

Volume 12 Issue 11

November 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 11 November 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: Performance Evaluation of SNMPv1/2c/3 using Different Security Models on Raspberry Pi

Authors: Eric Gamess, Sergio Hernandez

PAGE 1 – 9

Paper 2: Digital Economy and its Importance in the Development of Small and Medium Innovative Enterprises

Authors: Tatiana Korsakova, Lyudmila Dubanevich, Oleg Drozdov, Anna Mikhailova, Ekaterina Kamchatova

PAGE 10 – 17

Paper 3: Human Action Recognition in Video Sequence using Logistic Regression by Features Fusion Approach based on CNN Features

Authors: Tariq Ahmad, Jinsong Wu, Imran Khan, Asif Rahim, Amjad Khan

PAGE 18 – 25

Paper 4: Application-based Framework for Analysis, Monitoring and Evaluation of National Open Data Portals

Authors: Vigan Raca, Goran Velinov, Betim Cico, Margita Kon-Popovska

PAGE 26 – 36

Paper 5: Deep Learning for Arabic Image Captioning: A Comparative Study of Main Factors and Preprocessing Recommendations

Authors: Hani Hejazi, Khaled Shaalan

PAGE 37 – 44

Paper 6: Hardware Architecture for Adaptive Dual Threshold Filter and Discrete Wavelet Transform based ECG Signal Denoising

Authors: Safa MEJHOUDI, Rachid LATIF Wissam JENKAL, Amine Saddik, Abdelhafid EL OUARDI SATIE

PAGE 45 – 54

Paper 7: Machine Learning based Forecasting Systems for Worldwide International Tourists Arrival

Authors: Ram Krishn Mishra, Siddhaling Urolagin, J. Angel Arul Jothi, Nishad Nawaz, Haywantee Ramkissoon

PAGE 55 – 64

Paper 8: Analyzing the Sentiments of Jordanian Students Towards Online Education in the Higher Education Institutions

Authors: Bayan Alfayoumi, Mohammad Alshraideh, Saleh Al-Sharaeh, Martin Leiner, Iyad Muhsen AlDajani

PAGE 65 – 69

Paper 9: Comparative Study of Flooding Area Detection with SAR Images based on Thresholding and Difference Images Acquired Before and After the Flooding

Authors: Kohei Arai

PAGE 70 – 78

Paper 10: Developing of Middleware and Cross Platform Chat Application

Authors: Danny Sebastian, Restyandito, Kristian Adi Nugraha

PAGE 79 – 85

Paper 11: A Survey on Deep Learning Face Age Estimation Model: Method and Ethnicity

Authors: Hadi A. Dahlan

PAGE 86 – 101

Paper 12: Comparative Analysis of Supervised Machine Learning Techniques for Sales Forecasting

Authors: Stuti Raizada, Jatinderkumar R. Saini

PAGE 102 – 110

Paper 13: Machine Learning for Diagnosing Drug Users and Types of Drugs Used

Authors: Anthony Anggrawan, Christofer Satria, Che Ku Nuraini, Lusiana, Ni Gusti Ayu Dasriani, Mayadi

PAGE 111 – 118

Paper 14: Insights on Deep Learning based Segmentation Schemes Towards Analyzing Satellite Imageries

Authors: Natya S, Ramya K, Seema Singh

PAGE 119 – 129

Paper 15: DNA Profiling: An Investigation of Six Machine Learning Algorithms for Estimating the Number of Contributors in DNA Mixtures

Authors: Hamdah Alotaibi, Rashid Mehmood, Fawaz Alsolami

PAGE 130 – 137

Paper 16: Visualization of the Temporal Topic Model on Higher Education Preferences with Higher Education Ranking Indicators

Authors: Winda Widya Ariestya, Achmad Benny Mutiara, I Made Wiryana, Setia Wirawan

PAGE 138 – 143

Paper 17: Sparse Distributed Memory Approach for Reinforcement Learning Driven Efficient Routing in Mobile Wireless Network System

Authors: Varshini Vidyadhar, Nagaraj R, G Sudha

PAGE 144 – 152

Paper 18: A Systematic Review of Published Articles, Phases and Activities in an Online Social Networks Forensic Investigation Domain

Authors: Aliyu Musa Bade, Siti Hajar Othman

PAGE 153 – 160

Paper 19: Deep Learning based Neck Models for Object Detection: A Review and a Benchmarking Study

Authors: Sara Bouraya, Abdessamad Belangour

PAGE 161 – 167

Paper 20: Naïve Bayes Classification of High-Resolution Aerial Imagery

Authors: Asmala Ahmad, Hamzah Sakidin, Mohd Yazid Abu Sari, Abd Rahman Mat Amin, Suliadi Firdaus Sufahani, Abd Wahid Rasib

PAGE 168 – 177

Paper 21: Secured and Provisioned Access Authentication using Subscribed user Identity in Federated Clouds

Authors: Sudan Jha, Sultan Ahmad, Meshal Alharbi, Bader Alouffi, Shoney Sebastian

PAGE 178 – 187

Paper 22: Local Frequency Descriptor and Hybrid Features for Classification of Brain Magnetic Resonance Images using Ensemble Classifier

Authors: Shruthi G, Krishna Raj P M

PAGE 188 – 195

Paper 23: Mutual Informative Brown Clustering based Multiattribute Cockroach Swarm Optimization for Reliable Data Dissemination in VANET

Authors: D. Radhika, A. Bhuvaneswari

PAGE 196 – 203

Paper 24: Face Age Estimation and the Other-race Effect

Authors: Oluwasegun Oladipo, Elijah Olusayo Omidiora, Victor Chukwudi Osamor

PAGE 204 – 211

Paper 25: Polarity Detection of Dialectal Arabic using Deep Learning Models

Authors: Saleh M. Mohamed, Ensaf Hussein Mohamed, Mohamed A. Belal

PAGE 212 – 218

Paper 26: Challenges in Developing Virtual Reality, Augmented Reality and Mixed-Reality Applications: Case Studies on A 3D-Based Tangible Cultural Heritage Conservation

Authors: Ahmad Zainul Fanani, Khafiizh Hastuti, Arry Maulana Syarif, Prayanto Widyo Harsanto

PAGE 219 – 227

Paper 27: Trust-based Key Management Conglomerate ElGamal Encryption for Data Aggregation Framework in WSN using Blockchain Technology

Authors: T. G. Babu, V. Jayalakshmi

PAGE 228 – 236

Paper 28: Statistical Analysis for Revealing Defects in Software Projects: Systematic Literature Review

Authors: Alia Nabil Mahmoud, Vítor Santos

PAGE 237 – 249

Paper 29: A Hybrid Deep Neural Network for Human Activity Recognition based on IoT Sensors

Authors: Zakaria BENHAILI, Youssef BALOUKI, Lahcen MOUMOUN

PAGE 250 – 257

Paper 30: Bioinformatics Research Through Image Processing of Histopathological Response to Stonefish Venom

Authors: Mohammad Wahsha, Heider A. M. Wahsheh, Wissam Hayek, Haya Al-Tarawneh, Maroof Khalaf, Tariq Al-Najjar

PAGE 258 – 263

Paper 31: Real Time Distributed and Decentralized Peer-to-Peer Protocol for Swarm Robots

Authors: Mahmoud Almostafa RABBAH, Nabila RABBAH, Hicham BELHADAOUI, Mounir RIFI

PAGE 264 – 276

Paper 32: Improving Customer Churn Classification with Ensemble Stacking Method

Authors: Mohd Khalid Awang, Mokhairi Makhtar, Norlina Udin, Nur Farraliza Mansor

PAGE 277 – 285

Paper 33: Enhancing the Takhrij Al-Hadith based on Contextual Similarity using BERT Embeddings

Authors: Emha Taufiq Luthfi, Zeratul Izzah Mohd Yusoh, Burhanuddin Mohd Aboobaider

PAGE 286 – 293

Paper 34: UX Testing for Mobile Learning Applications of Deaf Children

Authors: Normala Mohamad, Nor Laily Hashim

PAGE 294 – 299

Paper 35: The Regularization Effect of Pre-activation Batch Normalization on Convolutional Neural Network Performance for Face Recognition System Paper

Authors: Abu Sanusi Darma, Fatma Susilawati Binti Mohamad

PAGE 300 – 310

Paper 36: Heuristics and Think-aloud Method for Evaluating the Usability of Game-based Language Learning

Authors: Kashif Ishaq, Fadhilah Rosdi, Nor Azan Mat Zin, Adnan Abid

PAGE 311 – 324

Paper 37: Towards Measuring User Experience based on Software Requirements

Authors: Issa Atoum, Jameel Almalki, Saeed Masoud Alshahrani, Waleed Al Shehri

PAGE 325 – 331

Paper 38: Machine Learning Driven Feature Sensitive Progressive Sampling Model for BigData Analytics

Authors: Nandita Bangera, Kayarvizhy N

PAGE 332 – 341

Paper 39: Thermal-aware Dynamic Weighted Adaptive Routing Algorithm for 3D Network-on-Chip

Authors: Muhammad Kaleem, Ismail Fauzi Bin Isnin

PAGE 342 – 348

Paper 40: A New Back-off Algorithm with Priority Scheduling for MQTT Protocol and IoT Protocols

Authors: Marwa O Al Enany, Hany M. Harb, Gamal Attiya

PAGE 349 – 357

Paper 41: Examining User Experience of Moodle e-Learning System

Authors: Layla Hasan

PAGE 358 – 366

Paper 42: Query Expansion based on Word Embeddings and Ontologies for Efficient Information Retrieval

Authors: Namrata Rastogi, Parul Verma, Pankaj Kumar

PAGE 367 – 373

Paper 43: A Novel Integrated Scheme for Detection and Mitigation of Route Diversion Attack in MANET

Authors: H C Ramaprasad, S. C. Lingareddy

PAGE 374 – 381

Paper 44: Multi-level Hierarchical Controller Assisted Task Scheduling and Resource Allocation in Large Cloud Infrastructures

Authors: Jyothi S, B S Shylaja

PAGE 382 – 394

Paper 45: A Review of a Biomimicry Swimming Robot using Smart Actuator

Authors: Muhammad Shafique Ashroff Md Nor, Mohd Aliff, Nor Samsiah

PAGE 395 – 405

Paper 46: Fuel Consumption Prediction Model using Machine Learning

Authors: Mohamed A. HAMED, Mohammed H.Khafagy, Rasha M.Badry

PAGE 406 – 414

Paper 47: Scalable and Reactive Multi Micro-Agents System Middleware for Massively Distributed Systems

Authors: EZZRHARI Fatima Ezzahra, EL ABID AMRANI Nouredine, YOUSSEFI Mohamed, BOUATTANE Omar

PAGE 415 – 426

Paper 48: Expert System in Enhancing Efficiency in Basic Educational Management using Data Mining Techniques

Authors: Fuseini Inusah, Yaw Marfo Missah, Najim Ussiph, Frimpong Twum

PAGE 427 – 434

Paper 49: Machine Learning for Predicting Employee Attrition

Authors: Norsuhada Mansor, Nor Samsiah Sani, Mohd Aliff

PAGE 435 – 445

Paper 50: Finding Good Binary Linear Block Codes based on Hadamard Matrix and Existing Popular Codes

Authors: Driss Khebbou, Reda Benkhoyya, Idriss Chana, Hussain Ben-azza

PAGE 446 – 451

Paper 51: EFPT-OIDS: Evaluation Framework for a Pre-processing Techniques of Automatic Optho-Imaging Diagnosis and Detection System

Authors: Sobia Naz, Radha Krishna Rao K. A, Shreekanth T

PAGE 452 – 462

Paper 52: A Delay-tolerant MAC Protocol for Emergency Care in WBAN Considering Preemptive and Non-preemptive Methods

Authors: Shah Murtaza Rashid Al Masud, Alope Kumar Saha

PAGE 463 – 473

Paper 53: Transformer based Contextual Model for Sentiment Analysis of Customer Reviews: A Fine-tuned BERT

Authors: Ashok Kumar Durairaj, Anandan Chinnalagu

PAGE 474 – 480

Paper 54: A New Energy-efficient Multi-hop Routing Protocol for Heterogeneous Wireless Sensor Networks

Authors: Rowayda A. Sadek, Doha M. Abd-alazeem, Mohamed M. Abbassy

PAGE 481 – 491

Paper 55: Improved GRASP Technique based Resource Allocation in the Cloud

Authors: Madhukar E, Raguathan T

PAGE 492 – 498

Paper 56: Ada-IDS: AdaBoost Intrusion Detection System for ICMPv6 based Attacks in Internet of Things

Authors: A. Arul Anitha, L. Arockiam

PAGE 499 – 506

Paper 57: Analytical Framework for Binarized Response for Enhancing Knowledge Delivery System

Authors: Chethan G S, Vinay S

PAGE 507 – 516

Paper 58: A Linguistic Analysis Metric in Detecting Ransomware Cyber-attacks

Authors: Diana Florea, Wayne Patterson

PAGE 517 – 522

Paper 59: Design and Implementation of Dynamic Packet Scheduling with Waiting Time Aware: DPSW2A

Authors: K Raghavendra Rao, B N Jagadesh

PAGE 523 – 529

Paper 60: Evaluating Domain Knowledge and Time Series Features for Automated Detection of Schizophrenia from EEG Signals

Authors: Saqib Hussain, Nasrullah Pirzada, Erum Saba, Muhammad Aamir Panhwar, Tanveer Ahmed

PAGE 530 – 535

Paper 61: Long Term Solar Power Generation Prediction using Adaboost as a Hybrid of Linear and Non-linear Machine Learning Model

Authors: Sana Mohsin Babbar, Chee Yong Lau, Ka Fei Thang

PAGE 536 – 545

Paper 62: HORAM: Hybrid Oblivious Random Access Memory Scheme for Secure Path Hiding in Distributed Environment

Authors: Snehalata Funde, Gandharba Swain

PAGE 546 – 553

Paper 63: Blockchain-based Secure Data Transmission for UAV Swarm using Modified Particle Swarm Optimization Path Planning Algorithm

Authors: M. Kayalvizhi, S. Ramamoorthy

PAGE 554 – 563

Paper 64: Resource Allocation in Spectrum Deployment for Cognitive Third-party Users

Authors: Arikatla Jaya Lakshmi, G. N. Swamy, M. N. Giri Prasad

PAGE 564 – 571

Paper 65: The Use of the Relational Concept in the Arabic Morphological Analysis

Authors: Said Iazzi, Abderrazak Iazzi, Saida Laaroussi, Abdellah Yousfi

PAGE 572 – 577

Paper 66: Development of Wearable System to Help Preventing the Spread of Covid-19 in Public Indoor Area

Authors: Annisa Istiqomah Arrahmah, Surya Ramadhan

PAGE 578 – 584

Paper 67: A Comparative Study of Segmentation Method for Computer-aided Diagnosis (CAD) Leukemia AML Subtype M0, M1, and M2

Authors: Wiharto, Wisnu Widiarto, Esti Suryani, Nurmajid Hidayatullah

PAGE 585 – 593

Paper 68: EC-Elastic an Explicit Congestion Control Mechanism for Named Data Networking

Authors: Asmaa EL-BAKKOUCHI, Mohammed EL GHAZI, Anas BOUAYAD, Mohammed FATTAH, Moulhime EL BEKKALI

PAGE 594 – 603

Paper 69: 1D-CNN based Model for Classification and Analysis of Network Attacks

Authors: Kuljeet Singh, Amit Mahajan, Vibhakar Mansotra

PAGE 604 – 613

Paper 70: Applying Grey Systems and Inverse Distance Weighted Method to Assess Water Quality from a River

Authors: Alexi Delgado, Anthonny Fernandez, Eduardo Lozano, Dennis Miguel, Félix León, Jhosep Arteta, Ch. Carbajal

PAGE 614 – 622

Paper 71: Unsupervised Machine Learning Approach for Identifying Biomechanical Influences on Protein-Ligand Binding Affinity

Authors: Arjun Singh

PAGE 623 – 629

Paper 72: Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes

Authors: Latifa Alzahrani

PAGE 630 – 637

Paper 73: Ontology-based Daily Menu Recommendation System for Complementary Food According to Nutritional Needs using Naïve Bayes and TOPSIS

Authors: Mujahidah Showafah, Sari Widya Sihwi, Winarno

PAGE 638 – 645

Paper 74: Emerging Requirement Engineering Models: Identifying Challenges is Important and Providing Solutions is Even Better

Authors: Hina Noor, Maheen Tariq, Anam Yousaf, Hafiz Wajid Ali, Arqam Abdul Moqeeet, Abu Bakar Hamid, Mahek Hanif, Huma Naz, Nabeel Tariq, Ijaz Amin, Osama Naseer

PAGE 646 – 656

Paper 75: An Advanced Ontology based Deep Learning for Computer-aided Interpretation of Mammography Images

Authors: Hamida Samiha Rahli, Nacéra Benamrane

PAGE 657 – 665

Paper 76: Electronic Commerce Product Recommendation using Enhanced Conjoint Analysis

Authors: Andrew Brian Osmond, Fadhil Hidayat, Suhono Harso Supangkat

PAGE 666 – 673

Paper 77: Normalisation of Indonesian-English Code-Mixed Text and its Effect on Emotion Classification

Authors: Evi Yulianti, Ajmal Kurnia, Mirna Adriani, Yoppy Setyo Duto

PAGE 674 – 685

Paper 78: Sign Language Gloss Translation using Deep Learning Models

Authors: Mohamed Amin, Hesahm Hefny, Ammar Mohammed

PAGE 686 – 692

Paper 79: Swapping-based Data Sanitization Method for Hiding Sensitive Frequent Itemset in Transaction Database

Authors: Dedi Gunawan, Yusuf Sulisty Nugroho, Maryam

PAGE 693 – 701

Paper 80: Software Security Static Analysis False Alerts Handling Approaches

Authors: Aymen Akremi

PAGE 702 – 711

Paper 81: CDRA: A Community Detection based Routing Algorithm for Link Failure Recovery in Software Defined Networks

Authors: Muhammad Yunis Daha, Mohd Soperi Mohd Zahid, Babangida Isyaku, Abdussalam Ahmed Alashhab

PAGE 712 – 722

Paper 82: A Reliable Lightweight Trust Evaluation Scheme for IoT Security

Authors: Hamad Aldawsari, Abdel Monim Artoli

PAGE 723 – 731

Paper 83: Multi-Criteria Decision-Making Approach for Selection of Requirements Elicitation Techniques based on the Best-Worst Method

Authors: Abdulmajeed Aljuhani

PAGE 732 – 738

Paper 84: e-Business Model to Optimise Sales through Digital Marketing in a Peruvian Company

Authors: Misael Lazo-Amado, Leoncio Cueva-Ruiz, Laberiano Andrade-Arenas

PAGE 739 – 748

Paper 85: A Fast and Efficient Algorithm for Outlier Detection Over Data Streams

Authors: Mosab Hassaan, Hend Maher, Karam Gouda

PAGE 749 – 756

Paper 86: Network Intrusion Detection System based on Generative Adversarial Network for Attack Detection

Authors: Abhijit Das, S G Balakrishnan, Pramod

PAGE 757 – 766

Paper 87: Near-ground Measurement and Modeling for Archaeological Park of Pisac in Cusco for LoRa Technology

Authors: Yhon D. Lezama, Jinmi Lezama, Jorge Arizaca-Cusicuna

PAGE 767 – 773

Paper 88: Development of Predictions through Machine Learning for Sars-Cov-2 Forecasting in Peru

Authors: Sha'om Adonai Huaraz Morales, Marissel Fabiola Mio Antayhua, Laberiano Andrade-Arenas

PAGE 774 – 784

Paper 89: Inclusive Education: Implementation of a Mobile Application for Blind Students

Authors: Alejandro Boza-Chua, Karen Gabriel-Gonzales, Laberiano Andrade-Arenas

PAGE 785 – 795

Paper 90: Design and Implementation of HSQL: A SQL-like language for Data Analysis in Distributed Systems

Authors: Anurag Singh Bhaduria, Atreya Bain, Jyoti Shetty, Shobha G, Arjuna Chala, Jeremy Clements

PAGE 796 – 803

Paper 91: Factors Influencing the Adoption of Cyber Security Standards Among Public Listed Companies in Malaysia

Authors: Mohamed Abdalla, Muath Jarrah, Ahmed Abu-Khadrah, Yusri bin Arshad

PAGE 804 – 810

Paper 92: Novel Algorithm Utilizing Deep Learning for Enhanced Arabic Lip Reading Recognition

Authors: Doaa Sami Khafaga, Hanan A. Hosni Mahmoud, Norah S. Alghamdi, Amani A. Albraikan

PAGE 811 – 816

Performance Evaluation of SNMPv1/2c/3 using Different Security Models on Raspberry Pi

Eric Gamess¹

MCIS Department
Jacksonville State University
Jacksonville, Alabama, USA

Sergio Hernandez²

Information Security
Citibank, New York
New York, USA

Abstract—The Simple Network Management Protocol (SNMP) is one of the dominant protocols for network monitoring and configuration. The first two versions of SNMP (v1 and v2c) use the Community-based Security Model (CSM), where the community is transferred in clear text, resulting in a low level of security. With the release of SNMPv3, the User-based Security Model (USM) and Transport Security Model (TSM) were proposed, with strong authentication and privacy at different levels. The Raspberry Pi family of Single-Board Computers (SBCs) is widely used for many applications. To help their integration into network management systems, it is essential to study the impact of the different versions and security models of SNMP on these SBCs. In this work, we carried out a performance analysis of SNMP agents running in three different Raspberry Pis (Pi Zero W, Pi 3 Model B, and Pi 3 Model B+). Our comparisons are based on the response time, defined as the time required to complete a request/response exchange between a manager and an agent. Since we did not find an adequate tool for our assessments, we developed our own benchmarking tool. We did numerous experiments, varying different parameters such as the type of requests, the number of objects involved per request, the security levels of SNMPv3/USM, the authentication and privacy protocols of SNMPv3/USM, the transport protocols, and the versions and security models of SNMP. Our experiments were executed with Net-SNMP, an open-source and comprehensive distribution of SNMP. Our tests indicate that SNMPv1 and SNMPv2c have similar performance. SNMPv3 has a longer response time, due to the overhead caused by the security services (authentication and privacy). The Pi 3 Model B and Pi 3 Model B+ have comparable performance, and significantly outperform the Pi Zero W.

Keywords—Simple network management protocol; SNMP; performance evaluation; benchmarks; raspberry pi

I. INTRODUCTION

The Simple Network Management Protocol (SNMP) is widely utilized for network monitoring and management. SNMPv1 and SNMPv2c use the Community-based Security Model (CSM), where the community (that can be seen as a password) is exchanged in cleartext between SNMP entities. This basic model of security opens many simple attacks against the protocol. Hence, a new version of SNMP was released and uses the User-based Security Model (SNMPv3/USM). The USM model brings strong authentication and privacy to SNMP. It was designed to work independently of other existing security infrastructures, and utilizes a separate user and key management infrastructure. Unfortunately, the

operational cost for deploying another user and key management infrastructure is significant, and network operators have been reluctant in its adoption [1]. To address this issue, the Transport Security Model (TSM) was later added to SNMPv3, and relies on well-accepted secure transport layers such as Secure Shell [2] (SSH), Transport Layer Security [3] (TLS), and Datagram Transport Layer Security [4] (DTLS).

The Raspberry Pi Foundation, a non-profit organization, has released a series of Single Board Computers (SBCs) that have been well-accepted by the community [5][6]. Due to its low cost (for approximately US\$10), the Raspberry Pi Zero W (RPi Zero W) is one of the best-selling SBCs of the foundation, and has a 32-bit single-core processor and a WiFi adapter. When more CPU power is required, users might consider the Raspberry Pi 3 Model B (RPi 3B) or the Raspberry Pi 3 Model B+ (RPi 3B+), both with a 64-bit quad-core processor, Ethernet, and WiFi, for approximately US\$35.

To facilitate the integration of Raspberry Pi SBCs into network management systems, we carried out an analytical performance analysis of different SNMP versions and security models for three different boards of the Raspberry Pi Foundation: (1) RPi Zero W, (2) RPi 3B, and RPi 3B+. To do so, we installed the agent of Net-SNMP [7], a well-known and comprehensive implementation of the SNMP protocol, on the three SBCs and ran some tests using a benchmarking tool that we developed. For better flexibility, the tool has numerous parameters and reports the “Response Time” defined as the required time to complete an SNMP request/response exchange between a manager and an agent. We performed intensive tests where we varied parameters such as the type of requests, the number of objects involved per request, the security levels of SNMPv3/USM, the authentication and privacy protocols of SNMPv3/USM, the transport protocols, and the versions and security models of SNMP. We think this study might be helpful for network administrators when integrating Raspberry Pis into SNMP-based network management systems.

The rest of the paper is structured as follows. Section II discusses the related work. An introduction to the SNMP protocol and its different versions and security models is made in Section III. We present the benchmark developed and used for the experiments in Section IV. The description of the test environment is done in Section V. Section VI reports and discusses the results of our evaluation of the SNMP protocol in many different scenarios. Finally, Section VII concludes the paper and gives directions for future work.

II. RELATED WORK

Some work has been done to evaluate the performance of SNMP. Andrey, Festor, Lahmadi, Pras, and Schönwälder [8] studied papers related to the evaluation of SNMP, in major research databases such as the IEEE Xplore and the ACM Digital Library. Their goal was to retrieve and classify techniques, approaches, and metrics employed by these studies, to propose a common framework for SNMP performance analysis. Hidalgo and Gamess [9] developed one of the first SNMP agents for Android smartphones with support for SNMPv1 and SNMPv2c. To validate the possibility of integrating them into network management systems, the authors did some performance evaluations of the maximum SNMP traffic that Android smartphones can support in a determined period of time. In their work, Corrente and Tura [10] analyzed the impact of security on SNMP, by considering SNMPv1, SNMPv2c, and SNMPv3/USM. They did experiments in a testbed and reported metrics such as the processing time, number of transactions per minute, CPU usage, and protocol overhead. To more efficiently use SNMP in mobile environments, the study in [11] proposed to add a superimposition model to its architecture. With simulations, the authors supported how the proposed superimposition architecture can improve the performance of SNMPv3/USM. Several studies are focused on comparing the performance of different network management solutions [12-16]. For example, the authors of [12] assessed the performance of SNMP-based and web services-based network monitoring systems. Their analysis was centered around SNMPv1 and SNMPv2c, and they reported results such as bandwidth usage, memory consumption, and roundtrip delay. Another work in this direction was done in [13], where Santos, Esteves, and Granville evaluated the performance of SNMP, NETCONF [17], and RESTful web services for router virtualization management. At the level of SNMP, the authors assessed SNMPv2c and SNMPv3/USM.

The previously mentioned efforts did not consider the new TSM model of SNMPv3. In the specialized literature, just a few projects have included this emerging standard. One of the first evaluations was done by Du, Shayman, and Rozenblit [18], before the publication of the RFCs that introduced the TSM model [19-21]. The authors modified the source code of Net-SNMP [7] and integrated the support of TLS [3] over TCP, for both SNMPv1 and SNMPv3. To demonstrate the viability of such a new development at the level of performance, the research team did some experiments in a testbed environment, and analyzed the performance of SNMPv1, SNMPv3/USM, and their non-standard SNMPv1 and SNMPv3 over TCP with TLS. A few years later, the work in [22] used a similar approach for SNMP over SSH. The authors did a non-standard modification of Net-SNMP [7] to carry SNMPv2c over SSH [2]. In a controlled environment, they assessed the performance of SNMPv2c and SNMPv3/USM, against their non-standard modified version of SNMPv2c over SSH. More recently, Schönwälder and Marinov [1] evaluated SNMPv3/USM and SNMPv3/TSM (with SSH, TLS, and DTLS) in a test environment. The testbed was made of computers connected through Ethernet. They reported metrics such as the response time to execute `snmpget` and `snmpwalk` (retrieving the

`ifTable` table [23]) commands, and the bandwidth utilization for `snmpwalk` (retrieving the `ifTable` table [23]). It is worth clarifying that `snmpget` and `snmpwalk` are basic applications shipped with Net-SNMP [7].

According to our search, the unique assessment work that covers SNMPv3/TSM and standard implementations of the protocols is described in [1]. Our paper not only includes SNMPv3/TSM, but we also believe that it will be of interest in the growing community of the Raspberry Pi [5][6].

III. INTRODUCTION TO SNMP AND ITS DIFFERENT VERSIONS AND SECURITY MODELS

The Simple Network Management Protocol (SNMP) was initially defined in August 1988 by RFC 1067 [24] as a protocol to monitor and control network devices, and it has been used extensively for over three decades now. SNMP allows configuring network devices remotely, collecting management data, and supporting the dissemination of event notifications [1]. Approved in 1990, SNMP became one of the main network protocols widely used as a de-facto standard by the industry to carry out the monitoring of assets for IP-based networks [25]. Nevertheless, the first version of SNMP, known as SNMPv1, is limited to meet all network management requirements that arise as a consequence of the interconnection complexity among systems, and is exposed to several security threats.

The architectural model of SNMP is straightforward and consists of network management stations, agents, and managed devices. Network management stations execute the applications which monitor and control network elements or managed devices. Agents are responsible for performing the network management functions requested by the network management stations, whereas managed devices may be hosts, gateways, terminal servers, switches, routers, among others.

The second version of SNMP, known as SNMPv2c, is an improvement of SNMPv1 without implementing security features. Neither SNMPv1 nor SNMPv2c can provide authentication, confidentiality, and integrity; therefore, they are exposed to multiple security threats, particularly those associated with authentication and privacy [26].

The third version of SNMP, known as SNMPv3, provides security features to the previous versions by introducing the User-based Security Model (USM), which is used to authenticate entities and provides encryption to secure the communication channel [10]. The authentication is performed using Hashed Message Authentication Code (HMAC) based on techniques such as Message Digest 5 (MD5) as well as Secure Hash Algorithm (SHA), while encryption for privacy is performed using Data Encryption Standard (DES) and Advanced Encryption Standard (AES), which are symmetric algorithms [27]. Also, SNMPv3 introduced a substantial complexity to SNMP architecture, since it implements its own user and key management infrastructure.

A. SNMPv1 and SNMPv2c

Both versions, SNMPv1 and SNMPv2c, rely on the Community-based Security Model (CSM) by which the community's name acts as a password and is transmitted over

the network in cleartext with the message. If the community's name is recognized, then the message should be processed. The use of the community's name without any encryption to verify that the message was sent by a trusted source is inherently insecure since it allows unauthorized individuals to capture it by using a packet analyzer or sniffer, and execute privileged actions. Hence, the security of the SNMP messages is dependent on the security of the channels over which the messages are sent.

SNMPv1 introduced five main Protocol Data Units: (1) `GetRequest`, (2) `GetNextRequest`, (3) `SetRequest`, (4) `GetResponse`, and (5) `Trap`. `GetRequest` is used by the manager to collect the value of one or more objects managed by the agent. The manager uses `GetNextRequest` message to request a series of consecutive variables managed by the agent. `SetRequest` is used by the manager to modify the value of one or more objects in a managed device. `GetResponse` is sent by agents to respond with data to get (`GetRequest` and `GetNextRequest`) and set (`SetRequest`) requests. `Trap` is used by the agent to notify that an event has occurred or that a condition is present. SNMPv1 does not allow manager-to-manager interactions [28].

Three new PDUs were added in SNMPv2c: (1) `GetBulkRequest`, (2) `InformRequest`, and (3) `Report`. The purpose of `GetBulkRequest` is the optimization of `GetNextRequest`, allowing to request the transfer of a large amount of data and reducing the number of requests and responses. `InformRequest` is used by a manager to send management information to other remote managers. Usage and precise semantics of `Report` are not specified; therefore, any SNMP administrative framework making use of this PDU must define it. SNMPv2c improved error-handling by including expanded error codes to differentiate types of error conditions reported through a single error code in SNMPv1 [29].

B. SNMPv3/USM

The User-based Security Model (USM) provides authentication and privacy capabilities at the SNMP message level. It defines three security levels that can be summarized as follows:

- Communication without authentication and privacy (`noAuthNoPriv`): From a security point of view, it is comparable to the CSM used by previous versions of SNMP. Neither authentication, nor encryption for privacy capabilities, are provided.
- Communication with authentication but without privacy (`authNoPriv`): It provides authentication. However, encryption for privacy is not provided by this level.
- Communication with authentication and privacy (`authPriv`): It provides both authentication and encryption for privacy capabilities.

The USM model implements its own user and key management infrastructure, making it unpractical to be implemented [1]. It relies on the existence of pre-shared keys between two communicating SNMP engines.

C. SNMPv3/TSM

The Transport Security Model (TSM) was designed to fit into the SNMP architecture as a Security Model that utilizes the services of a secure Transport Model. The TSM model does not provide security mechanisms such as authentication and encryption itself [19]. Instead, it was implemented to work with a variety of secure transport protocols, including Secure Shell [2] (SSH), Transport Layer Security [3] (TLS), and Datagram Transport Layer Security [4] (DTLS).

1) *SNMPv3/SSH*: The Secure Shell (SSH) protocol [2] is used for secure remote login and other secure network services over an insecure network. It comprises of three components:

- Transport Layer Protocol: it provides server authentication, confidentiality, integrity, and compression. It operates over a TCP connection, however, other reliable data streams can be used. Public-key cryptography is used to authenticate the server to the client and to establish a secure connection, which then uses a session key and a symmetric encryption algorithm to protect the connection.
- User Authentication Protocol: it authenticates the client-side user to the server and runs over the transport layer protocol. SSH can support multiple user authentication mechanisms including, but not limited to, password authentication, public-key authentication, and keyboard-interactive authentication (which supports challenge-response authentication mechanisms). Through the Generic Security Service Application Program Interface (GSS-API), SSH can also interact with the Kerberos protocol to authenticate users.
- Connection Protocol: it multiplexes the encrypted tunnel into several logical channels. It runs over the transport layer protocol and starts once the user authentication protocol has finished.

2) *SNMPv3/TLS*: The Transport Layer Security (TLS) protocol [3] provides authentication, integrity, and privacy at the transport layer. The TLS Transport Model (TLSTM) for SNMP consists of a model instantiation in the transport subsystem and details the elements of procedure for sending and receiving SNMP messages over TLS. TLSTM makes use of the X.509 public key infrastructure to provide authentication.

3) *SNMPv3/DTLS*: The Datagram Transport Layer Security (DTLS) protocol [4] is based on the TLS protocol and provides similar security capabilities. The main difference in comparison with TLS is that DTLS provides secure communication over unreliable datagram transports (e.g., UDP).

IV. METRICS AND BENCHMARKS

Let us define the "response time" as the time required for an SNMP manager to send a request and receive the associated response from the agent. We could not find a software tool on the Internet that fulfilled our need in computing the response

time with precision. Hence, we wrote our own benchmarking tool in the C programming language, using the Net-SNMP library [7]. Basically, a request/response exchange is done several times between our benchmarking tool and the agent. The benchmarking tool takes a timestamp before and after the interchange. The difference in timestamps is divided by the number of exchanges to get the average response time. Repeating the request/response exchange several times minimizes the error on the response time, due to low-precision clocks and any other processes that could be started by the operating systems and load the devices during the benchmark execution.

The benchmark has several parameters, including the version of SNMP, the community (only for SNMPv1 and SNMPv2c), the security name, security level (noAuthNoPriv, authNoPriv, and authPriv), the authentication protocol and passphrase, the privacy protocol and passphrase (only for SNMPv3/USM), the digital certificates for the benchmarking tool and the agent (only for SNMPv3/DTLS and SNMPv3/TLS), the number of sessions (numSessions), the number of requests/responses per session (sessionSize), the transport protocol (UDP, TCP, DTLS, and TLS), the IP address of the agent, and a list of parameters related to Object Identifiers (OIDs). The latter list will depend on the petitions. For example, for GetRequest and GetNextRequest petitions, it should be the list of OIDs to be resolved into values. For SetRequest petitions, it should be a list of triplets (OID to be altered, its type, and its new value). Fig. 1 gives the skeleton of the benchmark for computing the response time for a GetRequest petition. The line numbers have been added just for reference. Line 01 gets the starting timestamp. The external for-loop controls the number of sessions (numSessions). For each session, the internal for-loop controls the number of requests/responses per session (sessionSize). Each session consists of opening the session with the agent (Line 05), repeating the creation of the request (Line 07), exchanging the request and response with the agent (Line 09), and destroying the response once processed (Line 11), before closing the session (Line 13). Finally, Line 16 gets the ending timestamp, and the results are displayed.

```
01: gettimeofday(&timerStart, (struct timezone *) 0);
02: // Get the starting timestamp
03:
04: for(int i=0; i<numSessions; i++) {
05:   ss = snmp_open(&session); // Open an SNMP session
06:   for(int j=0; j<sessionSize; j++) {
07:     pdu = snmp_pdu_create(SNMP_MSG_GET); // Create request
08:     // Add pairs of (OIDs, null) to the request
09:     status = snmp_synch_response(ss, pdu, &response);
10:     // Process the response
11:     snmp_free_pdu(response);
12:   }
13:   snmp_close(ss); Close the SNMP session
14: }
15:
16: gettimeofday(&timerEnd, (struct timezone *) 0);
17: // Get the ending timestamp before showing the results
```

Fig. 1. Skeleton of the Code of the Benchmark to Compute the Response Time for a GetRequest.

V. DESCRIPTION OF THE TEST ENVIRONMENT

The testbed of Fig. 2 was used for the experiments. It consisted of a laptop, a wireless router, and SBCs from the Raspberry Pi Foundation. The laptop and SBCs were placed 4 meters from the wireless router, with no obstacles between them. Section V.A gives more details about the different models of SBCs (Raspberry Pi Zero W, Raspberry Pi 3B, and Raspberry Pi 3B+) that were used. The laptop had the following specifications: Microsoft Surface Book with an Intel Core i7-6600U CPU at 2.81 GHz, 16 GB of RAM, a 512 GB SSD, an NVIDIA GeForce GPU, and a Marvell AVASTAR Wireless-AC Network Adapter (dual-band wireless adapter with support to IEEE 802.11 a/b/n/g/ac). Debian amd64 10.11.0 was installed as the operating system. For the wireless network interconnection, a NETGEAR AC1200 Smart WiFi Router R6220 was employed. It had the following characteristics: an 880 MHz MediaTek processor with two radio bands (IEEE 802.11b/g/n in the 2.4 GHz band and IEEE 802.11a/n/ac in the 5 GHz band), 128 MB of flash, 128 MB of RAM, and five 10/100/1000 Mbps Ethernet ports (1 WAN and 4 LAN). In the 2.4 GHz band, the bandwidth can be set up to a maximum of 54, 145, or 300 Mbps. At the level of the 5 GHz band, a maximum of 173, 400, and 867 Mbps can be configured.

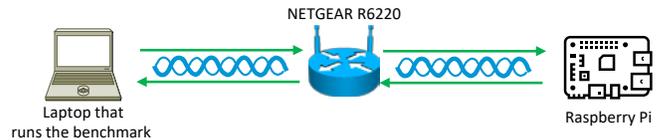


Fig. 2. Testbed for the Experiments.

A. Models of Raspberry Pi used in the Experiments

The Raspberry Pi Zero W (Raspberry Pi Zero W) is based on a 32-bit Broadcom BCM2835 single-core ARM1176JZF-S SoC @ 1.0 GHz, 512 MB of RAM, one 2.4 GHz IEEE 802.11b/g/n WiFi interface, one micro USB On-The-Go port, one mini HDMI connector, and one microSD card slot. The Raspberry Pi 3 Model B (Raspberry Pi 3B) is based on a 64-bit Broadcom BCM2837 quad-core Cortex-A53 SoC @ 1.2 GHz, 1 GB of RAM, one 10/100 Mbps Ethernet interface, one 2.4 GHz IEEE 802.11b/g/n WiFi interface, four USB 2.0 ports, one full-size HDMI connector, and one microSD card slot. The Raspberry Pi 3 Model B+ (Raspberry Pi 3B+) is based on a 64-bit Broadcom BCM2837B0 quad-core Cortex-A53 SoC @ 1.4 GHz, 1 GB of RAM, one Gigabit Ethernet interface over USB 2.0 (maximum throughput 300 Mbps), one dual-band 2.4 GHz and 5 GHz IEEE 802.11a/b/g/n/ac WiFi interface, four USB 2.0 ports, one full-size HDMI connector, and one microSD card slot.

B. Operating Systems for Raspberry Pi

Many operating systems are available for Raspberry Pi (e.g., Raspberry Pi OS, Debian, Ubuntu, RaspBSD, Kali Linux, OpenSUSE, RetroPie, LibreELEC, RISC OS). We opted for Raspberry Pi OS (32-bit), released in May 2021, which is the continuity of Raspbian (one of the most accepted OS for Raspberry Pi, worldwide). The Raspberry Pi Foundation offers three versions of this operating system that are compatible with all Raspberry Pi models: (1) Raspberry Pi OS Lite, (2) Raspberry Pi OS with Desktop, and (3) Raspberry Pi OS with Desktop and Recommended Software. The "Lite" version does

not have a GUI, and therefore it is faster since it does not have the full overload of a desktop environment. It is totally based on the command-line interface (terminal) and consists of 483 packages. The “Desktop” version has all the features of the “Lite” version, but also includes software such as Openbox as the window manager and LXDE (Lightweight X11 Desktop Environment) as the desktop environment. It consists of 1384 packages. The “Desktop and Recommended Software” version has all the “Desktop” version features, but also includes additional software such as LibreOffice, Firebird, Apache Ant, BlueJ, Greenfoot, OpenJDK Java Runtime Environment, OpenJDK Java Development Kit, Node.js, and Ruby. It consists of 2021 packages. We chose the “Lite” version since an SBC that is running an SNMP agent will most likely be headless, without the need of a GUI.

The Raspberry Pi Foundation also has a 64-bit version of its operating system that can be run only in 64-bit based hardware like the RPi 3B, RPi 3B+, RPi 4B, and RPi 400. That is, it is not suitable for the RPi Zero W. It is worth mentioning that it is still in the beta stage, and not directly advertised on the website of the Raspberry Pi Foundation, since they are still working on fixing issues that does not have the 32-bit version.

The performance of a Raspberry Pi will be noticeably affected by its microSD card. In the three SBCs, the original microSD card was replaced by a 64 GB SanDisk Extreme microSDXC UHS-I Memory Card (SDSQXA2-064G-GN6MA). It is considered as one of the fastest microSD cards of the market, with up to 160 MB/s and 60 MB/s for the reading and writing speeds, respectively.

