introduce deep representation learning techniques. In Section 3, we will describe the clustering algorithms that are utilized in joint deep clustering. In Section 4, we provide a survey of the joint deep clustering approaches, and in Section 5, we present the conclusions from the results of this survey.

## II. DEEP REPRESENTATION LEARNING

Deep representation learning techniques generate multiple levels or a hierarchy of representations. In this hierarchy, the high-level representations are constructed from multiple low-level ones. These techniques are based on deep ANNs. A typical (single-layer) neural network consists of input, hidden, and output layers. The input layer receives the raw input data, whereas the output layer produces the task results, such as object classification or clustering. The hidden layer applies nonlinear transformation to extract more abstract and composite representations from the input data. DNNs contain

more than one hidden layer, to apply multiple nonlinear transformations and create the representation hierarchy. The word “deep” refers to the multiple hidden layers in the neural network.

DNNs apply a supervised learning process, where a set of input–output pairs is provided for training. This learning process is composed of two passes: a forward pass (forward propagation) and a backward pass (backpropagation). The forward pass first randomly initializes the network parameters, that is, the connections, weights, and biases. Then, the input data are passed through the network layers, in the forward direction, to calculate the predicted output. Next, the predicted output is compared with the actual output through a task-specific loss function. An optimization technique, namely, stochastic gradient descent (SGD), is then applied to minimize the loss function. Conversely, the backpropagation process is initiated by updating the network weights so that the predicted output is closer to the actual output. This can be achieved by minimizing the error of each output neuron in the entire network.

In the following subsections, we discuss three DNN types that have been used as representation learning techniques for clustering tasks. The first is feedforward neural networks (FNNs), which fall into two categories: completely connected networks (FCNs) [10] and convolutional neural networks (CNNs) [11]; the second is deep belief network (DBNs), which are composed of a stochastic probabilistic component called a restricted Boltzmann machine (RBM); and the third is the autoencoder (AE), which comes in two types: the stacked AE (SAE) and convolutional AE (CAE).

#### A. Feedforward Neural Networks

The FNN [12] is the simplest type of neural network, where the connection between neurons does not form a cycle. The information in this type of network moves forward (in one direction) from the input neurons to the output neurons. In this case, there is no feedback from the output toward the input neurons. FNNs are arranged in the form of layers, as are all neural networks. Depending on the number of layers, an FNN can be a single- or a multilayer network. As mentioned above, FNNs fall into two types: FCNs and CNNs.

An FCN, also known as a multilayer perceptron (MLP) [13], consists of multiple completely connected (FC) layers, where each neuron in one layer is connected to every neuron in the previous layer. In addition, every one of these connections has its own weight. FCNs are composed of an input layer, an output layer, and an arbitrary number of hidden layers. This type of feedforward network is tailored for supervised learning.

Inspired by biological process, the neuron connectivity pattern in CNNs mimics the organization of the animal visual cortex. The first and core building block of a CNN is the convolutional layer, where each neuron is connected to only a few neurons in the previous layer. The same set of weights is used for every neuron. The second layer is the rectified linear unit (ReLU) layer, which applies an elementwise nonlinear activation function to retain the positive parts of the inputs and remove the negative ones by replacing them with zero. The reason for applying ReLU layers in a CNN is to increase the

nonlinearity of the inputs. A pooling layer is frequently inserted between two consecutive convolutional layers. The pooling layer applies a function to reduce the spatial size of the representation by combining the output of the set of neurons in one layer into a single neuron in the next layer. As a consequence, the number of parameters and computations throughout the network is reduced and overfitting is controlled. The final layer of a CNN is an FC layer to classify the input. Similar to FCNs, CNNs are designed for supervised learning, and specifically to classify image datasets.

Deep clustering algorithms that employ feedforward networks for unsupervised representation learning use clustering loss only to train the network. Hence, these algorithms aim to optimize the objective function,

$$L = L_c \quad (1)$$

where  $L$  is the algorithm loss function and  $L_c$  is the clustering loss function. In the absence of other measures and depending completely on the clustering loss, such deep clustering algorithms may lead to a distorted representation space, wherein all data points are assigned to tight clusters. Such a trivial solution results in a small amount of meaningless clustering loss. To alleviate this problem, and in addition to the careful design of the clustering loss function, suitable network parameter initialization is required to enhance the performance.

#### B. Deep Belief Network

DBNs [14] are a branch of DNNs, and are composed of a stack of RBMs [15] followed by a softmax layer that applies a softmax activation function to the input. An RBM is a two-layer neural network, where the first is the visible (input) layer and the second is the hidden layer. A DBN is trained by greedy layer-wise unsupervised learning with RBMs as the building blocks for each layer. Then, the parameters of the DBN are finetuned according to a task-specific loss function. DBN-based deep clustering algorithms finetune the network parameters using the clustering loss function only, and thus optimize an objective function similar to the feedforward network loss function in equation (1). Hence, careful clustering loss selection and good network parameter initialization affect the performance of the deep clustering algorithm.

#### C. Autoencoder

An AE [16] is a special type of neural network designed for unsupervised representation learning. It consists of three building blocks: an encoder, a bottleneck layer, and a decoder. The encoder maps the input  $x_i$  to its hidden representation  $z_i$  through a nonlinear function  $f_{W_1}(\cdot)$ , as in equation (2), and the decoder reconstructs the input  $x_i$  from its hidden representation  $z_i$  by using a transformation function  $g_{W_2}(\cdot)$  as in equation (3).

$$z_i = f_{W_1}(x_i) \quad (2)$$

$$y_i = g_{W_2}(z_i) \quad (3)$$

Here,  $W_1$  represents the encoding weight, and  $W_2$  the decoding weight. The encoder and decoder can comprise an FC network to construct an SAE [17], or a CNN to form a CAE [18]. The bottleneck layer controls the amount of information that traverses the network by learning a compressed representation of the input data. The learning problem can be

formulated as a supervised one that is aimed to output the reconstruction image  $y_i$  from the input  $x_i$ . The entire network can be trained by minimizing the reconstruction loss  $L_{r\_AE}$ , which measures the differences between the original input  $x_i$  and the reconstructed image  $y_i$ :

$$L_r = \frac{1}{n} \sum_{i=1}^n \|x_i - y_i\|^2 \quad (4)$$

AE-based deep clustering algorithms seek to optimize an objective function that combines clustering and reconstruction losses:

$$L = L_r + \gamma L_c \quad (5)$$

where  $\gamma$  is a coefficient to control the distortion of the representation embedding space. The existence of the reconstruction loss forces the algorithm to avoid trivial solutions and learn more feasible representations.

#### D. Variational Autoencoder

VAE [19] is a generative variant of AE that enforces the latent code to follow a predefined distribution. This goal is achieved by encoding the input data into two vectors instead of one: mean value and standard deviation. Unlike the output of the standard AEs that points directly to the encoded value in the latent space, VAE outputs point to the area where the encoded value can be. To be more specific, VAE initializes a probability distribution where the mean value controls the location point of the encoding center, and the standard deviation defines the area in which encoding can vary from the mean. As a consequence, VAE allows interpolation and generation of new samples. Mathematically, VAE measures the Kullback–Leibler (KL) divergence [20] from a prior distribution to approximate the variational posterior distribution. The objective function can be formulated as the following:

$$L_{r\_VAE} = E_{q(z|x_i)} [\log p(x_i|z)] \quad (6)$$

$$L_{VAE} = L_{r\_VAE} - \sum_{i=1}^n \text{KL}(q(z|x_i)||p(z)) \quad (7)$$

where  $L_{r\_VAE}$  represents the reconstruction loss of the VAE,  $p(z)$  is the prior over the latent variables,  $q(z|x_i)$  is the variational posterior to approximate the true posterior  $p(z|x_i)$ , and  $p(x_i|z)$  is the likelihood function. Gaussian distribution is the common choice as prior; however, VAE-based clustering algorithms should choose a distribution which can describe the structure of the clusters.