C. Compiling Net-SNMP

Net-SNMP [7] is a widely used open-source, comprehensive implementation of the SNMP protocol. It has support for all the versions of SNMP and consists of an agent (snmpd) and several client applications (snmpget, snmpgetnext, snmpset, snmpbulkget, snmpwalk, etc). Precompiled packets for Net-SNMP v5.7.3 are available in the repositories of Raspberry Pi OS. However, at the level of SNMPv3, they were compiled to support the USM model, but not the TSM model. Hence, a newer version of Net-SNMP (v5.8) was compiled and installed in all the Raspberry Pis. To this end, the commands of Fig. 3 were executed. The required libraries were first installed from the repositories. At the configuration level, the security models (both USM and TSM) and the transport protocols (UDP, TCP, UDPIPv6, TCPIPv6, DTLSUDP, TLSTCP, and SSH) were specified.

Table I shows the necessary time for each phase of the compilation and installation process (configuration, compilation, and installation) for the different Raspberry Pis that were used in this work. These results can be beneficial, since they shed light on the power of each SBC.

```
apt-get install libssl-dev libperl-dev libssh2-1-dev
tar zxvf net-snmp-5.8.tar.gz
cd net-snmp-5.8
./configure --with-security-modules=usm,tsm \
--with-transport=UDP,TCP,UDPIPv6,TCPIPv6,DTLSUDP,TLSTCP,SSH
make
make install
```

Fig. 3. Commands to Compile and Install Net-SNMP.

TABLE I. COMPILATION TIMES OF NET-SNMP

Command	RPi Zero W	RPi 3B	RPi 3B+
./configure	15m42s	4m31s	4m3s
make	62m26s	14m14s	12m28s
make install	4m8s	1m18s	1m7s

It is worth clarifying that the recent versions of Net-SNMP [7] have experimental support for SNMPv3/SSH. Despite many efforts, this research team could not successfully install and use it. There is little documentation on setting the environment of SNMPv3/SSH. Hence, we did not report results related to this specific security model in this paper.

VI. PERFORMANCE RESULTS AND ANALYSIS

Here, we describe the common parameters selected for all our experiments:

- We configured the radios of the equipment in the 2.4 GHz band. The wireless router was set up to a maximum of 54 Mbps.
- Recent versions of SNMP can use UDP or TCP as the transport protocol. SNMP was initially designed for UDP, and will most likely be used with UDP since most SNMP agents are developed to use this protocol (it requires less computing power than TCP). Hence, otherwise stated, our experiments were done using UDP as the transport protocol.
- SNMPv3/USM has two authentication protocols (MD5 and SHA-1) and two privacy protocols (DES and AES). Unless otherwise specified, in our experiments with SNMPv3/USM, we selected SHA-1 as the authentication protocol and AES as the privacy protocol, when used. SHA-1 was preferred due to the attack on MD5 [30]. AES was selected since DES has a relatively short 56-bit key that is easily breakable with modern computers [31][32]. In January 1999, distributed.net and the Electronic Frontier Foundation were the first to collaborate and publicly broke a DES key in less than 23 hours.
- The OIDs retrieved and modified in our experiments were strings of 32 characters.
- For the experiments with SNMPv3/DTLS, self-signed certificates were generated, using the RSA algorithm with 2048-bit keys.

They are many parameters that can be varied to analyze their effects on the performance of SNMP. In this study, we considered parameters such as the type of requests, the number of objects involved per request, the security levels of SNMPv3/USM, the authentication and privacy protocols of SNMPv3/USM, the transport protocols, and the versions and security models of SNMP. Also, to get consistent results, it is worth mentioning that we repeated each experiment at least fifteen times, and the results presented in the study is an average of them.

A. Type of Requests Variation

This experiment aims to study how varying the type of requests can affect the performance of SNMP on a Raspberry Pi. The PDUs available in SNMP are version-specific. However, `GetRequest`, `GetNextRequest`, and `SetRequest` are present in all the versions, and therefore are the most commonly used requests. In this first experiment, we compared the response time of these three requests for SNMPv1, SNMPv2c, SNMPv3/USM, and SNMPv3/DTLS. The experiment is focused on sessions with a single request/response exchange. Table II shows the results for the RPi Zero W, RPi 3B, and RPi 3B+ as an agent. The differences between `GetRequest` and `GetNextRequest` petitions are not noticeable. However, the response time for a `SetRequest` is much longer, due to the reading and writing speed in the microSD card (maximum 160 MB/s and 60 MB/s for reading and writing speed, respectively).

At the level of the SNMP versions, SNMPv1 and SNMPv2c have very similar performances. SNMPv3/USM and SNMPv3/DTLS have much longer response times due to the overhead of the authentication and privacy mechanisms. It is also worth mentioning that in this experiment, SNMPv3/USM outperforms SNMPv3/DTLS, with minor differences.

In all the subsequent experiments, we focused on `GetRequest` petitions, since they are the most common petitions, and the majority of deployments of SNMP are focused on monitoring (not configuring), which requires massive `GetRequest` and `GetNextRequest` petitions, rather than `SetRequest`.

B. Number of OIDs Variation

In this experiment, the impact of the number of OIDs in the response time of a `GetRequest` petition is studied, and it was varied from 1 to 32. The experiment is focused on sessions with a single request/response exchange.

Fig. 4 and Fig. 5 depict the results obtained for SNMPv1 and SNMPv2c, respectively. Our study seems to indicate that both have a very similar performance.

TABLE II. RESPONSE TIME OF DIFFERENT REQUESTS (MILLISECONDS)

Type of Request	Version	RPi Zero W	RPi 3B	RPi 3B+
GetRequest	v1	2.97	2.02	1.71
	v2c	2.99	2.01	1.73
	v3/USM	3.51	2.24	2.15
	v3/DTLS	3.95	2.44	2.36
GetNextRequest	v1	2.98	2.08	1.74
	v2c	2.96	2.05	1.72
	v3/USM	3.53	2.31	2.20
	v3/DTLS	4.02	2.47	2.33
SetRequest	v1	151.27	127.44	122.35
	v2c	151.35	127.50	122.37
	v3/USM	155.32	131.74	126.92
	v3/DTLS	157.21	135.87	131.56

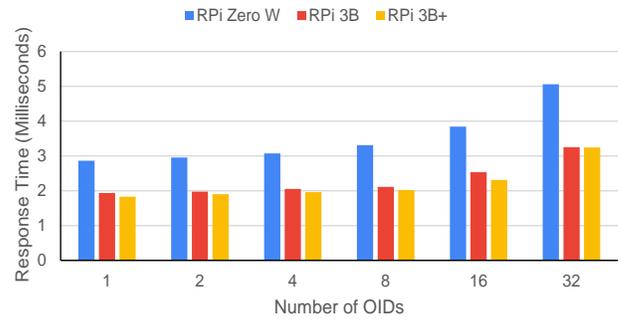


Fig. 4. Response Time for a GetRequest when Varying the Number of OIDs for SNMPv1.

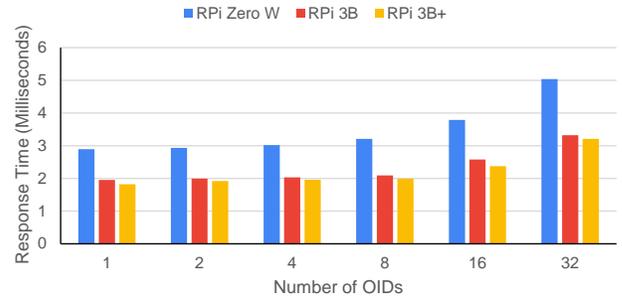


Fig. 5. Response Time for a GetRequest when Varying the Number of OIDs for SNMPv2c.

Fig. 6 and Fig. 7 show the results obtained for SNMPv3/USM with authPriv (SHA-1 and AES) and SNMPv3/DTLS, respectively. The response time for SNMPv3/USM is slightly longer than for SNMPv1 and SNMPv2c. SNMPv3/DTLS has the longest response time.



Fig. 6. Response Time for a GetRequest when Varying the Number of OIDs for SNMPv3/USM.

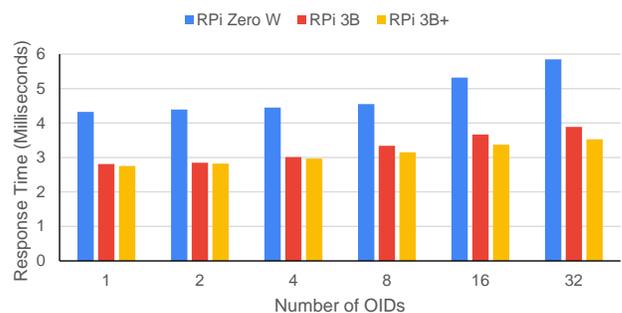


Fig. 7. Response Time for a GetRequest when Varying the Number of OIDs for SNMPv3/DTLS.

The tendency of this experiment indicates that the response time for a `GetRequest` will be linearly proportional to the number of OIDs. It is also noticeable that both the RPi 3B and the RPi 3B+ have similar results, which are much better than the RPi Zero W.

C. Security Level Variation for SNMPv3/USM using UDP and TCP as Transport Protocols for the RPi Zero W

The objective of this experiment is to analyze the impact of the security levels (noAuthNoPriv, authNoPriv, and authPriv) when using SNMPv3/USM on an RPi Zero W. The experiment is also aimed at understanding how the transport protocol (UDP or TCP) can affect the performance. To simplify the notation, let us abbreviate noAuthNoPriv as “nn”, authNoPriv as “an”, and authPriv as “ap”.

Fig. 8 depicts the total response time for our experiments for different numbers of requests/responses in a session (from 50 to 400 requests/responses). For each size of the session, six total response times are reported: (1) noAuthNoPriv with UDP, (2) noAuthNoPriv with TCP, (3) authNoPriv with UDP, (4) authNoPriv with TCP, (5) authPriv with UDP, and (6) authPriv with TCP. We selected SHA-1 and AES as the authentication and privacy protocols, respectively.

As indicated by our experiments, TCP has a slightly longer response time, but the differences with UDP are not significant. The variations due to the different privacy levels are more noticeable. As expected, noAuthNoPriv is the shortest response time, while authPriv is the longest.

D. Authentication and Privacy Protocols Variation for SNMPv3/USM using UDP as the Transport Protocol for the RPi Zero W

This experiment aims to assess the impact of the authentication protocols (MD5 and SHA-1) and the privacy protocols (DES and AES) when using SNMPv3/USM on an RPi Zero W.

Fig. 9 depicts the total response time of our experiments for different numbers of requests/responses in a session (from 50 to 400 requests/responses). For each size of the session, seven total response times are reported: (1) noAuthNoPriv, (2) authNoPriv with MD5, (3) authNoPriv with SHA-1, (4) authPriv with MD5 and DES, (5) authPriv with MD5 and AES, (6) authPriv with SHA-1 and DES, and (7) authPriv with SHA-1 and AES.

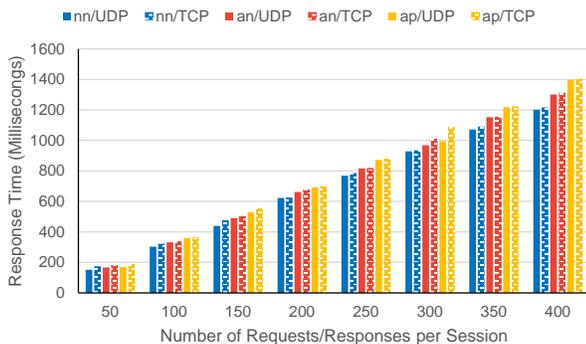


Fig. 8. Total Response Time for a Session of `GetRequest` for SNMPv3/USM when Varying the Security Level and the Transport Protocol.

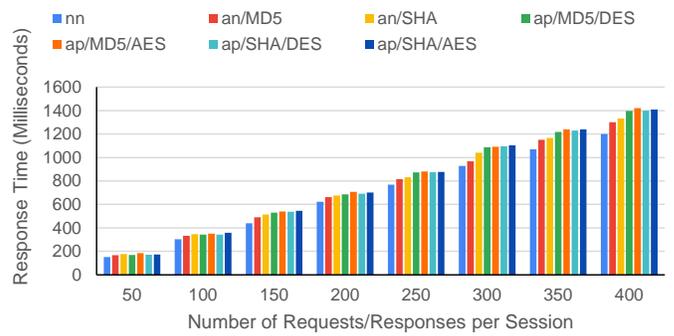


Fig. 9. Total Response Time for a Session of `GetRequest` for SNMPv3/USM when Varying the Authentication and Privacy Protocols.

Our results seem to indicate that MD5 is faster than SHA-1 as an authentication protocol. However, it is worth reminding that MD5 is now considered insecure [30]. Also, at the level of the privacy protocol, DES appears to be faster.

E. SNMPv3/USM vs SNMPv3/DTLS

In this experiment, we investigate the performance of SNMPv3/USM (SHA-1 and AES) vs. SNMPv3/DTLS on the RPi Zero W, RPi 3B, and RPi 3B+.

Fig. 10 depicts the total response time of our experiments for different numbers of requests/responses in a session (from 50 to 400 requests/responses). For each size of the session, six total response times are reported: (1) SNMPv3/USM (SHA-1 and AES) for RPi Zero W, (2) SNMPv3/DTLS for RPi Zero W, (3) SNMPv3/USM (SHA-1 and AES) for RPi 3B, (4) SNMPv3/DTLS for RPi 3B, (5) SNMPv3/USM (SHA-1 and AES) for RPi 3B+, and (6) SNMPv3/DTLS for RPi 3B+.

The best results are obtained by the RPi 3B+, while the worst correspond to the RPi Zero W. Also, this experiment confirmed that SNMPv3/USM has a better performance than SNMPv3/DTLS, as already mentioned in Section VI.A.

Notice that we also did experiments with SNMPv3/TLS. However, the obtained results were not stable at all, and we had significant variations of the response time from one test to another. Hence, we decided not to report them in this paper.

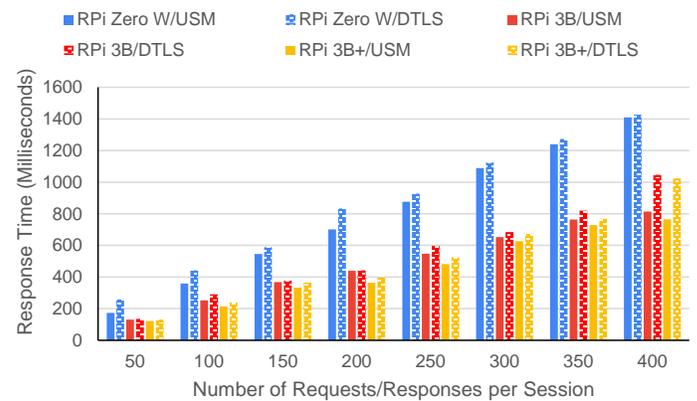


Fig. 10. Total Response Time for a Session of `GetRequest` for SNMPv3/USM and SNMPv3/DTLS.

F. Retrieving the Interface Table with snmpwalk when Varying the Number of Interfaces

As mentioned previously, Net-SNMP [7] has several client applications (snmpget, snmpgetnext, snmpset, snmpbulkget, snmpwalk, etc). In this experiment, we investigated the performance of snmpwalk by retrieving the interface table (ifTable [23]), when varying the numbers of interfaces, for SNMPv1, SNMPv3/USM (SHA-1 and AES), and SNMPv3/DTLS, on the RPi Zero W, RPi 3B, and RPi 3B+. snmpwalk uses GetNextRequest requests to query an agent for a portion of the object identifier space (e.g., a table). All objects in the subtree below a given OID are queried and their values are presented to the user. We varied the number of interfaces from 2 to 64, by creating additional dummy interfaces on the SBCs as specified in Fig. 11. The output of the application was discarded by redirecting it to /dev/null.

```
modprobe dummy
for i in $(seq $startValue $endValue)
do
echo "Creating interface eth${i} with address 10.0.0.${i}/32"
ip link add eth${i} type dummy
ip address add 10.0.0.${i}/32 dev eth${i}
ip link set up dev eth${i}
done
```

Fig. 11. Creation of Dummy Interfaces in the Agents.

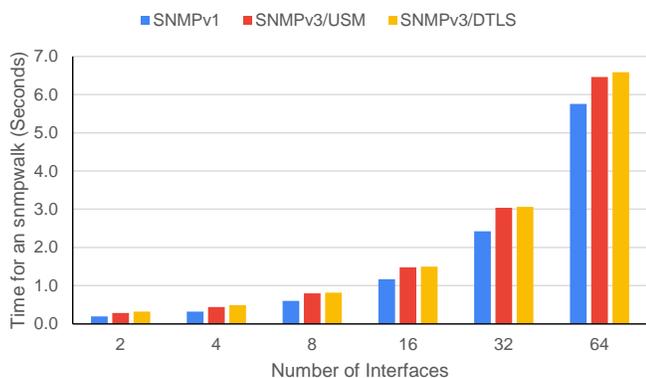


Fig. 12. Time to Retrieve the ifTable using Snmpwalk when Varying the Number of Interfaces for the RPi Zero W.

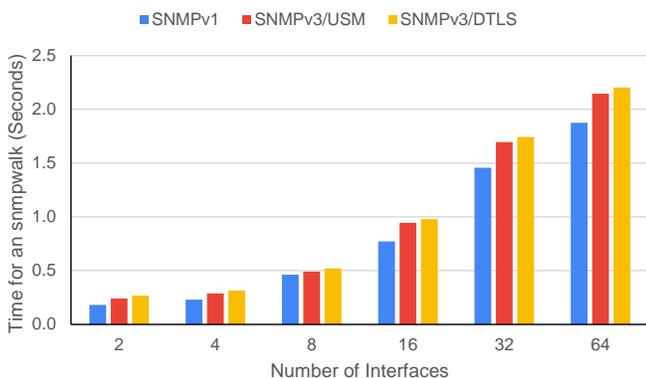


Fig. 13. Time to Retrieve the ifTable using Snmpwalk when Varying the Number of Interfaces for the RPi 3B.

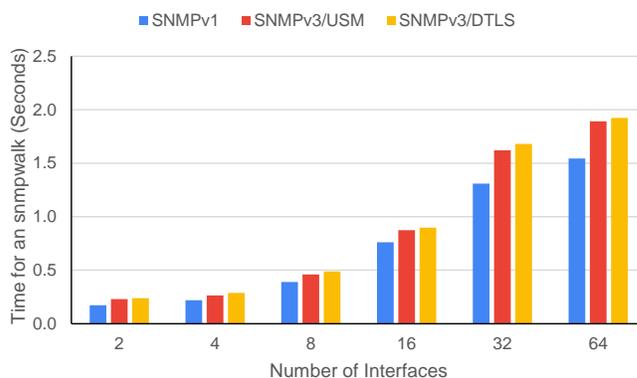


Fig. 14. Time to Retrieve the ifTable using Snmpwalk when Varying the Number of Interfaces for the RPi 3B+.

Fig. 12, 13, and 14 depict the time to retrieve the interface table (ifTable) through the snmpwalk application for the RPi Zero W, RPi 3B, and RPi 3B+, respectively. For small numbers of interfaces, SNMPv1 has results that are similar to the ones of SNMPv3/USM (SHA-1 and AES) and SNMPv3/DTLS. However, as the number of interfaces increases, the processing time becomes predominant over the transmission time, resulting in bigger differences between SNMPv1 and the other two versions of SNMP.

VII. CONCLUSION AND FUTURE WORK

Our experiments seem to indicate that SNMPv1 and SNMPv2c have similar performances. The assessment results of SNMPv3/USM and SNMPv3/DTLS are close to each other, with a slight advantage for the former. At the level of the SBCs, the RPi 3B and RPi 3B+ performed mostly equally, with the latter slightly outperforming the former. We found significant differences in the response time of GetRequest and SetRequest. We believe that these differences are due to the reading and writing access to the microSD cards (up to 160 MB/s and 60 MB/s for the reading and writing speeds, respectively).

Unfortunately, and despite all our efforts, we could not succeed in using SNMPv3/SSH with Net-SNMP. Also, SNMPv3/TLS gave inconsistent results from test to test, so we decided not to report them in this study.

As future work, we plan to evaluate SNMP, RESTCONF [17], and NETCONF [17] as management solutions in different scenarios. Also, with the growing adoption of IPv6, we are interested in analyzing the influence of the network protocol (i.e., IPv4 and IPv6) over the SNMP performance.

ACKNOWLEDGMENT

We are grateful to “Faculty Commons” and the “College of Science & Mathematics” at Jacksonville State University for partially funding this project.

REFERENCES

- [1] J. Schönwälder and V. Marinov, “On the Impact of Security Protocols on the Performance of SNMP,” IEEE Transactions on Network and Service Management, vol. 8, no. 1, March 2011, pp. 52–64.
- [2] M. Lucas, SSH Mastery: OpenSSH, PuTTY, Tunnels and Keys, Tilted Windmill Press; 2nd edition, February 2018.

- [3] E. Rescorla, The Transport Layer Security (TLS) Protocol Version 1.3, RFC 8446, August 2018.
- [4] E. Rescorla, H. Tschofenig, and N. Modadugu, The Datagram Transport Layer Security (DTLS) Protocol Version 1.3, Draft IETF, April 2021.
- [5] S. Monk, Programming the Raspberry Pi: Getting Started with Python, McGraw-Hill Education TAB, 3rd edition, June 2021.
- [6] L. Clark, Raspberry Pi 4: The Ultimate Step-by-Step Guide to Using Raspbian to Create Incredible Projects and Expand Your Programming Skills with the Latest Version of Raspberry Pi, independently published, February 2021.
- [7] Net-SNMP Home Page, <http://www.net-snmp.org>.
- [8] L. Andrey, O. Festor, A. Lahmadi, A. Pras, and J. Schönwälder, "Survey of SNMP Performance Analysis Studies," International Journal of Network Management, vol. 19, 2009, pp. 527–548.
- [9] F. Hidalgo and E. Gamess, "Integrating Android Devices into Network Management Systems based on SNMP," International Journal of Advanced Computer Science and Applications, vol. 5, no. 5, 2014, pp. 1–8.
- [10] A. Corrente and L. Tura, Security Performance Analysis of SNMPv3 with Respect to SNMPv2c, in Proceedings of the 2004 IEEE/IFIP Network Operations and Management Symposium (NOMS 2004), Seoul, South Korea, April 2004.
- [11] F. Duarte and A. Loureiro, "Performance Evaluation and Scalability Analysis of SNMPv3 with Superimposition in a Mobile Environment," Concurrent Engineering Research and Applications, vol. 9, no. 2, June 2001, pp 139–145.
- [12] A. Pras, T. Dreviers, R. van de Meent, and D. Quartel, "Comparing the Performance of SNMP and Web Services-Based Management," IEEE Transactions on Network and Service Management, vol. 1, no. 2, December 2004.
- [13] P. Santos, R. Esteves, and L. Granville, Evaluating SNMP, NETCONF, and RESTful Web Services for Router Virtualization Management, in Proceedings of the 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM 2015), Ottawa, ON, Canada, May 2015.
- [14] M. Ślabicki and K. Grochla, Performance Evaluation of SNMP, NETCONF and CWMP Management Protocols in Wireless Network, in Proceedings of the 4th International Conference on Electronics, Communications and Networks, Beijing, China, December 2014.
- [15] M. Ślabicki and K. Grochla, Performance Evaluation of CoAP, SNMP and NETCONF Protocols in Fog Computing Architecture, in Proceedings of the 2016 IEEE/IFIP Network Operations and Management Symposium (NOMS 2016), Istanbul, Turkey, April 2016.
- [16] Q. Gu and A. Marshall, Network Management Performance Analysis and Scalability Tests: SNMP vs CORBA, in Proceedings of the 2004 IEEE/IFIP Network Operations and Management Symposium (NOMS 2004), Seoul, South Korea, April 2004.
- [17] B. Claise, J. Clarke, and J. Lindblad, Network Programmability with YANG: The Structure of Network Automation with YANG, NETCONF, RESTCONF, and gNMI, Addison-Wesley Professional, 1st edition, May 2019.
- [18] X. Du, M. Shayman, and M. Rozenblit, Implementation and Performance Analysis of SNMP on a TLS/TCP Base, in Proceedings of the 2001 IEEE/IFIP International Symposium on Integrated Network Management, Seattle, WA, USA, May 2001.
- [19] D. Harrington and W. Hardaker, Transport Security Model for the Simple Network Management Protocol (SNMP), RFC 5591, June 2009.
- [20] D. Harrington, J. Salowey, and W. Hardaker, Secure Shell Transport Model for the Simple Network Management Protocol (SNMP), RFC 5592, June 2009.
- [21] W. Hardaker, Transport Layer Security (TLS) Transport Model for the Simple Network Management Protocol (SNMP), RFC 6353, July 2011.
- [22] V. Marinov and J. Schönwälder, "Performance Analysis of SNMP over SSH," Lecture Notes in Computer Science, vol. 4269. Springer, Berlin, Heidelberg, 2006. https://doi.org/10.1007/11907466_3
- [23] K. McCloghrie and M. Rose, Management Information Base for Network Management of TCP/IP-based Internets: MIB-II, RFC 1112, March 1991.
- [24] J. Case, M. Fedor, M. Schoffstall, and J. Davin, A Simple Network Management Protocol, RFC 1067, August 1988.
- [25] M. Julian, Practical Monitoring: Effective Strategies for the Real World. O'Reilly, 1st edition, November 2017.
- [26] D. Harrington, R. Presuhn, and B. Wijnen, An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks, RFC 3411, December 2002.
- [27] U. Blumenthal and B. Wijnen, User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3), RFC 3414, December 2002.
- [28] R. Presuhn, J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP), RFC 3416, December 2002.
- [29] J. Case, K. McCloghrie, M. Rose, and S. Waldbusser, Protocol Operations for version 2 of the Simple Network Management Protocol (SNMPv2), RFC 1448, April 1993.
- [30] T. Xie, F. Liu, and D. Feng, "Fast Collision Attack on MD5," IACR Cryptology ePrint Archive, vol. 2013, 2013.
- [31] M. Curtin, Brute Force: Cracking the Data Encryption Standard, Copernicus; 2005th edition, February 2005.
- [32] E. Biham and A. Biryukov, "An Improvement of Davies' Attack on DES," Journal of Cryptology, vol. 10, June 1997, pp. 195-205.

Digital Economy and its Importance in the Development of Small and Medium Innovative Enterprises

Tatiana Korsakova¹

Advanced Doctorate in Pedagogics
Associate Professor

Department of Management and Innovational Technologies
Institute of Management in Economical
Ecological and Social Systems
Southern Federal University
Taganrog, Russia

Lyudmila Dubanevich²

PhD in Economics
Associate Professor
Department of Economics
Moscow Economic Institute
Moscow, Russia

Oleg Drozdov³

PhD in Economics, Associate Professor
Faculty of Economics, Department of Economic Theory
St Petersburg University, St Petersburg, Russia

Anna Mikhailova⁴

PhD in Economics, Associate Professor
Department of Sociology and Human Resource Management
Finance and Economic Institute
North-Eastern Federal University, Yakutsk, Russia

Ekaterina Kamchatova⁵

Advanced Doctorate in Economics, Associate Professor
Department of Innovation Management
Institute of Industry Management
State University of Management, Moscow, Russia

Abstract—A single universally accepted definition, levels and interconnections of digital economy with other economies is not yet developed. Thus, various definitions of the digital economy have been investigated, as well as various approaches to describing the process of transformation of the digital economy for the correct establishment of these relationships. The article observes the relationship between the state of the digital economy, innovative small and medium enterprises, the development of small and medium businesses in general. The stage of transformation of the digital economy of Russia is determined at the second, intermediate stage of development and the main barriers to moving to the third level are pointed out. The dual role of the digital economy in the development of small and medium innovative enterprises is determined based on the selected model of R. Bukht & R. Heeks, the two directions of influence being the SMEs provision with necessary tools and the digital economy becoming the object of innovative development of SMEs. Finally, the assessment of the state of digital economy in Russia is given and the recommendations for its further implementation are given.

Keywords—Business; SMEs; entrepreneurship; Russia; digitalization

I. INTRODUCTION

The intensive development of information technology at the end of the 20th, beginning of the 21st century became an extraordinary phenomenon in terms of its scale and degree of influence and attracted great attention of the scientific community [1]. The patterns of implementation and digital products in all major areas of human activity: management, production, science, education, defense, medicine, etc. are

carefully studied by Russian and foreign researchers [2]. Such terms as digital economy (hereinafter referred to as DE) and digitalization of the economy are most often used to describe this level and the corresponding transformation process. In the context of studies related to the research of CE, the terms “innovation”, “innovative development”, and “innovative enterprise” usually appear.

The genesis of the above concepts, an accurate description of their characteristics and components seems to be a prerequisite for the correct description of the innovative capabilities of small and medium-sized businesses (hereinafter SMBs, SMEs) in the context of DE. The article discusses the history of the appearance of these concepts, marks the stages of transformation of their content in this regard.

Researchers in Russia and abroad use various interpretations and approaches in determining DE, innovative development of SMEs. The authors conducted an analysis of the formulations of Walter Oyken, specialists of the McKinsey Global Institute, the Global Development Institute, as well as the definitions of other researchers on the reviews [3, 4] in this regard. Then, despite the sufficient accuracy and clarity of the two-level approach of Professor R. M. Meshcheryakov [5], a choice was made in favor of the three-level approach of R. Bukht and R. Heeks with the third component, reflecting a qualitative change in the relationship of the digital economy and society [6]. The decision is dictated by the relevance of the model of R. Bukht and R. Heeks to the context of this work, as well as the possibility of an adequate representation of the process of phased development of DE within the

framework of a three-level approach. It should be emphasized that the two-level approach of Professor Meshcheryakov precisely describes this process in modern Russia, which is at the stage of transition to the third level of the Bukht-Heeks.

A similar study was conducted in relation to the concepts of “innovative enterprise”, innovative SMEs. A clear distinction of concepts allows us to differentiate the capabilities of SMEs and large businesses in a digital economy. The innovation potential is determined by their ability to detect, disclose, adapt and use new knowledge [7]. Innovative business development requires innovative approaches to its management as well [8]. The results of the study indicate the dual nature of the impact of DE conditions on the development of innovative small and medium endeavors, as well as on the development of SMEs in general. The inevitability of both positive and negative impacts on business depending on the direction of entrepreneurial activity was noted in particular.

II. LITERATURE REVIEW

The term “digital economy” was introduced by N. Negroponte in 1995 (according to other sources — Tapscott, 1996) to indicate the circulation of content on digital media characteristic of that era (music, films, pictures, games, etc.) [2]. The term “digital economy” continued to denote a relatively narrow segment of the production of digital products, the field of retail, and various services using the Internet, as well as services that ensure the development of the Internet services sector itself until 2005–2010. A similar outdated interpretation is still found in scientific articles, despite its obvious inadequacy due to the transformation of the concept’s content. Digital technologies have transformed from a market niche for specialists to general-purpose technologies that affect all sectors of the economy and society over the past twenty years [4]. The changes are so noticeable and so significant that the transformation of the content of DE concept can serve as a good example of the transition from quantity into quality. To describe qualitative changes, the initial, “classical” interpretation of the content of DE is no longer suitable. New approaches are required for this.

The wording given by Professor B. Panshin [2] will be used in this work. Interpretation of R. Meshcheryakov involves two levels [5]:

1) The classic one: the digital economy is presented as part of the economy that arose with the advent of digital technologies in the implementation of electronic goods and services (e-learning, sale of media content, telehealth, etc.);

2) The advanced one: social (economic) production using digital technologies. This is not just about e-goods, it means the whole chain of goods and services produced using digital technologies (logistics, Internet of things, Industry 4.0, a smart factory, fifth-generation communication networks, engineering services, prototyping, etc.).

DE is a part of the general economy at the first stage, and it is already a way of social production at the second stage. Indeed, today any country where the Internet is used as a first-level digital economy in accordance with the signs of the

classic and expanded interpretation of DE concept. The level will not change until the transition to Industry 4.0 and when the entire social product is created using digital technology in general. With this classification, the digital economy of Nigeria, Brazil, and Russia is at the first “classical level”, which is possible only with very rough and primitive gradations.

An analysis of the two-level approach of R. Meshcheryakov indicates its certain incompleteness, insufficient accuracy of determining the second level (stage). To identify this shortcoming, attention should be paid to the following fact. The second paragraph includes the Internet of things (IoT), Industry 4.0, but they are included along with logistics, engineering services, and prototyping. Meanwhile, it is widely believed that such phenomena as IoT and Industry 4.0 indicate the onset of the fourth industrial revolution today [9], [10], [11]. Since revolutionary changes mean a sharp transition to something qualitatively new, the emergence of IoT, the emergence and development of Industry 4.0 means a qualitative transition to a new level of the digital economy.

This important point was ignored in the classification of R. Meshcheryakov. Such significant phenomena as IoT and Industry 4.0 are presented in it as a simple extension of the scope of the application of digital technologies. This view is incorrect since the Internet of things and the fourth-generation industry are changing the way of production and the economy as a whole even more dramatically than the use of steam and electricity in due time. An enterprise of level 4.0 with digital prototyping, 3D printing, and robotic production is able to control the operation of the product without human intervention, make design changes, plan production, manufacture, and supply already updated products. Moreover, all this in the case of physical products, as for digital products, this is no marvel any more.

Thus, the second stage in the classification of Meshcheryakov is not expansion, but a qualitative revolutionary change in the industry. This could be named a revolutionary change in the whole way of social production if added to this is the transition to 5th generation communication networks, robotic logistics, and digital services. Under such circumstances, dividing DE into two levels: initial and “revolutionary high” seems to be overly primitive method of classification. It becomes logical to conclude that it is necessary to highlight an additional stage in the formation of the concept of the “digital economy”.

The authors formulated their own concept and definition of DE: “part of the total production volume, which is wholly or mainly produced on the basis of digital technologies by firms whose business model is based on digital products or services”. Three stages are distinguished.

In reality, since the third level is added in the process of transformation, the previous ones do not disappear. Moreover, the volumes of products manufactured on them can increase with a transition to a higher level in absolute terms, although their share in the volume of DE is declining in relative terms. The nominal value of DE stage (level) is determined by the prevailing level in its composition. A schematic image of the levels is [6]:

1) Digital (IT/ICT) sector (includes components production, Software and IT consulting, information services, telecommunications).

2) Digital economy (includes digital services, platform economy, sharing economy, Gig economy).

3) Digitalized economy (includes digital trade, industry 4.0, precision agrotechnics, algorithm economy).

It shows that the previous levels do not disappear but are part of the next. Almost 100% penetration of digital technologies is not only in all types of business but also in all areas of activity as a whole in accordance with the ideology of the model for this stage.

The distinction of the proposed levels is not indisputable but deserves attention. If the production of components is replaced with the production of “electronic goods”, then it is completely identical to the first level of R. Meshcheryakov. The content and boundaries of the 2nd and 3rd levels are undeniable, with the exception of the location of electronic commerce. This type of digital business should be considered an attribute of the 2nd level rather than a sign of the 3rd due to its massive distribution already at the border of the 1st and 2nd levels.

In the research existing scientific works were analysed in order to establish patterns of DE development and identify various aspects of its impact on the innovative development of SMEs. It allowed formulating and confirming the hypothesis of the dual influence of DE factors on business entities, to determine the types of activities that provide additional benefits, or vice versa, additional difficulties.

Transformation of the common using effects of new technologies in the digital level has its effect on each one branch of economics or social activity and characterizes digital economics. One of the indexes that describe the level of economic digitalization is the global connectivity index (GCI) that is presented by “Huawei Technologies Co. Ltd.” For this index creating has been analyzed 40 indicators of two groups of parameters: performance parameters and technological parameters to ensure transformation into the DE. And Huawei Technologies presents GCI each year. Has to be noted, there is data about the close directly proportional relationship of the GCI and Gross Domestic Product of the country [12], [13], [14].

The comparison of statistical Data from the Federal State Statistics Service (Rosstat), the Central Bank, specialized state and non-governmental institutions, as well as data from international organizations: the UN, the World Bank, the OECD, the EBRD, etc. was used as an empirical method. And a significant contribution to understanding the role of DE gives the legal base in the Russian Federation.

The system of procedures used provided an opportunity for a fairly clear idea of the dynamics of the role of DE in the innovative development of SMEs in the period 1990–2018 in general and it’s most likely value in the mid-term perspective.

III. GENERALIZATION OF THE MAIN STATEMENTS

To show the level of DE in RF it is necessary to consistently receive answers to questions by the presence of signs of all three levels. The results of the verification by attributes are presented in Table I.

It can be seen that DE in Russia is in a transitional state. So, all the signs of the 1st and 2nd levels are present, and part of the signs of the 3rd level: network business and electronic commerce [15]. GCI also demonstrates the little level of the DE. So, according to this index for 2020 the highest level of the country digitalization belongs to the United States (GCI score – 87), Singapore (GCI score – 81), and Switzerland (GCI score – 81). RF has gotten only 42 position (GCI score – 50) [16]. The RF economy of free earnings is slightly present, in the volume corresponding to the second level, the economy of joint consumption is even less noticeable, but both sectors are developing rapidly. It is important to note that often the term e-commerce is confused with the concept of e-business, which is significantly differentiated [15].

The transition to the third level depends on the development of two areas: Industry 4.0 and agricultural engineering. Not necessary to take specific types of agricultural machinery (plow, seeder), but, on the whole, agricultural culture as a complex of technologies at all levels of agricultural production, e.g. implementations of universal smart machines [17]. The transition to digital technologies in the agricultural sector will be primarily constrained by human resources and the existing material base. At the moment, both do not allow starting the introduction of DE, but there is the possibility of using innovative ICTs. For example, SMEs in agriculture could participate in international trade on the basis of the platform of the Unified Information Internet Space of the Agro-Industrial Complex [18] to increase the role of DE in developing the innovative component of SMEs.

TABLE I. PIECES OF EVIDENCE OF DE IN RUSSIA FOR RANKING BY THE BUKHT AND HEKS MODE

Evidence	Presence
Production of digital products	+
Information services	+
Software, IT consulting	+
Telecommunications	+
Digital services	+
Platform economy	±
Gig economy	±
Sharing economy	±
E-business	+
E-commerce	+
Industry 4.0	–
Precision agriculture	–
Algorithmic economy	–

In the world and Russian practice, the criteria for classifying a business as "small business" or "medium-sized" business is applied. The concept of "development of innovative SMEs" implies two components in the general case:

- Application of innovations and innovative technologies in the business processes of SMEs;
- SME participation in the innovative development of the economy.

The points are not conflicting. So, it is necessary to establish the role of DE in the application of innovations in SME business processes and consider the relationship between DE and the participation of SMEs in various innovative processes.

It is introduction of ICT and digital technologies in general (accounting IC, Internet, CPM, CAD systems, etc.) starting from about the 80s of the last century and to the present moment. Both of them are products of the DE.

An analysis of the global experience of innovative development indicates the significant role of SMEs in this process [19]. The following facts testify to this. 80% of the patents for the most important inventions of the 20th century were obtained by representatives of SMEs in the USA and Western Europe and belong to small firms. In the 21st century, according to the US National Science Foundation, the share of SMEs in the total number of high-tech companies approaches 90% [20]. The situation in Western Europe looks similar. Here, the distribution by country of the number of subjects of innovative SMEs in the total number of industrial enterprises is: 75% in Ireland, 66% in Germany, 49% in Finland, 46% in France, 40% in Italy, 39% in UK [21].

If we are looking at GCI, the leader in Europe in 2020 is Switzerland with a GCI score of 81. Other European countries' GCI rate is demonstrated in Table II.

So, Russia (GCI Score – 50) is in the near GCI level with Romania and Belarus (GCI Score 50 and 46, accordingly).

An analysis of Russian and foreign sources allow to highlight the following characteristic features of the participation of SMEs in the innovative development of production:

1) The SME sector is very active abroad in the field of innovative entrepreneurship, actively investing in research and development. The share of this sector in R&D expenditures is more than 30% in OECD countries. It fluctuates at the turn of 70% in Iceland and New Zealand [22]. The main source of R&D funding is the state in Russia. The total share of SMEs and large businesses in R&D expenses amounted to only 28% in 2015. Companies in the SME sector are initiating the bulk of innovation in the US. The following facts are cited in favor of this conclusion. SME receives 13 times more patents, implements twice as many inventions, implementation terms are half as fast as those of large corporations in the USA. The share of SME is ~ 50% of all innovations and latest technologies that form the level of scientific and technical

progress [23]. The share of innovative enterprises is 23% of the total number of SMEs in the European Union [22].

2) SMEs effectively ensure the transit of innovations from scientific developments to the applied sphere and reduce the time and cost of commercializing the results of research. SMEs demonstrate their willingness to work in conditions of high risk and uncertain market prospects.

3) The compact and flexible structure of SMEs is able to quickly adapt, and in favorable conditions, to quickly scale up the business.

4) The innovative activity of SMEs is highly effective. R&D cost-effectiveness in SME is four times higher than in a larger business, according to the US National Science Foundation. There is also evidence showing that innovative SMEs create 2.5 times more innovations per employee, while their implementation is faster and costs are 75% lower than for larger companies. [20], [21], [24].

TABLE II. GLOBAL CONNECTIVITY INDEX RATE OF THE EUROPEAN COUNTRIES [16]

Rank	ID	Country	GCI Score
3	CH	Switzerland	81
4	SE	Sweden	80
5	DK	Denmark	77
6	FI	Finland	76
7	NL	Netherlands	75
8	GB	United Kingdom	75
10	NO	Norway	73
14	LU	Luxembourg	70
15	DE	Germany	70
16	FR	France	70
18	IE	Ireland	69
19	BE	Belgium	66
20	AT	Austria	66
23	ES	Spain	61
24	EE	Estonia	61
25	PT	Portugal	61
26	IT	Italy	60
27	LT	Lithuania	58
28	CZ	Czech Republic	57
29	SI	Slovenia	56
31	HU	Hungary	54
32	SK	Slovakia	54
35	GR	Greece	52
36	BG	Bulgaria	52
38	HR	Croatia	51
39	PL	Poland	51
41	RO	Romania	50
47	BY	Belarus	46
51	RS	Serbia	45
53	UA	Ukraine	43

Investors, when making investment decisions, do this in relation to a specific subject of SMEs, and not the entire sector as a whole. There are studies showing that providing the mainstream of innovation, SMEs lose to large companies in such a key indicator as investment efficiency. Choi K.S. and Choi J. S. [25] obtained a result indicating a lower investment efficiency of SME companies compared to other companies.