#### E. Adversarial Autoencoder

Similar to VAE, AAE [21] utilizes a prior distribution to control the encoding of the input data. Hence, the decoder learns only the mapping from the prior distribution to the data distribution. The output of the AAE encoder, i.e. the encoded value, is fed as input to the decoder and to a special generative adversarial network (GAN) [19]. In AAE, the encoder and decoder together form the generator model ( $G$ ), while the GAN is known as discriminator ( $D$ ). Through the learning process, AAE establishes a min–max adversarial game between its generator and the discriminator. While the generator tries to map a generated sample from a prior distribution to the data space, the discriminator computes the probability to detect whether its input a real sample from the data distribution or a

fake sample from the generator. The training process of AAE is handled through two phases: (1) a reconstruction phase and (2) a regulation phase. During the reconstruction phase, the generator is trained to minimize the reconstruction loss of the generated sample and produce a reconstructed image of it. In the regulation phase, the discriminator parameters are updated to distinguish the real samples generated by the prior from the fake samples generated by the encoder. The discriminator network  $D$  is updated by the following discriminative loss ( $L_d$ ):

$$L_d = \frac{1}{n} \sum_{i=1}^n [\log D(\hat{z}_i) + \log(1 - D(z_i))] \quad (8)$$

where  $\hat{z}_i$  and  $z_i$  are the sample from prior distribution and input sample, respectively. Then, the discriminator is fixed, and the encoder is updated to confuse the discriminator by increasing the classification error of  $D$  on the input latent representation with generation loss  $L_g$ , as in the following equation:

$$L_g = \frac{1}{n} \sum_{i=1}^n \log(1 - D(z_i)) \quad (9)$$

AAE-based deep clustering algorithms optimize a loss function that combines reconstruction loss, generation loss, and clustering loss:

$$L_{AAE} = L_r + \alpha L_g + \beta L_c \quad (10)$$

where  $L_r$ ,  $L_g$ , and  $L_c$  represent the reconstruction loss defined in equation (4), the generation loss in equation (9), and a clustering loss, respectively.  $\alpha$  and  $\beta$  are hyperparameters to balance the importance of the generation loss and the clustering loss, respectively.

### III. CLUSTERING TECHNIQUES

As stated previously, clustering techniques can be divided into two types: hierarchical and partitional clustering. Hierarchical clustering methods iteratively merge smaller clusters into larger ones, or split large clusters into smaller ones. The difference between hierarchical algorithms includes the similarity measures that are used to determine which clusters should be merged or split. The results of hierarchical clustering are organized in a tree called a dendrogram, which shows the relationships between clusters. Conversely, partitional clustering seeks to decompose data into a set of disjointed groups. This decomposition is achieved based on the minimization of a specific objective loss function. Centroid-based algorithms, such as K-means [22, 23] and KL-divergence [20] clustering, distribution-based algorithms such as Gaussian mixture clustering [24], graph-based clustering algorithms such as spectral clustering [25] and RCC [26], and density-based algorithms such as DBSCAN [27] are all subtypes of partitional clustering algorithms. As existing joint deep clustering utilizes only centroid- and graph-based clustering, these two techniques are explained in the following subsections. Finally, we introduce some auxiliary clustering losses that are used in conjunction with other losses to guide deep representation learning.

#### A. Centroid-Based Clustering

Given a dataset  $X = \{x_1, \dots, x_n\}$  of  $n$  points together with its extracted representation  $Z = \{z_1, \dots, z_n\}$ , centroid-based clustering partitions the data points into clusters with central

representatives called centroids. These cluster centroids, denoted by  $\mathcal{M} = \{\mu_1, \dots, \mu_k\}$ , where  $k$  is a predefined number of clusters, do not necessarily belong to the dataset. In joint deep clustering algorithms, two centroid-based algorithms are utilized: K-means and KL-divergence clustering.

1) *K-means Clustering*: K-means clustering first randomly selects  $k$  centroids from the input data representations, each of which represents a cluster. A K-means algorithm minimizes the total mean squared error between the input data and cluster centroids according to the loss function:

$$L_{KM} = \sum_{j=1}^k \sum_{i=1}^n \|z_i - \mu_j\|_2^2 \quad (11)$$

An additional variation of the K-means loss function is the weighted least squares error, referred to as weighted K-means. It optimizes the cost function as:

$$L_{WKM} = \sum_{j=1}^k \sum_{i=1}^n S_{ij} \|z_i - \mu_j\|_2^2 \quad (12)$$

where  $S_{ij}$  is a similarity weight that encodes the closeness of a data point to a cluster centroid; i.e.,  $S_{ij}$  will be larger if the data point  $z_i$  is close to the centroid  $\mu_j$ . In the K-means learning process, the following two steps are repeated until convergence is reached:

- Point assignment update, which is accomplished by (i) calculating the mean distance from the data point to every cluster centroid, and (ii) assigning points to the cluster with the minimum mean among all clusters.
- Centroid update, which is computed according to the following equation, where  $m_j$  is the number of points in the  $j^{th}$  cluster:

$$\mu_j = \left(\frac{1}{m_j}\right) \sum_{i=1}^{m_j} z_i \quad (13)$$

K-means perform well when the distribution of the points is in circular form. Otherwise, K-means will attempt to group the points in circular form, which will affect the clustering result. To remedy this issue, K-means should be updated to employ a distribution-based model instead of a distance-based model.

Gaussian Mixture Model (GMM) [24] is a probabilistic soft clustering technique which tends to group points with the same distribution together. The clustering process starts by initializing the means and covariances of the Gaussian distribution for  $k$  clusters. Then, the expectations of all points assignments are calculated for all clusters. Furthermore, the distribution parameters are re-estimated, and the log-likelihood function is computed. This process continues until a predefined convergence criterion is reached.

2) *KL-divergence Clustering*: KL-divergence clustering is a soft assignment clustering technique, in which each data point is assigned to all clusters with varying probabilities. This algorithm is initiated using K-means to obtain  $k$  initial centroids. Next, the learning process is executed to optimize the following Kullback–Leibler (KL) divergence loss function:

$$L_{KLD} = KL(P||Q) = \sum_i \sum_j p_{ij} \log \left(\frac{p_{ij}}{q_{ij}}\right) \quad (14)$$

where  $P$  is an auxiliary target distribution and  $Q$  represents the data point soft assignments. The KL-divergence clustering algorithm refines the point assignments by learning from higher confidence points utilizing the auxiliary target distribution  $p_{ij}$ . Specifically, the algorithm matches the soft assignments  $q_{ij}$  with the target distribution  $p_{ij}$  by computing the KL divergence. The clustering algorithm iteratively performs the following steps until convergence is obtained or the maximum iteration is reached:

1) *Calculation of  $q_{ij}$* , the probability that a data point  $i$  belongs to cluster  $j$ . Two means of calculating  $q_{ij}$  exist: (1) student's t-distribution [28], as in equation (15), and (2) a multinomial regression [28] function, as in equation (16).

$$q_{ij} = \frac{(1 + \|z_i - \mu_j\|_2^2)^{-1}}{\sum_j (1 + \|z_i - \mu_j\|_2^2)^{-1}} \quad (15)$$

$$= \frac{\exp(\mu_j^T z_i)}{\sum_j \exp(\mu_j^T z_i)} \quad (16)$$

2) *Computing  $p_{ij}$* , a higher confidence distribution that can be obtained by calculating the soft cluster frequencies by considering the formula:

$$p_{ij} = \frac{q_{ij}^2 / \sum_i q_{ij}}{\sum_j (q_{ij}^2 / \sum_i q_{ij})} \quad (17)$$

3) Updating clusters centroids according to:

$$\mu_j = \mu_j - \frac{\lambda}{n} \sum_{i=1}^n \frac{\partial L_{KLD}}{\partial \mu_j} \quad (18)$$

## B. Graph-Based Clustering

Given a dataset  $X = \{x_1, \dots, x_n\}$  of  $n$  points together with their corresponding representation  $Z = \{z, \dots, z_n\}$ , graph clustering techniques first construct an undirected similarity graph  $G = (V, E)$ , where  $V = \{v_1, \dots, v_n\}$  denotes a set of vertices to represent the input data, and  $E$  is the set of edges between vertices. Several approaches for building a similarity graph [1] exist, two of which are specifically used in joint deep clustering. These approaches are the following:

- K-nearest neighbor (KNN) graph: this graph connects vertex  $v_i$  with vertex  $v_j$ , if  $v_j$  is within K-nearest neighbors of  $v_i$ . One problem common to KNN is that the graph is asymmetric, which means that if  $v_j$  is among the KNNs of  $v_i$ , then  $v_i$  is not necessarily among the KNNs of  $v_j$ . Hence, the constructed graph is a directed one. To alleviate this problem, there are two solutions; first, to insert an undirected edge between the two vertices  $v_i$  and  $v_j$ , if one of them is within the KNNs of the other; second, to restricts the edges, two vertices  $v_i$  and  $v_j$  are connected by an undirected edge only if they are both among the KNNs of each other. The resultant graph in the latter solution is called a mutual KNN graph.
- Completely connected graph: this graph simply connects all vertices with each other by weighted edges.