Investment efficiency (IE) of enterprise is calculated as a function of investment risk, profitability, and investment management costs, taking into account industry characteristics and limitations. The mathematical apparatus of modern economic science allows calculating IE for a number of economic indicators of the enterprise. Choi K.S. and Choi J. S. formulated the hypothesis of lower investment efficiency of companies in the SME sector. As theoretical assumptions, the researchers put forward the following points:

1) SME company is generally knowledgeable about investors, but investors are generally poorly informed about an SME representative.

2) SME business does not have enough specialists in the field of investments. Often small companies simply do not have the opportunity to hire them. Large companies have such specialists. Assuming that these two factors influence firms' investment performance, Choi K.S. and Choi J. S suggested that the SME sector will detect lower IE levels than other firms.

Choi K.S. and Choi J.S collected data for two years (2011–2013) for companies listed on the Korean Stock Exchange (KSE) and the Korean Securities Dealers Automated Quotations (KOSDAQ) to test their hypothesis. The selection was made according to the following *criteria*:

- 1) Only non-financial firms are studied.
- 2) Only those firms whose fiscal year ends in December are studied, the sample is 3549 companies/year.
- 3) Data is excluded if there are no indicators necessary for empirical analysis.
- 4) The maximum values of the variables are reduced by 5%, and the lowest by 5% is increased to reduce the effect of emissions.

A regression model was built, and the necessary calculations were made to process the results. Those showed that the level of investment efficiency of the SME business is lower in comparison with other firms. This means that companies in this sector have less potential for long-term growth due to lower IE. This conclusion is consistent with the assumptions of the researchers, confirming that the insufficient number of investment funds and the lack of specialists in the field of investment is the reason for the decrease in the investment efficiency of SMEs. Thus, laws are needed to facilitate lending to SMEs. An example of such legislative activity is the US experience.

The previous subsection defines the degree of participation of SMEs in innovation processes at the global and national levels. There are good reasons to compare their scales, evaluating the contribution of each object to the global and

national GDP to further examine the relationship between DE and SME participation in innovative development. Let's start with the digital economy. With respect to the reliable determination of its scale, there are significant obstacles [26]. Without ranking by importance, they are formulated as follows:

- 1) lack of generally accepted definition of DE;
- 2) lack of reliable statistics on the main DE components and aspects, especially in developing countries;
- 3) the methodology for measuring scale lags behind the development of DE.

On a global scale, depending on the definition and measurement methods used, the size of the digital economy is estimated to be from 4.5 to 15.5% of world GDP [22]. Let's move on to the scale of SMEs. So, according to the International Federation of Accountants, the contribution of SMEs is $\approx 55\%$ [27].

The contribution of DE to the country's GDP according to the report of the RAEC "Runet Economy / Digital Economy of Russia 2018" and also according to rough estimates amounted to 5.1% in Russia in 2018. The dynamics of the share of DE in the country's GDP is as follows: 1.6% in 2011, 1.8% in 2012, 2.1% in 2013, 2.2% in 2014, 2.1% in 2015, 3.9% in 2016, 4.6% in 2017, 5.1% in 2018 [28]. The growth of the digitalization level in the economics of RF is demonstrated also by GCI growth in the global rank: RF rises its position from 48 GCI Scope (2018) to 50 (2020). Moreover, if we determine the relationship between GDP and GCI we can see a close connection. However, nethermind of GCI Scope growing the range of the RF in GCI became lower (from 36 in 2018 to 42 in 2020) because of the better increase of other world digital economics [16], [29]. Moreover, if we determine the relationship between GDP and GCI we can see a close connection between these parameters (1).

$$\text{GDP (par)} = 1514 * \text{GCI} - 48390, \quad (1)$$

where the determination coefficient is 0.60, and the correlation coefficient is 0.77. This, according to the Chaddock ratio, indicates a close relationship between the factors (GDP and GCI) [30].

The share of SMEs in Russia's GDP was 21.9% in 2017 according to the FSSS. Thus, statistics show that Russia lags behind developed countries for each of the indicators. It follows that the Government of the Russian Federation should take measures to synchronously develop SMEs and DE to increase their contribution to the country's GDP. It is necessary to take into account their mutual influence in order to increase the growth rate for each indicator in this process.

IV. DISCUSSION

An analysis of the relationship between SMEs and DE in GDP, both globally and nationally, leads to firm conclusions. The above statistics show that in both cases, the share of SMEs in GDP significantly exceeds the share of DE. As applied to Russia, this means that using the potential of SMEs in the development of DE can equally significantly increase the share of the latter in the Russian economy. In the ideal

case, if the entire small and medium-sized business of Russia is "turned" today towards the DE, then the share of the latter in GDP can be increased to 21.9%, which would lead the Russian Federation to be the undisputed world leader in this indicator. Moving from an abstract concept to reality, Russia needs to additionally create an innovative sector of small business in volumes comparable to the existing, today, SME sector. The attractiveness of such a solution is obvious. If successful, the country rises in terms of the share of SMEs in GDP to the level of developed countries, while the strategic task of growing the digital economy to the level of ~ 20% of GDP and moving it to the third level on the Bukht&Heeks scale is automatically solved.

It becomes possible to describe how DE is related to the innovative activities of SMEs, and ultimately determine the role of DE in the innovative development of SMEs using the definition of a digital economy, the Bukht&Heeks scheme, data on the degree of participation of SMEs in innovation processes and the ratio of the scales of CEs and SMEs.

The influence of DE on the innovative development of SMEs occurs in two directions:

1) DE provides SMEs with modern digital tools for R&D. It is impossible to imagine an innovative process without the use of modern CAD, software for mathematical modeling, and digital three-dimensional modeling, software for engineering research and calculations using FEM methods, without digital products for processing results, cloud computing, visualization tools, as well as modern communication tools today. The same direction should also include products that support the business processes of SMEs (1C products, mobile communications, the Internet, CPM programs, text and image editors, etc.).

2) DE acts as an object of innovative activity of SMEs. SMEs create innovative products directly in the digital economy. Turning to the Bukht-Heeks scheme, it is easy to find that there are significant opportunities for growth in this direction. Theoretically, even one task, the full deployment of Industry 4.0, is able to load the entire SME sector for many years.

The experience of state support for SMEs in the USA (Atlantic innovative model) is of practical interest when considering the role of state support as a condition for the intensive development of interaction between the CE and SMEs [18], [19]. The model represents a support system for the entire innovation cycle from the generation of an idea to its commercial implementation. This provides long-term competitive advantages, in contrast to "piecewise" models of support for certain stages.

A successful form of state support for innovative SMEs in the USA is the popular global programs that have proven their effectiveness: SBIR (Small Business Innovation Research) and STTR (Small Business Technology Transfer). Financing for SMEs under the SBIR program is allocated at the first stages of the life cycle of innovative technology and product (in the "death valley"), which are critical. This allows the technology to reach the stage of successful commercialization

(SBIR/ STTR). The key link in the STTR program is the creation of joint ventures of SMEs, non-profit research institutes, and universities. It helps to separate fundamental science from commercializing of its achievements [31].

The law on intellectual property for products was developed under the above programs. Tax credits and the elimination of administrative barriers in the implementation of joint state and industrial R&D programs also had a positive effect.

All measures work not only to support the innovation process but also help to obtain a high-quality intellectual product from grantees. A grant means recognition of the value and prospects of ideas, which automatically promotes the brand in the innovation market.

- The SME Corporation.
- The central institute for the development of small and medium-sized enterprises.
- The Joint-Stock Company Russian Bank for the Support of Small and Medium Enterprises (JSC SME Bank).

These organizations provide significant support to entrepreneurial activity, provide financial, marketing, property assistance, provide access to public procurement and procurement of large manufacturing corporations. The share of organizations that are engaged in marketing innovation does not exceed 1.5% in Russia [32]. SME Corporation seeks to increase the participation of SMEs in innovation. The dynamics of the involvement of small and medium-sized businesses in the high-tech sector or the share of high-tech SME products in total deliveries to the largest customers of the Russian Federation is 7.5 in 2016, 10.98 in 2017, 12 in 2018, 12.4 in 2019, 13.4 in 2020 [33].

The total amount under contracts for the supply of high-tech products amounted to 29 billion rubles in 2020. The data show a positive trend, but at the same time, only 10% of entrepreneurs consider their products innovative in Russia [34]. Nevertheless, the functioning of such state institutions as the Fund for the Promotion of Innovations, Rosmolodezh, and the Regional Platform for Supporting Entrepreneurial Initiatives is gradually changing the situation for the better.

The problems in the speed of digitalization rate in RF are connected with:

- low using level of information technologies in business (including the sector of small and medium-sized innovative entrepreneurship);
- the lack of appropriate that is needed for introducing digitalization and to entry to the world market;
- the fear of the enterprises' and cooperations' chiefs, including in the small and medium-sized business sector, to introduce the possibilities of DE for increasing its competitiveness [12].

So, several steps can be introduced to raise the level of digitalization in economics. And first of all, it has to be the

REFERENCES

government support in preparing qualitative specialists and introducing digitalization and computerization in economics sectors (including common using); creating a digital economy system, especially in the field of small and medium-sized innovation entrepreneurship; incoming and raising of the international cooperation, especially in innovative and science cooperation [12] [35].

V. CONCLUSION

In accordance with the task, the concepts of the “digital economy” and “innovative development of small and medium-sized businesses” were studied and refined in the research process. An analysis of scientific sources and documents of international organizations confirmed the absence of a single universally accepted definition of a digital economy. In this regard, after analyzing various interpretations, the definition of R. Bukht and R. Heeks was adopted as the most accurate and comprehensive. Further application of this definition and the study of the state of the digital economy of Russia made it possible to establish the level of its development in accordance with the interpretation of the Bukht&Heeks. The digital economy of the Russian Federation is at the second, intermediate stage of development according to the results. The main barriers to moving to the third level, characteristic of developed countries, are a slight advance towards Industry 4.0 and the practical lack of precision agricultural technology.

The concept of “innovative development of small and medium-sized businesses” was also investigated. As a result, two components were distinguished:

1) Application of innovations, innovative technologies in the business processes of SMEs.

2) SME participation in the innovative development of the economy.

Studying the degree of participation of SMEs in global and national innovation processes, comparing the scale of the digital economy and SMEs, leads to the conclusion that there are two directions in the influence of the digital economy on the innovative development of small and medium businesses. In one of them, the digital economy provides SMEs with the modern tools necessary for the development and implementation of innovative products and also provides SMEs with the tools necessary for business processes in SMEs themselves.

In the next role, DE is the object of innovative development of SMEs, since within this sector, the demand for innovations is constantly generated. Given the cross-border nature of DE, it is a vast and attractive market for Russian SMEs with significant potential in this area. For its implementation, as the study of the US experience shows, a rational system of state support is needed. To this end, the necessary institutional and legal mechanisms have already been created in the Russian Federation, and funding is growing. However, at the same time, volumes of industrial financing remain low, which is one of the main problems of the digital economy and the innovative development of SMEs.

- [1] H. Bouwman, S. Nikou, and de M. Reuver, “Digitalization, business models, and SMEs: How do business model innovation practices improve performance of digitalizing SMEs?” *Telecommunications Policy*, vol. 43, no. 9, pp. 101828, 2019. DOI: 10.1016/j.telpol.2019.101828.
- [2] B. Panshin, “Digital economy: concepts and directions of development,” *The Science and Innovations*, vol. 3, no. 193, pp. 49–55, 2019.
- [3] N. V. Smorodinskaya, “Complication of the organization of economic systems in the conditions of nonlinear development,” *The Bulletin of the Institute of Economics of the Russian Academy of Sciences*, vol. 5, 2017. <http://spkurdyumov.ru/uploads/2018/06/uslozhnenie-organizacii-ekonomicheskix-sistem-v-usloviyax-nelineinogo-razvitiya.pdf>.
- [4] V. Efimushkin, “Infocommunication technological space of the digital economy,” *Digital transformation of business based on the next generation communicative technologies: the round table*. March 28 2017, NIU VSHE, 2017. <https://bi.hse.ru/data/2017/03/30/1168539176/KC28.03%20-%20Владимир%20Ефимушкин.pdf>.
- [5] A. Urmantseva, *Digital economy: How professionals understand this term*. RIA Nauka, 2017. <https://ria.ru/20170616/1496663946.html>.
- [6] R. Bukht, and R. Heeks, “Defining, conceptualising and measuring the digital economy,” *International Organisations Research Journal*, vol. 13, no. 2, 143–172, 2018.
- [7] A. S. Mikhaylov, A. A. Mikhaylova, O.V. Savchina, “Innovation security of cross-border innovative milieu,” *Entrepreneurship and Sustainability Issues*, vol. 6, no. 2, pp. 754–766, 2018. [http://doi.org/10.9770/jesi.2018.6.2\(19\)](http://doi.org/10.9770/jesi.2018.6.2(19)).
- [8] E. M. Akhmetshin, I. Morozov A. V. Pavlyuk, A. Yumashev, N. Yumasheva, and S. Gubarkov, “Motivation of personnel in an innovative business climate,” *European Research Studies Journal*, vol. 21, no. 1, pp. 352–361, 2018. <https://www.um.edu.mt/library/oar/handle/123456789/30284>.
- [9] T. Tolstykh, L. Gamidullaeva, and E. Shkarupeta, “Foreign and domestic initiatives for the development of industrial complexes in the conditions of the fourth industrial revolution,” *Fortus: economic & political researches*, vol. 1, no. 1, pp. 1–9, 2018.
- [10] A. Syritskiy, K. Potapov, A. Komshin, and M. Kiselev, “The fourth industrial revolution: Digital manufacturing and the industrial Internet of things,” *Standards and Quality*, vol. 6, pp. 64–68, 2018.
- [11] N. A. Yastreb, “The Fourth Industrial Revolution: Global Industrial Networks and the Internet of Things,” *Innovacionnyj vestnik “Region” (The “Region” Innovation Bulletin)*, vol. 4, pp. 22–26, 2014.
- [12] V. I. Talantsev, A. K. Ravnyanskiy, “The digital economy and its role in the development of small and medium-sized innovative entrepreneurship in Russia,” *Regional problems of economic transformation*, vol. 2, no. 88, pp. 80–86, 2018.
- [13] K. B. Kostin, “The role of digital technologies in the promotion of goods and services in global markets,” *Russian business*, vol. 18, no. 17, pp. 2451–2460, 2017.
- [14] I. P. Boiko, M. A. Evnevich, A. V. Kolyshkin, “Economics of the enterprise in the digital age,” *Journal of Russian entrepreneurship*, vol. 18, no. 7, pp. 1127–1136, 2017.
- [15] R. Štefko, R. Bačík, R. Fedorko, M. Oleárová, and M. Rigelský, “Analysis of consumer preferences related to the use of digital devices in the e-commerce dimension,” *Entrepreneurship and Sustainability Issues*, vol. 7, no. 1, pp. 25–33, 2019. [http://doi.org/10.9770/jesi.2019.7.1\(2\)](http://doi.org/10.9770/jesi.2019.7.1(2)).
- [16] Huawei Technologies Co.,Ltd., “Global Connectivity Index. GCI Ranking Table,” 2021. <https://www.huawei.com/minisite/gci/en/country-rankings.html>.
- [17] A. I. Vlasov, V. A. Shakhnov, S. S. Filin, and A. I. Krivoshein, “Sustainable energy systems in the digital economy: Concept of smart machines,” *Entrepreneurship and Sustainability Issues*, vol. 6, no. 4, pp. 1975–1986, 2019. [http://doi.org/10.9770/jesi.2019.6.4\(30\)](http://doi.org/10.9770/jesi.2019.6.4(30)).
- [18] V. I. Medennikov, “The impact of the digital economy on the export potential of small and medium enterprises in agriculture,” *Journal of Chemical Information and Modeling*, vol. 53, no. 9, pp. 1689–1699, 2013.

- [19] V. Zimmermann, KfW SME Innovation Report 2018, 2018. https://www.kfw.de/PDF/Download-Center/Konzernthemen/Research/PDF-Dokumente-Innovationsbericht/KfW-Innovationsbericht-EN/KfW-SME-Innovation-Report-2018_EN.pdf.
- [20] Ya. Ivanov, "Foreign experience of innovative development of small business," *Young Scientist*, vol. 12, pp. 306–308, 2013.
- [21] A.V. Balyshv, and E. S. Zinovyeva, "Promotion of science and innovation in the U.S.: Support for small enterprises in the small business innovation research (SBIR) program," *Vestnik Chuvashskogo Universiteta (Bulletin of the Chuvash University). Humanities*, vol. 4, pp. 292–301, 2013.
- [22] O. Shulaeva, "The role of development institutions in the support of small and medium-sized enterprises' innovative activities in Russia," *Theory and Practice of Social Development*, vol. 11, pp. 54–57, 2017.
- [23] M. Botnik, G. Sechenya, and N. Mikheeva, "System for assessing and monitoring the innovative development of Russian regions," *Innovacionnaya ekonomika (Innovative Economy)*, vol. 9, pp. 40–61, 2012.
- [24] Kirov Regional Fund for Entrepreneurship Support, Foreign experience in state support of innovative small and medium enterprises. (n.d.). <http://www.kfpp.ru/analytics/material/innovation.php>.
- [25] K. S. Choi, and J. Choi, "Small and medium business and investment decision," *Indian Journal of Science and Technology. Indian Society for Education and Environment*, vol. 8, no. 24, pp. 1–6, 2015.
- [26] UNCTAD. Digital economy report 2019: Overview, 2019. <https://unctad.org/en/pages/PublicationWebflyer.aspx?publicationid=2512>.
- [27] A. Christopher, The foundation for economies worldwide is small business, 2018. <https://www.ifac.org/knowledge-gateway/contributing-global-economy/discussion/foundation-economies-worldwide-small>.
- [28] K. Kh. Zoidov, S.V. Ponomareva, E. Simonova, and A. A. Yurieva, "Prospects for the development of the digital economy in Russia," *Regional problems of transforming the economy*, vol. 12, pp. 18–24, 2018.
- [29] Huawei Technologies Co.,Ltd., "Global Connectivity Index. GCI Ranking Table," 2019. <https://www.huawei.com/minisite/gci/en/country-rankings.html>.
- [30] R. Ireland, M. Hitt, "Achieving and maintaining strategic competitiveness in the XXIst century: The role of strategic leadership," *Academy of Management Executive*, vol. 13, no.1, 1999. <https://doi.org/10.5465/ame.1999.1567311>.
- [31] SBIR/ STTR. (n.d.). www.sbir.gov.
- [32] T. V. Pogodina, V. G. Aleksakhina, V. A. Burenin, T. N. Polianova, and L. A. Yunusov, "Towards the innovation-focused industry development in a climate of digitalization: The case of Russia," *Entrepreneurship and Sustainability Issues*, vol. 6, no. 4, pp. 1897–1906, 2019. [http://doi.org/10.9770/jesi.2019.6.4\(25\)](http://doi.org/10.9770/jesi.2019.6.4(25)).
- [33] SME Corporation. Providing support to small and medium-sized enterprises by the SME Corporation in the period 2015-2019, 2020. <https://corpmsp.ru/upload/001/%D0%9F%D1%80%D0%B5%D0%B7%D0%B5%D0%BD%D1%82%D0%B0%D1%86%D0%B8%D1%8F%2010.02%202020%D0%B3.pdf>.
- [34] Global Enterprise Monitoring (GEM) (n.d.). <http://smb.gov.ru/analytics/17925.html>.
- [35] J. R. Saura, "Using data sciences in digital marketing: Framework, methods, and performance metrics," *Journal of Innovation & Knowledge*, vol. 6, no. 2, pp. 92–102, 2021. <https://doi.org/10.1016/j.jik.2020.08.001>.

Human Action Recognition in Video Sequence using Logistic Regression by Features Fusion Approach based on CNN Features

Tariq Ahmad¹, Imran Khan³

School of Information and Communication Engineering
Guilin University of Electronic Technology
Guilin, China

Asif Rahim⁴

School of Cyberspace Security
Guilin University of Electronic Technology
Guilin, China

Jinsong Wu^{2*}

School of Artificial Intelligence
Guilin University of Electronic Technology
Guilin, China

Amjad Khan⁵

Hamdard Institute of Engineering & Technology
Hamdard University, Islamabad Campus
Islamabad, Pakistan

Abstract—Human Action recognition (HAR) gains too much attention due to its wide range of real world applications, such as video surveillance, robotics and computer vision. In video surveillance systems security cameras are placed to monitor activities and motion, generate alerts in undesirable situations. Due to such importance of video surveillance in daily life, HAR becomes the primary and key factor of video surveillance systems. Many researchers worked on human action recognition but HAR still a challenging problem, due to large variation among human to human and human actions in daily life, which make human recognition very challenging and makes surveillance system difficult to outperform. In this article a novel method is proposed by features fusion of pre-trained convolution neural network (CNN) features. Initially pre-trained CNN VGG 19 weights are exploited to extract fully connected 7th layer (FC7) of the selected dataset, subsequently pre-trained fully connected 8th layer features (FC8) extracted by employing pre-trained weights of the same neural network. However the resultant feature fused vector further optimized by employing two statistical features selection techniques, chi-square test and mutual information to select best features among them to reduced redundancy and increase performance accuracy of human action, a threshold value used for selecting best features. Furthermore the best features are fused, then grid search with 10 fold cross validation is applied for tuning hyper parameter to select best k fold and the resulting best parameter are feed to Logistic regression (LR) classifier for recognition. The proposed technique used You Tube 11 action dataset and achieved 98.49% accuracy. Lastly the proposed method compares with the existing state of the art methods which show dominance performance.

Keywords—Human action recognition; logistic regression; deep learning; convolution neural network; features fusion

I. INTRODUCTION

Human action recognition (HAR) is very popular among researchers, computer vision community, data engineers and data scientist due to its wide range of industrial and real life applications. One of the main inspirations which invite scholars to work in human action recognition is the wide domain of its

applications in computer vision, robotics, human computer interaction [1], and video surveillance [2], in the former HAR technique faced challenges due to similarity of visual contents whereas the later one faced challenges due to large variation among humans in real life. In video surveillance systems security cameras installed to monitor activities of human and generate alerts in undesirable situation, store videos and transmitting videos but due to huge variation among intrapersonal and personal activities of humans in real life make video surveillance systems difficult to outperform because human action recognition is the basic feature which directly impacts the performance of video surveillance system.

Human action is the motion of body portions by interacting with components in environment. Human action may be simple like movement of arm or leg e.g. walking activity of human includes arm and leg movements, and may be too complex like movement of entire body e.g. jumping of volleyball player, which includes movements of entire body of the player. HAR methods are used in wireless sensor networks [3], wearable sensor [4] and video HAR [5] but HAR is more popular in video based systems because video based HAR techniques are the basic building block of video surveillance system and video surveillance systems are extensively used in real life.

Human action recognition in videos sequence is the process of allotting labels to each category of videos to train the system, and the system enable to recognize various actions done by human in unseen videos, however in the context of videos an action is embodied using sequences of frames from which humans can easily understand by examining contents of numerous frames in sequence [6]. Human action recognition in videos is still challenging due to many factors such as class variation, angle variation [7] and environment. Researchers used many techniques for image classification and action recognition such as hand-crafted methods [8], and Histogram of Oriented Gradient (HOG), but such hand-crafted techniques have some limitations such as complex computations and lengthy videos which run continuously, however hand-crafted

*Corresponding Author.

techniques outperform in some domain of action recognition such as simple videos streaming.

In recent decade researcher also used deep learning networks methods for many applications of action recognition and image classification, over millions of multi-class images classified through CNN based approaches, which proved the accuracy is improved in classification problem [9], [10]. CNN based approaches shown significant improvement in many areas which give them too much consideration over hand-crafted features techniques. Many researchers presented their work for action recognition by using pre-trained weights of deep learning neural networks for features extraction, instead of training new deep network from scratch. For instant, building a new model from scratch need huge amount of data which is computationally expensive, relatively, on small dataset the deep learning network from scratch will be not outperform due to small amount of data.

In this paper, we used six frames per second of each video clip instead of thirty frames per second; we bounce five frames every second of every video clip, which reduce redundancy and computation complexity. In the proposed method weights of pre-trained CNN [9], used for feature extraction and then feed these deep features to logistic regression for action recognition of sequence frames of selected video dataset. The pre-trained CNN model was selected on the basis of its prior performance over classification problem and due to few limitations of hand-crafted features based methods we selected deep neural network based approach for feature extraction in the proposed research method. A detail overview presented in subsequent sections.

II. RELATED WORK

Over the years researchers presented their work for action recognition, based on hand-crafted and deep learning networks. Both techniques discuss in Section A and B respectively.

A. Hand-crafted based Features Extraction Techniques

Hand-crafted based approaches extract hand-crafted features from simple video clip for non-realistic actions, where a performer completes an action in a scene with simple context and situation; hand-crafted techniques extract low level feature map of human action in video sequence and feed these features to classifier such as ensemble, naive Bayes and (SVM) support vector machine for action recognition. In [11], action sketches were investigated by analysis of geometric characteristic such as space, time and volume (STV). In [12,] the author presented human action as three dimensions prepared from silhouettes in space, time and volume, moreover Poisson's equation used by them to examine two dimensions shape of actions and exposed space time features (STF) for non-realistic videos sequence, however two dimensions shape of actions for two different actions sometime caused the same shape and making the action recognition difficult. In [13], the author used realistic video dataset and extracted motion and static features; in addition they removed the noisy features by applying motion statistics and obtain stable features. However hand-crafted features techniques have certain drawbacks. For instant, STV based approach are not effective for recognition of numerous person activities in a scene. STF based approaches are not appropriate

for complex dataset however its shows significant result on simple dataset. These drawbacks can cause trouble for lengthy videos and real time applications with nonstop video streaming such as video surveillance systems.

B. Deep Neural Networks Techniques

In recent years several deep learning networks for action recognition, image classification, bioinformatics and person re-identification were presented and show significant accuracy in the respected fields. For instant, a straight forward execution were developed for human activity recognition [14], moreover they used 3D CNN filters in implementation and applied on videos frames in time domain to capture spatial and temporal information. They also claimed that their proposed technique collects optical and motion features, since video frames were linked to fully connected layer at the end of deep network.

A multi-resolution convolution neural network was presented in [15], to collect local spatial and temporal features, they used time axis for connectivity of features. They tested the experiment on YouTube one million videos dataset for human action recognition and acquired 63.9% recognition, they claimed that the proposed work reduce time complexity in training the system, but their recognition is still low for other large action recognition dataset such as UCF101[16] recognition was 63.3%.

Two stream convolution neural networks was presented in [17], to captured spatial and temporal features in video frames they used first stream, moreover the second stream captured optical flow of frames in dense. Asymmetric unidirectional 3D CNN was presented [18], for recognition they applied micro nets to increase feature learning skill of their proposed deep learning network and achieved good recognition rate. Deep learning based techniques have the capability to correctly detect unseen patterns in visual data because of its vast quantity of data for training and huge computational power for its processing.

III. CALLANGES AND CONTRIBUTIONS

In the recent decade significant contribution was made in human action recognition (HAR). Many approaches were applied in HAR aimed to acquire high recognition of human actions in the domain of HAR, but mostly hand-crafted based and deep learning based methods were presented in literature by researchers. In hand-crafted based approaches such as STV, action sketches were examined by geometric characteristics in time, space and volume but STV based approach was only effective for single actor action where an actor perform some action in the scene, STV got optimal results, conversely STV based approach was behind to solve the challenge of HAR where multiple actors perform actions in the scene. Some hand-crafted based approaches such as space, time features STF used human silhouettes to examine two dimensions shape of actions and expose space time features but STF was slow and consume huge amount of space.

Which deviate time and space tradeoff, in STF the two dimensions shape of action for two different actions sometime produced the same human action which caused difficulty in recognition and the final accuracy of the system affected. Beside hand-crafted approaches deep neural networks made

significant contribution towards solutions to the challenges faced by HAR, deep neural networks show significant results in many domains, In addition deep neural networks based approaches relies on very deep features and many real life applications which used HAR are also rely on deep features. However, an end to end HAR system depends on very deep features for outstanding results therefore in the proposed research deep neural networks based features extraction techniques is used. In this paper the main contributions towards the solutions to HAR in video sequence are:

- Utilizing VGG19 model to compute deep features and acquire two features vectors of our selected video dataset.
- Integrated the deep features of CNN and computing best features by applying Chi-2 and mutual information to reduce redundancy and increase performance.
- Integrated Chi-2 best features and mutual information features vector and apply grid search with 10 k-fold cross validation to tune hyper parameter and select best k-fold parameters.
- Finally, the resulting k-fold is feed to LR for final recognition to solve recognition problem.

IV. PROPOSED RESEARCH METHODOLOGY

In this section the proposed research methodology is discusses in details. An activity A_c in frames of video sequence V_d using CNN for features extraction and logistic regression (LR) for F_R sequence of frames to recognize A_c . Firstly we use pre-trained weights of CNN for feature extraction of frames F_R in video V_d with bounce of B_f such that bouncing of frames not affect the activity A_c . finally the features fed to logistic regression for activity A_c recognition.

A. Preprocessing of Input Frames of Video Sequence

Video is the collection of frames generally video is running at thirty frames per second but we take into consideration only six frames per second and bounce five frames at unit time which reduced redundancy and computational complexity, however the selected sequence of frames doesn't affect action in video and from the evaluation of experiment it achieved significant result. In the preprocessing phase we resize frames to 224x224 RGB of all categories which is the desire input shape of VGG 19 [9] for feature extraction. In the context of videos, frames are features of videos so every frame is zero centered to reduced computation and preprocessed all frames to subtract mean RGB pixel intensity from pre-trained weights of VGG 19 during feature extraction phase. VGG19 model trained on 1.3 million images and 143 million trainable parameters which allow VGG19 model to transfer the learned pattern from pre-trained weights to our selected dataset in feature extraction. The architecture of VGG19 model is given in Fig. 1.

Layer (type)	Output Shape	Param #
input_1 (InputLayer)	(None, 224, 224, 3)	0
block1_conv1 (Conv2D)	(None, 224, 224, 64)	1792
block1_conv2 (Conv2D)	(None, 224, 224, 64)	36928
block1_pool (MaxPooling2D)	(None, 112, 112, 64)	0
block2_conv1 (Conv2D)	(None, 112, 112, 128)	73856
block2_conv2 (Conv2D)	(None, 112, 112, 128)	147584
block2_pool (MaxPooling2D)	(None, 56, 56, 128)	0
block3_conv1 (Conv2D)	(None, 56, 56, 256)	285168
block3_conv2 (Conv2D)	(None, 56, 56, 256)	590080
block3_conv3 (Conv2D)	(None, 56, 56, 256)	590080
block3_conv4 (Conv2D)	(None, 56, 56, 256)	590080
block3_pool (MaxPooling2D)	(None, 28, 28, 256)	0
block4_conv1 (Conv2D)	(None, 28, 28, 512)	1180160
block4_conv2 (Conv2D)	(None, 28, 28, 512)	2359808
block4_conv3 (Conv2D)	(None, 28, 28, 512)	2359808
block4_conv4 (Conv2D)	(None, 28, 28, 512)	2359808
block4_pool (MaxPooling2D)	(None, 14, 14, 512)	0
block5_conv1 (Conv2D)	(None, 14, 14, 512)	2359808
block5_conv2 (Conv2D)	(None, 14, 14, 512)	2359808
block5_conv3 (Conv2D)	(None, 14, 14, 512)	2359808
block5_conv4 (Conv2D)	(None, 14, 14, 512)	2359808
block5_pool (MaxPooling2D)	(None, 7, 7, 512)	0
flatten (Flatten)	(None, 25088)	0
fc1 (Dense)	(None, 4096)	102764544
fc2 (Dense)	(None, 4096)	16781312
predictions (Dense)	(None, 1000)	4097000
Total params: 143,667,240		
Trainable params: 143,667,240		
Non-trainable params: 0		

Fig. 1. VGG19 Model Architecture.

VGG19 model used fix input shape of RGB images in the training phase, they used 1.3 million images for training the model, 50 thousand for validation and 100 K images for evaluation the experiment, stack of convolution layers conv1 and conv2 were employed to input RGB image with 3x3 filter size to extract low level features of images, passing the input RGB images from conv1 and conv2 the image RGB channel is converted to 64, in the first block of convolution layers, stride of 1 pixel used for sliding the filter map and max pool1 layer to reduce spatial size of conv1 and conv2 features. In the second block of convolution layers 3x3 conv1 and conv2 applied followed by max pool layer.

They used stride of 1 pixel for every convolution and 2x2 strides for max pooling layers; however activation function of ReLU [19], equipped in all hidden layers for rectification and introduced non-linearity form which the model learned complex useful features between inputs and response variables. Beside stack of convolution layers one flatten layer of 250,88 dimension applied and then followed by three fully connected layers FC1, FC2 each have 4096 channels depth and the last FC layer of 1000 channels, finally a soft-max function used for prediction of classes. The model trained on 143 million parameters, initial learning rate of 10^{-2} , momentum 0.9, number of iteration 370 K and mini batch-size of 256 used respectively. The proposed research methodology is given in Fig. 2. Where each step is discuss in subsequent sections.

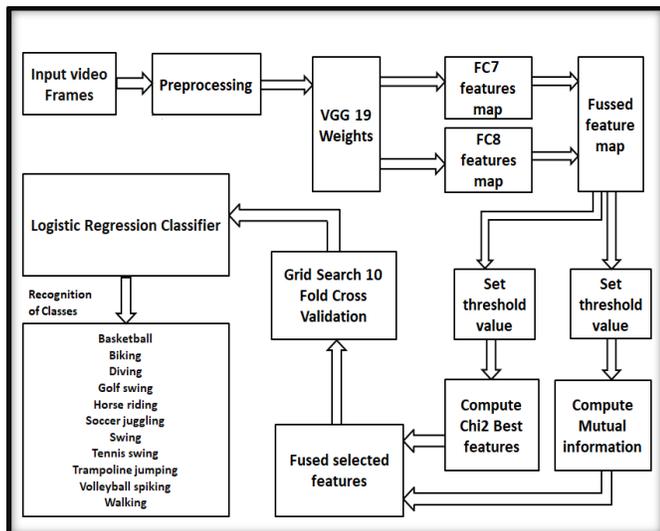


Fig. 2. Basic Building Block of Proposed Framework.

B. Features Extraction and Features Fusion

Video clip is the collection of frames where its running 30 frames at unit time by default but we used six frames per second and bounce five frames in each second because frames represents the story of the running video and at rate of 30 frames per unit time cause a very small movement in the story and cause redundancy, from which the system computational complexity increased, in Fig. 3. Scenario of a sample video clip is presented whereas frames are extracted in one second and frame to frame change in unit time occurs during frame

extraction. We passed frames of our selected dataset through VGG19 weights and extracted features from fully connected 7th and 8th layer respectively. If we represent the extracted features in vector representation of N data samples and d dimensions then the extracted features vectors can be denoted (N, d_1) and (N, d_2) where d_1 and d_2 represent the features dimensions of FC7 and FC8, respectively. In addition, the extracted features vectors can be express in equation such that

$$V^{(7)} = (N, d_1) \tag{1}$$

$$V^{(8)} = (N, d_2) \tag{2}$$

Where $V^{(7)}$ and $V^{(8)}$ represents extracted feature vectors of 7th and 8th layers of VGG19, respectively.

The given Fig. 4 shows the visualization effect of filters after applying VGG 19 activation function on the sample frame of selected dataset during features extraction. furthermore, in the proposed method, we used features fusion technique by applying vector addition to (1) and (2) and acquire fused vector V_f , however (1) and (2) used the same sample of data then in vector addition the size of N taken common.

Equation (1) and (2) by transformation of vector addition.

$$V_f = V^{(7)} + V^{(8)} \tag{3}$$

$$V_f = (N, d_1) + (N, d_2) \tag{4}$$

$$V_f = (N+N, d_1+d_2) \tag{5}$$

$$V_f = (N_i, d_n) \tag{6}$$

Where $N_i = N$ such that $N_i \neq N+N$ and $d_n = d_1+d_2$



Fig. 3. Frame to Frame Representation and Change in Frames Occurs in One Second.

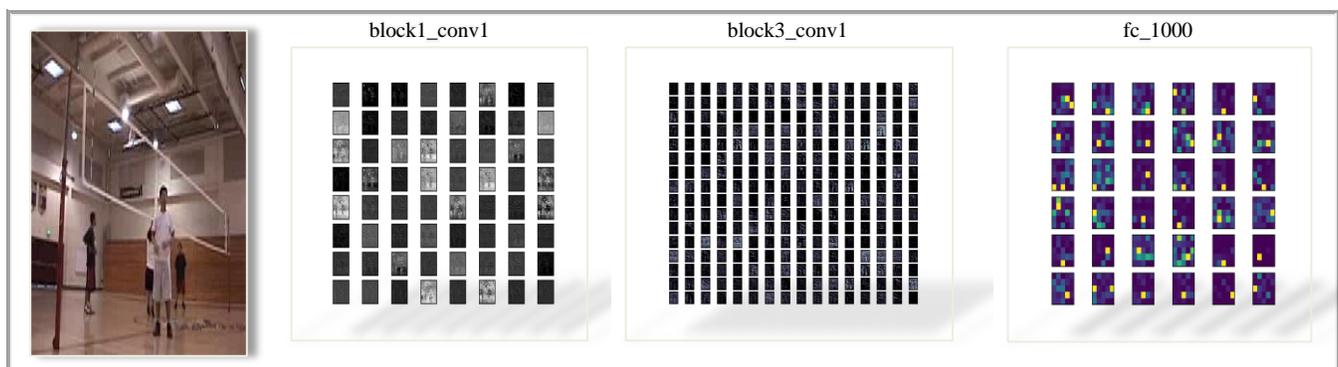


Fig. 4. Sample Frame of You Tube Dataset and Visualization of Filters after Applying Activation Function.

C. Features Selection

Feature selection is very useful when building a machine learning model because not all features in dataset are useful and adding all features to model may reduce the accuracy of model and generalization capacity. Furthermore, model complexity also increases with increasing the number of useless features. We have fused features vector V_f which contains redundant features, to decrease redundancy from features and select best features we apply two statistical feature selection techniques, chi-square test and mutual information on V_f . chi-square test compute between features and target variable and select best features based on chi-square scores, for instant if some features get low chi-square score then remove those features we applied a threshold value in our proposed method. The mathematical representation of chi-square:

$$X_c^2 = \frac{\sum (O-E)^2}{E} \quad (7)$$

Where

C = degree of freedom

O = observed values

E = expected values

We have fused features vector V_f and a matrix L_n where L_n represents class labels of training samples, however in chi-square features selection technique L_n consider as target variables of n dimension then by putting V_f and L_n in (7) we can get.

$$X_c^2 = \frac{\sum (V_f - L_n)^2}{L_n} \quad (8)$$

Here X_c^2 contains the score of each feature acquire from chi-square, moreover X_c^2 scores are applied to transformed fused features vector under certain threshold such that

$$Ch_b = X_c^2 T \rightarrow V_f \quad (9)$$

Where ch_b represents best chi-square features, \rightarrow denote transformation function and T is threshold value respectively. Beside chi-square feature selection, mutual information feature selection technique is also computed in the proposed research, mutual information between two variables is the measurement that how much information obtains one variable through the other variable. Mathematically formulation of mutual information is;

$$MI(A; B) \Delta D(P_{AB} \| P_A P_B) \quad (10)$$

Where A and B are independent variables, P_{AB} is joint probability density function of A and B , where P_A and P_B are marginal density function of variables A and B respectively. Consequently, (10) applied on V_f and L_n .

$$MI(V_f; L_n) \Delta D(P_{V_f} \| P_{V_f} P_{L_n}) \quad (11)$$

$$MI_h = MI(V_f; L_n) \Delta D(P_{AB} \| P_A P_B) T \rightarrow V_f \quad (12)$$

Where MI_h contains only those features which have high mutual information between V_f and L_n under certain threshold, \rightarrow used for transformation function and T denote threshold respectively. Besides Ch_b and MI_h , whereas the former holds

best score chi-square features and the later one contains high mutual information features, we fused both the vectors through vector addition.

$$V_S = Ch_b + MI_h \quad (13)$$

Where V_S denote selected features.

D. Logistic Regression

Logistic Regression (LR) widely used in many applications of data mining and machine learning techniques for data classification. LR delivers likelihoods and cover multi-class classification problem [20]. LR used the same principle of linear regression, furthermore LR techniques were applied through truncated newton to solve large optimization problem [21]. However LR applied in many imbalance and multi-class data to solve the classification problem. We can express LR mathematically as.

$$P = \frac{e^{a+bx}}{1+e^{-(b_0+b_1x)}} \quad (14)$$

Where we have fused selected vector V_S by feeding this vector to (14) and solve the classification problem for action recognition. In addition, prior to feeding V_S to (14) we choose a set of optimal hyper-parameter by grid search to get best fit of proposed LR model, and further we applied 10 k-fold cross validation to evaluate the proposed LR model.

For instant, we have fused selected features V_S which contains multi-class features and imbalance data samples because V_S fused features of videos frame and in context of videos, not all videos are same in size, some may be lengthy, short and medium in size. To avoid the imbalance data problem and balance all categories we gave equal class weights to every categories of selected dataset, because imbalance data directly impacts on average accuracy of machine learning model. Fig. 5 shows the imbalance frames for our selected dataset.

V. EXPERIMENTAL EVALUATION

In this section we will discuss the dataset and results of the proposed research methodology which based on pre-trained CNN features and select best features by using Chi-2 and mutual information. The experiment is evaluated on publically available benchmark You Tube 11 action dataset; first we tested our proposed method on three classifiers Logistic Regression (LR), Naïve Bayes (NB) and Random Forest (RF) and then chose best classifier among them based on performance result. We chose LR because LR achieved significant results. Table I show the comparison results of LR, NB and RF. Next, the proposed method using LR is compared with some of the existing state-of-the-art techniques of HAR. Initially the dataset divided into 80% for training and 20% for testing, according to machine learning standard protocol for data splitting. In the proposed research method we used deep learning framework, tensorflow for deep feature extraction, for features fusion and implementation of LR model we used python Sklearn library. Overall experiment tested on NVidia GTX 1080ti GPU and 16 GB of RAM used respectively.

A. You Tube Action Dataset

We tested and evaluate our proposed method using LR on you tube action dataset which is publically available, it

contains 11 action classes: basketball, biking, diving, golf, horse riding, soccer, swing, tennis, trampoline jumping, volleyball, and walking. The dataset contains 11 classes and each class provided a subset of 25 groups further, whereas every group of videos contains more than 4 videos clips, however the videos in same group share some similarity such as identical actors, background of video clips matched to other videos of the same group and equal viewpoint [27]. The given Fig. 6 shows some frames sample which represent different categories of You Tube 11 action dataset.

The dataset is very challenging due to pose and object appearance, cluttered background, large variation in camera motion, viewpoint, illumination condition and object scale, some videos of the same class captured when an actor done some actions in indoor background where others videos of the same class captured while an action done by actor some in outdoor background.

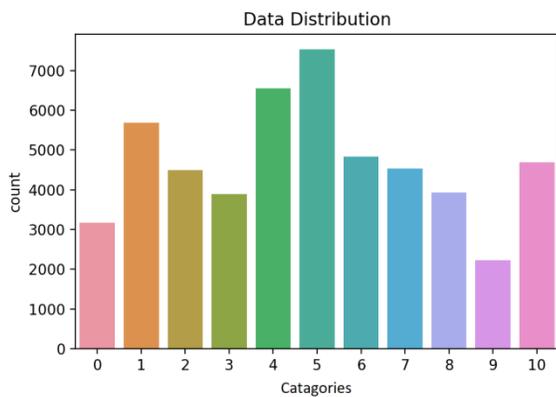


Fig. 5. Imbalance Frames of Selected Video Dataset.



Fig. 6. Different Samples Frames of You Tube Dataset.

B. Selection of Classifier

Selection of classifier to get optimal results to solve recognition problem faced by HAR, we tested our proposed method of features extraction and selection on three different classifier LR, NB and RF using you tube 11 dataset, whereas the feature are extracted through VGG19 model and select best features through Chi-2 and mutual information, for all the three classifier same methodology used for features extraction and features selection, the aim of testing the proposed method on three classifiers is to select best classifier among them and to check the consistency and validity of our results. The given Table I reported the recognition accuracy, F1 score, recall and precision of all the three classifiers. We choose LR to solve recognition problem faced by HAR because LR achieved 98.55% F1 score, 98.57% recall and 98.53% precision where NB achieved 78.41% F1 score, 80.71% recall and 77.97% precision and FR achieved 93.22% F1 score, 92.55% recall and 94.06% precision by using the selected dataset respectively. The given Fig. 7 shows comparison results of LR, NB and RF on test samples of YouTube dataset by using the proposed method of feature extraction and selection. LR classifier got optimal results over Naïve Bayes and Random forest; the former achieved 79.50% accuracy whereas the later one achieved 93.23% and selected LR achieved 98.49% recognition accuracy on test data. The selection of LR in the proposed research is not only based on accuracy, but we used total four metrics for the selection criteria of classifier, further, from evaluation results of LR, NB and RF which exploit our proposed method of features extraction and selection shows the validity and consistency in results.

TABLE I. NB, RF AND LR RESULTS COMPARISON

Method	Accuracy	F1 score	Recall	Precision
Navie Bayes	79.50%	78.41%	80.71%	77.97%
Random forest	93.23%	93.22%	92.55%	94.06%
Logistic Regression	98.49%	98.55%	98.57%	98.53%

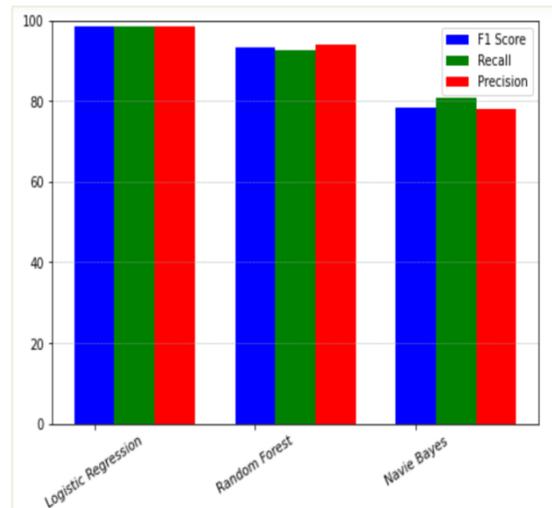


Fig. 7. Comparison of LR, NB and RF Tested on You Tube Action Dataset.

C. Proposed LR Comparison with Existing Techniques

The proposed method using LR achieved 98.49% average accuracy on test samples of You Tube action dataset given in Table II, dominating the Wang, Wu, Yang, Xu, Peng techniques having 84.1%, 87.0%, 88.0%, 89.3%, 93.8% accuracy, respectively. The confusion matrix of You Tube action dataset evaluated on test samples is given in Fig. 8. The proposed LR method achieved more than 98% accuracy for seven classes among eleven. The class “walking” reported 96.7% accuracy because some other classes interfere and reported false prediction of 3.3%, similarly class “biking”, “swing” and “trampoline jumping” accuracy are 97.7%, 97.7% and 97.8% reported respectively because other classes intervene due to same view point, background etc. and affect average recognition accuracy. Fig. 9 shows class wise accuracy of You Tube action recognition dataset which are evaluated on test data. Our proposed method using LR achieved significant results and by comparison with existing state of the art techniques we conclude that our method is best fit for solving the recognition problem of HAR.

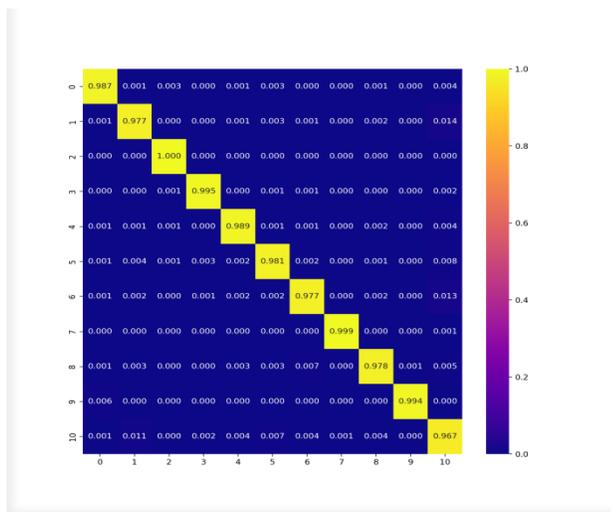


Fig. 8. Confusion Matrix of You Tube Dataset using LR.

TABLE II. COMPARISON OF AVERAGE ACCURACY OF PROPOSED METHOD FOR ACTION RECOGNITION WITH STATE-OF-THE-ART TECHNIQUES

Method	You Tube Dataset
Wang[22]	84.1%
Wu[23]	87.0%
Yang[24]	88.0%
Xu[25]	89.3%
Peng[26]	93.8%
Proposed	98.49%

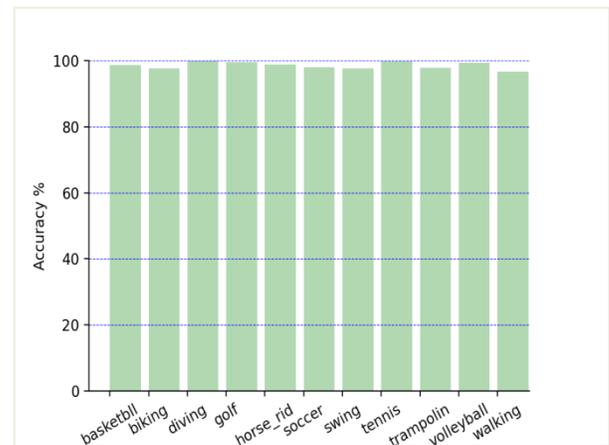


Fig. 9. Class wise Accuracy of Test Samples of You Tube Dataset.

VI. CONCLUSION AND FUTURE WORK

Human action recognition (HAR) under many viewpoints is a major challenge to correctly recognize the activity of human. In this work we proposed a new approach for HAR. First we extracted deep features from fully connected 7th (FC7) and 8th (FC8) layers of pre-trained model namely VGG19, and next, integrate the two features vector to select best features among them by applying Chi-2 and mutual information, later Logistic Regression used for classification by feeding the best features acquired from Chi-2 and mutual information. The aim of selection of best features is to improve accuracy and reduce redundancy from features, however feeding noisy features to the system must be consume more time and make the system computation expensive. The experiments are conducted on You tube 11 action dataset and the proposed method outperform, from the experiment we concluded that features extraction from pre-trained model perform better for improvement of recognition. Our method achieved 98.49% average accuracy on you tube 11 dataset and by comparison with existing state-of-the-art-techniques our method dominating in performance. In future, we are planning to use some advance dataset UCF 50 and UCF101 which contains 50 and 100 categories of human actions respectively. Furthermore we are planning to use gaited recurrent unit (GRU) to solve the recognition problem of HAR.

ACKNOWLEDGMENT

This work is supported in part by the School of Information and Communication Engineering, Guilin University of Electronic Technology, the School of Artificial Intelligence, Guilin University of Electronic Technology, the National Natural Science Foundation of China (No’s, 6217011456, 6216010122).

REFERENCES

- [1] S. A. Aly, T. A. Alghamdi, M. Salim, and A. A. Gutub, "Data dissemination and collection algorithms for collaborative sensor devices using dynamic cluster heads," *Trends Appl. Sci. Res.*, vol. 8, no. 2, pp. 55–72, 2013.
- [2] A. Nanda, P. K. Sa, S. K. Choudhury, S. Bakshi, and B. Majhi, "A neuro-morphic person re-identification framework for video surveillance," *IEEE Access*, vol. 5, pp. 6471–6482, 2017.
- [3] R. Zhao, W. Xu, H. Su, Q. Ji, "Bayesian Hierarchical Dynamic Model for Human Action Recognition," Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), 2019, pp. 7733–7742.
- [4] S. Rahimi, A. Aghagolzadeh, M. Ezoji, "Human action recognition based on the Grassmann multi-graph embedding," *Signal, Image and Video Processing* volume 13, pages 271–279, 2019.
- [5] A-A. Liu, Y-T. Su, W-Z. Nie, M. Kankanhalli, "Hierarchical Clustering Multi-task Learning for Joint Human Action Grouping and Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, DOI:10.1109/TPAMI.2016.2537337, February 2016.
- [6] P. Zhang, C. Lan, J. Xing, W. Zeng, J. Xue, N. Zheng, "View Adaptive Neural Networks for High Performance Skeleton-based Human Action Recognition," *IEEE Transactions on Pattern Analysis and Machine Intelligence*, PP. 99, DOI:10.1109/TPAMI.2019.2896631.
- [7] Z. Tu, W. Xie, Qi. Qin, R. Poppe, R. C. Veltkamp, B. Li, J. Yuan, "Multi-stream CNN: Learning representations based on human-related regions for action recognition" *Pattern Recognition (IF7.74)*, Pub Date : 2018-07-01, DOI: 10.1016/j.patcog.2018.01.020.
- [8] Y. Hu, L. Cao, F. Lv, S. Yan, Y. Gong, and T. S. Huang, "Action detection in complex scenes with spatial and temporal ambiguities," in *Proc. IEEE 12th Int. Conf. Comput. Vis.*, Sep./Oct. 2009, pp. 128–135.
- [9] K. Simonyan, A. Zisserman, "Very Deep Convolutional Networks for Large-Scale Image Recognition". *ICLR* 2015.
- [10] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "ImageNet classification with deep convolutional neural networks," in *Proc. Adv. Neural Inf. Process. Syst.*, 2012, pp. 1097–1105.
- [11] A. Yilmaz and M. Shah, "Actions sketch: A novel action representation," in *Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2005, pp. 984–989.
- [12] L. Gorelick, M. Blank, E. Shechtman, M. Irani, and R. Basri, "Actions as space-time shapes," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. no. 12, pp. 2247–2253, Dec. 2007. 29.
- [13] J. Liu, J. Luo, and M. Shah, "Recognizing realistic actions from videos "in the wild"," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR)*, Jun. 2009, pp. 1996–2003.
- [14] S. Ji, W. Xu, M. Yang, and K. Yu, "3D convolutional neural networks for human action recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 1, pp. 221–231, Jan. 2013.
- [15] A. Karpathy, G. Toderici, S. Shetty, T. Leung, R. Sukthankar, and L. Fei-Fei, "Large-scale video classification with convolutional neural networks," in *Proc. IEEE Conf. Comput. Vis. Pattern Recognit.*, Jun. 2014, pp. 1725–1732.
- [16] K. Soomro, A. R. Zamir, and M. Shah. (2012). "UCF101: A dataset of 101 human actions classes from videos in the wild." arXiv preprint arXiv:1212.0402, 2012.
- [17] K. Simonyan and A. Zisserman, "Two-stream convolutional networks for action recognition in videos," in *Proc. Adv. Neural Inf. Process. Syst.*, 2014, pp. 568–576.
- [18] H. Yang, C. Yuan, B. Li, Y. Du, J. W. Xing, Hu et al. (2019) "Asymmetric 3d convolutional neural networks for action recognition". *Pattern Recogn* 85:1–12.
- [19] A. Fred M. Agarap "Deep Learning using Rectified Linear Units (ReLU)," [online]. Available: <https://arxiv.org/pdf/1803.08375.pdf>.
- [20] T. Hastie, R. Tibshirani, and J. Friedman, (2009), "The Elements of Statistical Learning", 2nd ed., Springer Verlag.
- [21] P. Komarek, and Moore, A. (2005b), "Making logistic regression a core data mining tool with TR-IRLS", *Proceedings of the Fifth IEEE Conference on Data Mining*.
- [22] H. Wang, A. Klaer, C. Schmid, and C. Liu, "Dense trajectories and motion boundary descriptors for action recognition," *IJCV*, vol. 103, no. 1, pp. 60–79, 2013.
- [23] X. Wu, D. Xu, L. Duan, J. Luo, and Y. Jia, "Action recognition using multilevel features and latent structural svm," *IEEE Trans. Circuits Syst. Video Technol.*, vol. 23, no. 8, pp. 1422–1431, 2013.
- [24] X. Yang and Y. Tian, "Action recognition using super sparse coding vector with spatio-temporal awareness," in *ECCV*, 2014, pp. 727–741.
- [25] X. Xu, I. Tsang, and D. Xu, "Soft margin multiple kernel learning," *IEEE Transactions on Neural Networks and Learning Systems*, vol. 24, no. 5, pp. 749–761, 2013.
- [26] X. Peng, C. Zou, Y. Qiao, and Q. Peng, "Action recognition with stacked fisher vectors," in *ECCV*, 2014, pp. 581–595.
- [27] J. Liu, J. Luo and M. Shah "Recognizing realistic actions from videos "in the wild"," 2009 IEEE Conference on Computer Vision and Pattern Recognition, DOI: 10.1109/CVPR.2009.5206744.

Application-based Framework for Analysis, Monitoring and Evaluation of National Open Data Portals

Vigan Raca¹, Goran Velinov², Betim Cico³, Margita Kon-Popovska⁴

Ss Cyril and Methodius University in Skopje

Faculty of Computer Science and Engineering, Skopje, North Macedonia^{1,2,4}

Metropolitan University of Tirana, Faculty of Computer Science and IT, Tirana, Albania³

Abstract—Open Government Data (OGD) portals are considered of significant national importance towards transparency and accountability improvement. The continuous publication of data in OGD portals introduces the need for high-quality data and the qualitative portal itself. This paper aims to address the data quality issues through a framework composed of several components aimed at measuring and monitoring the OGD portals in an automated way. Through this proposed framework, is intended to monitor and evaluate OGD quality, respectively OGD portals, and to show their progress/regress based on accumulated scores for different periods. The advantage of the proposed framework is the compatibility with any OGD Portal due to its flexibility of integration. The integration interface consists of only a few basic metrics but is necessary that almost the OGD portal possesses and can produce very compressive results. The other advantage is the possibility of extraction of collected data for further analysis and the introduction of artificial intelligence (AI) for prediction purposes to point out how the OGD portals will stand in the next period.

Keywords—Open data; government; datasets; evaluation; portals; framework

I. INTRODUCTION

Nowadays, the trend of open data is developing at a rapid pace, while constantly increasing amounts of open data boost of development. In this regard, the role of the European Directive for using and re-using public sector data boosts the new trend towards opening up government data [1, 2]. This trend of development has gained the attention of governments and other public sector bodies for opening their data. Thus, regardless of the administrative levels, the public sector bodies are one the main publishers and holders of information for i.e. registered companies, maps [3]. The public sector data entailed the possibility for use and reuse for commercial purposes [4] while the main goal remains the increase of quality of transparency and accountability of governments [5].

Initially, in 2009 the White House promoted the Open Government Data (OGD) initiative [6] which called on all democratic states to become part of this initiative by opening their data. A few years later, in 2011, the initiative named after "Open Government Partnership", in cooperation with civil society, was established and it aims to advance and promote open data. So far, 78 countries are members of this partnership that serve more than 2 billion people to promote and

strengthen the transparency and accountability of governments and increase public participation in policymaking. These institutional and global developments show that the promotion of open data has continued over the years resulting in an overall increase in the number of datasets in the disposition of citizens, scholars, businesses, and similar. Regarding terminology, in the literature exist different acronyms that differ from each other. Sometimes is referred to Open Government Data (OGD), but somewhere is used the short acronym "Open Data". When the term "Open Data" is used, it includes whatever data such: government, businesses, health, insurances, mappings, etc. But when the term includes the compound acronym as "government" or "national" it is sure that it referred to public data produced by public sector bodies [7].

The open data as a term has been addressed in early years, while the quality of open data was addressed first in 2006 by Berners-Lee is the first who published a scheme dedicated to open data quality which was based on 5 levels represented as stars [8]. This scheme is based on the quality of file format publication and rates file formats based on stars. While, data quality as a general concept is addressed in the early 90s when Wang et al discussed the dimensions for measuring data quality [9, 10]. leveled equations, graphics, and tables are not prescribed, although the various table text styles are provided.

The paper is organized as follows: Section 2 explains the methodology employed in this research; Section 3 addresses theoretical and other practices of OGD, national portals, existing frameworks, and existing portals that measure the quality of open data at the national level; Section 4 discusses the proposing and building of framework build, the scoreboard for measuring the quality of portals, the web-service for collecting information from national open data portals, data collection and classification, processing, and provision of real-time results through the dashboard, and the possibility of using of an API for data analysis by anyone or any third-party application.

II. LITERATURE REVIEW

The wide range of OGD may include data from various public sectors, agencies, the local level of government, ministries, universities, and many other public sectors, but all of these intersect in a portal entitled national portal or OGD

Portal [11]. The OGD portal is a national single point where public sector bodies (organizations) of the country make their data available with the purpose of strengthening transparency and integrity.

In addition, the OGD portals are a simple website interface through which they facilitate the use of published data so that citizens and other non-governmental actors can use them. The data published on these portals are usually recorded in the form of metadata organized in rows and columns containing different information depending on the government sector bodies [12].

These OGD portals have constantly changed, contributing to the needs and demands [13]. Initially, they only intended to serve as interfaces where data in the form of datasets are published, then over time and need, they have advanced, enriching themselves with other features [14]. The addition of other features based on needs has pushed forward a more efficient use of data [15]. The addition of various search filters, the provision of more information on the data producer, grouping in the form of data types such as (economy, public safety, finance, justice), etc., are some of the advancements in time. In combination with the above-mentioned functionalities, those OGD portals have developed their application programming interfaces (APIs) to allow the consumption and query of the data by the third-part application in an automated manner [15, 16]. The API is a software intermediary that allows two applications to talk to each other. The availability of this feature has greatly facilitated the work, where access to the resources of OGD portals can be automatically provided for the use of published data through a third application completely automatic.

The availability of APIs, especially for government open data portals, has given them many opportunities in addition to the automated use of resources, and also opened the way for analysis and quality measurement of portals, and publishing data [17]. In this context, several portals have been developed that aim to monitor the quality of open data portals at the national level including the global open data index [18], open data watch [19], open data barometer [20] etc. Compared with mentioned portals above, there is used a different approach proposing a new evaluation model. This model in principle is based on those portals but, unlike them, the proposed framework monitors and evaluates them in real-time by providing the following information: number of datasets, organizations, groups, tags, licenses, and type of datasheet formats.

Another characteristic of the proposed framework is that it uses a benchmark based on a multidimensional model that makes it a perfect combination. A framework in the context of data quality is a kind of assessment tool that helps to measure the data quality of organizations aimed to improve the quality. This combination uses file formats of published datasets and information about these datasets. All this nomenclature is defined as a framework model which easily interacts and expands with various national open data portals by connecting to their APIs. Initially will be applied to open data portals in

six western Balkan countries¹ (Albania, Bosna and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia).

III. RELATED WORK

This research paper analyzes and discusses the existing approaches that have been proposed and adopted for monitoring and evaluation of OGD quality. In addition, it discusses the actual frameworks proposed as well as current tools and portals for evaluation of OGD data quality aimed to propose the development of a new evaluation model framework employing qualitative and quantitative approaches combined and interacted to provide compressive evaluation results. This perfect combination is conceptualized as a framework model consisting of several other components discussed in further sections.

A. Existing Approaches and Tools

Open government data portals have continuously developed and advanced, particularly in developed countries where this revolution has initially begun [21]. Numerous needs for access to data have also influenced the further development and advancement of national OGD portals. This development and advancement include the improvement of data quality and quality of portals as well.

When it comes to quality, so far various aspects of data quality from the definition, types, dimensions, techniques, strategies, and multidimensional proposals have circulated [22, 23]. In this respect, different frameworks for measuring data quality have been developed. Since the purpose of research is based first on designing and conceptualizing a framework for measuring the quality of open government data, for this reason, different frameworks have been analyzed. According to Maurino et al. quality is related to dataset level, but the evaluation is performed at the portal level by aggregating the values computed on each dataset [24].

In addition to current frameworks developed, continuous progress has been made by building portals with the aim of monitoring and measuring OGD quality. In this context, different portals are available today such: open data index, open data barometer, open watch data, open data EU, etc. Some of them measure only OGD quality but some others monitor also the number of resources published by OGD portals in the context of datasets, organizations, licenses, etc.

Each of these portals uses its methodology based on the framework through which the quality of open data is measured or monitored. Based on the analysis performed, the frameworks that use classification of datasets based on the profile, for example (economics, judiciary, finance, law enforcement, statistics, health, etc.), as well as for each field questionnaires have been applied on publication of data such as: are they licensed? Are they in machine (readable) format, are they available? Can this data be manipulated by asking for sprawl? How often are the data published? etc. So, these types of calculations are used in the open data index frameworks, open data barometer using scores for each part of the

¹ Countries are listed based on alphabetic order

evaluation, and deriving the average result for each national OGD portal by ranking portals based on countries.

The following sections will discuss the features of each by comparing them.

The Open Data Barometer (OBD) is an advanced system that evaluates government open data. This system relies on score listing countries based on questionnaires on policies, implementation, and impact of data initiatives as well as openness assessment built from 14 data types for each country. So, this system evaluates datasets through a review process in 14 different areas such as legislation, transport, health, crime, procurement, etc.

Open Data Index (ODI) is a crowd-sourced indicator dedicated to the openness of datasets, which was founded by the Open Knowledge Foundation. Furthermore, the information on the datasets is collected based on the open data census, creating an index for each country, and scoring them by undergoing a process by going through 9 attributes based on the Open Definition. This rating system has an ideal value of 100 (maximum) for each attribute. The maximum weight is 30 points that are dedicated if the database is license open. While datasets that are not accessible have a score of 0.

Open Data Monitor, unlike the two systems mentioned above, is another similar system, so it has almost the same purpose, where in addition to evaluating the quality of OGD, it also monitors the available resources, presented in the visual form using the most innovative technologies. This system has a framework that is based on the dataset and metadata from OGD resources. The process of gathering the necessary information from national open data portals keeps it in a structured form for further processing. In this context, it uses analytical and visual methods to be user-friendlier for users and to give results in visual forms, unlike others that display in statistical form. Another value of this system is that it enables comparison between countries to also see visually the results of each. The platform uses the exposed APIs of the open data portals of the national level of the EU members. In terms of functions, this system offers a range of analytical functions such as comparison of public bodies (national/local), metadata quality, selection of catalogs for different fields, license information, published dataset formats, last updated, percentages, etc. All of these are characterized based on qualitative and quantitative methods. Quantitative refers to the quantity (number of resources) available, while qualitative includes the analytical functions mentioned above.

So, if compared to open data index and open data barometer, the open data monitor system is not global, but it is dedicated only to EU countries, it also uses analytical tools and displays data in a very attractive way using tools for data visualization. It is important to note that the latter (open monitor data) in contrast shows information only until 2015, while the open data index and open data barometer display data based on the current global situation. Since our research aims to measure the quality of portals and monitor them, the analysis of existing frameworks will help build a multi-functional framework that performs quality measurements and monitors at very frequent periods each week.

In addition to analyzing existing OGD evaluation portals, few scientific articles have been reviewed related to benchmark frameworks. According to Renta Machova et al, they have used other data sources and different information they have collected [25]. Also, the framework proposed by them consists of more than 20 metrics that complicate the process of evaluation due to the high probability of changing and updating portal APIs. Also, is not sure if all portals possess those metrics information. While according to Antonio Vetro et al they also have proposed a framework that is based on two dimensions consisting of several metrics of around dataset and other metrics for evaluating data quality of data within the dataset [26]. So, besides the information about the publication of the dataset this framework measures the quality of data inside the dataset (records). It is very valuable, but there is not implemented in any machine for performing an automatic evaluation, but they have applied it manually by checking each portal separately. Referring to Peter Parycek et al, they have developed a method for evaluation of OGD that is applied in the city of Vienna [27].

This method is based on surveys prepared and sent to respondents. A framework proposed by them is more suitable for regulating data publication and provides recommendations on how to publish high qualitative data than evaluation of existing data published.

Therefore, compared with those frameworks, the proposed framework uses a different approach, it can be easily scalable and can be implemented and integrated into application in a very easy way. Initially, the information target to collect is very basic, so most of the portals possess this information, and the probability to change the APIs or missing this information is very low. This empowers the proposed framework because with only a few metrics will be possible to evaluate and monitor the OGD portals at any time. Based on the discussion about existing frameworks, something different will be proposed that will fit any portal, be well integrated, and works independently with no need for human intervention.

Once collecting and storing of data into the database will be performed from target portals, another feature of the proposed framework is the ability to share data through the API to anyone that may be interested in further development, analysis, or using any third-party application, it is possible only by integration or API provided.

IV. RESEARCH METHODOLOGY AND METHODS

This research utilizes a qualitative approach applying mixed methods that combine analytical rigor and data gathering, as well as monitoring and evaluation.

Intention to build a framework model for monitoring and evaluation of the quality of OGD portals based on a scoreboard that displays the scores for each dimension metric is based on specific methodology. In this respect, the proposal for the build-up of the framework model is divided into several phases as follows:

Phase I. Analysis of OGD National portals, their review, and general evaluation of whether these portals provide APIs as a prerequisite for further monitoring and evaluation.

Phase II. Identify resources within selected portals, what APIs they offer, and find common denominators to ensure that all selected portals meet each parameter set.

Phase III. Proposing of benchmark framework design based on analysis of existing OGD portals. This proposed framework will perform monitoring of OGD portals and evaluate quality.

The proposed framework is designed taking into account the following steps:

- 1) Analysis of existing frameworks for measuring the quality of open government national portals.
- 2) Targeting data sources for application of the framework.
- 3) Defining the dimensions to be applied.
- 4) Defining metrics for each dimension.

Phase IV. Once the framework is defined, it remains to be integrated into the framework model, which consists of several components, starting initially with the first component of the web service that will have several roles:

- 1) Integration/interconnection with APIs of targeted portals in this research.
- 2) Collection of data required for the Framework definition in Phase III.

Phase V. Once the necessary data has been provided, there is now another phase, which deals with the processing of this data, the analysis, and displaying of the data. Furthermore, within this phase, there will be some processes as follows:

- 1) Data processing through validation and cleaning process.
- 2) Application of the application-level framework for measuring the quality of the processed results.
- 3) Display results in the Web interface (dashboard) in real-time for OGD portals that have been selected.

Phase VI. Developing an API and making it available to anyone. It will provide the data collected by saving time and work because there is not necessary to connect each portal APIs for getting data, since this data already exists but will be shared through an API.

V. ANALYSIS OF OPEN GOVERNMENT DATA PORTALS

The main purpose of this research is to propose and build a system or tool that will consist of many components defined as a framework model that monitors and measures the quality of national open data portals in an automated way. Therefore, a basic prerequisite for building a framework is the definition of basic needs. Thus, first, it is necessary to analyze portals that will be the target of monitoring and evaluation, which include Western Balkans national open government data portals, (Albania, Bosnia and Herzegovina, Kosovo, North Macedonia, Montenegro, and Serbia) [31-36].

Various analyses over the OGD national portals can be applied using different criteria [28]. In this respect, five criteria analysis will be used for designing a benchmark framework and these criteria include the following questions:

1. Does the portal provide and have an available API for connection?
2. Does the portal provide the datasets for each publisher?
3. Does the portal provide the file format types published for each dataset?
4. Does the portal provide the published dates and last updates of datasets published?
5. Does the portal provide the license used for each dataset?

These five criteria are the fundamental precondition for the selection of government portals for further monitoring and evaluation.

Since the term “a framework” has been used everywhere in this research, it means that will be applied to only a few OGD portals, but with the potential to be applied to other OGD portals. For the building of the framework, initially, some preconditions have been defined starting with information that should be collected because for sure that designing of the framework will be based on such information. In this regard, the analysis of available information will be performed, respectively what information the national OGD portals offer and if all OGD portals share this information.

The following table shows the necessary information and information identified in each government portal analyzed. The same information will also be used for designing the framework model.

The data defined in Table I, in addition, to building the framework model will assist the web service how to know what data to collect from the portals.

Moreover, the analysis depicts the lack of proper organization, so no standard has been used compared to the open government portals of other EU member states. Even though these portals support more than one language, the mother tongue of the countries dominates. For example, when a dataset or resource is published, the same should be published in at least another international language (English); however, these publications are mainly done in the mother tongue language.

The analysis also highlights the inadequate standards of file formats used for data publishing. In this context, it emphasizes that portals also use formats of published metadata that are out of range according to open data standards. In addition, there are identified about 20 types of dataset file-formats including formats that have used compression (.zip, .rar) that are out of any criteria. For instance, Cyrillic letters are out of any standard for extensions or international standards, yet they are used.

TABLE I. THE TARGET OF INFORMATION TO BE COLLECTED

	Target Data	Types of Information
Quantitative	Datasets	Number of Datasets
	Publishers	Number of Organizations
	Groups	Number of Groups
	Licenses	Number of Licenses
Qualitative	Datasets	Dataset File Format Types
	Publishers	Publisher's Names
	Groups	Public Sectors Bodies
	Licenses	Types of Licenses

There are other cases where the publication date is outside the standard or they show no information concerning the data published. This context complicates the qualitative evaluation of the data. Thus, it was necessary to use techniques for equivalence of this data, to be able to evaluate the data. Lack of up-to-date dataset descriptions (What database is it? Who owns it?). In addition, these are only a few of the findings that have been identified during the analysis of portals and which at the same time have complicated and challenged the measurement of data quality. Then the lack of the type of licenses, under what license the published data operate, the lack of frequent updating, or the date of the publication itself, so all these are some of the findings during the analysis phase of the portals.

Therefore, this leads to the need to build a mechanism that would fix these problems during the publication phase where it would ensure the high quality of the published metadata but also the portal itself that serves that data.

Therefore, this is the reason why this paper, in addition to measuring the quality of data, also measures the quality of the national open data portals themselves.

In addition to these findings, the possibilities offered by these national open data portals for the automatic consumption of data that supports third-party applications. In this aspect, is almost clear that each portal provides the possibility of consuming data through APIs, so there is an API available, while each has its limits in the context of what they offer. CKAN based API mainly dominates, but some are based on DKAN. This also fulfills the primary condition, the collection of initial data. Although the documentation on how to consume these APIs, exists in their mother portals, even in the national portals they have published additional documentation, this also facilitates the use of the method for data collection.

CKAN² is the world's leading open-source data portal platform. It makes easy publishing, sharing, and working with data. In addition, it is a kind of data management system that provides a powerful platform for cataloging, storing, and accessing datasets with a rich front-end, full API (for both data and catalog), visualization tools, and more [29].

DKAN³ is a Drupal-based open data portal based on CKAN, the first widely adopted open-source open data portal software. CKAN stands for Comprehensive Knowledge Archive Network [30].

Table II presents the APIs of the Western Balkan countries, where this framework model will be applied.

TABLE II. NATIONAL OGD PORTALS APIS AND URLS

Country	OGD National Portal URL	API Model
Albania	https://opendata.gov.al/	CKAN
Bosna and Herzegovina	https://opendata.ba	DKAN
Kosovo	https://opendata.rks-gov.net/	CKAN
Montenegro	https://data.gov.me	CKAN*
North Macedonia	https://data.gov.mk/	CKAN
Serbia	https://data.gov.rs	CKAN*

² CKAN, (www.ckan.org/about/).

³ DKAN Open Data Platform (ww.getdkan.org)

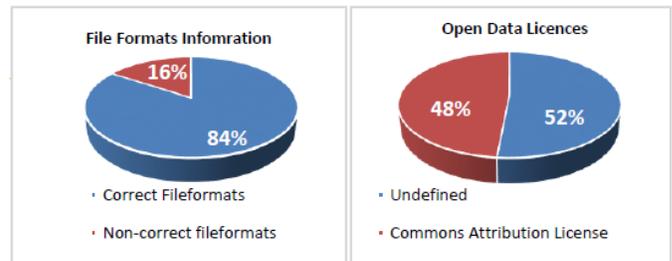


Fig. 1. (a) Analysis of File Formats Published; (b) Analysis of Licenses.

CAKAN* means that national portals have developed their API for providing information but is based on the CAKAN model. It is important to note that it is well explained with detailed information on how to use API. Apart from the investigation of APIs from the Western Balkans OGD national portals, there is analyzed the target information defined in Table I, with the attention of possible interventions on quality improvement if needed. Therefore, Fig. 1 shows the analyzed information for (a) file formats and (b) open licenses.

B. Authors and Affiliations

Correct file formats include formats published in PDF, DOC, XSL, XSLX, CSV, HTML, XML and JSON. Non-correct means the other types. While regarding licenses, the Open Data Commons Attribution License is a license agreement intended to allow users to freely share, modify, and use this Database subject only to the attribution requirements set out in Section 4⁴ (Open Data Commons Attribution License ODC-By).

VI. PROPOSING OF FRAMEWORK

The proposal for the building of the framework model consists of several components and each component has its role. Because the analysis performed over OGD Portals, it precisely defines all the flaws and what information is available and can be collected from the portals for the framework model to perform its function. Fig. 2 presents all block components.

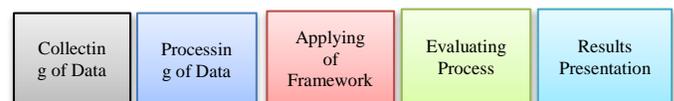


Fig. 2. The Components of Proposed Model.

First, this component means building a web service that will collect data from the OGD national portals that are targets for monitoring and evaluation. Second, this component will do data processing through insertion into the local database and data preparation. Third, conceptualization and designing of the framework. Fourth, implementation of a framework into the software application, and the fifth component is dedicated to results showing in a dashboard. The following sections explain the role and function of each component separately.

A. Collecting of Data

The first step to secure the information mentioned in the sections above is to develop a web service that will be able to

⁴ <https://opendatacommons.org/licenses/>

communicate with OGD national portals of the Western Balkan countries using the APIs available. Depending on the need, the web service can monitor and collect information on a daily, weekly, or monthly basis, made possible through configuration. Since the government data portals are open, during the analysis they did not show that they publish a large number of resources daily, the web service developed can run on a schedule on a daily, weekly basis, or monthly basis. But it depends on needs.

For the development of web services, the Microsoft .NET platform is used. The reason for using the Microsoft platform is due to practical experience and not for any other reason. Yet, this could be developed using other platforms such as java, python, visual basic, etc. Regarding the functionality of the web service, it is compiled to run as a console application. It means that the web service will not be running all the time but is configurable to run on schedule. It depends on how frequently portals publish resources or how often is needed to have refreshed results.

This process is called "Snapshot". Let's say the last snapshot is (01/08/2021 12:33), which means that the monitoring and evaluation process was performed on the data collected by (01/08/2021 12:33), indirectly the last run of web-service for collecting information was at 01/08/2021 12:33. Moreover, snapshots can be created on each day, which indirectly means that the web service will run each day at a specific date and time, respectively based on the schedule configuration. Running of web-service is not a process that only establishes connections to respective APIs, but on the other hand, it collects information. Fig. 3 shows the information that the web service will collect.

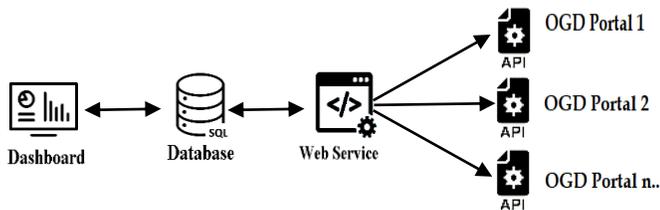


Fig. 3. Collecting of Types of Information.

B. Processing Data

After collecting the targeted data, there is another extra-independent process called data processing. Within this process, three other sub-processes are performed (insertion, validation, and data cleansing). These are very important to prepare the data for further evaluation and analysis.

1) *Data inserting*: For the collected data to be always accessible and available, there is necessary to be stored somewhere. For this purpose, a small, but very useful database is developed. This database will also be used for other purposes such: processing of information, analysis, statistics, and showing other results. The database is developed in Microsoft SQL Server 2016 (Express Edition) but does not limit the possibilities of using other platforms. There is no reason why this platform is used, other than experience and cost-free.

As mentioned above, the analyzed portals have relatively low-quality data, so the preparation of data is inevitable, to increase the quality and enable a more accurate assessment. Given that, the web service does not do this job, it will only collect data but another sub-process will be needed (Data Preparation).

The insertion process is based on an algorithm built for this purpose, which collects the resources defined in Fig. 2 and stores them in this database based on the logic explained in Fig. 4.

```
public static void GetDataKosovo()
{
    int PortalID = 1;
    string Organisation = "";
    string OrganisationURL = "";
    int Datasets = 0;
    using (OGDEntities db = new OGDEntities()) {
        var datasetList = db.Datasets.Where(x =>
            x.PortalID == 1).ToList();
        db.Datasets.RemoveRange(datasetList);
        db.SaveChanges();

        var FileFormat = db.FileFormat.Where(x =>
            x.Organisations.PortalID == 1).ToList();
        db.FileFormat.RemoveRange(FileFormat);
        db.SaveChanges();

        var all = db.Organisations.Where(x => x.PortalID
            == 1).ToList();
        db.Organisations.RemoveRange(all);
        db.SaveChanges(); }
}
```

Fig. 4. Collecting and Inserting of Data.

2) *Data correction*: Once all the data defined above have been successfully collected and stored into the database, these data will be subject to the validation process for making it ready for further processes. After the data review process, it identifies that a few data should be corrected and validated. In this matter, have been set some criteria's for correcting and validating data and figured out which data should be subject to validation. The fields of data that should be validated and corrected include publication date-time or last updates, name of licenses, and file format extensions. The next paragraph will discuss the problems of poor data quality gathered. First, there is checked for formats (extensions) of datasets, and in initial findings figure out that about 16% of them are out of range of open data standards (open data standard). Many file extensions were published in the wrong format for i.e. instead of JSON is used "GEJSON" or in the Cyrillic Alphabet in the native language is written. Second, we applied the validation to the date/time and updated dates of datasets published.

This is because each portal has used its time format such as (2020-01-10, 20-Feb-21 or Jan-03-2021 or May / 12/2021), therefore based on these facts is needed the validation of time, turning them into an acceptable standard YYYY / MM / DD. The same was done with licenses, because in the findings during the analysis, about 52% of licenses were undefined, or not in the standards defined by open knowledge (Licenses - Open Data Commons: legal tools for open data).

After completing the process of data correction and validation, the precondition for data comparison between portals has been completed, but there are some issues with unnecessary data and the existence of numerous null values.

3) *Data cleansing*: In addition to the validation process, which means the transformation of data from one data to another without spoiling its character, we have also applied data cleansing. This sub-process has been very adequate, initially to remove useless information about the framework. Web-service collects different information, depending on how they are published, but does not use any method that validates or corrects them during the inserting process because it would complicate the whole process. Therefore, after collecting and inserting data into the database, we have applied a procedure that cleans by removing unnecessary data. During the data review process, we are faced with a lot of null values, lack of a standard for the naming of datasets and organizations for i.e. some dataset names and organization names have used the underline or line between words, some others have used spaces between, some other have used short letters for every publication made, etc.

First, removing of "null" values, and then unnecessary spaces between the names of organizations and datasets. Second, using the operations "Trim" and "Upper" for formatting the file formats extensions to have a standard and to increase evaluation accuracy.

Moreover, both sub-processes (data correction and data validation) are implemented in stored procedures of the database and both of them are triggered every time after the new snapshot. It means that every time the web service is run and after collected data is successfully inserted into the database, then those stored procedures will be triggered (executed). Fig. 5 shows two examples of data cleaning and data validation used by the framework.

```

BEGIN
SET NOCOUNT ON;
UPDATE dbo.Datasets
SET DatasetLastUpdate = null
WHERE DatasetLastUpdate =
'1900-01-01 00:00:00.000'
GO
UPDATE FileFormat
SET FileFormat =
UPPER(fileformat)
GO
UPDATE FileFormat
SET FileFormat= 'XLSX'
WHERE fileformat like '%XLSX%'
GO
UPDATE FileFormat
SET FileFormat= 'XML'
WHERE fileformat like '%XML'
END

BEGIN
SET NOCOUNT ON;
WITH cte AS (SELECT FileFormat,
OrganisationID, ROW_NUMBER() OVER
(PARTITION BY FileFormat,
OrganisationID
ORDER BY
FileFormat,OrganisationID
) row_num
FROM dbo.FileFormat
)
DELETE FROM cte WHERE
row_num > 1;
DELETE f from
dbo.FileFormat f
inner join
dbo.Organisations o on o.id =
f.OrganisationID
WHERE o.Organisation = '955'
END
    
```

Fig. 5. Examples of Data Validation and Data Cleansing.

C. Conceptual Design of Framework

Once the data preparation process has been completed, i.e., the data served is ready for further processing, this paves the way for the design or development of the framework. Where in the state of art, we had argued quite well, the existing

frameworks, showing the features and characteristics of each. Now designing the framework is considered the main work that also gives the main value of research. The proposed framework will be two-dimensional, which means it performs two different functions: monitoring national portals and measuring their quality. Therefore, for this purpose, will be used two indicators: Qualitative Indicator and Quantitative Indicator.