The weight of an edge  $w_{ij}$  between two vertices  $v_i$  and  $v_j$  represents the similarity between them. Because the graph should express the local neighborhood relationship, a Gaussian similarity function is usually utilized.

The graph is represented by an adjacency matrix, in which the similarity  $w_{ij}$  between every two vertices is included. Two graph-based clustering algorithms are utilized in joint deep clustering techniques: spectral clustering [25] and robust continuous clustering (RCC) [26]. We briefly explain these two approaches.

1) *Spectral clustering*: After the construction of the similarity graph and the extraction of the adjacency matrix, the spectral algorithm transforms the data into a low-dimensional space. To achieve this, another graph representation matrix is computed, the Laplacian matrix. The graph Laplacian matrix  $\mathcal{L}$  is computed as:

$$\mathcal{L}_{ij} = \begin{cases} d_i, & \text{if } i = j \\ w_{ij}, & \text{if } (i, j) \in E \\ 0, & \text{if } (i, j) \notin E \end{cases} \quad (19)$$

where  $d_i$  is the degree of the vertex  $v_i$ , which can be computed as:

$$d_i = \sum_{\{j|(i,j) \in E\}} w_{ij} \quad (20)$$

Then, the Laplacian matrix is utilized to find the eigenvalues  $\lambda$  and eigenvectors  $v$ , such that.

$$\lambda \mathcal{L} = \lambda v \quad (21)$$

Once the eigenvectors have been obtained, the low-dimensional data transformation is completed. Finally, a K-means clustering algorithm, explained in section 3.1, is applied to the transformed data (eigenvectors) to create clusters.

2) *Robust Continuous Clustering (RCC)*: This approach operates on a set of representations  $U = \{u_1, \dots, u_n\}$  for the original dataset  $X$ , where  $X$  and  $U$  have the same dimensionality. This algorithm minimizes the loss function.

$$L_{RCC} = L_{data} + \lambda L_{pairwise} \quad (22)$$

where  $\lambda$  is a coefficient that balances the two objective terms. The first term  $L_{data}$  is the data loss that constrains the representations to remain near the corresponding data points. The data loss can be computed as:

$$L_{data} = \sum_{i=1}^n \|z_i - u_i\|_2^2 \quad (23)$$

The second term, which is the pairwise loss  $L_{pairwise}$ , is designed to encourage the representations to merge, and pulls them together according to.

$$L_{pairwise} = \sum_{(p,q) \in E} w_{pq} \rho(\|u_p - u_q\|_2; \mu) \quad (24)$$

where  $\{w_{pq}\}$  represents appropriately defined weights,  $\mu$  is a scale parameter, and  $\rho$  is a redescending M-estimator that can be calculated according to a scaled Geman–McClure function [29]:

$$\rho(x; \mu) = \frac{\mu x^2}{\mu + x^2} \quad (25)$$

The first stage in the RCC learning procedure is initialization, which includes the following steps:

1) Construction of the similarity graph  $G_1 = (V, E)$  using mutual KNN.

2) Initialization of the data representation with  $u_i = z_i$ .

3) Initialization of the line process  $\mathbb{L} = \{\ell_{pq}\}$ , where  $\ell_{pq}$  is an auxiliary variable between two connected vertices  $v_p$  and  $v_q$  with  $\ell_{pq} = 1$ .

4) Initialization of a scale parameter  $\mu$  with  $\mu \gg \max\|z_p - z_q\|_2^2$ .

The optimization is aimed to reveal the cluster structure latent in the data; thus, the number of clusters does not need to be known in advance. The following optimization steps are recursively repeated until a maximum iteration number is reached, or the difference between the clustering loss in two consecutive iterations is less than a predetermined threshold.

1) Update  $\ell_{pq}$  according to the following formula.

$$\ell_{pq} = \left( \frac{\mu}{\mu + \|u_p - u_q\|_2^2} \right)^2 \quad (26)$$

2) Update the representations  $U = \{u_1, \dots, u_n\}$  using the following equation:

$$UM = Z \quad (27)$$

where

$$M = I + \lambda A \quad (28)$$

$I$  is the identity matrix,  $e_i$  is an indicator vector with the  $i^{th}$  element set to 1, and  $A$  is computed as the following:

$$A = \sum_{(p,q) \in E} w_{pq} \ell_{pq} (e_p - e_q)(e_p - e_q)^T \quad (29)$$

Update the value of  $\lambda$  as.

$$\lambda = \frac{\|Z\|_2}{\|A\|_2} \quad (30)$$

Update the value of  $\mu$  as.

$$\mu = \max\left(\frac{\mu}{2}, \frac{\delta}{2}\right) \quad (31)$$

where  $\delta$  is a threshold set to be the mean of the lengths of the shortest 1% of the edges in  $E$ . Then, RCC constructs a new graph  $G_2 = (V, \mathcal{E})$  with  $\varepsilon_{pq} = 1$  if  $\|u_p^* - u_q^*\|_2 > \delta$ . Finally, the algorithm outputs the clusters given by the connected vertices of  $G_2$ .

### C. Auxiliary Clustering Losses

Some clustering loss functions are designed to guide deep representation learning techniques to extract feasible clustering-oriented representations; they cannot, however, output clusters. These functions are known as auxiliary clustering losses. Considering a dataset  $X = \{x_1, \dots, x_n\}$  of

$n$  points together with its extracted representations  $Z = \{z_1, \dots, z_n\}$ , we present the auxiliary clustering losses that have been used in joint deep representation clustering algorithms.

1) *Balanced assignment loss*: Balanced assignment loss is used in conjunction with other clustering loss to enforce balanced clustering assignments. The difference between two distributions,  $f$  and  $u$ , is measured based on KL divergence as follows:

$$L_{BA} = KL(f||u) = \frac{1}{n} \sum_i \sum_j p_{ij} \log \left( \frac{f_j}{u_j} \right) \quad (32)$$

where  $P$  is the target distribution proposed in equation (17)  $u$  is the uniform distribution, and  $f$  is the probability distribution, which can be calculated as.

$$f_j = \frac{1}{n} \sum_i p_{ij} \quad (33)$$

2) *Locality-preserving loss*: Locality-preserving loss preserves the local structure property of the original data by pushing the nearby points together as.

$$L_{LP} = \sum_{i,j \in N_k(i)} S_{ij} \|z_i - z_j\|_2^2 \quad (34)$$

where  $N_k(i)$  is the set of  $k$  nearest neighbors of the data point  $x_i$  and  $S_{ij}$  is a similarity measure between  $x_i$  and  $x_j$ .

3) *Group sparsity loss*: Group sparsity loss was inspired by spectral clustering, where a block-diagonal similarity matrix is utilized for representation learning. Specifically, the hidden units are divided into  $k$  groups, where  $k$  is the number of clusters. For each data point  $x_i$ , after its representation  $z_i$  has been extracted, a  $k$  group unit  $\{f^j(x_i)\}_{j=1}^k$  is obtained. Then, the group sparsity is computed as.

$$L_{GS} = \sum_{i=1}^n \sum_{j=1}^k \lambda \sqrt{n_g} \|f^j(x_i)\|_2 \quad (35)$$

where  $f(x_i)$  is the representation encoding function,  $\lambda$  is a constant, and  $n_g$  is the group size.

4) *Self-expressiveness loss*: Self-expressiveness loss is a property where a point in a subspace can be expressed as a linear combination of other points in the same subspace. Let  $X$  be a column matrix of all data points; the self-expressiveness can then be represented as  $X = XC$ , where  $C$  is the self-representation coefficient matrix. By minimizing a certain norm of  $C$ , and under the assumption that the subspaces are independent,  $C$  is guaranteed to have a block-diagonal structure. This ensures that  $c_{ij} \neq 0$ , where  $x_i$  and  $x_j$  are two data points lying in the same subspace. The matrix  $C$  can then be leveraged by spectral clustering to construct the affinity matrix. Given this fact, each data representation  $z_i$  in a latent subspace is approximated by a weighted linear combination of other points  $\{z_j\}_{j=1}^n$  with weights  $c_{ij}$ . To encode self-expressiveness, the following auxiliary clustering loss function is introduced:

$$L_{SE} = \lambda_1 \|C\|_p + \frac{\lambda_2}{2} \|Z - ZC\|^2, \text{ s. t. } (\text{diag}(c) = 0) \quad (36)$$

where  $\lambda_1$  and  $\lambda_2$  are two regularization parameters to account for data corruption, and  $\|\cdot\|_p$  represents an arbitrary matrix norm.

#### IV. JOINT DEEP CLUSTERING

Given a dataset  $X = \{x_1, \dots, x_n\}$  of  $n$  points, the goal of joint deep clustering techniques is simultaneously to learn a low-dimensional representation  $Z = \{z_1, \dots, z_n\}$  for the data and to cluster it into groups jointly. This can be accomplished by optimizing a joint loss function that combines two losses: the representation learning loss and the clustering loss. Then, the low-dimensional representations, network parameters (weights and biases), and clustering parameters and assignments are updated jointly. In this section, we survey these algorithms, and provides a taxonomy from the perspective of clustering algorithms. Table I summarizes existing joint deep clustering algorithms.

##### A. Deep Kullback–Leibler Divergence Clustering

Guo et al. [28] proposed improved deep embedded clustering (IDEC), an algorithm that simultaneously learns low-level representation and cluster assignment. The IDEC algorithm consists of two phases: (1) parameter initialization, and (2) parameter optimization and clustering. In the initialization phase, IDEC initiates a denoising SAE [17], which reconstructs a data point  $x$  from a corrupted (noisy) version  $\tilde{x}$  to force the encoder and decoder to capture implicitly the structure of data that generate distribution. The SAE is trained based on reconstruction loss to obtain initial values for the network's weights and biases. The clusters' centroids are initiated by applying K-means to the representations extracted from the encoder element. When the initialization is completed, IDEC removes noise from the data to apply clustering to the representation learned from the clean data. When noise has been removed, the denoising SAE degenerates into a traditional SAE, which constrains the dimension of the hidden representation  $Z$  to be less than the dimension of the input data  $X$ . Then, the optimization and clustering phase is executed by finetuning using KL divergence as clustering loss and SAE reconstruction loss. This results in the joint loss function

$$L_{IDEC} = L_r + \lambda L_{KLD} \quad (37)$$

where  $L_r$  is the reconstruction loss in equation (4),  $L_{KLD}$  is the KL-divergence clustering loss in equation (14), and  $\lambda$  is a regularization parameter to balance the two terms. Clustering is achieved by alternating between computing the soft assignment based on the student's t-distribution formula in equation (15), and auxiliary target distribution in equation (17). IDEC jointly optimizes the cluster centers  $\mu_j$  and the network parameters  $\theta$  using an SGD algorithm [30]. The gradient is calculated for the clustering loss  $L_c$  with respect to the cluster centroid  $\mu_j$  and point representation  $z_i$ , and then is utilized in backpropagation. Experimental results have demonstrated the importance of locality preservation. Guo et al. [31] developed a deep clustering method with CAEs (DCEC) for image clustering; the DCEC framework is very similar to the IDEC model, but instead of an SAE, DCEC employs a CAE to better incorporate the relationship between image pixels. The effectiveness of CAE over SAE has also been demonstrated for image datasets.

TABLE I. SUMMARY OF JOINT DEEP CLUSTERING ALGORITHMS

Algorithm	Clustering Technique	Network Architecture	Joint Loss Function	Main Contribution
IDEC	KL-divergence	SAE	$L_{IDEC} = L_r + \lambda L_{KLD}$	Joint version of DEC [35], the first well-known deep clustering algorithm.
DCEC		CAE		Improves on IDEC by using CAE instead of SAE.
ADEC		AAE	$L_{ADEC} = L_r + \alpha L_g + \beta L_{KLD}$	Preserve the relevance between representation learning and clustering and reach to better trade-off between feature drift and feature randomness issue.
DEPICT		CAE	$L_{DEPICT} = L_{r, DEPICT} + L_{KLD} + L_{BL}$	Ensures balanced clustering assignments that provide robust and superior results over image datasets.
DEN	K-means	SAE	$L_{DEN} = L_r + \alpha L_{LP} + \beta L_{GS}$	Learns clustering-oriented representations with the following properties: (1) locality preservation and (2) group sparsity.
DCN			$L_{DCN} = L_r + \lambda L_{KLM}$	First algorithm to perform K-means and representation learning simultaneously.
DKM			$L_{DKM} = L_r + \lambda L_{WKM}$	Updates DCN to use weighted K-means instead of traditional K-means.
DMC			$L_{DMC} = (1 - \alpha)L_r + \alpha L_{LP, DMC} + \beta L_{WKM}$	Utilizes deep SAE to improve the traditional multimaniifold clustering algorithm.
DSC-Nets	Spectral Clustering	CAE	$L_{DSC-Nets} = L_r + L_{SE}$	Utilizes deep CAE to improve the traditional spectral clustering algorithm.
DASC		AAE	$L_{DASC} = L_r + \alpha L_g + \beta L_{SE}$	Learns subspace clustering-friendly representations using AAE and self-expressiveness constraint.
DSC			$L_{DSC} = L_r + L_g + \text{spectral clustering}$	More robust to noise; since it enforces the reconstruction constraints for the latent representations and their noisy versions.
DCC	RCC	SAE	$L_{DCC} = \frac{1}{D} L_r + \frac{1}{d} (L_{data, DCC} + \lambda L_{pairwise, DCC})$	Utilizes deep SAE to improve on the traditional RCC algorithm.

Similar to IDEC, Zhou et al. [21] introduced Deep Embedded Clustering With Adversarial Distribution Adaptation (ADEC). Instead of SAE, ADEC utilizes AAE to learn from data space to feature space. With a backpropagation algorithm, ADEC iteratively optimizes the following objective function:

$$L_{ADEC} = L_r + \alpha L_g + \beta L_{KLD} \quad (38)$$

where  $L_r$ ,  $L_g$ ,  $L_{KLD}$  is the reconstruction loss defined in (9), the generation loss in (9), and the KL-divergence clustering loss in equation (14), respectively, and  $\alpha$  and  $\beta$  are hyperparameters to balance the importance of the generation loss and the clustering loss, respectively. In deep learning, the optimization of a neural network's loss function whose secondary component highly competes with the primary one may lead to feature drift. As a result, the global learning process will be affected, since the features learned by the primary loss can be easily drifted by updating the secondary one. Discarding one of the primary or secondary losses will lead to substitution of a significant portion of true labels for random ones, known as feature randomness. Mrabah et al. [32] enhanced the IDEC approach to reach a better trade-off between feature drift and feature randomness using AAE complemented with data augmentation.

Dizaji et al. [33] proposed the deep embedded regularized clustering (DEPICT) model to learn data representation and

perform the clustering task. DEPICT has a complicated network architecture composed of a softmax layer on top of a multilayer CAE. More specifically, DEPICT consists of four components: two encoders, one decoder, and one softmax layer. The encoder and decoder elements of the DEPICT network are referred to as paths.