1) *Quantitative indicator*: This indicator is based on the quantitative methodology, which will have a monitoring role, which will monitor portals that count publishers, datasets, licenses, and group datasets based on the file format that is published based on the 5-star scheme. Furthermore, in Table III, we present the metrics that this indicator uses:

TABLE III. METRICS OF OPENNESS INDICATOR (QUANTITATIVE)

Scores	Description	Key
★	whatever format pdf, image, doc, text	Open License
★★	machine-readable structured format .xml, .xlsx	Readable
★★★	non-proprietary structured format, csv	Open Format
★★★★	RDF Standards xml, html, json	URL
★★★★★	Linked to other data sources	Linked Data

Each dataset is subject to the process of evaluation, evaluation based on the file format that has been published. Observations are used to give (scores) for each metric that will be applied over datasets.

2) *Qualitative indicator*: Unlike the quantitative indicator, here it will do processing of information that characterizes a dataset. In this aspect, it is characterized by four main features of the dataset which we estimate affect their quality as well as the portal itself. Table IV presents the metrics used by this indicator for evaluating datasets giving it a score.

TABLE IV. METRICS OF DATASET INDICATOR (QUALITATIVE)

Observation	Metric	Description
[DAV]	Availability	Dataset is available in the portal
[DAC]	Accessibility	Dataset can be freely downloaded
[DAD]	Discoverability	Dataset is searchable (query data)
[DAT]	Timeless	Dataset is up to date

D. Assessment and Evaluation

The Framework mentioned in the above session, consisting of two indicators (quantitative and qualitative), will be applied to the framework, practically different functions translated into SQL will be used, which will produce the right results. Practically, as soon as the process of importing or inserting data from the web service in the Database has been completed, as well as the process of validation, correction, and cleaning, the data are ready for evaluation. In addition to these processes, another pre-evaluation process will be data modeling so that the application of the framework is easier.

In this regard, have been created and used several Database Views in particular for monitoring portals in quantitative terms, how many databases are available, and how many organizations publish data. Dynamic Views have been used to reflect the results dynamically on every update that may happen. This is shown in Fig. 6.

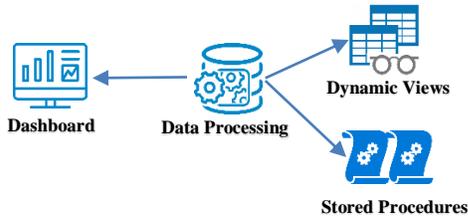


Fig. 6. Data Processing and Evaluation.

The whole monitoring process is based on VIEWS, so this is the reason for using Dynamic rather than static Views due to the changes of results dynamically based on last updates. Moreover, the proposed framework is divided into several segments; each segment uses a stored procedure, so there is no technical possibility for the whole framework to be incorporated in one stored procedure. This is due to a lot of calculations that have to be done for providing evaluation results. However, these segments depend on the metrics, which means that each metric is a stored procedure in itself.

These stored procedures will be used by the front-end part (Dashboard) illustrated in Fig. 6 quantitative indicator part, then the stored procedure of grouping and evaluating the datasets based on the file formats based on So, depending on the evaluation required, it will call and execute a specific stored procedure. Let's say, if the interest is in the 5-star scheme of Berners-Lee, will be executed and the result will be returned. However, if the interest is in the qualitative indicator, then the procedures for each metric will make their calculations and will yield the result, or both indicators, for each metric we measure by giving points (scores). For example, the data openness evaluation, which is based on the 5-star scheme, measures how open the datasets are based on the publication formats, here the evaluation is done from 1 to 5. Finally, the average for the portal. As for the qualitative indicator, this is based on the quality of the dataset based on the surrounding factors explained in Table VI.

In contrast, here the ideal or maximum value is 1 per metric, while 5 maximum values if a dataset contains all metrics. Here too a series of calculations are performed in the background, where in addition to deriving the average for each dataset that is subject to evaluation, the general average per portal is also derived. This is very important in the analytical and comparative part between open data portals. Fig. 7 presents some parts of the code for specific metrics.

```

SELECT
    PortalID,
    CONVERT (NUMERIC(10,2),
    (@avaliability/COUNT(Dataset
    AvariabilityURL))) as
    Avariability,
    CONVERT (NUMERIC(10,2),
    (@accessibility/COUNT(Dataset
    Accesability))) as
    Accesability,
    CONVERT (NUMERIC(10,2),
    (@discoverability/COUNT(Dat
    asetDiscoverability))) as
    Discoverability,
    CAST(@timeless AS
    DECIMAL(10,2)) as Timeless
FROM dbo.Datasets
WHERE PortalID = @PortalID
GROUP BY PortalID

SET @1star = (
SELECT SUM(number) from
dbo.FileFormat
WHERE FileFormat in ('PDF',
'DOC', 'DOCX', 'TXT'))
SET @2star = (
SELECT SUM(Number) from
dbo.FileFormat
WHERE FileFormat in ('XLS',
'XLSX'))
SET @3star = (
SELECT SUM(Number) from
dbo.FileFormat
WHERE FileFormat in
('CSV'))
SET @4star = (select
SUM(Number) from
dbo.FileFormat
WHERE FileFormat in
('HTML', 'JSON', 'XML'))
    
```

Fig. 7. Openness and Dataset Evaluations (SQL Code).

E. Presentation of Results

All calculations discussed in the section above, based on different scenarios are performed on the database level, so the results were displayed by SQL. To present these results in the right visual form, it was necessary to create a public portal in the form of interactive dashboards.

Therefore, for this purpose, a web application is developed using the .NET platform, which displays the monitoring results and measures the quality of government open data portals. The following section reflects some of the results obtained from the calculations performed to give the value final framework model, starting from the front dashboard that displays the monitoring results (see Fig. 10 in Appendix). While in Fig. 11 (Appendix), are presented the displayed results on the openness dashboard, which presents how open the portals are.

The evaluation was performed using calculations based on the openness dimension i.e., file formats of the datasets, grouping, and counting them.

The results are based on the quantitative indicator, as they do not use any other measuring feature of the dataset except the statistical one, i.e. counting and grouping. Furthermore, Table V shows the results of the qualitative indicator, i.e. the quality of the datasets, ranking the portals based following indicator metrics (Availability, Accessibility, Discoverability, and Timeless) shown in Table V.

TABLE V. DATASET INDICATOR AVERAGES (QUALITATIVE)

Country	Availa.	Access.	Discov.	Timeless
Albania	1	1	0.48	0.41
Bosna and Herzegovina	1	0.98	0	0
Kosovo	1	1	1	0.17
Montenegro	1	1	1	0.33
North Macedonia	1	1	0.81	0.25
Serbia	1	1	0	0.26

Regarding the results expressed in Fig. 8 and 9 in the background, a series of calculations are performed, but very important to show the countries' averages.

According to a mathematical point of view, for evaluating and measuring the averages of openness, the calculation is formulated using the following formula:

$$\gamma = \frac{\sum(1 \text{ star}) * 1 + \sum(2 \text{ star}) * 2 + \sum(3 \text{ star}) * 3 + \sum(4 \text{ star}) * 4 + \sum(5 \text{ star}) * 5}{\sum \text{Total datasets}} \quad (1)$$

This equation calculates the average of how open the governments are by adding the whole number of datasets rated with 1 star, then with 2 stars, so on up to 5 and proportional to the total number of datasets published for the portal. This formula is applied for cases when a dataset is published in only one format.

In addition, during the analysis of OGD national portals, this research finds out that some organizations (publishers) publish their datasets in multiple formats, for i.e. "Agency of Statistics" have published two datasets, in two file formats (CSV and JSON), while the dataset remained the same because it has the same unique ID and the same name. So, for situations like that, the formula above (1) does not promise the accuracy of results, because it calculates the total number of datasets and does not check and find out if the same dataset is published in multiple file formats. Thus, for this reason, a new approach for defining datasets published in multiple file-formats has been used.

This new approach is based on two levels of evaluation, first identification and then evaluation. Table VI illustrates this situation.

TABLE VI. IDENTIFICATION OF MULTIPLE FORMAT DATASETS

Datasets		★	★★	★★★	★★★★	★★★★★	Total	
Level I	Publisher	Dataset1	0	0	0	x		x
		Dataset2	0	y	0	0		y
		Dataset n			x	y		x + y
Level II	Publisher	Dataset 1						x
		Dataset 2						y
		Dataset n						y

Table VI shows that two levels of classification have been used; first, it makes classification of datasets based on file formats and counts the total number of datasets per organization (publisher). Then, after the first level is performed, the second level identifies if any of the datasets are published in multiple file format and counts only the number of higher file formats as total by removing from the calculation of other formats published.

Referring to Table VI, in the first round of calculation "Dataset n", has multiple values (x+y), while in the second round, is identified that this dataset.

$$\delta = \frac{\sum H(n \text{ star}) * n}{\sum H \text{ Datasets}} \quad (2)$$

H – means the highest Star of the dataset.

The final equation for generating the total average of result will be:

$$f(x) = \gamma + \delta \quad (3)$$

f(x) – is the function of calculating the overall average of openness calculation.

Based on this function, Fig. 8 shows the averages of evaluation of OGD nation portals. Results have been grouped on monthly basis to show progress.

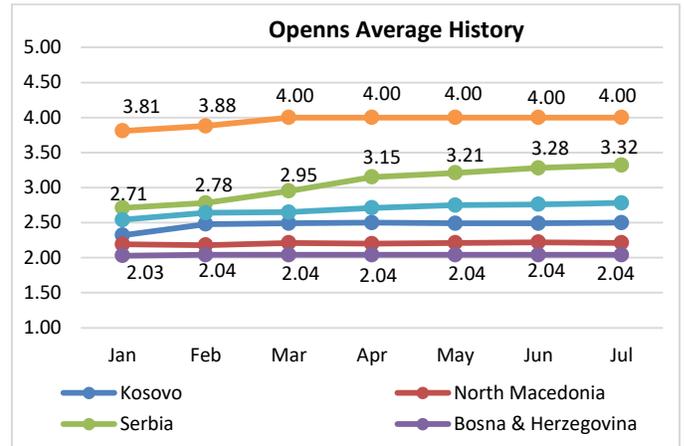


Fig. 8. Openness Averages.

In addition, the calculation of dataset quality is based on formula (4). It calculates the total average per OGD portal, respectively, it sums all the values obtained per metric in proportion to the total number of metrics used.

$$\lambda = \frac{\sum(Avaliab.) + \sum(Access.) + \sum(Discover.) + \sum(Timelss) + \sum(n..)}{\sum(Metrics)} \quad (4)$$

Fig. 9 shows the results produced by this formula, which is applied in the background of the application, respectively in the database implemented through SQL functions. The highest value is 1 and the lowest is 0.

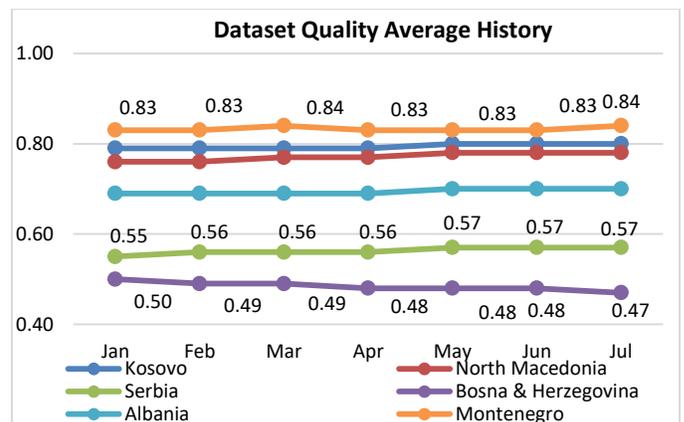


Fig. 9. Dataset Quality Averages.

In addition, the application also generates statistics, where all the results expressed in graphs, are summarized using a statistics dashboard. Statistics may change in the meantime or after each run of the web service because the data will be

refreshed. All this is done automatically without the need for the human factor to intervene.

Moreover, all the data collected by the portals through the web service, after being subjected to the process of validation and clearance, can be accessible to anyone who needs this data. For this purpose, there is necessary to make available an API, which upon request returns the basic results that the web service collects such: datasets, organizations, licenses, file format types. All this is organized through a JSON API, where depending on the request, i.e. for which national portal they are required, it also returns the data. This is made available, to provide data for call part application, or anyone who needs for educational, scientific, or business purposes to have the data ready without having to develop any additional web services that take from the portals of the western Balkan countries.

VII. RESULT AND DISCUSSION

Through this proposed framework model is intended to monitor and evaluate OGD quality, respectively OGD portals constantly or at any time with no need for human input. An additional value of the proposed framework is that it will have the ability to show the progress/regress made by each OGD national which has been subject to monitoring and evaluation and scored in different periods.

Because of data possessed through the data collection component (web-service), the proposed framework model can show results at any time but it also can be configured to run on schedule on weekly basis or monthly basis depending on needs. Storing of evaluation history scores for each OGD Portal and visualization of results through the graphs about the progress or regress of countries gives another value to this framework. In addition to monitoring and evaluation affinities, the proposed model shares the API that will be available to the wider community or it can be used by third-party software applications with the purpose of further analysis and evaluation or extending the research by conceptualizing any new framework.

Therefore, another value for future work would be considered adding of "data prediction" feature. This feature would be possible and could be easily integrated using Artificial Intelligent (AI). This feature could be able to predict how these countries (OGD national portals) are going to publish in the coming months or a specific period. For instance, if there will be used a simple method i.e. 80/20 that means using 80% of training data and 20% of testing data, it would be easier to forecast the profiles of countries, the number of dataset publications by each publisher, types of dataset file formats and the number of file formats, publishing frequency, etc.

All these predictive data could be forecast for a specific period i.e. 6 to 12 months or probably in next 2 years.

VIII. CONCLUSION

Based on the study and analysis of existing frameworks for the evaluation of OGD portals, this research employed a new approach that is conceptualized and implemented through a flexible framework. This framework is considered flexible because of its adoption to any OGD portal and the ability to be

available to the wider community for further research and analysis. Since the framework is composed of several components, it employs qualitative and quantitative approaches that are combined and interacted to provide compressive evaluation and monitoring results of OGD national portals.

ACKNOWLEDGMENT

We would like to thank the Laboratory of FINKI (Faculty of Computer Sciences and Engineering at Ss. Cyril and Methodius University) for providing all hardware and software resources for building and publication of the whole project including all components as well as hosing the project for further analysis and research. Without this reflection, would not be possible to evaluate the OGD Portals.

REFERENCES

- [1] Janssen, K.. "The influence of the PSI directive on open government data: An overview of recent developments. *Government Information Quarterly*", 28(4), 446-456. D.E. Perry, A.L. Wolf, Foundations for the study of software architecture, ACM SIGSOFT Softw. Eng. Notes 17 (4) (1992) 40-52.
- [2] European Commission. Proposal for a Directive of the European Parliament and of the Council on the re-use and commercial exploitation of public sector documents, COM (2002) 207 final 18 European Commission (2008).
- [3] Vickery, G. Review of recent studies on PSI re-use and related market developments. Information Economics, Paris , 2011.
- [4] Rosacker, Kirsten M., and David L. Olson. "Public sector information system critical success factors." *Transforming Government: People, Process and Policy* (2008).
- [5] Ubaldi, B. Open Government Data: Towards Empirical Analysis of Open Government Data Initiatives. Tech. rep., OECD Publishing. (2013).
- [6] O. Whitehouse. Transparency and Open Government. [Online]. Available: <https://obamawhitehouse.archives.gov/the-press>. 2009.
- [7] Magalhaes, Gustavo, Catarina Roseira, and Sharon Strover. "Open government data intermediaries: A terminology framework." *Proceedings of the 7th International Conference on Theory and Practice of Electronic Governance*. 2013.
- [8] Berners-Lee, T. Linked data-design issues. Tech. rep., W3C, <http://www.w3.org/DesignIssues/LinkedData.html>. (2006)
- [9] Wang, R. & Strong, D. Beyond accuracy: What data quality means to data consumers. *J. Manage. Inform. Syst.* 12, 4. (1996).
- [10] Wand, Y. & Wang, R. Anchoring data quality dimensions in ontological foundations. *Comm. ACM* 39, 11. (1996).
- [11] Thorsby, J., Stowers, G. N., Wolslegel, K., & Tumbuan, E. Understanding the content and features of open data portals in American cities. *Government Information Quarterly*, 34(1), 53-61. (2017).
- [12] Van der Waal, S., Węcel, K., Ermilov, I., Janev, V., Milošević, U., & Wainwright, M. Lifting open data portals to the data web. In *Linked Open Data--Creating Knowledge Out of Interlinked Data* (pp. 175-195). Springer, Cham. (2014).
- [13] Umbrich, J., Neumaier, S., & Polleres, A. Quality assessment and evolution of open data portals. In *2015 3rd international conference on future internet of things and cloud* (pp. 404-411). IEEE. (August, 2015).
- [14] Ham, J., Koo, Y., & Lee, J. N. Provision and usage of open government data: strategic transformation paths. *Industrial Management & Data Systems*. (2019).
- [15] Kalampokis, E., Karamanou, A., Nikolov, A., Haase, P., Cyganiak, R., Roberts, B., ... & Tarabanis, K. A. Creating and Utilizing Linked Open Statistical Data for the Development of Advanced Analytics Services. In *SemStats@ ISWC*. (October, 2014).

[16] Yang, S. Quality Diagnosis of Library-Related Open Government Data: Focused on Book Details API of Data for Library. Journal of the Korean Society for Information Management, 2020 37(4), 181-206.

[17] Thorsby, J., Stowers, G. N., Wolslegel, K., & Tumbuan, E. Understanding the content and features of open data portals in American cities. Government Information Quarterly, 34(1), 53-61. (2017)

[18] ODI- Global Open Data Index (Methodology - Global Open Data Index (okfn.org))

[19] Open Data Inventory—Global Index of Open Data - Open Data Inventory (opendatawatch.com), (2021).

[20] Methodology | Open Data Barometer (opendatabarometer.org), (2021).

[21] Sayogo, D. S., & Pardo, T. A. Exploring the motive for data publication in open data initiative: Linking intention to action. In 2012 45th Hawaii International Conference on System Sciences (pp. 2623-2632). IEEE.(January, 2020).

[22] Strong, D. M., Lee, Y. W., & Wang, R. Y. Data quality in context. Communications of the ACM, 40(5), 103-110. (1997).

[23] Milani, M., Bertossi, L., & Ariyan, S. Extending contexts with ontologies for multidimensional data quality assessment. In 2014 IEEE 30th International Conference on Data Engineering Workshops (pp. 242-247). IEEE. (March, 2014).

[24] Maurino A., Spahiu B., Batini C., & Viscusi G. Compliance with Open Government Data Policies: an empirical evaluation of Italian local public administrations, Twenty Second European Conference on Information Systems, Tel Aviv,(2014).

[25] Máchová, R., Hub, M., & Lnenicka, M.. Usability evaluation of open data portals: Evaluating data discoverability, accessibility, and reusability from a stakeholders’ perspective. Aslib Journal of Information Management. (2018).

[26] Vetrò, A., Canova, L., Torchiano, M., Minotas, C. O., Iemma, R., & Morando, F. Open data quality measurement framework: Definition and application to Open Government Data. Government Information Quarterly, 33(2), 325-337. (2016).

[27] Parycek, P., Höchtl, J., & Ginner, M. Open government data implementation evaluation. Journal of theoretical and applied electronic commerce research, 9(2), 80-99. (2014).

[28] Nikiforova, A., & McBride, K. Open government data portal usability: A user-centred usability analysis of 41 open government data portals. Telematics and Informatics, 2021 58, 101539. (2021).

[29] CKAN, (<https://ckan.org/about/>).

[30] DKAN Open Data Platform (<https://getdkan.org>).

[31] Open data Montenegro (<https://data.gov.me>).

[32] Bosna and Herzegovina (<http://opendata.ba>).

[33] North Macedonia (<https://data.gov.mk/>).

[34] Serbia, Data.gov.rs. (<https://data.gov.rs>).

[35] Albania, OpenData Faqja Kryesore (<https://opendata.gov.al>).

[36] Kosovo, RKS Open Data (<https://opendata.rks-gov.net>).

APPENDIX

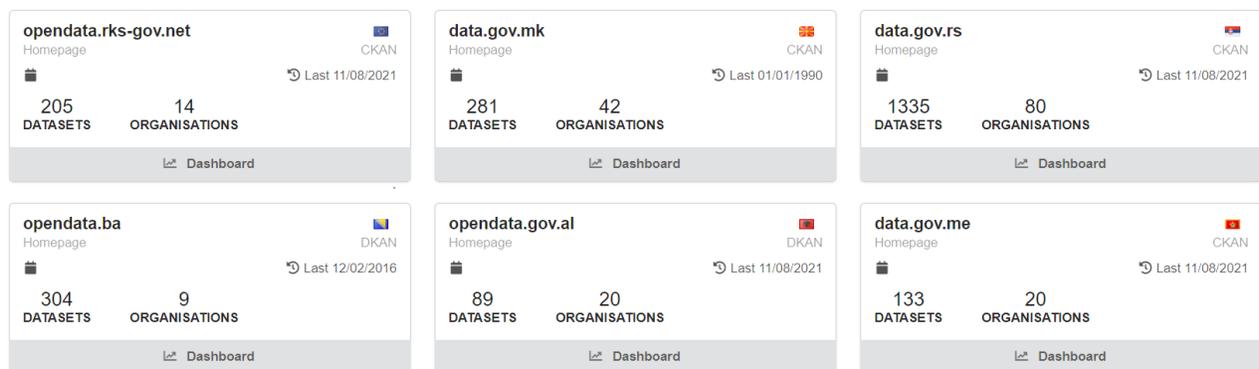


Fig. 10. Monitoring of OGD National Portals (Front-end of Portal Developed).

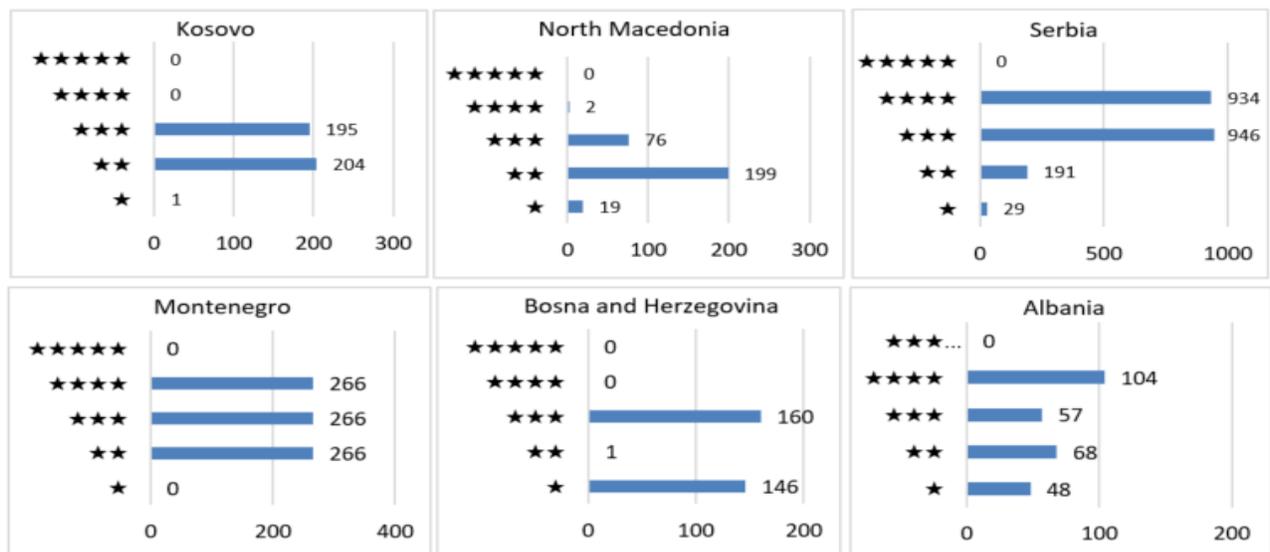


Fig. 11. Openness Evaluation (Evaluation results Presented by Graphs for each Country OGD Portal).

Deep Learning for Arabic Image Captioning: A Comparative Study of Main Factors and Preprocessing Recommendations

Hani Hejazi^[0000-1111-2222-3333], Khaled Shaalan^[0000-0003-0823-8390]

Faculty of Engineering and IT
The British University in Dubai UAE

Abstract—Captioning of images has been a major concern for the last decade, with most of the efforts aimed at English captioning. Due to the lack of work done for Arabic, relying on translation as an alternative to creating Arabic captions will lead to accumulating errors during translation and caption prediction. When working with Arabic datasets, preprocessing is crucial, and handling Arabic morphological features such as Nunation requires additional steps. We tested 32 different variables combinations that affect caption generation, including preprocessing, deep learning techniques (LSTM and GRU), dropout, and features extraction (Inception V3, VGG16). Moreover, our results on the only publicly available Arabic Dataset outperform the best result with BLEU-1=36.5, BLEU-2=21.4, BLEU-3=12 and BLEU4=6.6. As a result of this study, we demonstrated that using Arabic preprocessing and VGG16 image features extraction enhanced Arabic caption quality, but we saw no measurable difference when using Dropout or LSTM instead of GRU.

Keywords—Deep learning; NLP; Arabic image captioning; Arabic text preprocessing; LSTM; VGG16; INCEPTION V3

I. INTRODUCTION

Social media has increased the number of images uploaded to the web. In June, 2019 Facebook received 300 million photos a day, while Instagram received 95 million [1]. Additionally, the advent of smart devices and cameras in public places has created a challenge for automatic captioning of images to search for images by content or by human language, as well as for video context descriptions.

Image Captioning (IC) involves a lot of work since it starts with detecting and identifying objects, then it relates these detected objects, and finally it translates them into human understandable text by using their language syntax and semantics. A lot of efforts were done to overcome these challenges and a good result was achieved using deep learning techniques.

Most of the work was based on western languages. As a result, language translation was applied to benefit from these models in different languages, but the results were not as good

as the original language model. For example [2] and [3] show that building an image captioning model that generates Arabic captions outperforms an English based model with the aid of Arabic translation.

Many factors were studied to understand the effect of which on captioning, like Preprocessing method, Deep learning technique, Dropout usage, and image classifier.

1) *Dataset*: One public Dataset was found for this task [2] based on Flickr8K but with just three Arabic captions for each image. However, the original Flickr8K has five captions per image. Fig. 1 illustrates two samples of this Dataset.

2) *Image Features Extraction*: Building CNN is common for this task, but it requires a big dataset and high processing power. An alternative way is to use a pre-trained model, as an example [2] used VGG16 [4] as a features extractor. Our work also utilized Inception V3 [5], which provides a well-optimized trained model that can be utilized even without pre-processing and training.

3) *Arabic Text Preprocessing*: Arabic is obviously different from English and needs preprocessing. It might have diacritic signs which affect the word's meaning and use, but it is commonly ignored [6]. Moreover, we noticed that the conjunction Waw "(و)" in the Arabic Dataset is attached to the next word like "ويقول" (and-he-says). As per our preprocessing rule, if the letter Waw "و" (and) appears separately, it is removed as we remove all single character occurrences. Due to this, we decided to fix the typo.

4) *Models*: Experiments were conducted with two deep learning algorithms (GRU and LSTM), two image classifiers, and four preprocessing methods, resulting in 32 models. They were compared based on their performance.

5) *Evaluation*: Bilingual evaluation understudy (BLEU) metric is used to evaluate between different language translation and image captioning accuracy. For the purpose of comparing the effects of each understudy factor, we have used BLEU-1, BLEU-2, BLUE-3, and BLUE-4.



1 الناس يتزلجون على تلة مغطاة بالثلوج.
2 المتزلجين في الزي الموحد يتقدمون نوبلا على منحدر ثلجي.
3 هناك أربعة متزلجين على الثلج يتزلجون على جانب التل.

1 كلب يقف على مقعد على الثلج.
2 كلب يقف على مقعد بينما الثلج يتساقط.
3 الكلب يقف على شيء بينما الثلج يسقط حوله.

Fig. 1. Sample Images with Three Captions from [2] Dataset.

The contribution of this paper is to:

- Build 32 models using different parameters: 2 Deep learning methods (LSTM, GRU) X 2 With/Without Dropout X 4 Preprocessing techniques X 2 image classifiers (VGG16, INCEPTION V3), and compare the results to show the most significant factors.
- Compare the four Arabic language preprocessing techniques and compare their effects to illustrate the importance of preprocessing for Arabic versus English, where all reviewed articles do not preprocess the text.
- Develop an Arabic Image Captioning model that outperforms the best results on the publicly available dataset and use the latest Arabic Image Captioning (AIC) dataset as input to the model. Analyze the results from the perspective of Arabic preprocessing and the model's performance.

In the next section we review the related work done for both Arabic and English IC. In Section III, Methodology, experiment, and Dataset are described, then the results are discussed and comparisons were illustrated to show the enhancement achieved by each experimented factor in Section IV, at the last section we give some concluding remarks.

II. RELATED WORK

Recent work on Image Captioning is reviewed for both Arabic and English. We noticed that there is a lack of Arabic image captioning datasets available for tackling this task in Arabic compared to English.

A. English Image Captioning

The author in [7] introduced a convolution framework for image captioning consisting of four parts that begin with embedding layer for the input text, embedding for the input image, and then convolution model at the end embedding for output generation. A comparison is made against the LSTM

model on the challenging MSCOCO dataset. Another experiment was done based on feed forward network that can operate over all words in parallel, and the results outperformed the baseline LSTM model.

The author in [8] introduced a novel method for image captioning by using visual regions relationships, graph neural network and context aware attention mechanism for caption generation, memorizing previous visual content was the competitive edge in the model. The model is trained and tested on MSCOCO and Flickr30K Dataset, the reported results showed that this model can outperform the state-of-the-art attention-based methods as per the authors.

The author in [9] proposed new Visual Question Answering (VQA) model based on Cascading Top-Down attention (CTDA) captioning where each keyword in question is mapped to a region in the image. A good performance was demonstrated with VQA V2.0 and V1.0 datasets.

The author in [10] applied reinforcement learning with self-critical sequence training (SCST) with CIDEr metric as a reward. It is applied on MSCOCO dataset and the result was promising in its time.

The author in [11] introduced Bottom-up attention CNN by dividing the image into regions and features vector. The model was built on MSCOCO Dataset and showed a promising result.

The author in [12] built a model for captioning images, which was then applied to question answering based on MSCOCO datasets.

B. Arabic Image Captioning

The author in [2] have built end to end model for Arabic Image Captioning (AIC) based on image features extractor VGG16 and LSTM for language model. Also introduced a new public dataset for AIC. They found that directly generating captions from an Arabic dataset yielded better

results than translating captions from English datasets based on models generated from those datasets.

The author in [3] has used a subset of Fliker8K that consists of 2000 images and their Arabic caption in Jason file. A CNN was used for image features extraction for captions using LSTM. Two models for English and Arabic captions were introduced and the results showed that Arabic based captioning from genuine Arabic dataset has better results than those derived from English-to-Arabic translation dataset.

While the author in [13], explored generating the text based on the Arabic root using CNN ImageNet and mapping each root to an image region. Then finding the best word to describe the image using root words trained on RNN. The caption is generated through a dependency tree representing the generated words and their relations. 405,000 images from newspapers with their captions as well as those provided by Fliker8K were translated by professional translators. Unfortunately, this dataset was not yet made public.

The author in [14] also used two datasets: one with 5358 captions for 1176 images translated by human and the second has 150 images along with 750 captions. RNN was used. The evaluation showed promising results for a larger dataset.

The objective of this section is to provide a review of the various methods used for Image Captioning and to compare them with AIC research so we can identify any gaps that need to be addressed.

It is obvious that applying machine learning approach to AIC requires big data. Our study indicates that there is less research performed in AIC and this can be due to a lack of publicly available dataset for this task. Moreover, no results yet outperformed English captioning performance.

The majority of work is focused on reapplying the deep learning method used in English image captioning without considering the Arabic language and differences. As a result, we decided to examine the factors that influence Arabic image captioning. In addition, we found one public Arabic image captioning dataset that we can use for our experiments. Using this dataset, we will choose different factors that affect the task. The purpose is to identify factors that can outperform these studies' results.

III. METHODOLOGY

In this section, we describe the characteristics of the AIC dataset. We show how we apply the preprocessing task to produce appropriate training datasets. Nevertheless, we describe Deep learning models that act as image classifiers which we are able to use for extracting features from the images.

A. Dataset

For the Image Captioning (IC) task, finding or creating a dataset is crucial in general for having better prediction results. In English, there are many benchmark IC Datasets. For example, Flickr8K [15] contains 8000 images with 5 English captions per image. Likewise, Flicker30K [16] contains 30,000 images with 150,000 captions.

Flickr30K entities [17] are reusable images which contain the caption text for either a specific entity or region and can be used for searches or retrieval tasks.

The largest dataset is MS COCO [18] that contains more than half million captions, 330,000 images with five independent captions for consistent evaluation.

- 1) A little girl in a dress playing with a soccer ball.
- 2) A little girl in a colorful dress is playing with a blue and red soccer ball.
- 3) Girls in brightly-colored clothes plays with a blue ball.
- 4) The young girl is kicking a blue and red soccer ball.
- 5) Young girl in blue dress stepping over a soccer ball.

For Arabic captioning, [2] introduced the first publicly available AIC dataset that is based on Fliker8K, with 8000 images, 6000 for training, 1000 for validation, and the remaining 1000 for testing. Fig. 1 shows a sample of images and captions from this dataset. The author in [2] translated Flickr8K output using Google Translate API and the best three translations is post-edited, if needed by human expert. Since the dataset was generated by machine translation, some low-quality Arabic sentences appear in Fig. 2).



1 الفتاة الصغيرة ترفس كرة القدم الرقراء والحمراء.
2 فتاة صغيرة في ثوب لعب كرة القدم.
3 تلعب فتاة صغيرة في ثوب ملون بكرة القدم الرقراء والحمراء.

Fig. 2. Sample Image with Translated English Caption Result in Inaccurate Arabic Sentences from [2] Dataset.

B. Preprocessing Techniques

We have used four Preprocessing techniques. Each technique generates a different dataset, namely: A, B, C, and D. Below, we provide the detailed description of each of which:

1) *Original Text (Method A)*: To evaluate the effect of text preparation in the experiment, we used the captions as is.

2) *Base Preprocessing (Method B)*: Both [2], [19] used the traditional technique proposed by [6]. In this method, punctuation, diacritics, non-Arabic letters, single letter words were dropped. Also, a lexicographic normalization process took place to unify similar letters: including "ي" - "ى", "ا" - "آ", "أ" - "إ", "ؤ" - "و", "ة" - "ه", "ة" - "ه", "ك" - "ك", "ك" - "ك".

3) *Removing the Alef with the Nunation (Method C)*: We have noticed that when removing Tanween diacritic the extra Alef is not removed. So, we removed this extra Alef too, such that the word "قميصًا" (shirt-with extra nunation-) becomes "قميص" (shirt-without nunation-) instead of "قميصا" (shirt-with Alef as partial nunation-). Applying this technique would reduce the total vocabularies because in the previous method each surface form was considered a different vocabulary as illustrated in Fig. 3. Moreover, we separated and removed the Waw conjunction from next word, e.g. "ويقول" (and-he-says) becomes "يقول" (he-says).

4) *Full Preprocessing (Method D)*: We partially followed Method C, but we kept the conjunction Waw. In all previous methods all single letter words was removed including the isolated conjunction Waw, e.g. "و" becomes "يقول" but we think this highly affect syntactic and semantic of the captions. Fig. 3 shows differences in the frequency counts for preprocessing methods B, C, and D.

The final caption is then surrounded by a start and end tags. The length of each caption is set to 25 words; shorter captions are padded with nulls.

Table I shows the output of the four preprocessing methods along with their statistics. Since we dropped words with single appearance we can notice in the third column of the table a big reduction in the repeated vocabularies count. For example, applying Method C to the dataset produces 9,713 unique vocabularies but only 5,344 of them were repeated and the remaining 4,369 should be removed.

The reason of having these words sparse in the caption dataset might be due to misspelled words or the use of rare words. If size of the dataset is small, it might make the caption not a good representative for the Arabic Language model, since many words rarely appear or do not appear at all. This raises the need for a big enough dataset for AIC.

Low frequency words affect the prediction process, so they have to be treated at the preprocessing stage since often they are typos. Fig. 3 shows how the proposed methods C and D reduced the occurrences of words with just one appearance from 4963 (Method B) to 4369 a decrease of about 12%. As per (Fig. 3), the number of low frequency words reduced in most cases, but we can observe an increase of the number of words with 12 and 13 frequency; this might be due to the matching between words with low frequencies after applying the preprocessing task.

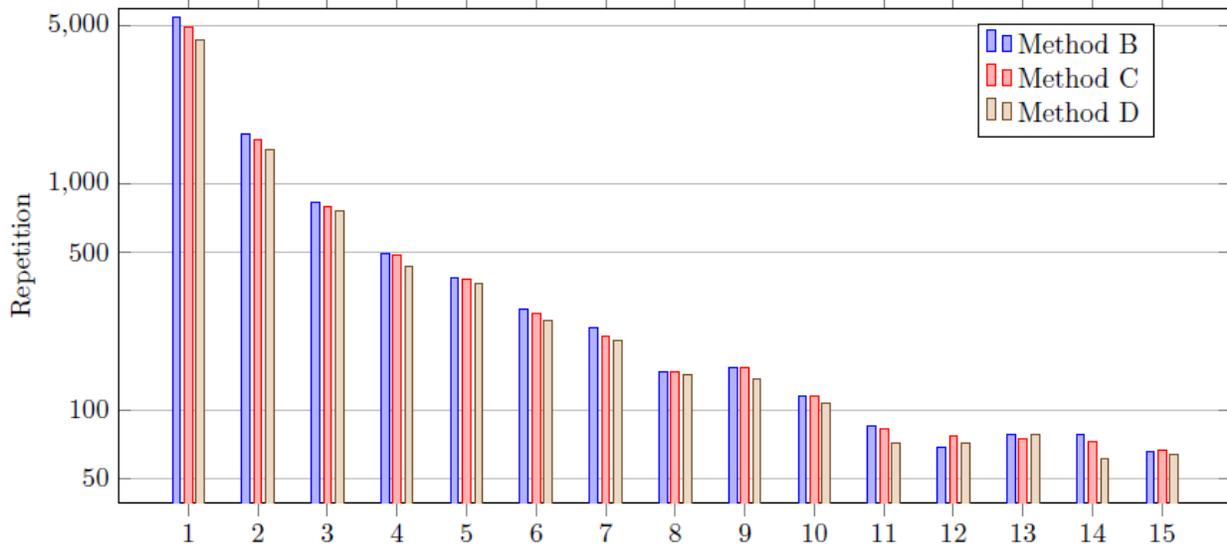


Fig. 3. Variation in the Frequency Counts for Each Preprocessing Method (Rare Counts).

TABLE I. PREPROCESSING METHODS USED, WITH SAMPLE CAPTIONS AND NUMBER OF DETECTED VOCABULARIES

Preprocessing method	Sample Caption	Total Vocabularies	Unique Vocabularies	Unique Repeated Vocabularies
Method A	صبي يرتدي نظارات و قميصًا أحمر	179,532	11,386	5,893
Method B	صبي يرتدي نظارات قميصا احمر	178,176	10,692	5,729
Method C	صبي يرتدي نظارات قميص احمر	178,175	9,713	5,344
Method D	صبي يرتدي نظارات و قميص احمر	183,342	9,714	5,345

C. Models

Recurrent Neural Networks (RNN) is best used for time series data, but it suffers from the short term memory problem or the vanishing gradient where the earlier inputs effect starts to be exponentially smaller when we move more steps forward in the prediction. We can resolve this by using one of the following variations: Gated Recurrent Unit (GRU) or Long Short Term Memory (LSTM) where a gates are used to control the older sequence information by saving in memory unit and propagate to next units.

Since text is considered a Time Series prediction we propose to use GRU and LSTM network in our experiment and compare their performance and effect on the results.

D. Experiment

Experiments were designed to test the impact of our independent variable on the quality and accuracy of Arabic captions. We have conducted experiments that involved 32 variable combinations: 4 Datasets, 2 image classifiers, 2 dropout usage, and 2 Deep Learning methods.

Fig. 4 shows the experiment design where we have indicated four labels to highlight the variant stages of the experiments. In the first stage (1) images are passed to one of two features extractors (Inception V3, VGG16). Next, a vector that contains image features is produced, captions are preprocessed using the four methods then tokenized, and then passed to embedding layer.

Afterwards, a dropout layer is used, if required by experiment, and the results are passed to either LSTM or GRU. At the end a Dense layer is used for prediction. Each model is saved, and test images are passed to it for caption prediction. All predicted captions are recorded and compared

with the actual ones. BLEU- 1/2/3/4 scores are calculated and stored per each experiment. Table II shows the recorded results which we analyze and discuss in the next sections. In each experiment one path is chosen at a time until all combinations are covered. Many experiments were repeated with lower epoch when Overfitting is detected.

The configuration of the hardware used is: Intel(R) Core(TM) i7 10th generation (6 core, 12 logical processors) with NVIDIA GeForce GTX1 1650 (4GB) for processing, 16 GB RAM Memory, total accumulated training time for latest models about 7 hours.

The collected experiment data was analyzed to find the effect of each factor. Also, a t-test is applied to find the significance of each variable.

E. Overfitting

Since the size of Dataset is small training and testing (validation) loss value is monitored after each epoch, if the testing loss increases or stays the same while the training loss decreased, this means an overfitting is detected and we observe a lower prediction accuracy from that model.

Then lower number of epochs are made to reach the lower testing loss value and a better model accuracy (BLEU measure).

F. Evaluation

To evaluate each experiment result, BLEU-1/2/3/4 are used. BLEU is a precision-based metric that ranges between zero (lowest) and one (best). The number of n-grams that appears in the candidate text is compared to total n-grams in the reference text. This metric is used by [2], which we use to compare our results with their results.