Thus, there are three paths in the DEPICT architecture. The first path is called the noisy encoder, which is the encoder part of the denoising CAE that accepts noisy input data to infer noisy hidden representations. The second path is called the noisy decoder (or just decoder), and is the decoder element of the denoising CAE for reconstructing the input from the learned noisy representations. The decoder element consists of a strided CNN, which is similar to the traditional one, except that the value of the convolutional kernel stride is greater than 1. The third path is called the clean encoder, a CNN that accepts clean input data to infer clean hidden representations. The clean and the noisy encoder paths share the same network parameters, i.e., weights and biases. The softmax layer (the fourth component of the network) is stacked on top of the noisy encoder top layer and clean encoder top layer to obtain the clustering assignments. The first phase of the algorithm is initialization, where the network parameters, cluster centroids, and target distribution are initialized. Instead of initializing the network parameters randomly, DEPICT assigns the weights from a Gaussian distribution, where the input and output variances are the same for each layer. This initialization

approach is known as Xavier (or normalized) initialization [34]. Next, DEPICT is trained with reconstruction loss only (without clustering loss) to obtain initial embedded representations for the input data. Then, the K-means clustering technique is applied to obtain the initial cluster centroids and the initial target distribution  $P$ , when the initialization phase is complete, the optimization and clustering phase starts. In the softmax layer, DEPICT iteratively minimizes the following three-term joint loss function:

$$L_{\text{DEPICT}} = L_{\text{r\_DEPICT}} + L_{\text{KLD}} + L_{\text{BL}} \quad (39)$$

where  $L_{\text{KLD}}$  and  $L_{\text{BL}}$  are the KL-divergence and balanced assignment losses that were introduced in equations (14) and (32), respectively. The first term is a data-dependent regularization term, which is a reconstruction loss function introduced in DEPICT designed to enhance the representation learning process and avoid the overfitting problem. The reconstruction loss between the noisy decoder and the clean encoder representations is computed as.

$$L_{\text{r\_DEPICT}} = \frac{1}{n} \sum_{i=1}^n \sum_{l=1}^{L-1} \frac{1}{|z_i^l|} \|z_i^l - \hat{z}_i^l\|_2^2 \quad (40)$$

where  $n$  is the size of the input data,  $L$  is the number of noisy decoder and clean encoder layers,  $l$  is the layer number,  $|z_i^l|$  is the  $l^{\text{th}}$  layer output size,  $z_i^l$  is the  $l^{\text{th}}$  layer of clean representations (from the clean encoder), and  $\hat{z}_i^l$  is the  $l^{\text{th}}$  layer of noisy representations (from the noisy decoder). The second term of the DEPICT joint loss function is the KL-divergence clustering loss. A multinomial logistic regression function is employed to perform the soft clustering assignment. Note that DEPICT computes the soft assignment predictions  $Q$  based on noisy representations that are extracted from the noisy encoder, whereas the target distribution  $P$  is computed from the clean representations extracted from the clean encoder path. The third term is a regularization term that encourages balanced cluster assignments and avoids the allocation of clusters to outlier samples. The effectiveness of DEPICT has been proven empirically, especially in terms of the running time complexity.

### B. Deep K-Means Clustering

Huang et al. [36] introduced a deep embedding network, referred to as DEN, to learn clustering-oriented representations using a three-layer SAE. Similar to that of most deep clustering algorithms, the DEN learning procedure is composed of two phases: initialization (pretraining) and optimization. In the pretraining phase, a three-layer DBN [14] is trained based on the contrastive divergence loss only, to initialize the SAE parameters. Then, the learned representation from the DBN is fed into the three-layer SAE to begin the joint training optimization process. In this phase, the DEN minimizes the joint loss function.

$$L_{\text{DEN}} = L_{\text{r}} + \alpha L_{\text{LP}} + \beta L_{\text{GS}} \quad (41)$$

where  $L_{\text{r}}$  is the reconstruction loss in equation (4),  $L_{\text{LP}}$  is the locality-preserving auxiliary clustering loss defined in (34), and  $L_{\text{GS}}$  is the group sparsity auxiliary clustering loss expressed in equation (35) with  $S_{ij} = \exp\left(\frac{\|x_i - x_j\|_2^2}{t}\right)$ . Further,  $\alpha$ ,  $\beta$ , and  $t$  are tuning parameters. By considering these two auxiliary

clustering losses, the DEN imposes two constraints on the learned representations: the first is the locality-preserving constraint to preserve the local structure property of the original data, and the second is the group sparsity constraint. These are imposed to facilitate the clustering process, and ensure that the learned representation incorporates cluster information, and thus, is more suitable for clustering. After the optimization phase, the traditional K-means clustering algorithm is employed to perform clustering.

Yang et al. [37] proposed a dimensionality reduction and K-means clustering framework named the deep clustering network (DCN). A DNN, specifically an SAE, is utilized by the DCN for dimensionality reduction and representation learning. The DCN algorithm is initiated by a pretraining stage based on reconstruction loss to initialize the SAE weights and biases. To initialize the cluster centroids, K-means clustering is applied to the obtained representations from the pretraining. Then, the joint training phase is executed by iteratively optimizing the joint loss function.

$$L_{\text{DCN}} = L_{\text{r}} + \lambda L_{\text{KM}} \quad (42)$$

where  $L_{\text{r}}$  is the reconstruction loss as defined in equation (4),  $L_{\text{KM}}$  is the K-means clustering loss function described in equation (11), and  $\lambda$  is a regularization parameter, which balances the reconstruction error by finding K-means-oriented hidden representations. Instead of applying the traditional SGD for the optimization process, the DCN introduces an alternating SGD optimization algorithm to update its parameters. There are three sets of parameters to be updated in a DCN: cluster centroids, data point cluster assignments, and network parameters. The proposed alternating SGD suggests that each set of parameters should be treated as a subproblem; thus, DCN optimizes the subproblems with respect to one of the cluster centroids, data point assignments, and network parameters while keeping the other two sets fixed. For instance, to update network parameters, both the cluster centroids and data point assignment are fixed, and then the corresponding gradient is calculated by backpropagation.

Fard et al. [38] proposed a deep K-means clustering algorithm named deep K-means (DKM), which is very similar to the DCN [37]. DKM differs from the DCN in the clustering loss only, where weighted K-means is employed instead of K-means. Equation (43) shows the DKM joint loss function:

$$L_{\text{DKM}} = L_{\text{r}} + \lambda L_{\text{WKM}} \quad (43)$$

where  $L_{\text{r}}$  is the reconstruction loss as defined in equation (4),  $L_{\text{WKM}}$  is the weighted K-means clustering loss function described in equation (12), and  $\lambda$  regulates the trade-off between seeking good representation and good clustering results. The similarity weight of the K-means loss function is computed according to the softmax function.

$$S_{ij, \text{DKM}} = \frac{\exp(-\alpha \|z_i - z_{\mu_j}\|_2^2)}{\sum_{j'=1}^k \exp(-\alpha \|z_i - z_{\mu_{j'}}\|_2^2)} \quad (44)$$

where  $z_i$  is the learned representation of data point  $x_i$ ,  $k$  is the number of clusters,  $z_{\mu_j}$  is the representation of the cluster centroid  $\mu_j$ , and  $\alpha$  is a coefficient such that when its value is 0,

all of the data points in the embedding space are very close, and when its value is relatively high, the points are sparse in the space. The network architecture and learning process of DKM is similar to that of DCN, except that instead of alternating between continuous gradient updates and discrete cluster assignment steps, DKM relies on the gradient update only to learn both the representation and clustering parameters.

Chen et al. [39] proposed a deep manifold clustering algorithm called deep manifold clustering (DMC) to address multimanifold clustering (MMC) [40]. DMC's architecture is similar to that of DEN [36], where an SAE [17] is employed for representation learning and a DBN [14] is utilized to initialize the SAE parameters. In DMC, a locality-preserving auxiliary clustering loss is introduced such that the locality of a manifold can be interpreted as similar inputs, and therefore, should have similar representations. Thus, a data point can be recovered using the representation of its nearby point. Based on this observation, the DMC [39] locality-preserving loss function is defined as.

$$L_{LP\_DMC} = \frac{1}{k} \sum_{j \in N_k(i)} \|y_i - x_j\|_2^2 \quad (45)$$

where  $y_i$  is the reconstructed image of data point  $x_i$  and  $N_k(i)$  is the indices set of  $k$  nearest neighbors of  $x_i$ . After the SAE weights and cluster centroids have been initialized, the joint training procedure proceeds by iteratively optimizing the joint loss function:

$$L_{DMC} = (1 - \alpha)L_r + \alpha L_{LP\_DMC} + \beta L_{WKM} \quad (46)$$

where  $L_r$  is the reconstruction loss defined in equation (4),  $L_{LP\_DMC}$  is the locality-preserving loss function defined in equation (45),  $L_{WKM}$  is the weighted K-means clustering loss function presented in equation (12),  $\alpha$  balances the importance between the reconstruction of  $x_i$  itself and its local neighborhood, and  $\beta$  is a parameter to balance the contribution of the first two terms and  $L_{WKM}$ . DMC uses the Gaussian-dependent kernel as the similarity weight of the weighted K-means loss function.

$$S_{ij\_DMC} = \frac{\exp(-\alpha \|z_i - z_{\mu_j}\|_2^2 / 2\sigma)}{\sum_{j'=1}^k \exp(-\alpha \|z_i - z_{\mu_{j'}}\|_2^2 / 2\sigma)} \quad (47)$$

Here,  $\sigma$  is the kernel bandwidth. The keystone point of DMC is to find the manifold center, because the cluster centers are most probably surrounded by nearby points with lower local density, and because they are at a relatively large distance from any points with a higher local density. Therefore, DMC calculates the density of the new representation by computing two metrics: the local density of a point, and its distance to points with higher density. The local density  $\rho_i$  of the representation  $z_i$  is defined as.

$$\rho_i = \sum_{j=1}^n e^{-\frac{d_{ij}}{\hat{\Delta}}} \quad (48)$$

where  $d_{ij}$  is the distance between the representation  $z_i$  and  $z_j$  and  $\hat{\Delta}$  is a cut-off distance. Then, the points in the new embedding space are sorted based on their density in descending order, denoted by  $\{\lambda_i\}_{i=1}^n$  with  $\rho_{\lambda_1} \geq \rho_{\lambda_2} \geq \dots \geq \rho_{\lambda_n}$ . The distance metric is therefore calculated as.

$$\xi_{\lambda_i} = \begin{cases} \min_{\lambda_j} \{\Delta_{\lambda_i \lambda_j}\}, i \geq 2 \\ j < i \\ \max_{\lambda_j} \{\xi_{\lambda_j}\}, i = 1. \end{cases} \quad (49)$$

Next, a third metric is defined as

$$\gamma_i = \rho_i \xi_i \quad (50)$$

Similarly, the points in the new embedding space are sorted based on  $\gamma_i$ , as computed in equation (44) in descending order, and denoted by  $\{\pi_i\}_{i=1}^n$  with  $\gamma_{\pi_1} \geq \gamma_{\pi_2} \geq \dots \geq \gamma_{\pi_n}$ . Assuming that the number of clusters  $k$  is known in advance, the cluster centers are determined by considering the  $k$  largest  $\gamma$ . The experiments reported in [39] showed that DMC outperformed the state-of-the-art multimanifold clustering methods.

### C. Deep Spectral Clustering

Ji et al. [41] introduced deep subspace clustering networks (referred to as DSC-Nets) based on CAE [18] to learn nonlinear mapping. The network architecture of DSC-Nets includes three parts: a CNN encoder, a middle layer called the self-expressive layer, and a CNN decoder. In the self-expressive layer, the neurons are completely connected using linear weights without bias and nonlinear activation. The purpose of this FC layer is to encode the self-expressiveness property, as explained in section 3.3. Each node in this self-expressive layer is a representation  $z_i$ , and the weights correspond to the matrix  $C$  in equation (36) which are further used to construct affinities between all data points. Therefore, essentially, the self-expressive layer enables the network to learn the affinity matrix directly. First, DSC-Nets pre-train the CAE without the self-expressive layer to initialize the encoder and decoder parameters. Then, in the finetuning process, the DSC-Nets deep network is first trained, and the following joint loss function is recursively optimized:

$$L_{DSC-Nets} = L_r + L_{SE} \quad (51)$$

where  $L_r$  is the reconstruction loss defined in equation (4) and  $L_{SE}$  is the self-expressiveness loss as expressed in (36). When the training is completed, the parameters of the self-expressive layer are used to build an affinity matrix for spectral clustering, as explained in section 3.2. The experiments reported in [41] showed that DSC-Nets yielded superior results for small datasets. However, this method cannot be applied on large datasets because of the memory complexity of the algorithm [19].

Similar to DSC-Nets, in [42], Zhou et al. proposed deep adversarial subspace clustering (DASC) model which learns subspace clustering-friendly representations using AAE and self-expressiveness constraint. Given that, DASC optimizes the following objective function:

$$L_{DASC} = L_r + \alpha L_g + \beta L_{SE} \quad (52)$$

where  $L_r$ ,  $L_g$ , and  $L_{SE}$  represent the reconstruction loss defined in (4), the generation loss in (9), and the self-expressiveness loss that defined in (36), respectively, and  $\alpha$  and  $\beta$  are hyperparameters to balance the importance of the generation loss and the clustering loss, respectively. Upon the

completion of the training process, spectral clustering is applied to the resulting affinity matrix.

Yang et al. in [43] presented a deep spectral clustering (DSC) approach based on AAE. In the proposed approach, the generator is a dual AE network (one encoder and two decoders) to enforce the reconstruction constraints for the latent representations and their noisy versions. As a consequence, the resulting latent representation will be more robust to noise. Hence, the reconstruction loss is updated to be in the following format:

$$L_{r\_DSC} = \frac{1}{n} \sum_{i=1}^n \|\tilde{y}_i - y_i\|^2 + \delta L_r \quad (53)$$

where  $L_r$  is the reconstruction loss in (4),  $y_i$  is the reconstructed image of input  $x_i$ ,  $\tilde{y}_i$  is the reconstructed image of the noisy version of the input  $x_i$ , and  $\delta$  balances the strength of the two losses. Then, the mutual information estimation is employed to boost the discriminator with more information from the inputs. To achieve this, the feature map of the middle convolutional layer of the encoder is extracted and combined with the latent representation to obtain a new feature map. Therefore, the generation loss will be as follows:

$$L_{g\_DSC} = -\beta \left[ \frac{1}{n} \sum_{i=1}^n \log D(x_i, z_i) + \log(1 - D(x_i, z_i)) \right] - \frac{\beta}{hw} \left[ \sum_{i,j} \frac{1}{n} \sum_{k=1}^n \log D(C_{ij}, z_k) + \log(1 - D(C_{ij}, z_k)) \right] + \gamma L_{KL} \quad (54)$$

where  $D$  is the discriminator,  $C_{ij}$  represents the feature vector of the middle feature map at coordinates  $(i, j)$ ,  $z_i$  is the latent representation of input  $x_i$ ,  $L_{KL}$  is the KL-divergence loss in equation (14),  $h$  and  $w$  represent the height and width of the feature map, and  $\beta$  and  $\gamma$  are balancing parameters. Furthermore, the latent representations are embedded into the eigenspace to cluster them using a spectral clustering technique.