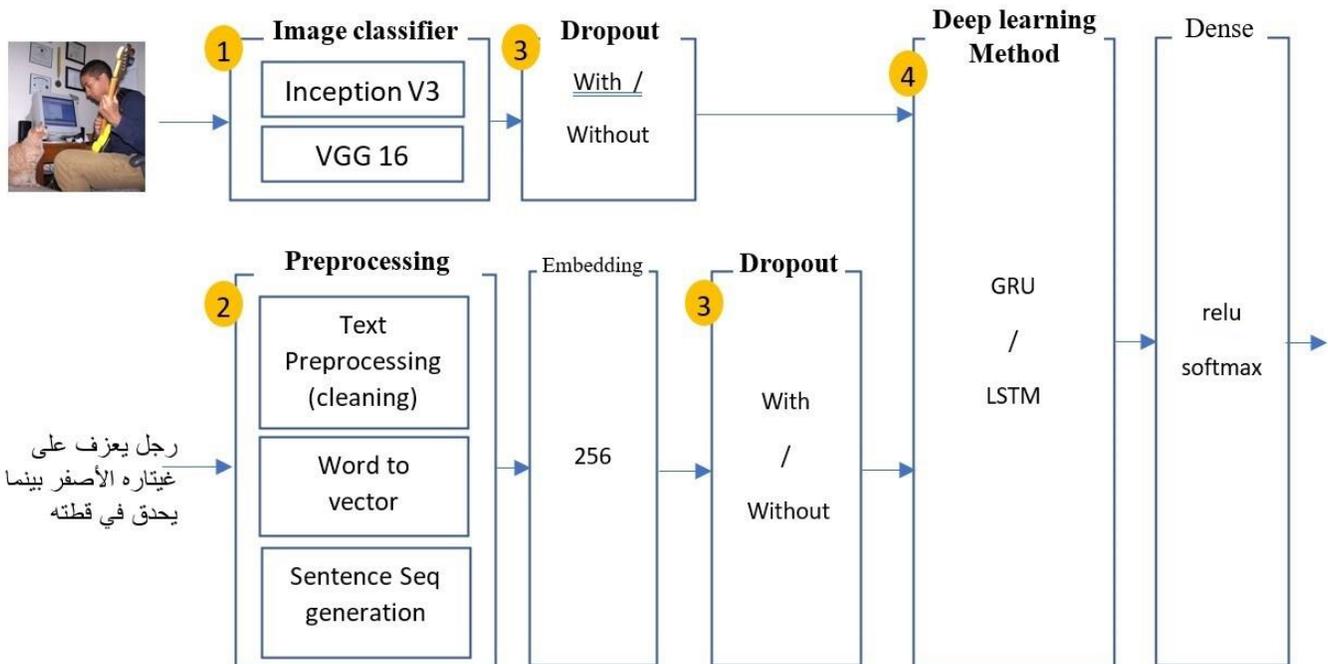


Fig. 4. Experiment Flow that Yields a Total of 32 Experiments: (1) Two Image Classifiers, (2) 4 Preprocessing Methods, (3) Dropout, (4) Two Deeplearning Techniques.

TABLE II. BLEU-1/2/3/4 RESULT OF THE EXPERIMENT PER VARIABLES COMBINATIONS

Image Classifier	Model	Dataset	Dropout				No Dropout			
			1	BLEU%		4	1	BLEU%		4
				2	3			2	3	
Inception V3	GRU	A	26.6	13.4	6.8	3.6	29.5	14.9	7.8	4.2
Inception V3	GRU	B	28.3	14.7	7.4	3.0	28.3	13.5	6.7	3.0
Inception V3	GRU	C	30.1	15.8	7.9	3.9	29.9	15.7	8.3	4.6
Inception V3	GRU	D	34.1	17.7	9.5	5.3	29.9	16.6	9.4	5.1
Inception V3	LSTM	A	24.4	10.7	4.8	1.8	22.6	10.7	5.1	2.0
Inception V3	LSTM	B	27.6	11.7	4.7	2.0	24.1	11.4	5.1	2.1
Inception V3	LSTM	C	27.8	13.5	6.5	3.0	26.3	11.1	4.5	2.1
Inception V3	LSTM	D	31.8	15.3	8.0	4.6	27.1	12.2	5.7	2.9
VGG16	GRU	A	24.6	13.3	7.2	4.0	24.0	12.9	6.4	3.1
VGG16	GRU	B	23.5	13.2	7.1	3.6	28.2	15.1	8.3	4.6
VGG16	GRU	C	31.1	17.5	9.0	4.1	30.8	16.8	8.8	4.4
VGG16	GRU	D	26.5	15.1	8.8	5.1	36.5	21.4	12.0	6.6
VGG16	LSTM	A	33.6	20.1	11.2	6.4	32.3	18.5	9.8	5.3
VGG16	LSTM	B	33.9	19.5	10.5	5.7	31.2	17.9	9.7	5.5
VGG16	LSTM	C	35.1	20.9	11.5	6.3	33.1	18.9	10.1	5.2
VGG16	LSTM	D	30.7	18.2	10.1	5.4	34.2	19.9	10.8	6.1

IV. RESULT

In this section, we present results from 32 experiments. Table II shows the BLEU results of each experiment. Fig. 5 illustrates these results.

A. BLEU

BLEU-1/2/3/4 was used to measure accuracy of each model prediction. Table II shows the results of these experiments.

We can notice that the best BLEU scores achieved from using VGG16 with GRU on the Dataset generated using the method D, and without dropout, are BLEU-1=36.5, BLEU-2=21.4, BLEU-3=12, and BLEU-4=6.6.

B. Preprocessing Methods Comparison (Datasets)

Each Dataset is produced using a different Preprocessing method, we compared the three Datasets (B,C,D) to show the effect of Preprocessing on the results accuracy. Fig. 6 illustrates the BLEU-1's result.

We can notice that the proposed new Preprocessing methods give higher BLEU measure. The reason might be due to less infrequent words that arise from consistent typo, such as concatenating Waw with the next word, or keeping the Alef of nunation, which produces a vocabulary that is irrelevant to the original word.

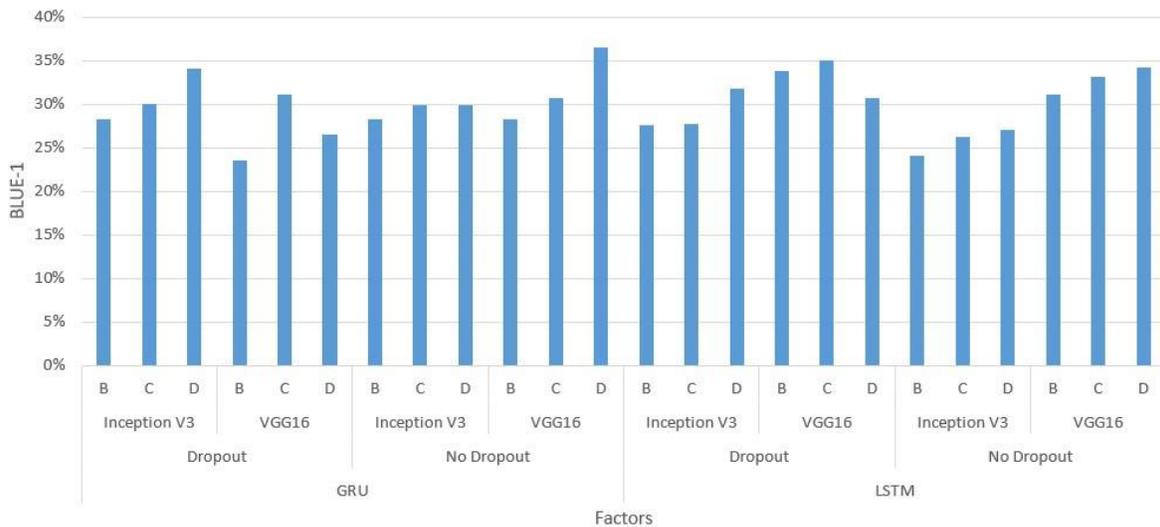


Fig. 5. Experiments Results for BLEU-1 upon Different Parameters.

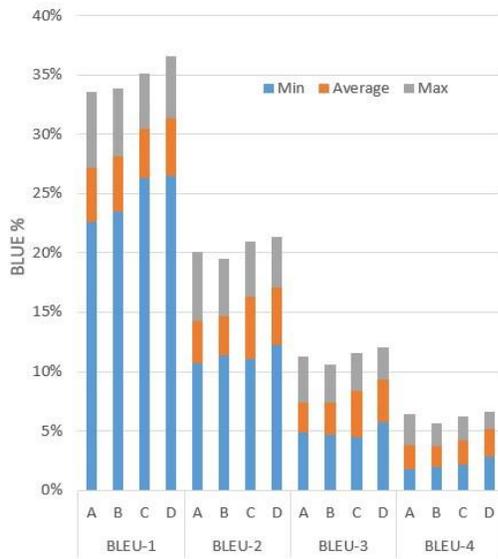


Fig. 6. Average, Minimum, and Maximum Value of BLEU-1/2/3/4 achieved per each Preprocessing Method.

A paired-samples t-test was conducted to compare the Dataset C with the Dataset B. There is a significant difference in the scores from Dataset C (M=0.1482, SD=0.1045) and Dataset B (M=0.1346, SD=0.0978) under the conditions: $t(31)=5.0344$, $p = .000019$.

These results suggest that removing the Alef of the nunation affect the BLEU results and increases it.

Another paired-samples t-test was conducted to compare Dataset D with Dataset C. There was a significant difference in the scores for Dataset C (M=0.1482, SD=0.1045) and Dataset D (M=0.1571, SD=0.01044) under the conditions: $t(31)=-2.2136$, $p = .000019$. These results suggest that keeping the Waw in the preprocessing phase affect the BLEU results and increases it.

C. Image Features Model Comparison

We involved two image models to extract image features, VGG16 and Inception v3. Fig. 7 illustrates a comparison of BLEU results of both models.

A paired-samples t-test was conducted to compare using VGG16 and Inception V3 as image features extractor.

There is a significant difference in the scores for VGG16 (M=0.1564, SD=0.1011) and Inception V3 (M=0.1294, SD=0.0976) under the conditions: $t(63)=5.6714$, $p = .00000038$. These results suggest that using VGG16 over Inception V3 affect the BLEU results and increases it.

D. DropOut Comparison

We have studied the impact of using the Dropout with Arabic image captioning process. Fig. 8 illustrates the results of experiments with/without Dropout.

A paired-samples t-test was conducted to compare the results with and without Dropout. There was not a significant difference in the scores for using Dropout (M=0.1423, SD=0.1005) and not using dropout (M=0.1436, SD=0.01001) conditions; $t(63)=-0.46$, $p = .647$.

There is no evidence that using Dropout will affect the BLEU results of the generated captions.

E. GRU vs LSTM

Two Deep Learning methods were compared (GRU, LSTM). Fig. 9 illustrates the BLEU results per each method.

The use of GRU or LSTM as a text prediction model was compared using a paired-samples t-test. There is no significant difference in the scores for GRU (M=0.142, SD=0.097) and LSTM (M=0.1438, SD=0.01035) under the conditions: $t(63)=0.419$, $p = .6766$.

These results cannot support that using GRU instead of LSTM may affect the BLEU results of the generated captions.

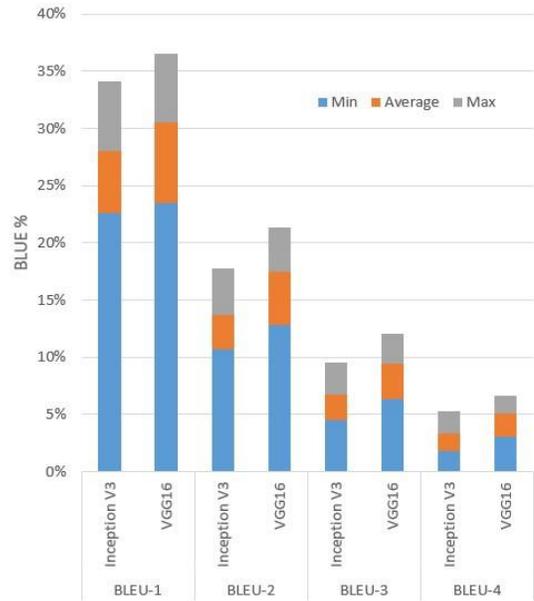


Fig. 7. Average, Minimum, and Maximum Value of BLEU-1/2/3/4 achieved per each Image Features Extraction Model.

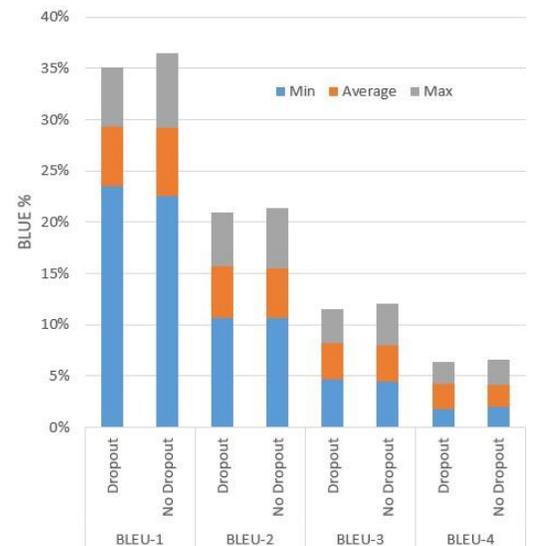


Fig. 8. Average, Minimum, and Maximum Value of BLEU-1/2/3/4 achieved per Dropout usage.



Fig. 9. Average, Minimum, and Maximum Value of BLEU-1/2/3/4 achieved per each Deep Learning Method.

V. CONCLUSION

Arabic Image Captioning resources are scarce. Fortunately, one public dataset is available. We created an AIC model with tuned factors that outperformed the best results on the publicly available dataset. According to paired t-tests conducted on the results, Arabic text preprocessing and image features extractors have a major role to play in improving the AIC results. For the purpose of comparison, two preprocessing techniques for Arabic captions were proposed and found to yield better results.

A total of 32 experiments were conducted to analyze the effects of four variables. We considered the following variables: preprocessing techniques (original text, normal preprocessing, Alef removal with nunation, and keeping conjunction Waw), Waw typo correction, Deep learning techniques (LSTM, GRU), inclusion and exclusion of Dropout, and two Image features extraction methods (Inception V3, VGG16).

As a result, BLEU1=36.5, BLEU-2=21.4, BLEU-3=12, and BLEU-4=6.6 were the best results we reached. The results were compared using paired t-tests, and the Arabic preprocessing methods exhibited an enhanced level of quality, and VGG16 significantly outperformed Inception V3. Using Dropout or LSTM instead of GRU, however, did not have a major effect.

VI. LIMITATIONS AND FUTURE WORK

The main limitation was the relatively small Dataset size since there was only one publicly available Dataset for AIC. Other Preprocessing and Deep learning methods could be included in the comparisons but doing that will increase the number of experiments and require more resources, therefore we can consider it in the future work.

As a future work, researchers can benefit from the outcomes of this study by employing it to their future research, particularly, a larger dataset can be created and made public to avail linguistic resources research in this area.

Not to mention, having a big dataset provides several possibilities to tailor the use of extra deep learning techniques

and come up with better word representation and features that can significantly improve the performance of the Arabic Image Captioning.

REFERENCES

- [1] D. Stout, Social Media Statistics, 2020 (accessed June 27, 2020).
- [2] O. ElJundi, M. Dhaybi, K. Mokadam, H. M. Hajj, and D. C. Asmar, "Resources and end-to-end neural network models for arabic image captioning." in VISIGRAPP (5: VISAPP), 2020, pp. 233-241.
- [3] R. Mualla and J. Alkheir, "Development of an arabic image description system," International Journal of Computer Science Trends and Technology (IJCTST), vol. 8 no. 3, 2018.
- [4] K. Simonyan and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," arXiv preprint arXiv: 1409.1556, 2014.
- [5] C. Szegedy, V. Vanhoucke, S. Ioffe, J. Shlens, and Z. Wojna, "Rethinking the inception architecture for computer vision," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2016, pp. 2818-2826.
- [6] A. Shoukry and A. Rafea, "Preprocessing Egyptian dialect tweets for sentiment mining," in The Fourth Workshop on Computational Approaches to Arabic Script-based Languages, 2012, p. 47.
- [7] J. Aneja, A. Deshpande, and A. G. Schwing, "Convolutional image captioning," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2018, pp. 5561-5570.
- [8] J. Wang, W. Wang, L. Wang, Z. Wang, D. D. Feng, and T. Tan, "Learning visual relationship and context-aware attention for image captioning," Pattern Recognition, vol. 98, p. 107075, 2020.
- [9] W. Tian, R. Zhou, and Z. Zhao, "Cascading top-down attention for visual question answering," in 2020 International Joint Conference on Neural Networks (IJCNN). IEEE, 2020, pp.1-7.
- [10] S. J. Rennie, E. Marcheret, Y. Mroueh, J. Ross, and V. Goel, "Selfcritical sequence training for image captioning," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, 2017, pp. 7008-7024.
- [11] 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," in Proceedings of the IEEE conference on computer vision and pattern recognition, 2018, pp. 6077-6086.
- [12] J. Wu, Z. Hu, and R. J. Mooney, "Generating question relevant captions to aid visual question answering," arXiv preprint arXiv:1906.00513, 2019.
- [13] V. Jindal, "Generating image captions in arabic using root-word based recurrent neural networks and deep neural networks," in Proceedings of the AAAI Conference on Artificial Intelligence, vol. 32, 2018.
- [14] H. A. Al-Muzaini, T. N. Al-Yahya, and H. Benhidour, "Automatic arabic image captioning using rnn-lstm-based language model and cnn," International Journal of Advanced Computer Science and Applications, vol 9, no.6, 2018.
- [15] M. Hodosh, P. Young, and J. Hockenmaier, "Framing image description as a ranking task: Data, models and evaluation metrics," Journal of Artificial Intelligence Research, vol. 47, pp. 853-899, 2013.
- [16] P. Young, A. Lai, M. Hodosh, and J. Hockenmaier, "From image descriptions to visual denotations: New similarity metrics for semantic inference over event descriptions," Transactions of the Association for Computational Linguistics, vol. 2, pp. 67-78, 2014.
- [17] B. A. Plummer, L. Wang, C. M. Cervantes, J. C. Caicedo, J. Hockenmaier, and S. Lazebnik, "Flickr30k entities: Collecting region-to-phrase correspondences for richer image-to-sentence models," in Proceedings of the IEEE international conference on computer vision, 2015, pp. 2641-2649.
- [18] X. Chen, H. Fang, T.-Y. Lin, R. Vedantam, S. Gupta, P. Dollár, and C. L. Zitnick, "Microsoft coco captions: Data collection and evaluation server," arXiv preprint arXiv:1504.00325, 2015.
- [19] H. D. Hejazi, A. A. Khamees, M. Alshurideh, and S. A. Salloum, "Arabic text generation: Deep learning for poetry synthesis," in Advanced Machine Learning Technologies and Applications: Proceedings of AMLTA 2021. Springer International Publishing, 2021, pp. 104-116.

Hardware Architecture for Adaptive Dual Threshold Filter and Discrete Wavelet Transform based ECG Signal Denoising

Safa MEJHOUDI¹, Rachid LATIF², Wissam JENKAL³, Amine Saddik⁴
Laboratory of Systems Engineering and Information Technology
ENSA, Ibn Zohr University
Agadir, Morocco

Abdelhafid EL OUARDI⁵
SATIE
Paris-Saclay University
Gif-sur-Yvette, France

Abstract—The ECG signal, like all signals obtained when instrumenting a data acquisition system, is affected by noises of physiological and technical sources such as Electromyogram (EMG) and power line interferences, which can deteriorate its morphology. To overcome this issue, it's subjected to apply a preprocessing step to remove these noises. Filtering techniques are complex computations becoming more common in medical applications, which must be completed in real-time. As a result, these applications are geared at integrating high-performance embedded architectures. This paper presents an FPGA (Field Programmable Gate Array) embedded architecture designed for an ECG denoising hybrid technique based on the Discrete Wavelet transform (DWT) and the Adaptive Dual Threshold Filter (ADTF), dedicated to handle with noises affecting ECG signals. The architecture was designed following a hardware-software codesign using a high-level description language and synthesized to be implemented on different FPGAs due to the structural description flexibility. The global architecture was divided into a set of functional blocks to allow parallel processing of ECG data. The simulation results confirm the high performance of the system in noise reduction without affecting the morphology of the signal. The process takes 0.3 ms with an acquisition frequency of 360 Hz. The whole architecture requires a small area in different FPGAs in terms of resources utilization. It uses less than 1% of the total registers for all FPGA devices which represents a total of 292 registers for Cyclone III LS, Cyclone IV GX, Cyclone IV E, and Arria II GX; and a total of 329 registers for Cyclone V. The logic elements occupancy varies between 3% using Cyclone V and 60% using Cyclone IV GX freeing up space for other parallel processing tasks.

Keywords—ECG signal; DWT; ADTF; hybrid technique; hardware-software codesign; FPGA

I. INTRODUCTION

The ECG or electrocardiogram is an electrophysiological signal whose trace describes the heart's electrical activity captured by electrodes puted on the surface of the body. This signal is currently used for the prevention and detection of cardiovascular diseases [1], [2]. Intelligent diagnostic systems have emerged to better use ECG data in large quantities whose analysis is difficult manually [3]. These systems make it possible to improve the quality of the signal (noise filtering), the enhancement of relevant information, the extraction of information that is not visible by direct visual analysis, as well as to propose a diagnosis that can provide sufficient help to doctors to make the right decisions [4]. Noise degrades the

precision and accuracy of the analysis. Signal denoising is then highly desirable and essential.

For this reason, numerous methods are utilized like Digital Filters (FIR/IIR) [5], [6], Empirical Mode Decomposition (EMD) and Ensemble EMD (EEMD) based methods [7], [8], Dual-Tree Wavelet Transform (DT-WT) [9], Discrete Wavelet Transform (DWT) [10], [11], [12], and Adaptive Filtering [13], [14], [15].

Digital filters are used for denoising by selecting the useful information frequency band or the noisy frequency bands[16]. Thus, high reduction of noise increases the order of the filter a lot, which can increase the complexity and the processing time. EMD methods disintegrate the noisy signal into IMFs (Intrinsic Mode Functions) and eliminate the noisy ones [8], which can destroy the signal. Wavelet methods put in view time and frequency information and decompose the signal into details and approximations [17]. Adaptive filtering can be used in several cases, as ADTF [14], which is performant in high-frequency noise reduction.

The study we present in this paper concerns the denoising of ECG signals using an algorithm based on the DWT and the ADTF. The hybridization of the tow algorithms was published by Jenkal et al. in [11], this technique aims to combine the advantages of both ADTF and DWT methods to deal with deferent noises, especially high-frequency noises, EMG (Electromyogram) noises, and power line interferences.

The results of this technique were evaluated using Matlab and compared to others methods in [11] and it offers high performances in terms of Mean Square Error (MSE), Percent Root mean square Difference (PRD), Signal-to-Noise Ratio Improvement (SNRimp), and Signal-to-Noise Ratio Output (SNRout).

Analyzing ECG signals in large quantities using this technique requires complex calculations with a need for rapid and real-time processing, which pushes us to move towards hardware implementation on high-performance embedded architectures. FPGA (Field Programmable Gate Array) seems to be good choice for high performance and low power [18]; which are essential needs to applications like signal processing, especially cardiac signals. In addition, low-cost FPGAs can be used for the implementation, as well the system can be moved anywhere.

The approach presented in this article is an original method of our research team published for the first time in [11], validated under Matlab in terms of filtering performance of ECG signals; the goal of this work is the on-board implementation of this method to put it into practice for the supervision of patient cardiac data.

For an FPGA implementation, the two filters, ADTF and DWT, are designed using the VHDL (VHSIC Hardware Description Language) under the Quartus II tool and the Modelsim simulation environment. The algorithm proves the high performance in noise reduction, maintaining the morphology and essential features of the original signal. The simulation results shows that the system has a processing time of 0.3 ms operating at 50 KHz, which respects largely the real-time constraint. The given architecture can be implementable in low-cost FPGAs families because of the modest area that it occupies, and gives possibility to add other blocks for more processing stages as QRS and abnormalities detection. Thus the global architecture uses less than 1% of the total registers for 5 FPGA devices: Cyclone IV Gx, Cyclone IV E, Cyclone III LS, Cyclone V, and Arria II Gx. The logic elements occupancy varies between 3% using Cyclone V and 60% using Cyclone IV GX. The total used pins are 28 for the whole architecture, representing 9% for Cyclone IV E and Cyclone III LS, 10% for Cyclone V, 16% for Arria II GX, and 35% for Cyclone IV GX.

The rest of this paper is organized as follows:

The first section describes the ECG signal with an overview of related work.

The second section presents the hybrid technique based DWT and ADTF algorithms.

The third section depicts the VHDL implementation of the whole algorithm, and a discussion of the given results.

Finally, a conclusion and perspectives are presented in the last section.

II. ECG SIGNAL DENOISING OVERVIEW

The cardiovascular system comprises the heart and the vascular system, where the main function is to ensure an adequate continuous blood flow with sufficient pressure to the organs and tissues to meet energy needs and cell renewal. Diagnosing his condition appears to be a vital task for the prevention of cardiovascular disease [19]. The electrocardiogram (ECG) signal remains one of the predominant and most widely used tools for this purpose.

The ECG is the recording of the heart's electrical activity moving in time and corresponding to the depolarization and repolarization of the heart muscle [20]. Fig. 1 represents the recording of the cardiac cycle, where the P wave reflects atrial depolarization, the QRS complex visualize the ventricular depolarization, and the T wave represents the ventricular repolarization.

Nowadays, diagnosis is done in an automatic manner where an automated ECG processing system usually consists of four successive stages [21] as follows: signal preprocessing, waves detection, features extraction, and finally, abnormalities detection and classification.

The signal preprocessing (or denoising) step essentially eliminates the different noises that affect the ECG signal during its acquisition. These noises are two types: physiological noises including muscle noise (EMG), and technical noises incorporating power line interference [22]. Due to its low-frequency band, ECG is too sensitive to these noises. Several techniques have been proposed to deal with this problem, such EMD or methods using banks of filters, wavelet transform, and adaptive filtering.

Infinite Impulse Response (IIR) and Finite Impulse Response (FIR) filters are digital filters used for ECG denoising. The denoising operation is based on frequency bands selection related to useful information in the signal and the noise frequency bands [16]. For excellent denoising, the number of needed coefficients increases a lot which results in a high computational and increases the delay.

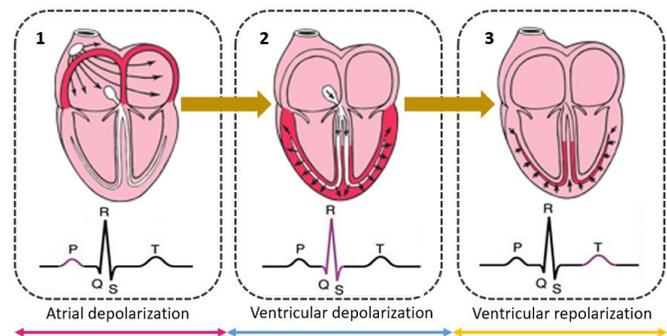


Fig. 1. Successive Stages of Depolarization/repolarization of the Heart Resulting Different Waves P, QRS, and T.

EMD methods are also very used to denoise ECG signals where the signal is disintegrated into a set of IMFs [23], [8]. The filtering is done by eliminating the noisy IMFs that can affect useful information in the signal. To overcome this issue, the mode-mixing is removed using Ensemble EMD.

Wavelet methods highlight time and frequency information simultaneously [17], where the signal is decomposed into different resolutions to give details and approximations, then thresholding techniques are used to denoise the signal.

Adaptive filtering proves the good performance for ECG denoising in some cases, ADTF as an example, is a good solution for high-frequency noise reduction [14], [4], [24]. The main advantage of this method is the low complexity compared to other methods like EMD and DWT. The ADTF complexity has a linear form depending on the signal size only, when the EMD and DWT also have a linear complexity but depending on different parameters.

Some techniques can gather two or more methods to benefit from their advantages together. The ADTF is reunited to DWT in [11], the next section details more this technique.

III. MATHEMATICAL STUDY OF THE ALGORITHM

A. ADTF Algorithm

The ADTF algorithm calculates, in the first step, three parameters: the average of the chosen window (μ), the lower

and higher thresholds (Lt and Ht, respectively). Following the equations:

$$\mu = 1/W \sum_{i=n}^{n+W} Input(i) \quad (1)$$

$$Lt = \mu - [(\mu - Min) * \alpha] \quad (2)$$

$$Ht = \mu + [(Max - \mu) * \alpha] \quad (3)$$

Where W is the window length, $Input(i)$ is the input ECG signal, Min and Max are the minimum and maximum values of the window samples. While α is the thresholding coefficient with $0 < \alpha < 1$.

The value of α varies to adjust the thresholding operation according to the noise concentration in the signal [14]; in case of a high concentration of noise, lower values of α are favored; otherwise, higher values can be tolerated.

B. DWT Algorithm

In different signal processing applications, the transformation of signals into frequency domain is very important. To obtain the frequency spectrum of a signal, Fourier transform is the most used. Biological signals, like ECG, have different temporal and frequency characteristics. For example, they are not stationary, and it is precisely in their characteristics (statistical, frequency, temporal, spatial) that reside most of the information they contain. A transformation that provides information on the frequency content while preserving the location to have a time-frequency representation is essential to analyze them.

The discrete wavelet transform studies the signal in various frequency bands with different resolutions by decomposition into a rough estimate and more precise information through two functions, called scale function and wavelet function, which are associated with the low pass and the high pass filters, respectively. The high pass filter provides the wavelet coefficients or details noted D, the low pass filter provides the approximation coefficients noted A. This approximation is, in turn, decomposed by a second pair of filters, the process is explained in Fig. 2.

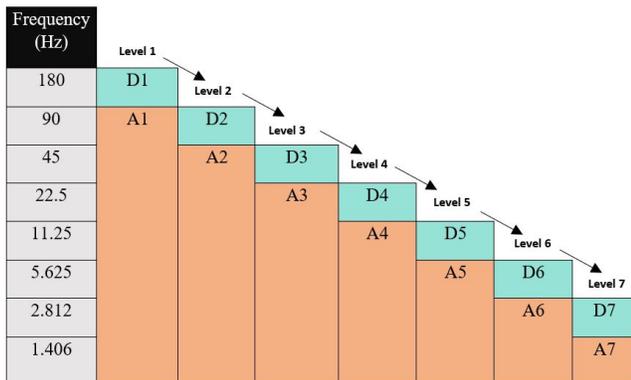


Fig. 2. Signal Decomposition using DWT.

The signal decomposition corresponds to the convolution of the signal ($x(n)$) with the impulse response of the low pass and high pass processing filters h and g as presented in Fig. 3.

(4) and (5) are the equations of these filters for one decomposition level.

$$A[k] = \sum x[n] * h(2k - n) \quad (4)$$

$$D[k] = \sum x[n] * g(2k - n) \quad (5)$$

Where $A[k]$ is the approximation given by the low-pass filter, $D[k]$ is the detail given by the high-pass filter, $x[n]$ is the discretized form of the original signal, $h[n]$ and $g[n]$ are, respectively, the half-band of the low-pass and high-pass filters.

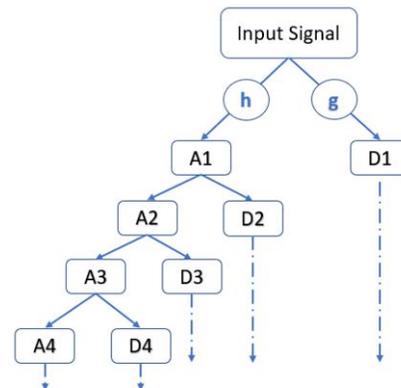


Fig. 3. DWT Decomposition.

Generally, the mother wavelet is chosen based on the closeness between the wavelet and the processed signal. For ECG signal we opted to use the Daubechies as mother wavelet because of the similarity between them especially Db4 wavelet as it can be seen in fig. 4.

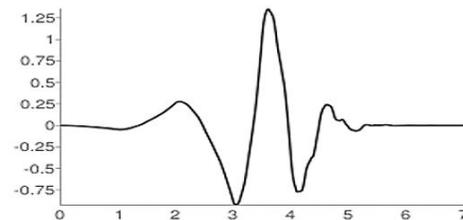


Fig. 4. Daubechie 4 Wavelet.

Signal denoising using DWT consists of the following three steps:

The wavelet transform of the observed signal, which consists of the decomposition of the signal into details and approximations.

The thresholding of the coefficients resulting from the decomposition or elimination of details containing noise.

The inverse wavelet of the modified coefficients to restore useful information that has effectively undergone the denoising operation.

To obtain a perfect reconstruction, the analysis and synthesis filters satisfy the condition presented in (6), where $h(z)$ and $h'(z)$ are, respectively, the analysis and the synthesis low pass filters, $g(z)$ and $g'(z)$ are the analysis and the synthesis high pass filters respectively.

$$h(-z).h'(z) + g(-z).g'(z) = 0 \quad (6)$$

In [10] and [25], the performance of DWT in ECG signal processing is presented, especially in the baseline wander noise removing, the architecture is implemented in a low-cost FPGA as the Xilinx ARTIX 7.

C. Hybrid Technique

The hybrid technique is a marriage between ADTF and DWT; this combination permits to reduce, successively, the noise from ECG signal. The whole process is described in Fig. 5, where the ECG signal is subjected to two stages of noise reduction:

The first step of this method is the application of the ADTF in the noisy signal; the chosen window is 10 samples, the α coefficient is equal to 0.1(10%), Table I shows the influence of α coefficient in the denoising in terms of signal-to-noise ratio improvement (SNRimp) with Gaussian noise of 10 dB as confirmed in [11].

TABLE I. α COEFICENT INFLUENCE IN THE ADTF DENOISING

α values	5%	10%	15%	20%	
101 MIT-BIH	6.82	8.69	7.54	7.16	SNRimp
115 MIT-BIH	8.72	9.20	8.92	8.60	

The second step is the *DWT* application on the corrected signal by the first step, where the signal is decomposed into many frequency bands. The wavelet mother used in this case is *debauchies dB4*; the coefficients of this wavelet are the closest to the ECG signal in terms of similarity, as it can be shown in Fig. 4. After decomposition, the details *D1* and *D2* concentrate an important quantity of noise, so we opted to eliminate these details. Then, the inverse DWT is applied to have the denoised signal.

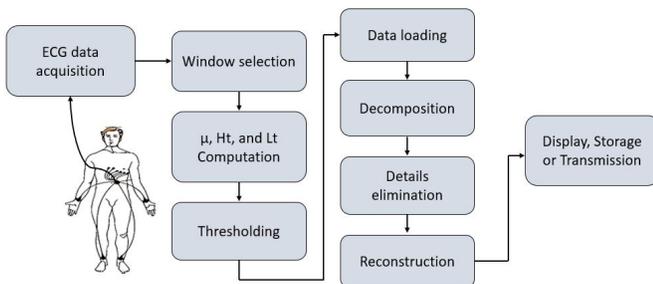


Fig. 5. The Algorithm Block Diagram.

Fig. 6 shows clearly the contribution of this combination of the two methods compared to the application of DWT alone.

The simulation is done using the signal 100 of the MIT-BIH database[26], with an additive Gaussian noise of 5 dB. (a) represents the noisy signal, (b) the corrected signal using the DWT, and (c) shows the corrected signal using the hybrid method (ADTF+DWT).

Fig. 7 presents the comparison of the denoising results between the ADTF technique only and the hybrid technique, which combines the ADTF with the DWT, on some signals from the MIT-BIH Physionet database with 5 dB of Wight Gaussian Noise.

The fusion of the two techniques provides better results, in terms of PRD, especially for a high density of noise. Taking, for example, the case of the signal 100 from the MIT-BIH database correlated with Gaussian noise of 5 dB, the filtering result using only the ADTF gives a value of the PRD of 24.55 while the hybrid method provides 18.26. The same for signal 103, the parameter PRD is equal to 25.23 with the ADTF and 19.61 with the hybrid method.

The following part dissects the results of this technique dedicated to implementation on an FPGA, where a detailed description of the hardware architecture is presented, with the simulation results and the report on the use of the hardware resources of different FPGA families.

IV. RESULTS AND DISCUSSION

A. Hardware Architecture

As the implementation target is FPGA in this work, we opted for the VHDL to describe the algorithm's behavior and architecture. Quartus II software is used for synthesis. Quartus II synthesis tool transform the code design into a synthesizable Register Transfer Level (RTL) with gate-level netlist. Modelsim ALTERA tool is used for simulation to verify the good behavior of the designed architecture.

VHDL is a hardware description language used to describe the behavioral o the studied algorithm; then, the functional VHDL description can be converted into a logic gate schema that can be implemented in FPGA boards [18]. The proposed architecture is dedicated to being implemented on different FPGA targets, so it is based on a structural description separated on a set of blocks. The various blocks describe the ADTF/DWT modules separately to make it possible to process the modules simultaneously, which permits reducing the processing time.

The architecture of the proposed method is composed by two main blocks, the first for the ADTF denoising stage and the second for the DWT denoising stage, Fig. 8 shows the RTL schema of the global architecture.

The ADTF block incorporates three functional blocks: the ADTF-LOAD (*FB1*), a shift register to prepare the signal window for the second functional block, ADTF-TREATMENT (*FB2*), the latter calculates the necessary parameters for the ADTF process. The third functional block, ADTF-TEST (*FB3*), applies the thresholding operation to the median value of the window.

The output of the first block goes through the second block, where a window of eight elements is prepared by the DATA-LOAD functional block (*FB4*); then DWT, details elimination,

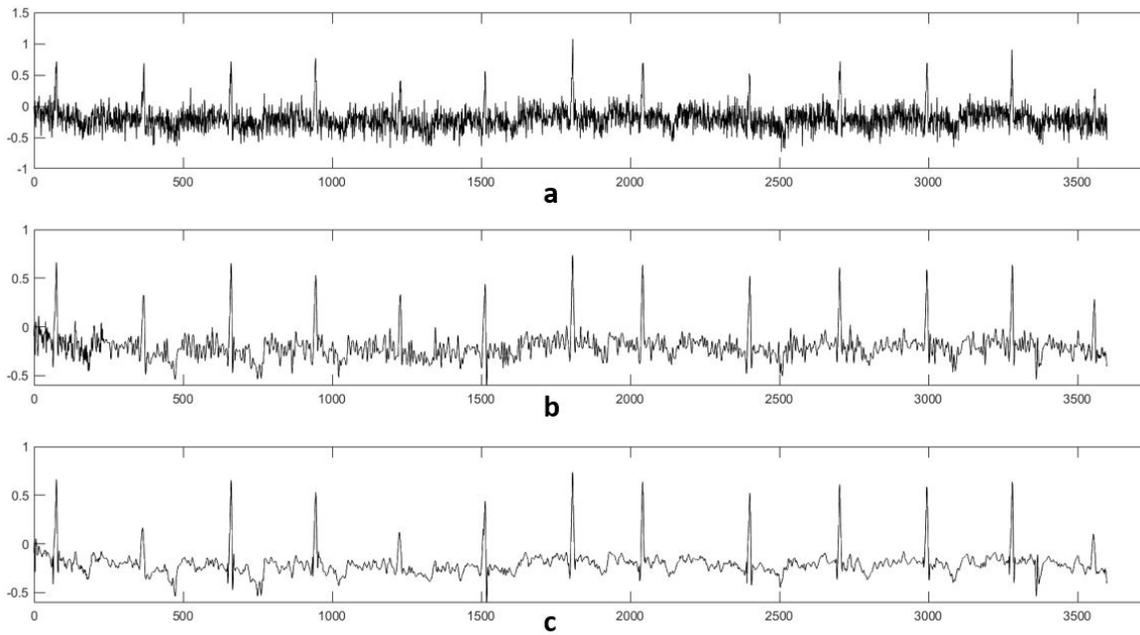


Fig. 6. Comparison of the Denoising Techniques Applied to the Signal 100 of the MIT-BIH Database, with a High Level of White Gaussian Noise (5dB): (a) is the Noisy Signal, (b) is the Filtred Signal using DWT and (c) is the Filtred Signal using the Hybrid Technique.

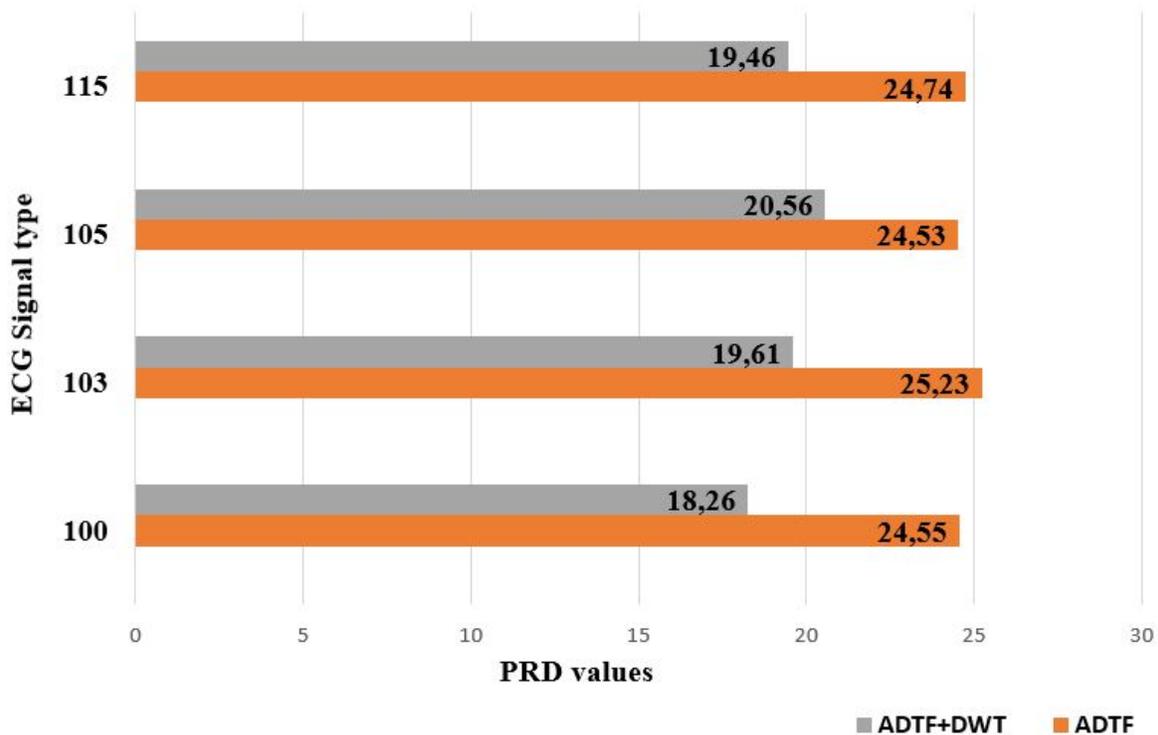


Fig. 7. PRD Comparison of Denoising Results using the ADTF and the Hybride Techniques.

and inverse DWT are applied on this part of the signal by the DWT-IDW functional block (*FB5*).

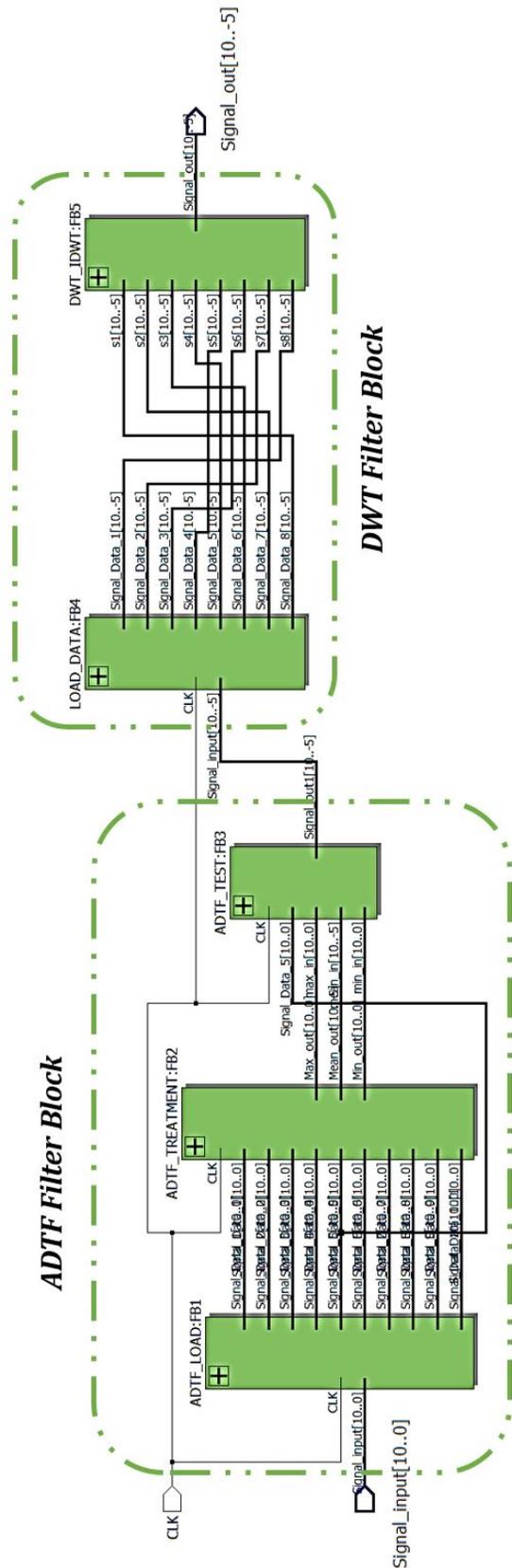


Fig. 8. Hardware Architecture of the Hybrid Technique.

The purpose of FB1 (Fig. 9) is to prepare the window for the functional blocks; it receives the input ECG signal with a frequency of 360Hz (the *MIT_BIH* database) and gives a window of 10 samples in the output based on a shift register. This permits the online processing of cardiac signals.

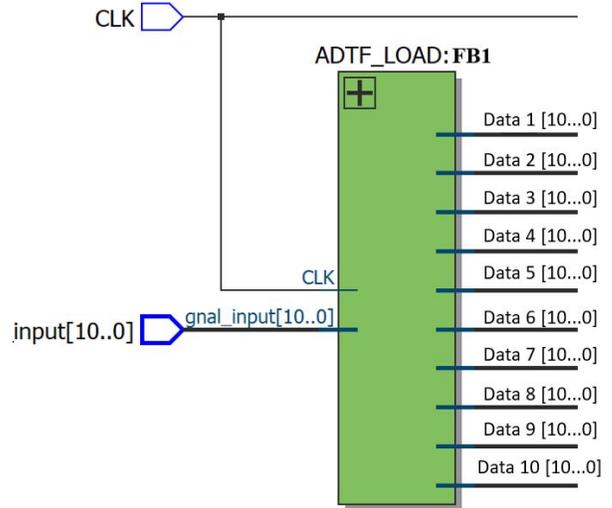


Fig. 9. The ADTF Load Functional Block: FB1.

The FB2 (Fig. 10) computes the average, the maximum, and the minimum of the window received from FB1. The result of the average computation is coded in 30 bits, and its minimized, for resources optimization, to 16 bits: 11 bits for the integer part and the rest 5 bits for the fractional fixed-point part. The maximum and minimum are coded in 11 bits, and they are calculated using loop tests.

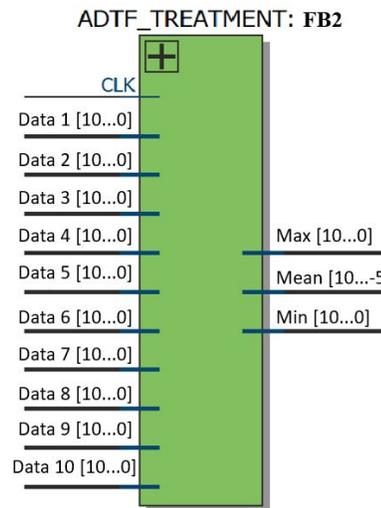


Fig. 10. The ADTF Treatment Functional Block: FB2.

The FB3 (Fig. 11) aims to apply the denoising operation by calculating the Higher and Lower threshold (H_t and L_t) using the parameters received from FB2. To compute the H_t and the L_t , the α coefficient is used as mentioned in the equations

(2,3). A register of 11 bits is reserved to memorize the α value where $\alpha = 0.1$, so one bit for the integer part to represent the zero and 10 bits to represent the fractional part.

For the correction stage, the median value of the selected window is compared to the integer part of the two thresholds. Then the assignment of the results to the output of the module. The output can take one of the tree values: it can be the same as the median value if this last is in the margin between the Ht and the Lt, or it takes the Ht or the Lt, respectively if it exceeds the Ht or it is less than the Lt.

The output size is coded in 16 bits, 11 bits for the integer part, and 5 bits for the fractional part. If the median value is affected to the output, which is coded in 11 bits, five zeros are added to the fractional fixed-point part.

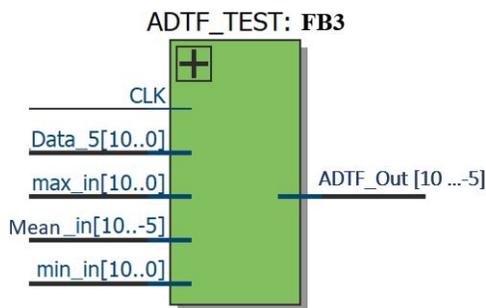


Fig. 11. The ADF Test Functional Block: FB3.

The output of the ADF denoising block is the input of the second block, which concerns the DWT denoising where FB4 (Fig. 12) consists of loading eight samples of the signal, which will be a part of the signal to which the DWT is applied. This size is imposed by the number of coefficients of the mother wavelet dB4, which are eight. The output, therefore, is a window of eight elements coded in 16 bits.

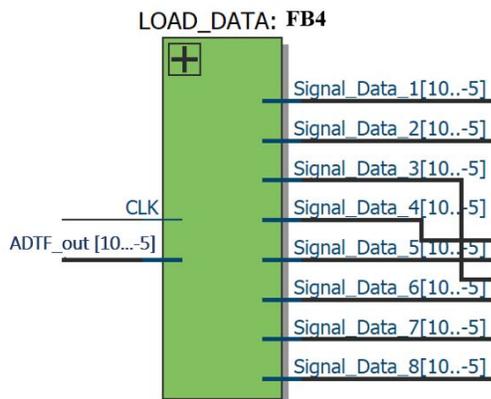


Fig. 12. The Load Data Functional Block: FB4.

The FB5 (Fig. 13) is the main functional block of the second block, where the wavelet transform is applied to the eight elements. The signal is decomposed into two levels to extract details from levels 1 and 2; then, the denoising

process eliminates the extracted details. The input FB5 is eight elements from the previous FB4, coded in 16 bits. The output represents the result of the decomposition, denoising, and reconstruction operations, which is resized to 16 bits: 11 bits for the integer part and 5 bits for the fractional part.

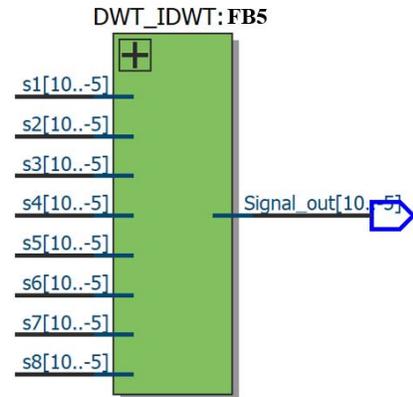


Fig. 13. The DWT-IDWT Functional Block: FB5.

B. Simulation Results

MIT-BIH Arrhythmia of Physionet [26], an International database, is used to test the functioning of the VHDL architecture; It contains 48 records of a half-hour. These signals are sampled with a frequency of 360 Hz and a 11-bits resolution. For the test, White Gaussian Noise (WGN) with SNR levels of 5dB, 10dB and 20dB are correlated to the original signals before the denoising process.

The simulation is done in Modelsim ALTERA software in order to evaluate the good behavior of the VHDL architecture of the hybrid technique. Fig. 14 shows the simulation results of the hybrid technique applied to signal 100 of the MIT-BIH database to which we added a White Gaussian Noise of 20 dB. The simulation results demonstrate the high performance of the algorithm in noise reduction without distortion of the original signal, and therefore conservation of its morphology as is clearly shown in Fig. 14

Once the architecture is synthesized, the implementation is the next step after timing verification. In Fig. 15, timing Simulation of Hybrid-top-level-module of the architecture is visualized. As it can be seen, the system response in 0.3 ms using a processing clk of 50Khz which largely responds to the real-time constraint, with an acquisition frequency of 360 Hz.

C. Hardware Resources Consumption and Discussion

Table II details the resources utilization for the implementation of the hybrid technique on FPGA INTEL-ALTERA boards. It shows a comparison between different boards in terms of total logic elements, used registers, number of pins, used embedded multipliers, and DSP blocks.

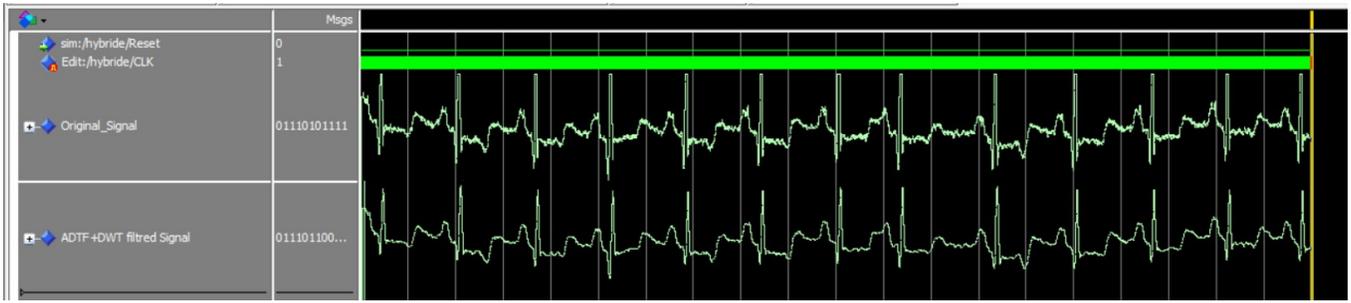


Fig. 14. Simulation Result of the Denoising Applied to the Signal 100 of the MIT-BIH Database.

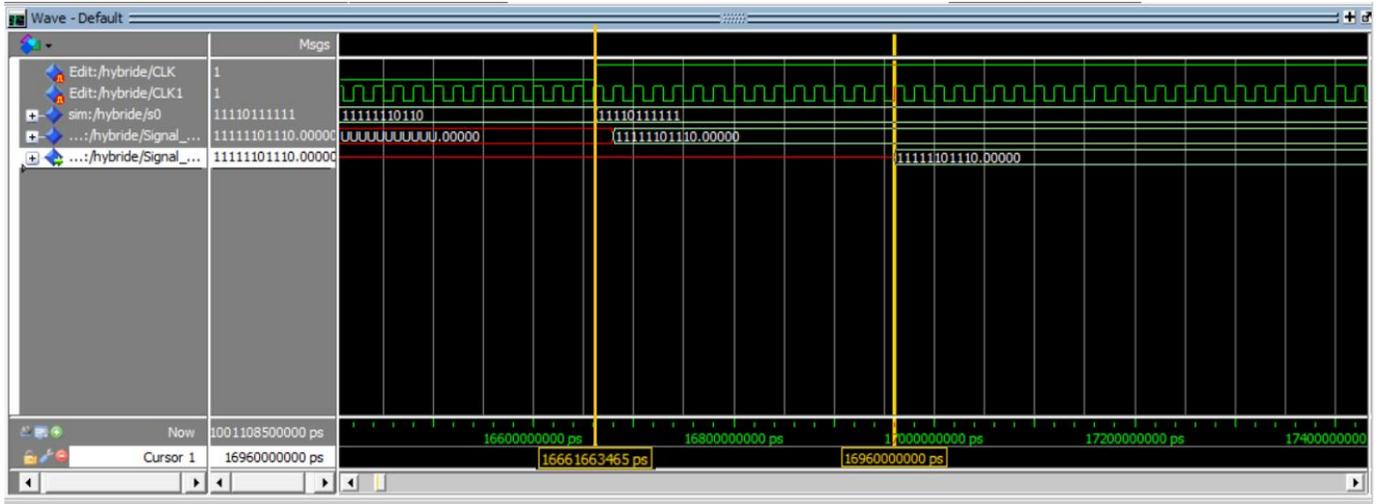


Fig. 15. Timing Simulation of Hybrid-top-level-Module.

TABLE II. HARDWARE RESOURCES UTILIZATION OF THE IMPLEMENTATION ON DIFFERENT FPGAs OF INTEL-ALTERA

	Cyclone IV GX	Cyclone IV E	Cyclone III LS	Arria II GX	Cyclone V
Total logic elements	17538 (60%)	17513 (44%)	17500 (25%)	46%	1623 (3%)
Total registers	292 (< 1%)	292 (< 1%)	292 (< 1%)	292 (< 1%)	329
Total pins	28 (35%)	28 (9%)	28 (9%)	28 (16%)	28 (10%)
Total memory bits	0%	0%	0%	0%	0%
DSP blocks	-	-	-	4 (2%)	127 (81%)
Embedded multiplier 9-bit elements	8 (5%)	8 (3%)	8 (2%)	-	-

The used devices in the comparison are classified in the range of low-cost and low-power technologies, so the architecture of the hybrid technique does not need expensive FPGA boards to ensure high performance. The study is done for Cyclone III, Cyclone IV, Cyclone V, and Arria II families.

The hybrid architecture uses less than 1% of the total registers for all FPGA devices which is a total of 292 for Cyclone IV GX, Cyclone III LS, Cyclone IV E, and Arria II GX; and a total of 329 for Cyclone V as it can be shown in Fig. 16. The logic elements occupancy varies between 3% using Cyclone V and 60% using Cyclone IV GX as it can be seen in Fig. 17. The global architecture uses a total of 28 pins,

11 pins for the input signal, which is coded in 11 bits, 16 pins for the output or corrected signal, and one pin for the clock with a percentage of 9% for Cyclone IV E and Cyclone III LS, 10% for Cyclone V, 16% for Arria II GX, and 35% for Cyclone IV GX as mentioned in fig.18 .

DSP blocks are available only in the Cyclone V and Arria II technologies; these blocks contain optimized units for some arithmetic operations, multiplication, for example, so the architecture uses 4 DSP blocks in the case of Arria II GX, which represents 2% of the total blocks, and 127 DSP blocks using Cyclone V which is an 81% of the available DSP blocks for this device. The other devices use the embedded multiplier

9-bit elements in place of DSP blocks to optimize multiplications, so the architecture needs eight embedded multiplier 9-bit, which is 5% for the Cyclone IV GX, 3% for Cyclone IV E, and 2% for Cyclone III LS as shown in Fig. 19. While there is no need for memory blocks in the architecture.

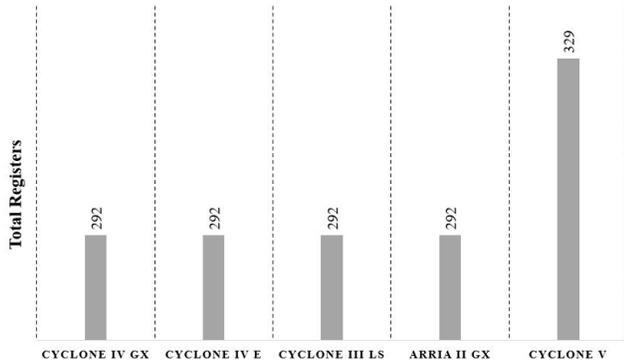


Fig. 16. Total Registers used by the Architecture in Different FPGA Families.

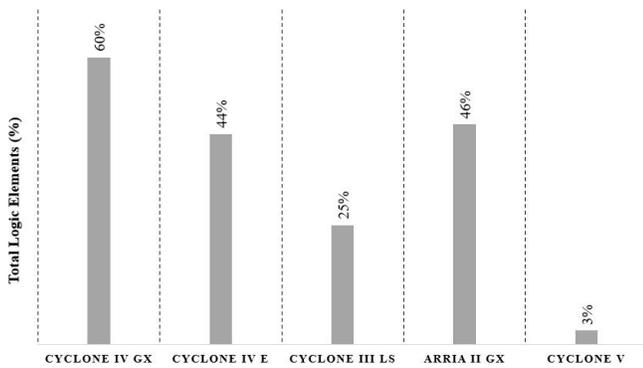


Fig. 17. Total Logic Elements used by the Architecture in Different FPGA Families.

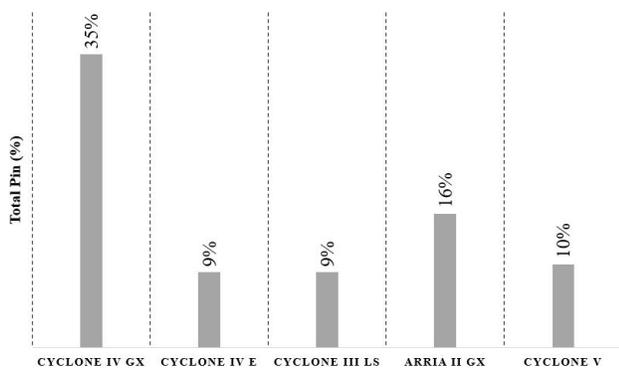


Fig. 18. Total Pins used by the Architecture in Different FPGA Families.

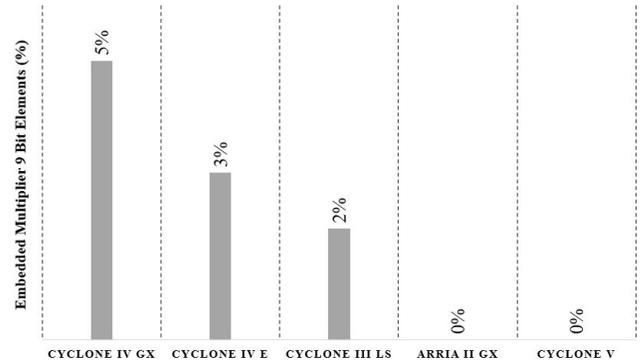


Fig. 19. Embedded Multiplier 9-bit Elements used by the Architecture in Different FPGA families.

V. CONCLUSION

In this paper, a hardware architecture of a hybrid technique-based ECG signals denoising is presented to satisfy the exigency of medical applications as ECG monitoring in terms of real-time processing, low power consumption, and portability. The algorithm is firstly evaluated in Matlab for validation; then, a VHDL description is presented for FPGA implementation purposes. The given architecture is adequate to be implementable on low-cost FPGA families because of the small area it requires and the possibility it gives to add other blocks for more processing tasks such as QRS and abnormalities detection. The simulation results show that the system's response takes 0.3 ms, responding to the real time processing constraint imposed by an acquisition period of 2.77 ms.

This study opens the way to design a global architecture permitting the extraction of necessary characteristics for the heart rate computation and heart diseases detection afterward; in order to put in practice a system allowing real-time monitoring of patients cardiac state.

ACKNOWLEDGMENT

We would like to thank the CNRST (National Centre for Scientific and Technical Research) of Morocco for the support (scholarship number: 588UIZ2017).

ABBREVIATIONS

ADTF:	Adaptive Dual Threshold Filter
Ht:	Higher Threshold
Db4:	Daubechie 4
IIR:	Infinite Impulse Response
DT-WT:	Dual-tree Wavelet Transform
IMF:	Intrinsic Mode Functions
DWT:	Discrete Wavelet Transform
Lt:	Lower Threshold
DWT-IDWT:	DWT-Inverse DWT
MSE:	Mean Square Errors
ECG:	Electrocardiogram
PRD:	Percentage Root-mean-square Difference parameter
EMD:	Empirical Mode Decomposition
RTL:	Register Transfer Level
EEMD:	Ensemble EMD
SNRimp:	Signal to Noise Ratio Improvement
EMG:	Electromyogram
VHDL:	VHSIC Hardware Description Language
FIR:	Finite Impulse Response
WGN:	White Gaussian Noise
FPGA:	Field Programmable Gate Array

REFERENCES

- [1] P. Mundhe and A. Pathrikar, "Design of an Effective Algorithm for ECG QRS Detection using VHDL," vol. 3, no. 7, pp. 2012–2015, 2014.
- [2] S. Mejhoudi, R. Latif, A. Elouardi, and W. Jenkal, "Advanced Methods and Implementation Tools for Cardiac Signal Analysis," *Advances in Science, Technology and Innovation*, pp. 95–103, 2019.
- [3] C. Venkatesan, P. Karthigaikumar, and R. Varatharajan, "FPGA implementation of modified error normalized LMS adaptive filter for ECG noise removal," *Cluster Computing*, vol. 22, pp. 12 233–12 241, 2019. [Online]. Available: <https://doi.org/10.1007/s10586-017-1602-0>
- [4] S. Mejhoudi, R. Latif, W. Jenkal, and A. Elouardi, "Real-Time ecg signal denoising using the adtf algorithm for embedded implementation on fpgas," *Proceedings of 2019 IEEE World Conference on Complex Systems, WCCS 2019*, 2019.
- [5] J. M. Leski and N. Henzel, "ECG baseline wander and powerline interference reduction using nonlinear filter bank," *Signal Processing*, vol. 85, no. 4, pp. 781–793, 2005.
- [6] Z. ul Haque, R. Qureshiy, M. Nawazy, F. Y. Khuhawar, N. Tunioz, and M. Uzairx, "Analysis of ECG signal processing and filtering algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 10, no. 3, pp. 545–550, 2019.
- [7] M. A. Kabir and C. Shahnaz, "Denoising of ECG signals based on noise reduction algorithms in EMD and wavelet domains," *Biomedical Signal Processing and Control*, vol. 7, no. 5, pp. 481–489, 2012. [Online]. Available: <http://dx.doi.org/10.1016/j.bspc.2011.11.003>
- [8] M. Rakshit and S. Das, "An efficient ECG denoising methodology using empirical mode decomposition and adaptive switching mean filter," *Biomedical Signal Processing and Control*, vol. 40, pp. 140–148, 2018. [Online]. Available: <https://doi.org/10.1016/j.bspc.2017.09.020>
- [9] O. El B'charri, R. Latif, K. Elmansouri, A. Abenaou, and W. Jenkal, "ECG signal performance de-noising assessment based on threshold tuning of dual-tree wavelet transform," *BioMedical Engineering Online*, vol. 16, no. 1, pp. 1–18, 2017.
- [10] E. M. El Hassan and M. Karim, "An FPGA-based implementation of a pre-processing stage for ECG signal analysis using DWT," *2014 2nd World Conference on Complex Systems, WCCS 2014*, pp. 649–654, 2015.
- [11] W. Jenkal, R. Latif, A. Toumanari, A. Dliou, O. El B'Charri, and F. M. R. Maoulainine, "An efficient algorithm of ECG signal denoising using the adaptive dual threshold filter and the discrete wavelet transform," *Biocybernetics and Biomedical Engineering*, vol. 36, no. 3, pp. 499–508, 2016. [Online]. Available: <http://dx.doi.org/10.1016/j.bbe.2016.04.001>
- [12] O. E. E. B'charri, R. Latif, W. Jenkal, and A. Abenaou, "The ECG Signal Compression Using an Efficient Algorithm Based on the DWT," *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 7, no. 3, pp. 181–187, 2016.
- [13] S. Pongponsoi and X. H. Yu, "An adaptive filtering approach for electrocardiogram (ECG) signal noise reduction using neural networks," *Neurocomputing*, vol. 117, pp. 206–213, 2013. [Online]. Available: <http://dx.doi.org/10.1016/j.neucom.2013.02.010>
- [14] W. Jenkal, R. Latif, A. Toumanari, A. Dliou, and O. El B'charri, "An efficient method of ecg signals denoising based on an adaptive algorithm using mean filter and an adaptive dual threshold filter," *International Review on Computers and Software*, vol. 10, no. 11, pp. 1089–1095, 2015.
- [15] S. Mejhoudi, R. Latif, A. Saddik, W. Jenkal, and A. El Ouardi, "Speeding up an Adaptive Filter based ECG Signal Pre-processing on Embedded Architectures," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 5, pp. 361–369, 2021.
- [16] P. Bhaskar and M. Uplane, "High Frequency Electromyogram Noise Removal from Electrocardiogram Using FIR Low Pass Filter Based on FPGA," *Procedia Technology*, vol. 25, no. Raerest, pp. 497–504, 2016. [Online]. Available: <http://linkinghub.elsevier.com/retrieve/pii/S2212017316304844>
- [17] P. N. Malleswari, C. Hima Bindu, and K. Satya Prasad, "An investigation on the performance analysis of ECG signal denoising using digital filters and wavelet family," *International Journal of Recent Technology and Engineering*, vol. 8, no. 1, pp. 166–171, 2019.
- [18] P. Radhakrishnan and G. Themozhi, "FPGA implementation of XOR-MUX full adder based DWT for signal processing applications," *Microprocessors and Microsystems*, vol. 73, p. 102961, 2020. [Online]. Available: <https://doi.org/10.1016/j.micpro.2019.102961>
- [19] M. Wasimuddin, K. Elleithy, A.-S. Abuzneid, M. Faezipour, and O. Abuzaghle, "Stages-based ecg signal analysis from traditional signal processing to machine learning approaches: A survey," *IEEE Access*, vol. 8, pp. 177 782–177 803, 2020.
- [20] A. Kumar, H. Tomar, V. K. Mehla, R. Komaragiri, and M. Kumar, "Stationary wavelet transform based ecg signal denoising method," *ISA transactions*, vol. 114, pp. 251–262, 2021.
- [21] Ö. F. Ertuğrul, E. Acar, E. Aldemir, and A. Öztekin, "Automatic diagnosis of cardiovascular disorders by sub images of the ecg signal using multi-feature extraction methods and randomized neural network," *Biomedical Signal Processing and Control*, vol. 64, p. 102260, 2021.
- [22] S. Chatterjee, R. S. Thakur, R. N. Yadav, L. Gupta, and D. K. Raghuvanshi, "Review of noise removal techniques in ecg signals," *IET Signal Processing*, vol. 14, no. 9, pp. 569–590, 2020.
- [23] G. Han, B. Lin, and Z. Xu, "Electrocardiogram signal denoising based on empirical mode decomposition technique: An overview," *Journal of Instrumentation*, vol. 12, no. 3, 2017.
- [24] W. Jenkal, R. Latif, A. Elouardi, and S. Mejhoudi, "FPGA Implementation of the Real-Time ADTF process using the Intel-Altera DE1 Board for ECG signal Denoising," *Proceedings of 2019 IEEE World Conference on Complex Systems, WCCS 2019*, 2019.
- [25] A. Deshmukh and M. M. Waje, "Fpga Implementation of Dwt for Ecg Signal Pre-Processing," *NOVATEUR PUBLICATIONS International Journal of Research Publications in Engineering and Technology*, vol. 3, no. 8, pp. 2454–7875, 2017.
- [26] [Online]. Available: <https://physionet.org/>

Machine Learning based Forecasting Systems for Worldwide International Tourists Arrival

Ram Krishn Mishra¹
Department of Computer Science
BITS Pilani, Dubai Campus
Dubai, United Arab Emirates 345055

Siddhaling Urolagin²
Department of Computer Science
BITS Pilani, Dubai Campus
Dubai, United Arab Emirates 345055

J. Angel Arul Jothi³
Department of Computer Science
BITS Pilani, Dubai Campus
Dubai, United Arab Emirates 345055

Nishad Nawaz⁴
Department of Business Management,
College of Business Administration
Kingdom University, Riffa, Kingdom of Bahrain

Haywantee Ramkissoon⁵
College of Business, Law, and Social Science,
Derby Business School,
University of Derby, Derby, United Kingdom

Abstract—The international tourist movement has overgrown in recent decades, and travelers are considered a significant source of income to the tourism economy. When tourists visit a place, they spend considerable money on their enjoyment, travel, and hotel accommodations. In this research, tourist data from 2010 to 2020 have been extracted and extended with depth analysis of different dimensions to identify valuable features. This research attempts to use machine learning regression techniques such as Support Vector Regression (SVR) and Random Forest Regression (RFR) to forecast and predict worldwide international tourist arrivals and achieved forecasting accuracy using SVR is 99.4% and using RFR is 84.7%. The study also analyzed the forecasting deadlock condition after covid-19 in the sudden drop of international visitors due to lockdown enforcement by all countries.

Keywords—Tourists; forecasting; machine learning; Covid-19

I. INTRODUCTION

The tourism industry plays a significant role in economic development, with several countries focusing on building the best possible policies for international travelers. Tourism is playing a significant role in contributing to multi-dimensional economic growth [1]. Multiple business sector economies across the globe rely on tourism to create employment opportunities, improve infrastructure, and foster cultural interchange between visitors and residents. Tourism can reap more benefits through a multi-stakeholder engagement approach[2]. Tourists rely on local transportation, accommodation, food and beverage, entertainment, and very importantly, visitors may want to buy new things which are not available in their local places. Such transactions contribute to mobilization of the local economy. hence contributing to the local economy. According to a World Tourism Organization (WTO) study in 2020, the percentage of people who travel for enjoyment as family and solo trips have increased from 50% in 2000 to 55% in 2019 [3]. The revenue generated from international tourists' arrivals can help the Country's economy and significantly contribute to balance payment of downgraded sectors such as unemployment, transportation, and healthcare [4].

One of the main motives for tourists to travel is to visit a new place to escape the monotony of boring routine life.

The solo or family trip helps ease stress and get a unique environment for a happier and healthier experience. The host country aims to provide the best possible facilities to tourists even when there are high-demand referrals. The forecasting system can help host countries prepare for the tourist requirements well in advance. Forecasting is a technique for creating accurate and optimize predictions[5] based on previous data. Fig. 1 shows the process of forecasting Systems. Many business stakeholders adopt the forecasting for various variables, including projecting future costs, quantity, or planning the budget. The major problems researchers face for developing a forecasting system is to collect the actual data. Two sources are there to gather the data, the first primary source contains first-hand information gathered directly by the organization. The data is generally collected by various surveys, focus groups, or interviews and direct methods of obtaining data make it more reliable and accurate to build the systems. Second, secondary sources are data that has already been collected and processed by a third party. The forecasting process is sped up by receiving data in a well-organized and compiled format.

A tourism forecasting system helps administration in planning and arranging essential things for tourists. With rapid infrastructure, economy, and politics changes, forecasting systems help to get things done on prior deadlines. Government organization and associated stakeholders which are involved in tourism planning required highly accurate forecasting system. With the help of forecasting system, they can adopt the required changes in much better and faster way. When there is no availability of highly accurate forecasting systems, these organization face difficulties[6]. In simple words, the meaning is, to minimize the possibility of the decision failing to attain the coveted goals. Hence an accurate prediction is very essential to the government.

Machine learning methods have attracted significant attention in tourism research [7] for better results than traditional approaches. Some machine learning methods like Neural Networks (NN) and SVR play a big role in forecasting time. Most of the techniques applied in prediction and tourism modelling are categorized into four categories: time series model, econometrics model, Artificial Intelligent (AI) techniques, and qualitative methods. AI techniques have been applied across

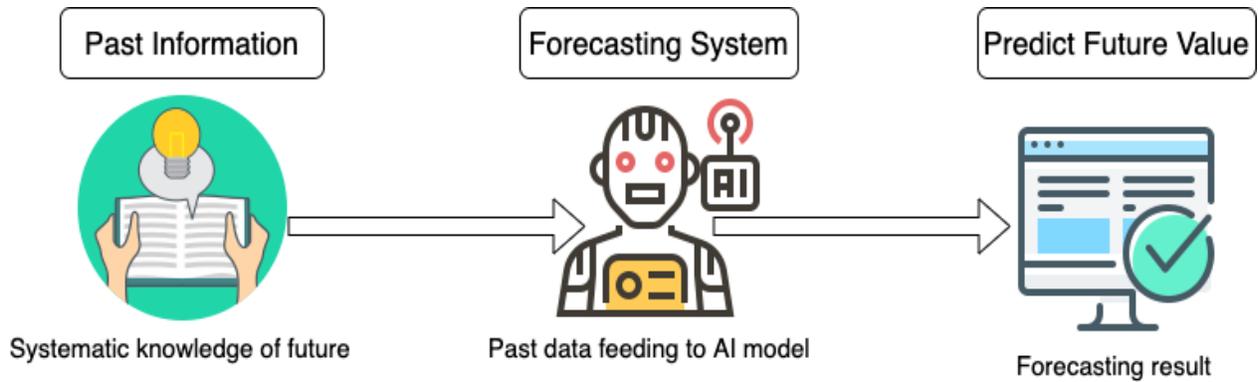


Fig. 1. Forecasting Systems.

several domains and in a variety of data structures.

In the current study, the ten-years tourists arrival data have been collected for developing forecasting systems. Many countries can use the proposed methods for tourist arrival forecasting for arranging the required facilities. This can inform tourism policy by forecasting tourism revenue. The forecast can assist the government in creating temporary job opportunities in the tourism sector for a particular period in that year. The advantage is that it can promote seasonal work in tourism and assist those whose livelihoods depend on tourism. Most of the work in tourism has been focused on domestic tourism forecasting [8]–[10]. Due to the rare availability of data, there are existing challenges in developing proper tourist forecasting systems. This study develops a worldwide tourist forecasting system by applying machine learning techniques such as SVR and RFR. The machine learning methods [11], [12] have been tested with different kinds of feature selection techniques and clear identification of attributes before feeding into the model. Developed tourist forecasting systems will help to analyze the flow of tourists internationally and in the host country. This system will also help to identify the transport traffic and facilitate the number of flights between two countries, arranging or extending local transport systems and analyzing the required number of rooms in hotels. The COVID-19 pandemic had sudden travel restrictions across borders. The year 2020 was the worst in tourism history in international tourist arrivals. The SARS-COV-2 virus has led to a setback in the current forecasting Systems. In this study, we retrieve the forecasting data and compare the results with the current covid-19 scenario.

A tourism forecasting system helps to plan and arrange essential things for tourists. With rapid infrastructure, economy, and politics changes, forecasting systems help to get things done on prior deadlines. Government organization and associated stakeholders which are involved in tourism planning required highly accurate forecasting system. With the help of forecasting system, they can adopt the required changes in much better and faster way. When there is no availability of highly accurate forecasting systems, these organization face difficulties[6]. In simple words, the meaning is, to minimize the possibility of the decision failing to attain the coveted goals. Hence an accurate prediction is very essential to the government.

Machine learning methods have attracted significant attention in tourism research [7] for better results than traditional approaches. Some machine learning methods like Neural Networks (NN) and SVR play a big role in forecasting time. Most of the techniques applied in prediction and tourism modelling are categorized into four categories: time series model, econometrics model, Artificial Intelligent (AI) techniques, and qualitative methods. AI techniques have been applied across several domains and in a variety of data structures.

In the current study, we have collected ten-year prior visitor history data to develop forecasting systems. Many countries can use the proposed methods for tourist arrival forecasting for arranging the required facilities. This can inform tourism policy by forecasting tourism revenue. The forecast can assist the government in creating temporary job opportunities in the tourism sector for a particular period in that year. The advantage is that it can promote seasonal work in tourism and assist those whose livelihoods depend on tourism. Most of the work in tourism has been focused on domestic tourism forecasting [8]–[10]. Due to the rare availability of data, there are existing challenges in developing proper tourist forecasting systems. This study develops a worldwide tourist forecasting system by applying machine learning techniques such as SVR and RFR. The machine learning methods [11], [12] have been tested with different kinds of feature selection techniques and clear identification of attributes before feeding into the model. Developed tourist forecasting systems will help to analyze the flow of tourists internationally and in the host country. This system will also help to identify the transport traffic and facilitate the number of flights between two countries, arranging or extending local transport systems and analyzing the required number of rooms in hotels. The COVID-19 pandemic had sudden travel restrictions across borders. The year 2020 was the worst in tourism history in international tourist arrivals. The SARS-COV-2 virus has led to a setback in the current forecasting Systems. In this study, we retrieve the forecasting data and compare the results with the current Covid-19 scenario.

II. LITERATURE SURVEY

A forecasting system for tourism will provide direct and indirect benefits to the government, society, people, business, services, and economy of the country. Tourism contributes

TABLE I. COMPARISON OF MODELS AND USED REGIONS

Reference Number	Region Focused	Research Objects	Data Frequency	Methodologies	Performance Measure	Variables
[13]	Las Vegas	Tourism Demand	Monthly	Logistic Growth Regression	MAPE, RMSPE, DM.	Tourist Arrivals
[14]	Taiwan	Inbound Tourism	Half Yearly, Annually	SARIMA- GARCH	MAPE, MAD, RMSE.	Tourist Arrivals
[15]	Hong Kong	Inbound Tourists	Monthly	Sparse GPR	MAE, MAPE, MSE.	Tourist Arrivals
[16]	Taiwan	Outbound Tourism	Monthly	SARIMA	MAPE	Tourist Arrivals
[17]	South Tyrol	Tourism Demand	Monthly	SARIMA.	MAPE, R.M.S.E., M.S.E., MAD	Tourist Arrivals

to GDP, employment, visa services, and tourism-related businesses. Given the significant positive impacts of tourism, performing the prediction on the number of tourist visitors, the time, when tourists visit the places, the duration of tourist's visits will provide crucial information to the government. Researchers are keen to develop an accurate forecasting system and to find a novel approach to deal with different sizes of data datasets. The seasonal ARIMA, v-Support Vector Regression and Multi-Layer Perceptron (MLP) Neural Networks models were applied on monthly data for the tourist arrival in Turkey and proposed an approach to select the model in a given time series [11]. Combined techniques have been discussed to predict tourism demand [18]. The authors combined ACF, NN, and Genetic Algorithms (GA) to perform the classification. A framework has been suggested based on the Generalized Dynamic Factor Model (GDFM) to generate the composite search index [19]. It has improved the forecast accuracy as compared to the traditional time series model and Principal Component Analysis (PCA) model. Decomposition based on eigen were used to reduce the dimensions [20] in time series data prediction. Wang Jun et.al. [21] have proposed the forecasting model by combining ANN and a clustering algorithm and compared this model with other ANN-based and ARIMA model; this model performed better than other related methods. For the multisource data and passenger flow volume, authors have proposed a new algorithm by merging the non-linear, genetic algorithm and S.V.R. Karo Solat, et al. [22], have used elliptically symmetric principal components for predicting exchange rates. Forecasting data belongs to the regression category; researchers have applied the methods such as regression, the Delphi method, moving average models, ARIMA, MLP, GRNN, radial bias function (RBF) among others. Shaolong Sun et.al. have developed a tourist arrival forecasting model. One of the most widely used time series forecasting models is the ARIMA. However, the latter does not perform better with multi-source data [23]. The authors proposed the Kernel Extreme Learning Machine (KELM) models to improve the forecasting accuracy and robustness analysis on the Baidu Index and Google Index data. According to the authors in [24], the most used time series analysis model for the prediction of tourist arrivals is ARIMA and was used extensively in the last few years. Authors used Seasonal Autoregressive Integrated Moving Average (SARIMA) with Generalised Autoregressive Conditional Heteroskedasticity (GARCH) to forecast tourist arrivals in Taiwan [25]. In [26], the authors have used SARIMA to predict the demand for traveling by air. Hence, all these studies, research, and work done demonstrated that enhanced ARIMA models lead to better predictions.

Accurate tourist forecasts are essential because they provide crucial information to tourism practitioners and academics when making decisions about resource allocation, priority, and risk assessment. Based on an extant review of the litera-

ture [27], prediction methods in tourist arrivals can be categorized into Machine Learning (ML) models and techniques of time series analysis. With reference to model building, tourism demand prediction studies depend strongly on variables that are input to the model [28]. These variables are supposed to be strongly connected to tourism demand, with no missing or incorrect values. Tourism demand prediction components can be defined in several ways using various parameters. They can be classified into indicators and determinants, depending on the relationship with tourism demand establish ML methods for estimating the number of tourists coming to Turkey. In their work, Linear Regression and NN-MLP are implemented to create multivariate tourism predictions for Turkey. They compare performances of the predictions in the context of Relative Absolute Error (RAE), Root Relative Squared Mean (RRSE) and Correlation Coefficient (R) measurements depicting MLP for regression produces enhanced performance. Extensively used ML models consist of Artificial Neural Networks (ANN) and SVR Authors in [29] have used the method SVR and "Fly Optimization Algorithm (FOA)" together for predicting tourism arrivals. In [13], a prediction model has been suggested, which amalgamates "Back-Propagation Neural Network (BPNN)" and "Empirical Mode Decomposition (EMD)". This model foretells how many tourists will visit the place. Li et al. [14] enhanced BPNN by incorporating the PCA and DE (ADE) algorithm to predict how many tourists are willing to visit the place in the future. Outcomes of the work in [13] and [14] revealed that enhanced BPNN was outperforming ARIMA Authors in [30] created a new structural NN model, forecasting the number of tourists willing to visit the place in the future. The outcomes demonstrated that none of the models were superior in any of the situations.