#### D. More Deep Clustering Algorithms

Shah et al. [44] presented deep continuous clustering (DCC), a framework for joint nonlinear embedding learning and clustering. The DCC framework integrates an RCC algorithm [44] with an SAE [17] as a deep representation learning technique. DCC consists of two stages: initialization and optimization. During the initialization stage, the denoising SAE is trained based on reconstruction loss only to initialize the network parameters, i.e., weights and biases. Then, the SAE is finetuned, using the reconstruction loss only, to complete the initialization. At the end of this stage, the learned representation  $Z$  is obtained from the bottleneck layer to have the initialization  $U = Z$ . Then, the optimization is conducted by minimizing the joint loss function.

$$L_{DCC} = \frac{1}{D} L_r + \frac{1}{d} (L_{data\_DCC} + \lambda L_{pairwise\_DCC}) \quad (55)$$

where  $L_r$  is the AE reconstruction loss in equation (4),  $D$  is the dimensionality of the original input dataset, and  $d$  is the dimensionality of the lower-dimensional representations  $Z$ . DCC modifies the data loss introduced in RCC [44] as.

$$L_{data\_DCC} = \sum_{i=1}^n \rho(\|u_i - z_i\|_2; \mu_1) \quad (56)$$

where  $\rho$  is the scaled Geman–McClure function defined in equation (25). The pairwise loss is also modified by DCC as.

$$L_{pairwise\_DCC} = \sum_{(i,j) \in E} w_{ij} \rho(\|u_i - u_j\|_2; \mu_2) \quad (57)$$

The parameters  $\mu_1$  and  $\mu_2$  control the radii of the convex basins of the estimators. The weights  $w_{ij}$  are computed based on.

$$w_{ij} = \frac{\frac{1}{n} \sum_{k=1}^n N_k}{\sqrt{N_i N_j}} \quad (58)$$

where  $N_i$  is the degree of  $u_i$  in the graph. To balance the different terms, DCC sets  $\lambda$  and  $A$  according to equations (29) and (30), respectively. The network parameters, the representatives  $U$ , and the lower-dimensional representations  $Z$  are updated by an SGD optimization algorithm [45] through backpropagation. Other DCC parameters, such as  $\lambda$ , are iteratively updated during the optimization as in the RCC algorithm [44].

Jiang et al. [46] proposed Variational Deep Embedding (VaDE), a probabilistic generative clustering technique within a VAE framework. In VaDE, Mixture-of-Gaussian is assumed to be the prior of the probabilistic clustering. To model the data generative procedure, VaDE utilizes GMM to pick a cluster from which a latent embedding is generated. Then, VAE decodes the latent embedding into an observable. Then, VAE is trained to maximize the evidence lower bound (ELBO) [19] according to VAE loss ( $L_{VAE}$ ) in equation (7). After maximizing the ELBO, the cluster assignment can be inferred by the learned GMM model. GMVA [47] is another probabilistic clustering algorithm based on VAE with a Gaussian mixture as a prior distribution. The main contribution of this algorithm is in introducing the minimum information constraint [48] to the VAE in order to overcome the problem of cluster degeneracy, caused by the over-regularization of the VAE. The GMVA approach is more complex than VaDE, and has shown worse results in practice [19]. However, both VaDE and GMVA suffer from high computational complexity [19].

Mukherjee et al. [49] addressed the problem of clustering in the latent space of GAN [19] by introducing the ClusterGAN framework. In order to establish non-smooth geometry of the latent space, a mixture of discrete and continuous latent variables is utilized. To accommodate that mixture of variables, a new backpropagation algorithm is introduced to obtain the latent variable given a data input. The experimental results showed that GAN is able to preserve latent space interpolation across different categories.

As shown in Table I, we compared the studied joint deep clustering algorithms based on their clustering technique, loss functions, and main contributions. From the presented review, deep clustering algorithms with autoencoders are the most common technique and this due to two reasons. We can summarize these two points as: (1) the ability to combine the autoencoders with the most clustering algorithm, (2) autoencoders reconstruction loss is capable to learn feasible representations and avoid trivial solutions. It is important to note that, the computational cost of autoencoder based deep clustering algorithms is highly affected by the clustering loss. However, for computational feasibility, such algorithms have limited network depth due to the symmetry architecture of autoencoder. On the other hand, deep clustering algorithms

with VAE, AAE, and GAN minimize the variational lower bound on the marginal likelihood of data which make them theoretically guaranteed. Unfortunately, these clustering techniques suffer from high computational complexity. Comparing VAE deep clustering algorithms with AAE and GAN clustering algorithms, AAE and GAN algorithms are more flexible and diverse than VAE algorithms. Nonetheless, AAE and GAN based clustering algorithms have slow convergence rate.

## V. CONCLUSION

Recently, clustering algorithms have benefited from the new deep learning research field. In fact, new active research studies are focused on integrating deep representation learning with clustering tasks. Beyond joint deep clustering algorithms, more recent algorithms have been proposed, some of which have been classified as separated deep clustering approaches, and others categorized as combined deep clustering techniques, but not joint. DeepCluster, clustering by unmasking, rank-constrained spectral clustering, SDEC, parameter-free clustering, and learning deep graph representation are all examples of not-joint deep clustering algorithms.

In this article, we reviewed the existing joint deep clustering algorithms by describing their network structure and analyzing their objective functions. Based on the survey of algorithms discussed here, theoretical analysis of how and why jointly optimizing reconstruction and clustering losses significantly improves the clustering performance is itself significant. Also, studying whether deep supervised learning techniques, such as data augmentation and regularization, are applicable and useful for deep unsupervised clustering is meaningful. Exploring the feasibility of applying the proposed joint deep clustering algorithms on sequential data is highly encouraged. Moreover, exploring the viability of combining deep clustering techniques with other unsupervised learning tasks such as transfer learning is strongly recommended.

## ACKNOWLEDGMENT

The authors are grateful for the support of the Research Center of the College of Computer and Information Sciences, King Saud University. The authors thank the Deanship of Scientific Research and RSSU at King Saud University for their technical support.

## REFERENCES

- [1] D. Xu and Y. Tian, "A Comprehensive Survey of Clustering Algorithms," *Ann. Data Sci.*, vol. 2, no. 2, pp. 165–193, 2015.
- [2] I. T. Jolliffe, "Principal Components in Regression Analysis," in *Principal component analysis*, Springer, 1986, pp. 129–155.
- [3] M. Li and B. Yuan, "2D-LDA: A statistical linear discriminant analysis for image matrix," *Pattern Recognit. Lett.*, vol. 26, no. 5, pp. 527–532, Apr. 2005.
- [4] B. Schölkopf, A. Smola, and K.-R. Müller, "Nonlinear Component Analysis as a Kernel Eigenvalue Problem," *Neural Comput.*, vol. 10, no. 5, pp. 1299–1319, 1998.
- [5] I. National and D. Recherche, "Generalized Discriminant Analysis Using a Kernel Approach," *Neural Comput.*, vol. 12, no. 1, pp. 1–13, 1994.
- [6] J. B. Tenenbaum, V. De Silva, and J. C. Langford, "A global geometric framework for nonlinear dimensionality reduction," *Science (80-. )*, vol. 290, no. 5500, pp. 2319–2323, 2000.
- [7] Yuexian Hou, Peng Zhang, Xingxing Xu, Xiaowei Zhang, and Wenjie Li, "Nonlinear Dimensionality Reduction by Locally Linear Inlaying," *IEEE Trans. Neural Networks*, vol. 20, no. 2, pp. 300–315, 2009.
- [8] G. E. Hinton, S. Osindero, and Y.-W. Teh, "A fast learning algorithm for deep belief nets," *Neural Comput.*, vol. 18, no. 7, pp. 1527–54, 2006.
- [9] G. E. Hinton and R. R. Salakhutdinov, "Reducing the dimensionality of data with neural networks," *Science (80-. )*, vol. 313, no. 5786, pp. 504–507, 2006.
- [10] W. F. Schmidt, M. A. Kraaijveld, and R. P. W. Duin, "Feed forward neural networks with random weights," in *Proceedings - International Conference on Pattern Recognition*, 1992, vol. 2, pp. 1–4.
- [11] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet Classification with Deep Convolutional Neural Networks," *Adv. Neural Inf. Process. Syst.*, pp. 1–9, 2012.
- [12] D. Svozil, V. Kvasnicka, and J. Pospichal, "Introduction to multi-layer feed-forward neural networks," 1997.
- [13] M. W. Gardner and S. R. Dorling, "Artificial neural networks (the multilayer perceptron) - a review of applications in the atmospheric sciences," *Atmos. Environ.*, vol. 32, no. 14–15, pp. 2627–2636, Aug. 1998.
- [14] N. Lopes and B. Ribeiro, "Deep Belief Networks (DBNs)," in *Machine Learning for Adaptive Many-Core Machines-A Practical Approach*, Springer, 2015, pp. 155–186.
- [15] H. Lee, R. Grosse, R. Ranganath, and A. Y. Ng, "Unsupervised learning of hierarchical representations with convolutional deep belief networks," *Commun. ACM*, vol. 54, no. 10, pp. 95–103, 2011.
- [16] Y. Bengio, "Learning deep architectures for AI," *Found. Trends Mach. Learn.*, vol. 2, no. 1, pp. 1–27, 2009.
- [17] P. Vincent, H. Larochelle, I. Lajoie, Y. Bengio, and P. A. Manzagol, "Stacked denoising autoencoders: Learning Useful Representations in a Deep Network with a Local Denoising Criterion," *J. Mach. Learn. Res.*, vol. 11, pp. 3371–3408, 2010.
- [18] B. Leng, S. Guo, X. Zhang, and Z. Xiong, "3D object retrieval with stacked local convolutional autoencoder," *Signal Processing*, vol. 112, pp. 119–128, 2015.
- [19] E. Min, X. Guo, Q. Liu, G. Zhang, J. Cui, and J. Long, "A Survey of Clustering with Deep Learning: From the Perspective of Network Architecture," *IEEE Access*, vol. 6, pp. 39501–39514, 2018.
- [20] J. R. Hershey and P. A. Olsen, "Approximating the Kullback Leibler divergence between Gaussian mixture models," in *ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings*, 2007, vol. 4, pp. IV-317-IV-320.
- [21] W. Zhou and Q. Zhou, "Deep Embedded Clustering With Adversarial Distribution Adaptation," *IEEE Access*, vol. 7, pp. 113801–113809, 2019.
- [22] J. MacQueen, "Some methods for classification and analysis of multivariate observations," in *Proceedings of the fifth Berkeley Symposium on Mathematical Statistics and Probability*, 1967, vol. 1, pp. 281–296.
- [23] J. A. Hartigan and M. A. Wong, "Algorithm AS 136: A K-Means Clustering Algorithm," *Appl. Stat.*, vol. 28, no. 1, p. 100, 1979.
- [24] G. Celeux and G. Govaert, "Gaussian parsimonious clustering models," *Pattern Recognit.*, vol. 28, no. 5, pp. 781–793, May 1995.
- [25] A. Y. Ng, M. I. Jordan, and Y. Weiss, "On spectral clustering: Analysis and an algorithm," in *Advances in Neural Information Processing Systems*, 2002, pp. 849–856.
- [26] S. A. Shah and V. Koltun, "Robust continuous clustering," *Proc. Natl. Acad. Sci. U. S. A.*, vol. 114, no. 37, pp. 9814–9819, 2017.
- [27] M. Ester, H.-P. Kriegel, J. Sander, and X. Xu, "A Density-Based Algorithm for Discovering Clusters in Large Spatial Databases with Noise," in *Proceedings of the 2nd International Conference on Knowledge Discovery and Data Mining*, 1996, pp. 226–231.
- [28] X. Guo, L. Gao, X. Liu, and J. Yin, "Improved deep embedded clustering with local structure preservation," in *IJCAI International Joint Conference on Artificial Intelligence*, 2017, pp. 1753–1759.

- [29] S. Geman and D. E. McClure, "Statistical methods for tomographic image reconstruction," *Bull. Int. Stat. Inst.*, vol. 52, no. 4, pp. 5–21, 1987.
- [30] L. Bottou, "Large-Scale Machine Learning with Stochastic Gradient Descent," in *Proceedings of COMPSTAT'2010*, Physica-Verlag HD, 2010, pp. 177–186.
- [31] X. Guo, X. Liu, E. Zhu, and J. Yin, "Deep Clustering with Convolutional Autoencoders," in *International conference on neural information processing*, 2017, vol. 10635 LNCS, pp. 373–382.
- [32] N. Mrabah, M. Bouguessa, and R. Ksantini, "Adversarial Deep Embedded Clustering: on a better trade-off between Feature Randomness and Feature Drift," *IEEE Trans. Knowl. Data Eng.*, pp. 1–1, 2020.
- [33] K. G. Dizaji, A. Herandi, C. Deng, W. Cai, and H. Huang, "Deep Clustering via Joint Convolutional Autoencoder Embedding and Relative Entropy Minimization," in *Proceedings of the IEEE International Conference on Computer Vision*, 2017, vol. 2017-Octob, pp. 5747–5756.
- [34] X. Glorot and Y. Bengio, "Understanding the difficulty of training deep feedforward neural networks," in *Journal of Machine Learning Research*, 2010, vol. 9, pp. 249–256.
- [35] J. Xie, R. Girshick, and A. Farhadi, "Unsupervised Deep Embedding for Clustering Analysis," in *International conference on machine learning*, 2016.
- [36] P. Huang, Y. Huang, W. Wang, and L. Wang, "Deep embedding network for clustering," in *22nd International conference on pattern recognition*, 2014, pp. 1532–1537.
- [37] B. Yang, X. Fu, N. D. Sidiropoulos, and M. Hong, "Towards K-means-friendly Spaces: Simultaneous Deep Learning and Clustering," 2017.
- [38] M. M. Fard, T. Thonet, and E. Gaussier, "Deep k-Means: Jointly clustering with k-Means and learning representations," *arXiv Prepr. arXiv1806.10069*, 2018.
- [39] D. Chen, J. Lv, and Z. Yi, "Unsupervised multi-manifold clustering by learning deep representation," in *AAAI Workshop - Technical Report*, 2017, vol. WS-17-01-, pp. 385–391.
- [40] R. Souvenir and R. Piess, "Manifold clustering," in *Proceedings of the IEEE International Conference on Computer Vision*, 2005, vol. I, pp. 648–653.
- [41] P. Ji, T. Zhang, H. Li, M. Salzmann, and I. Reid, "Deep subspace clustering networks," in *Advances in Neural Information Processing Systems*, 2017, vol. 2017-Decem, pp. 24–33.
- [42] P. Zhou, Y. Hou, and J. Feng, "Deep Adversarial Subspace Clustering," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2018, pp. 1596–1604.
- [43] X. Yang, C. Deng, F. Zheng, J. Yan, and W. Liu, "Deep spectral clustering using dual autoencoder network," in *Proceedings of the IEEE Computer Society Conference on Computer Vision and Pattern Recognition*, 2019, vol. 2019-June, pp. 4061–4070.
- [44] S. A. Shah and V. Koltun, "Deep Continuous Clustering," *arXiv Prepr. arXiv1803.01449*, 2018.
- [45] I. Goodfellow, Y. Bengio, and A. Courville, "Deep Learning," *Nature*, vol. 521, no. 7553, p. 800, 2016.
- [46] Z. Jiang, Y. Zheng, H. Tan, B. Tang, and H. Zhou, "Variational deep embedding: An unsupervised generative approach to Clustering," in *IJCAI International Joint Conference on Artificial Intelligence*, 2017, pp. 1965–1972.
- [47] N. Dilokthanakul et al., "Deep Unsupervised Clustering with Gaussian Mixture Variational Autoencoders," 2016.
- [48] D. P. Kingma, T. Salimans, R. Jozefowicz, X. Chen, I. Sutskever, and M. Welling, "Improved variational inference with inverse autoregressive flow," in *Advances in Neural Information Processing Systems*, 2016, pp. 4743–4751.
- [49] S. Mukherjee, H. Asnani, E. Lin, and S. Kannan, "ClusterGAN: Latent Space Clustering in Generative Adversarial Networks," *Proc. AAAI Conf. Artif. Intell.*, vol. 33, pp. 4610–4617, 2019.