Fernandes et al. state that Artificial Intelligence (AI) has played an essential role in attaining outstanding applications in predicting the demand of tourists in the region. Despite that, many of the AI methods used till now are not deep architectures. They have little ability for researching greater non-linearities, especially when data is big-scale and vague patterns [31]. The authors have come up with a new deep learning technique called the "Stacked Autoencoder" with "Echo-State Regression (SAEN) which helped in predicting demand for tourism [32]. SAEN is employed in four different tourism situations and the outcome of the prediction reveals that SAEN is better than the standard models. A big data based system for tourism forecasting is proposed [33]. The authors have included leading indicators such as price index which improved the performance of the model. In [34], the authors present the Real-Value Genetic Algorithm (RGA) to specify the available parameter of SVR, called GA-SVR. It optimizes each parameter of SVR at the same time from training data. Afterward, they forecast tourism demand in China. Moreover, they carried out a comparison between BPNN and

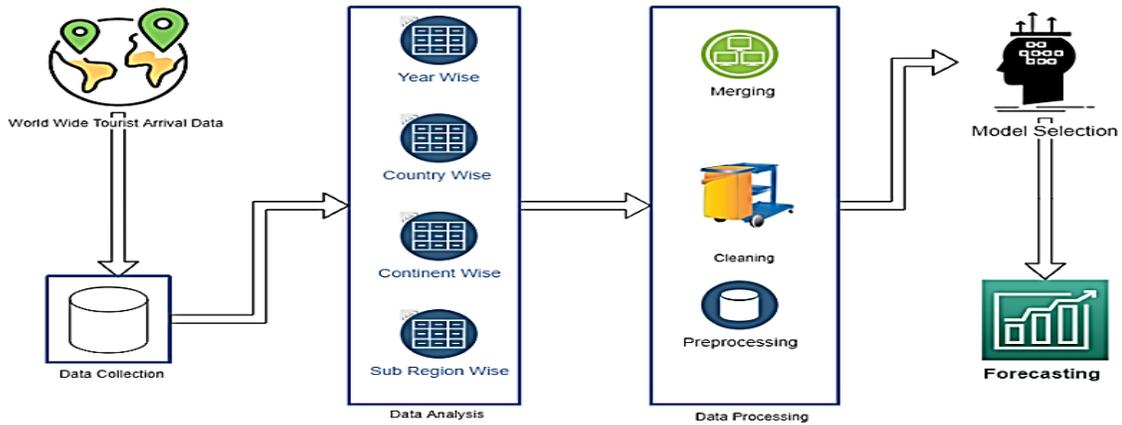


Fig. 2. Tourist Forecasting Systems.

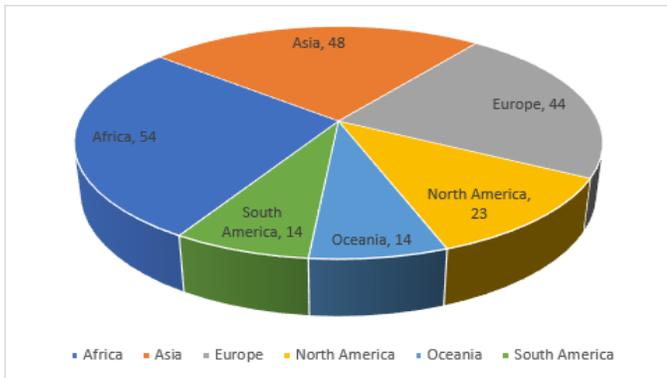


Fig. 3. Continent and Associated Number of Countries.

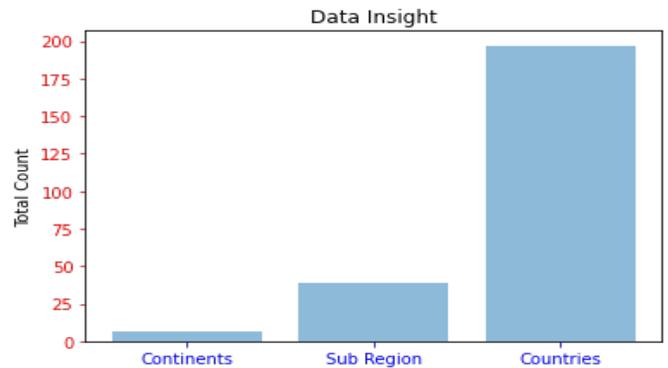


Fig. 4. Data Insights.

time series models. This comparison helped them know that SVR has a good predicting capability. Moreover, the authors have mentioned eight sections. One section presents studies associated with SVR, while another section summarizes the current methods to the option of hyperparameters. Another section details the GA-SVR technique and the rest of the sections deal with the analysis of outcomes, the origin of the data, etc. Various NN models were developed in [34] on cross learning to predict time series data. The principal components of prediction are "Determinants". Traditional economic ideas, like "consumption behavior theory" and "utility theory" indicate that factors, for example, cost, earning, and publicising affect the demand of tourist arrivals. It can be seen [1], [16] [16][29] to have a complete examination of tourism demand prediction studies. All these studies notice that the functioning of predicting models differs based on various considerations, for example, the data's frequency, prediction horizon's length, the source countries, and the destination. What made us concentrate on the data-driven methods in accordance with ML, is the dearth of agreement about the most correct model to predict tourism demand. In [35], the authors notice that the technique of SVM based is much signified to deal with traits of the tourist's data. They contrast and differentiate the predicting accuracy of various ML models to ARMA using month-wise tourist visits from 13 countries coming to Hong Kong. They

considered the years from 1985 to 2008, and from their work, they obtained the best correct results with ML techniques. The requirement for further correct predictions had given rise to more dependency on ML models to get better-sophisticated forecasts of tourists.

In [29], the authors have employed a "Rough Sets Approach" to predict demand for tourism in Hong Kong from the US and UK Gaussian Process Regression (GPR) has been used in past years for prediction. It is a supervised learning approach followed by generalized linear regression to forecast data locally. To bridge the gap, the authors in [13], [19] have designed a prediction test to contrast GPR to NN and SVR. Their primary objective behind this study was to examine the relative advancement of ML techniques' prediction accuracy through a linear stochastic procedure employing two substitute approaches. First is the direct one, which predicts the aggregate series. The second approach is using the same models to predict the particular series for the regions one by one. Finally, the predicting performance of both methods was compared. Weather forecasting can be applied using Deep Learning (DL) techniques also. DL can be used in various fields like entertainment, visual recognition, and including forecasting such as tourism forecasting, forecasting stock prices, etc. The authors have compared the performance of the prediction of "Recurrent Neural Network (RNN)", "Conditional Restricted

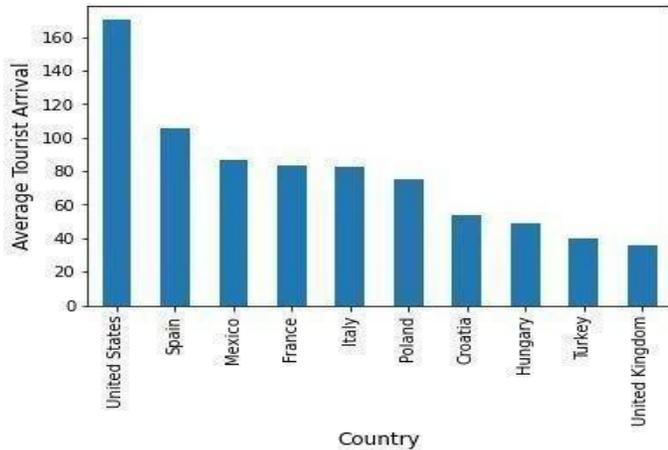


Fig. 5. Average Tourist Arrival in Top 10 Most Visited Countries.

Boltzmann Machines (CRBM)” and ”Convolution Neural Network (CNN)” [15]. Authors in [13] give an introduction to principles of ANN and they also provide a stage-by-stage guide to methods they have applied for building a NN for predicting tourist arrivals. They have involved many rules and have included some points of discussion among the authors to apply ANN effectively. A comparison of various forecasting methods is shown in Table I.

III. METHODOLOGY

This research proposes tourist forecasting systems in Fig. 2. To predict international tourist arrivals, the methods adopted are data collection from globally trusted sources, followed by data analysis, data processing, and the creation of a machine learning model. The machine learning techniques include SVR and RFR.

1) *Data Collection and Analysis:* This research draws on historical data to tackle the forecasting challenges and develop the predictive model. A substantial amount of data gathered by the government or other public entities is made available. These data sets are referred to as public data since they do not require specific authorization to use them. The data is gathered from reliable online sources and official tourist websites of countries. This dataset contains tourist arrivals for most of the countries between 2010 to 2020. Since data for nearly 13 countries are not available on the internet, those countries are not included in proposed forecasting system. In addition, the tourism industry suffered greatly because of Covid-19 in terms of visitor arrivals. As a result, data for 2020 is not available for most of the countries. Whatever data have been found for year 2020 been used for Covid-19 analysis in respective to international tourist arrivals.

Fig. 3 shows the number of countries on a particular continent. Fig. 4 depicts the data insights of number of continents, sub-regions and countries. Africa has the highest number of countries, i.e. 48 and South America has the lowest, i.e. 12 countries. Continent wise number of countries are Africa = 48, Asia = 45, Europe = 43, North America = 23, Oceania = 13, South America = 12.

Fig. 5 shows a graphical representation of average tourist

arrivals in the top 10 countries. The United States has the highest number of tourist arrivals while the United Kingdom comes in number 10. These top 10 countries decide the flow of international tourists and make common global tourism policies.

Year vs average analysis essentially explains the distribution of arrival data as well as the year-by-year data association of annual arrivals. In most cases the year-wise data is matching with average data, there are not many changes in tourist arrivals as depicted in Fig. 6. scatter plot depicts the annual data points distribution and it can be seen Fig. 7(a) and 7(b) that data is not equally aligning in years 2011 and 2012.

Correlation matrix shows the relationship between two variables which is shown in Fig. 8. If the variables are highly correlated then the value will be closer to 1. In Table the data is ranging from year 2010 to 2019 and average.

A. Data Preprocessing

The significance of preprocessing data must be comprehended first before moving on to developing forecasting system. It has the potential to make or ruin forecasting. The self-lag differencing method have been used to preprocess the data where the previous 3 years had been used for training and 4th year for forecasting.

Table II shows the originally annual collected data for 10 countries. This data is in the form of raw data which cannot be directly fed to the forecasting model, so before moving ahead preprocessing steps have been applied. The previous day's, month's, and year's data are very important to make the prediction. In other words, the value at time $t-1$ has a significant impact on the value at time t . Lags are the past values, therefore $t-1$ is lag 1, $t-2$ is lag 2, and so on. The lag features-based data preparation techniques have been used and after the process the result that have been found is shown in Table III.

Table III depicts the data preparation of county United States after removing the null values from Table IV. For the year 2013, International tourist's arrival counted 179.31 million and lag 3 values is T-3 which is 162.28 million, lag 3 is 147.27 million, and lag 1 is 162.28. The data is now ready for the next step to develop the machine learning based forecasting systems.

What are the variations in the top 5 arrivals countries have been shown in Fig. 9, which shows that the United States is at the top and Spain is in second place, but the growth of tourist arrivals are growing year by year. France having variations every year means ups and down in arrivals year by year.

B. Machine Learning Models

Machine learning technique has inspired due to the wide variety of applications in multiple domains. Machine learning has proven to perform better on complicated data and tasks, and this is a reason for draining it for adopting into the forecasting systems. Below are the models with different parameters that have been applied in this research:

a) Support Vector Regression

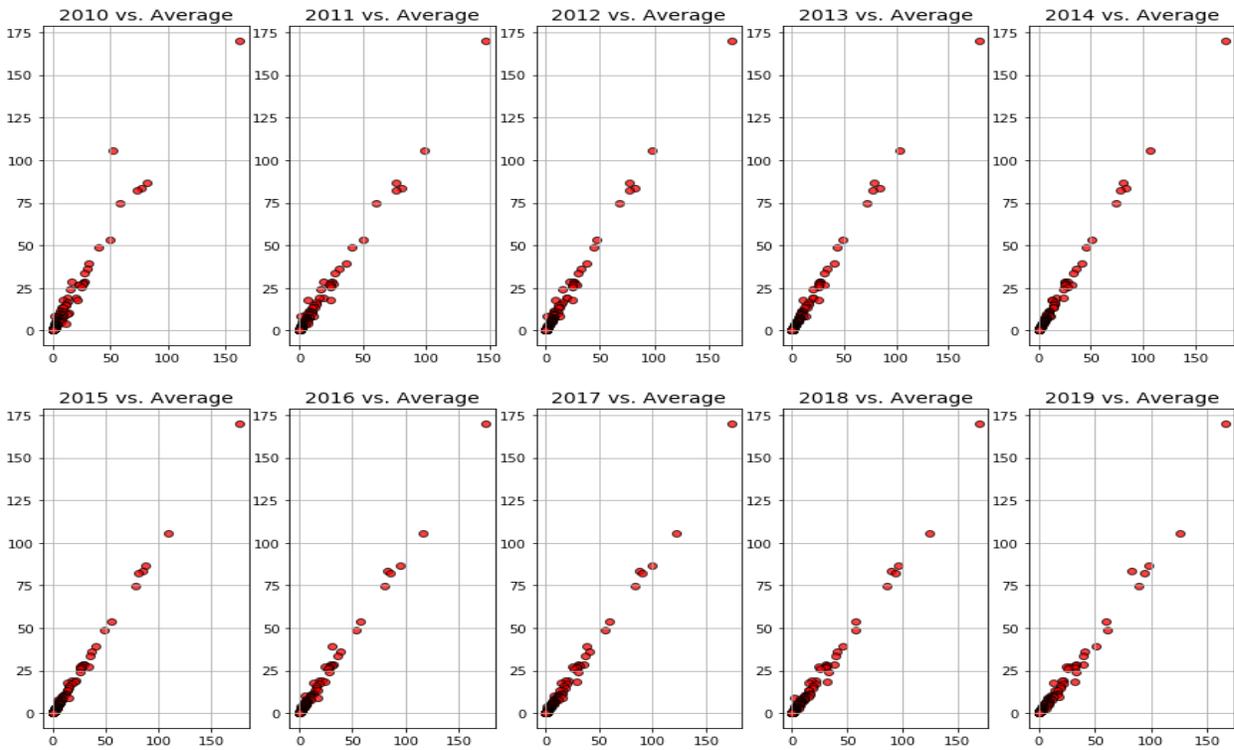


Fig. 6. Year Wise vs Average Data Analysis.

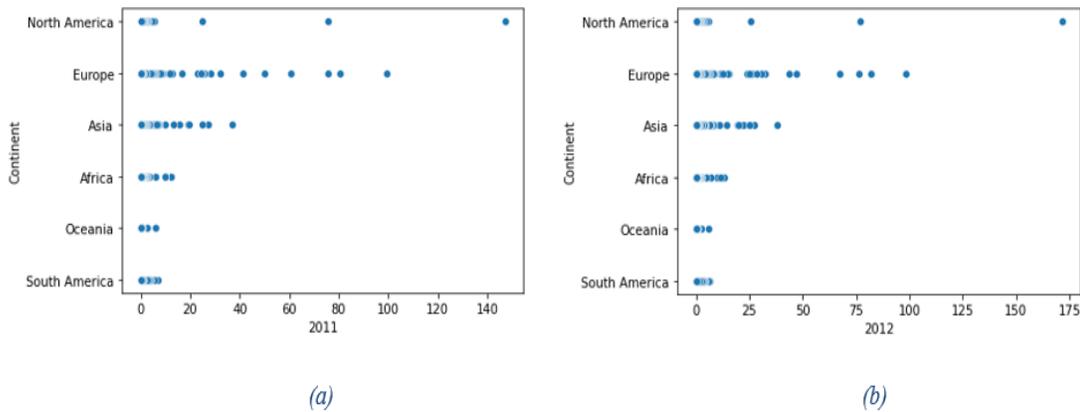


Fig. 7. Continent Wise Visitors.

The Support Vector Regression (SVR) is adopted from support Vector Machine (SVM) for the regression type data to predict the value. While dealing with real number data, the SVM changes its variant as regression. The output for real type data has infinite possibilities, and researchers have to see all possible solutions to decide the final prediction. While dealing with real time data, the primary idea is to minimize equation 1 and in case, if problem is linear then support vector regression is represented by equation 2 and error minimization has given in equation 3:

$$y = x\beta + b \quad (1)$$

$$y = \sum_{n=1}^N (\alpha - \alpha t_i)(x_i, x) + b \quad (2)$$

$$\frac{1}{2} \|w\|^2 + c \cdot i = 0n(-'i) \quad (3)$$

below constraints need to be taken care with linear support vector regression.

$$y_i - wx_i + b \leq (\epsilon + \epsilon_i)$$

$$y_i - wx_i + b \leq (\epsilon + \epsilon_i)$$

$$\epsilon + \epsilon_i \geq 0$$

	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	average
2010	1.000000	0.976896	0.983223	0.979965	0.977214	0.975066	0.969347	0.965850	0.960944	0.954744	0.978670
2011	0.976896	1.000000	0.996823	0.994666	0.993701	0.992311	0.989119	0.988839	0.987720	0.983506	0.995519
2012	0.983223	0.996823	1.000000	0.998577	0.996685	0.993896	0.989054	0.986908	0.984558	0.979785	0.995978
2013	0.979965	0.994666	0.998577	1.000000	0.998143	0.996192	0.991541	0.989083	0.985106	0.981448	0.996627
2014	0.977214	0.993701	0.996685	0.998143	1.000000	0.998723	0.994362	0.992298	0.989028	0.986123	0.997962
2015	0.975066	0.992311	0.993896	0.996192	0.998723	1.000000	0.997104	0.996010	0.992620	0.990546	0.998753
2016	0.969347	0.989119	0.989054	0.991541	0.994362	0.997104	1.000000	0.998885	0.994670	0.992894	0.997401
2017	0.965850	0.988839	0.986908	0.989083	0.992298	0.996010	0.998885	1.000000	0.997743	0.996477	0.997030
2018	0.960944	0.987720	0.984558	0.985106	0.989028	0.992620	0.994670	0.997743	1.000000	0.998795	0.995017
2019	0.954744	0.983506	0.979785	0.981448	0.986123	0.990546	0.992894	0.996477	0.998795	1.000000	0.992453
average	0.978670	0.995519	0.995978	0.996627	0.997962	0.998753	0.997401	0.997030	0.995017	0.992453	1.000000

Fig. 8. Correlation Matrix of Tourist Arrivals.

TABLE II. SAMPLES OF COLLECTED DATA

Country	2010	2011	2012	2013	2014	2015	2016	2017	2018	2019	2020
Finland	3.67	4.19	4.23	2.8	2.73	2.62	2.79	3.18	3.22	3.29	0.0988
Paraguay	3.17	3.37	3.66	3.54	3.46	4.1	4.32	4.74	4.18	4.37	0.308
Netherlands	10.88	11.3	11.68	12.78	13.93	15.01	15.83	17.92	18.78	20.13	0.47
Qatar	1.7	2.06	2.32	2.61	2.84	2.94	2.94	2.26	1.82	2.14	0.551
Croatia	49.01	49.97	47.19	48.35	51.17	55.86	57.59	59.24	57.67	60.02	1.48
United States	162.28	147.27	171.63	179.31	178.31	176.86	175.26	174.29	169.32	166.01	2.68
Hungary	39.9	41.3	43.57	43.61	45.98	48.35	52.89	54.96	57.67	61.4	3.686
Ukraine	21.2	24.54	25.06	26.03	13.23	13.03	13.73	14.58	14.34	13.71	3.965

TABLE III. PREPROCESSING OF COLLECTED DATA

Country	Year	T-3	T-2	T-3	Arrival
United States	2010	NaN	NaN	NaN	162.28
United States	2011	NaN	NaN	162.28	147.27
United States	2012	NaN	162.28	147.27	171.63
United States	2013	162.28	147.27	171.63	179.31
United States	2014	147.27	171.63	179.31	178.31
United States	2015	171.63	179.31	178.31	176.86
United States	2016	179.31	178.31	176.86	175.26
United States	2017	178.31	176.86	175.26	174.29
United States	2018	176.86	175.26	174.29	169.32
United States	2019	175.26	174.29	169.32	166.01

TABLE IV. PREPROCESSED DATA AFTER REMOVAL OF NAN VALUES

Country	Year	T-3	T-2	T-3	Arrival
United States	2013	162.28	147.27	171.63	179.31
United States	2014	147.27	171.63	179.31	178.31
United States	2015	171.63	179.31	178.31	176.86
United States	2016	179.31	178.31	176.86	175.26
United States	2017	178.31	176.86	175.26	174.29
United States	2018	176.86	175.26	174.29	169.32
United States	2019	175.26	174.29	169.32	166.01

b) Random Forest Regressor A tree structure of data arrangement gives an actual estimator. Random forest follows the pattern of the decision tree, where each data node will be split into daughter nodes. While splitting the data nodes, a split criterion is being chosen to be appropriately partitioned. All the data nodes at the bottom are terminal. In the case of regression data, the predicted value at a node is the average response

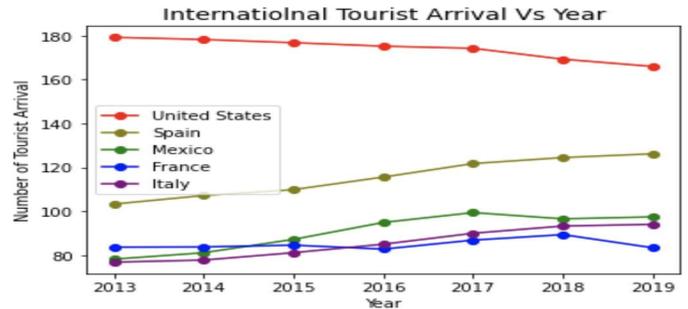


Fig. 9. Top 5 Country Tourist Variations Comparisons.

variable for all observers in the nodes. Splitting criteria for regression is chosen by equation (4).

$$RSS = \sum_{left} (y_i - y_l^*) + \sum_{right} (y_i - y_r^*) \quad (4)$$

Where

$$y_l^* = \text{mean } y \text{ value for left node}$$

$$y_r^* = \text{mean } y \text{ value for right node}$$

Sometimes dealing with classified data where the predicted class is the most common class in the node, which is also known as the majority vote. So far classification tree estimated probability calculated members of each class.

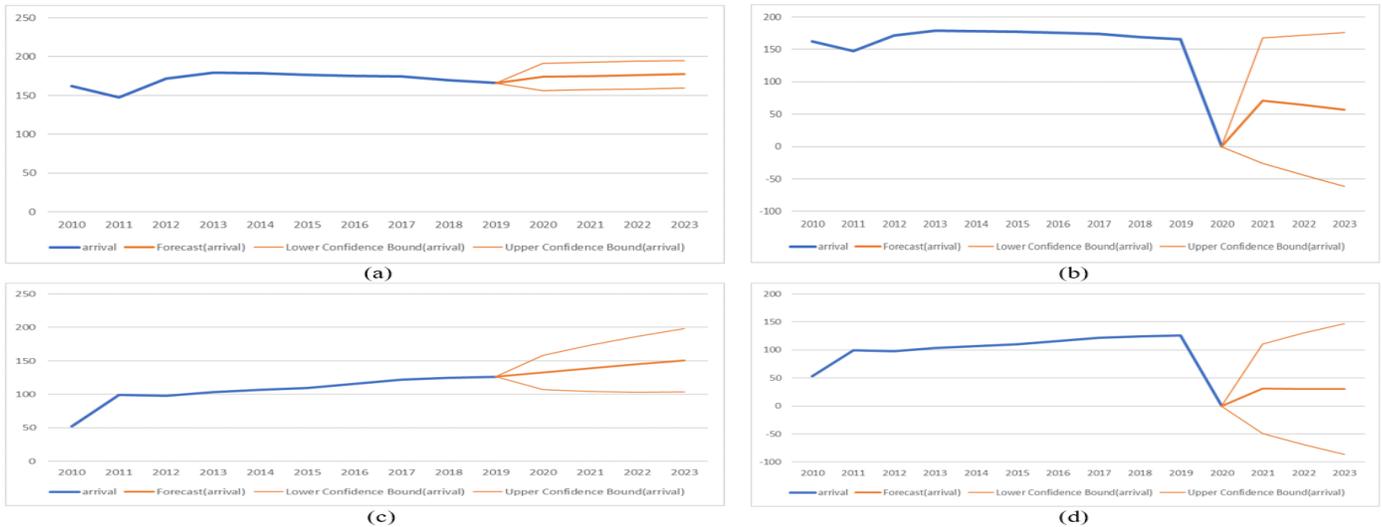


Fig. 10. Forecasting Trend before and after Covid for USA and Spain.

Splitting criteria for classified data is given by Gini index, which is shown in equation (5).

$$Gini = N_l \sum_{k=1, \dots, K} P_{kl}(1 - P_{kl}) + N_r \sum_{k=1, \dots, K} P_{kr}(1 - P_{kr}) \quad (5)$$

Where

P_{kl} = proportion of class k in left node.

P_{kr} = proportion of class k in right node.

A random forest is a meta estimator that uses averaging to increase predictive precision and control over-fitting by fitting several classifying decision trees on different sub-samples of the dataset. Although the sub-sample size is the same as the initial input sample size, the samples are drawn with substitution. For classification tasks, the Decision Tree and Random Forest models are often used. However, the concept of Random Forest as a regularizing meta-estimator over a single decision tree is better illustrated by extending it to regression problems. In this way, it can be shown that a single decision tree is vulnerable to overfitting and learning false associations in the face of random noise. At the same time, an adequately built Random Forest model is more resistant to such overfitting.

IV. EXPERIMENTAL RESULT

The experimental results are collected using the following setup. Dataset used contained tourist arrivals for mostly all global countries. Python 3.7 was used along with scikit-learn, NLTK and NumPy libraries for each learning algorithm used, the regression techniques, and the confusion matrix. First, baseline results have been obtained using SVR, and then RFR model have been used to train data. The number of features is 11, and data partitioning between training of 2/3 and testing is 1/3.

It is essential to evaluate the model using testing data once it has been trained. To verify the model's correctness,

numerous evaluation matrices have been utilized. This study focuses mostly on R-Squared, a commonly used effectiveness accuracy metric as shown in Table V. R-Square determines if the data is near the fitted regression line. The regression model, it's also known as the coefficient of determination or the value of multiple determination. R-squared is defined as the percentage of the variance in the response variable that is explained by a linear model.

TABLE V. EXPERIMENTAL RESULTS

Model Name	R-Square
SVR (Kernel='linear')	0.994
SVR (Kernel='rbf')	0.863
RFR (Tree Model)	0.847

The R-squared value is always between 0 and 100%. In this research two models have been considered: SVR with different kernels and RFR with tree model. The partitioning of data between training and testing is 67% and 33% and found that the accuracy which is shown in Table V for SVR (kernel=linear) is 0.994, with kernel RBF is 0.863. The random forest regression works well for small size dataset and found R-Square result is 0.847.

V. FORECASTING BEFORE AND AFTER COVID-19

The graphs plot the forecasting regression per covid and post covid for the next 4 years and found that normal forecasting upper boundary line is going as usual however when Covid-19 enforced the restriction around the world then tourist arrival has drastically resulted null.

Fig. 10(a) shows the forecasting before covid-19 for the Country USA and Fig. 10(b) depicts the forecasting during the existence of Covid-19. As per the graph visualization upper bound forecasting is reviving in the year 2022. The same things can be seen in Fig. 10(c) without Covid-19 and Fig. 10(d) after Covid-19 for the Country Spain and differences can be observed as like USA.

VI. DISCUSSION

The collected worldwide tourist arrival data from different trusted and official web portals are analysed to forecast future international tourist arrivals. Such analysis can mobilized the tourism industry. Table II has shown a different kind of collected data and time-frequency with applied methods by the researcher in [16], and the studies from [36]–[38] show that most of the collected data is focused on a specific region in a country. The focus is to align with the objective of the United Nations World Tourism Organization (UNWTO) to work on collective universal data and analyze the impact of tourism due to worldwide tourist movements.

The collected data has the frequency of yearly and building optimized machine learning models[39] of this variety of data having a lot of challenges. The actual data is from the year 2010 to 2019; in 2020 international travel was heavily impacted due to place confinement [37]. Whole world is gone through a very worst situations due to covid and many technological techniques have been used to analyze and predict the situations. This study emphasizes the comparative study before the Covid-19 pandemic of actual forecasting and how suddenly forecasting systems stopped predicting the correct values once the global health pandemic started. Handling the future pandemic situations and fulfilling the basic requirement for new arrivals, forecasting models will help not only to governing bodies but also to hospitality service provides such as hotels, restaurant, transportation, etc. The pandemic has also given a crises situation in healthcare industries and how basic medicine facilities can be provided to tourists who could not return to his/her country due to lockdown enforcement.

VII. CONCLUSION

Digitalization has made the whole world a village, it remains important to have collective forecasting of data that represents the whole globe. The UNWTO, and the World Travel and Tourism Council (WTTC) are working continuously on improving the global tourism facilities by analyzing the demand and increasing number of arrivals. This research focused on overall worldwide data with machine learning approaches such as support vector regression and random forest regression and the result shows that support vector regression has given better results as compared to random forest regression.

Since the number of vistors for any country is not exactly known, building the model with multiple techniques would give an analytic view for the comparative study. This is the reason for developing the model by using machine learning. Since the collected data is on annual frequency, it doesn't fit well with deep learning techniques so consideration for this work is machine learning techniques i.e., support vector regression and random forest regression. A future extension of this work would be a clustering-based forecasting system where the groups of data would be based on countries with most arrivals, mid arrival countries, and low arrival countries. The focus is to collect monthly data to forecast the season-wise and finding the most interesting month of a tourist visit.

ACKNOWLEDGMENT

The authors would like to thanks Intelligent Computing Lab, Department of Computer Science at BITS Pilani, Dubai

Campus for infrastructure and computing facilities.

REFERENCES

- [1] A. Jelušić, "Modelling tourist consumption to achieve economic growth and external balance: Case of Croatia," *Tourism and Hospitality Management*, vol. 23, no. 1, pp. 87–104, 2017, doi: 10.20867/thm.23.1.5.
- [2] H. Ramkissoon, "COVID-19 Place Confinement, Pro-Social, Pro-environmental Behaviors, and Residents' Wellbeing: A New Conceptual Framework," *Frontiers in Psychology*, vol. 11, no. September, pp. 1–11, 2020, doi: 10.3389/fpsyg.2020.02248.
- [3] UN World Travel Organization, "International Tourism Highlights," Unwto, pp. 1–24, 2019.
- [4] S. Aynalem, K. Birhanu, and S. Tesebay, "Employment Opportunities and Challenges in Tourism and Hospitality Sectors," *Journal of Tourism & Hospitality*, vol. 05, no. 06, 2016, doi: 10.4172/2167-0269.1000257.
- [5] S. Pervaiz, Z. Ul-Qayyum, W. H. Bangyal, L. Gao, and J. Ahmad, "A Systematic Literature Review on Particle Swarm Optimization Techniques for Medical Diseases Detection," *Computational and Mathematical Methods in Medicine*, vol. 2021, 2021, doi: 10.1155/2021/5990999.
- [6] G. González-Rivera, P. Loungani, and X. (Simon) Sheng, "Forecasting issues in developing economies," *International Journal of Forecasting*, vol. 35, no. 3, pp. 927–928, 2019, doi: 10.1016/j.ijforecast.2019.04.005.
- [7] H. Rezapouraghdam, A. Akhshik, and H. Ramkissoon, "Application of machine learning to predict visitors' green behavior in marine protected areas: evidence from Cyprus," *Journal of Sustainable Tourism*, 2021, doi: 10.1080/09669582.2021.1887878.
- [8] G. Athanasopoulos and R. J. Hyndman, "Modelling and forecasting Australian domestic tourism," *Tourism Management*, vol. 29, no. 1, pp. 19–31, 2008, doi: 10.1016/j.tourman.2007.04.009.
- [9] T. Baldigara, "Modelling domestic tourism in Croatia," *Turisticko poslovanje*, vol. 43, no. 22, pp. 19–38, 2018, doi: 10.5937/turpos1822019b.
- [10] J. Wu and Z. Ding, "Improved grey model by dragonfly algorithm for chinese tourism demand forecasting," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 12144 LNAI, no. September, pp. 199–209, 2020, doi: 10.1007/978-3-030-55789-8_18.
- [11] H. Drucker, C. J. C. Surges, L. Kaufman, A. Smola, and V. Vapnik, "Support vector regression machines," *Advances in Neural Information Processing Systems*, no. May 2018, pp. 155–161, 1997.
- [12] M. R. Segal, "Machine Learning Benchmarks and Random Forest Regression," *Biostatistics*, pp. 1–14, 2004, [Online]. Available: <http://escholarship.org/uc/item/35x3v9t4.pdf>
- [13] Y. H. Liang, "Forecasting models for Taiwanese tourism demand after allowance for Mainland China tourists visiting Taiwan," *Computers and Industrial Engineering*, vol. 74, no. 1, pp. 111–119, 2014, doi: 10.1016/j.cie.2014.04.005.
- [14] F. L. Chu, "Using a logistic growth regression model to forecast the demand for tourism in Las Vegas," *Tourism Management Perspectives*, vol. 12, pp. 62–67, 2014, doi: 10.1016/j.tmp.2014.08.003.
- [15] A. G. Salman, B. Kanigoro, and Y. Heryadi, "Weather forecasting using deep learning techniques," *ICACSA 2015 - 2015 International Conference on Advanced Computer Science and Information Systems, Proceedings*, pp. 281–285, 2016, doi: 10.1109/ICACSA.2015.7415154.
- [16] B. Petrevska, "Predicting tourism demand by A.R.I.M.A. models," *Economic Research-Ekonomska Istrazivanja*, vol. 30, no. 1, pp. 939–950, 2017, doi: 10.1080/1331677X.2017.1314822.
- [17] Y. W. Chang and M. Y. Liao, "A seasonal ARIMA model of tourism forecasting: The case of Taiwan," *Asia Pacific Journal of Tourism Research*, vol. 15, no. 2, pp. 215–221, 2010, doi: 10.1080/10941661003630001.
- [18] H. Zou and Y. Yang, "Combining time series models for forecasting," *International Journal of Forecasting*, vol. 20, no. 1, pp. 69–84, 2004, doi: 10.1016/S0169-2070(03)00004-9.
- [19] J. Bowden, "A logistic regression analysis of the cross-cultural differences of the main destination choices of international tourists in China's main gateway cities," *Tourism Geographies*, vol. 8, no. 4, pp. 403–428, 2006, doi: 10.1080/14616680600922104.

- [20] P. Nystrup, E. Lindström, J. K. Møller, and H. Madsen, "Dimensionality reduction in forecasting with temporal hierarchies," *International Journal of Forecasting*, vol. 37, no. 3, pp. 1127–1146, 2021, doi: 10.1016/j.ijforecast.2020.12.003.
- [21] A. Aslanargun, M. Mammadov, B. Yazici, and S. Yolacan, "Comparison of ARIMA, neural networks and hybrid models in time series: Tourist arrival forecasting," *Journal of Statistical Computation and Simulation*, vol. 77, no. 1, pp. 29–53, 2007, doi: 10.1080/10629360600564874.
- [22] K. Solat and K. P. Tsang, "Forecasting exchange rates with elliptically symmetric principal components," *International Journal of Forecasting*, vol. 37, no. 3, pp. 1085–1091, 2021, doi: 10.1016/j.ijforecast.2020.11.007.
- [23] K. Y. Chen and C. H. Wang, "Support vector regression with genetic algorithms in forecasting tourism demand," *Tourism Management*, vol. 28, no. 1, pp. 215–226, 2007, doi: 10.1016/j.tourman.2005.12.018.
- [24] C. Goh, R. Law, and H. M. K. Mok, "Analyzing and forecasting tourism demand: A rough sets approach," *Journal of Travel Research*, vol. 46, no. 3, pp. 327–338, 2008, doi: 10.1177/0047287506304047.
- [25] N. Kamel and A. Atiya, "Tourism demand forecasting using machine learning methods," *Aiml*, no. January, 2008, [Online]. Available: <http://infos2007.fci.cu.edu.eg/tourism/07184.pdf>
- [26] N. Kim and Z. Schwartz, "The accuracy of tourism forecasting and data characteristics: A meta-analytical approach," *Journal of Hospitality Marketing and Management*, vol. 22, no. 4, pp. 349–374, 2013, doi: 10.1080/19368623.2011.651196.
- [27] H. Song and G. Li, "Tourism demand modelling and forecasting-A review of recent research," *Tourism Management*, vol. 29, no. 2, pp. 203–220, 2008, doi: 10.1016/j.tourman.2007.07.016.
- [28] J. G. Brida and N. Garrido, "Tourism forecasting using SARIMA models in Chilean regions," *International Journal of Leisure and Tourism Marketing*, vol. 2, no. 2, p. 176, 2011, doi: 10.1504/ijltm.2011.038888.
- [29] O. Claveria and S. Torra, "Forecasting tourism demand to Catalonia: Neural networks vs. time series models," *Economic Modelling*, vol. 36, pp. 220–228, 2014, doi: 10.1016/j.econmod.2013.09.024.
- [30] W. Lijuan and C. Guohua, "Seasonal SVR with FOA algorithm for single-step and multi-step ahead forecasting in monthly inbound tourist flow," *Knowledge-Based Systems*, vol. 110, pp. 157–166, 2016, doi: 10.1016/j.knosys.2016.07.023.
- [31] E. Noersasongko, F. T. Julfia, A. Syukur, P., R. A. Pramunendar, and C. Supriyanto, "A Tourism Arrival Forecasting using Genetic Algorithm based Neural Network," *Indian Journal of Science and Technology*, vol. 9, no. 4, pp. 3–7, 2016, doi: 10.17485/ijst/2016/v9i4/78722.
- [32] S. Sun, Y. Li, S. Wang, and J. e. Guo, "Tourism demand forecasting with tourist attention: An ensemble deep learning approach," arXiv, 2020.
- [33] A. Guizzardi, F. M. E. Pons, G. Angelini, and E. Ranieri, "Big data from dynamic pricing: A smart approach to tourism demand forecasting," *International Journal of Forecasting*, vol. 37, no. 3, pp. 1049–1060, 2021, doi: 10.1016/j.ijforecast.2020.11.006.
- [34] A. A. Semenoglou, E. Spiliotis, S. Makridakis, and V. Assimakopoulos, "Investigating the accuracy of cross-learning time series forecasting methods," *International Journal of Forecasting*, vol. 37, no. 3, pp. 1072–1084, 2021, doi: 10.1016/j.ijforecast.2020.11.009.
- [35] S. Sun, Y. Wei, K. L. Tsui, and S. Wang, "Forecasting tourist arrivals with machine learning and internet search index," *Tourism Management*, vol. 70, no. February 2018, pp. 1–10, 2019, doi: 10.1016/j.tourman.2018.07.010.
- [36] J. G. Brida and W. A. Risso, "Research note: Tourism demand forecasting with sarima models - The case of south tyrol," *Tourism Economics*, vol. 17, no. 1, pp. 209–221, 2011, doi: 10.5367/te.2011.0030.
- [37] Y. Yao et al., "A paired neural network model for tourist arrival forecasting," *Expert Systems with Applications*, vol. 114, pp. 588–614, 2018, doi: 10.1016/j.eswa.2018.08.025.
- [38] C. F. Chen, M. C. Lai, and C. C. Yeh, "Forecasting tourism demand based on empirical mode decomposition and neural network," *Knowledge-Based Systems*, vol. 26, pp. 281–287, 2012, doi: 10.1016/j.knosys.2011.09.002.
- [39] W. H. Bangyal, K. Nisar, A. A. B. A. Ibrahim, M. R. Haque, J. J. P. C. Rodrigues, and D. B. Rawat, "Comparative Analysis of Low Discrepancy Sequence-Based Initialization Approaches Using Population-Based Algorithms for Solving the Global Optimization Problems," *Applied Sciences* 2021, Vol. 11, Page 7591, vol. 11, no. 16, p. 7591, Aug. 2021, doi: 10.3390/APP11167591.

Analyzing the Sentiments of Jordanian Students Towards Online Education in the Higher Education Institutions

Bayan Alfayoumi¹, Mohammad Alshraideh^{2*}

Saleh Al-Sharaeh³, Prof. Dr. Martin Leiner⁴, Dr. Iyad Muhsen AlDajani⁵

Computer Science Department, The University of Jordan, Amman, Jordan^{1,2,3}

Jena Center for Reconciliation Studies (JCRS), Friedrich Schiller University, Jena, Germany^{4,5}

Abstract—Sentiment analysis and opinion polling are two areas that have grown significantly over the past decade. Opinion research and sentiments analysis in the online education environment can truly reflect the learning state of students and educators and experts in the field; providing the theoretical basis needed to further review educational procedure and conduct. This study aims to shed light on identifying and visualizing students' objective feelings based on an exploration of the subject matter and materials of learning and gathering sentiments from university Facebook groups at various levels and layers in detail. The proposed method is a qualitative descriptive research method that includes data pre-processing, subject discovery, sentiment analysis, and visualization. In relative terms, 39.7% of text messages were positive and 52.3% of text messages were negative and understanding the narrative of these feelings and their impact on the online learning environment.

Keywords—Online education; students; sentiment analysis; online education; online environment; online social media

I. INTRODUCTION

With the rapid development of Web 2.0 and online social media, educational institutions are increasingly using online learning environments and online community platforms to create a more convenient learning environment [4]. This is considered an online training in the online environment platform.

Synchronous and asynchronous online education makes virtual reality a social model through teaching, research, other online activities, interactive learning, collaborative learning, and self-directed learning. In a nutshell, online learning consists of three basic components: technology, education, and academic emotional interaction.

The purpose of enhancing academic-emotional interaction is to develop learners' sense of belonging to the community, so that learners remain in the community for a longer period of time, ready to continue learning at a higher level. Academic sentiments are commonly known as records hidden in the text of online activities in the learning community, such as documents, statements, and sentences. The procedures and techniques of Sentiment Analysis, Calculating Weights, and Understanding Meaning allow you to observe and understand the experiences of emotions associated with the learning

process and to account for notes on best practices in future online references of online training.

This paper mainly contributes to the development of new methods and approaches examining the use of online education and other possible explanations. We analyze a collection of 10,000 student messages from university Facebook groups (posts and comments and likes) and explore the potential of automated methods for understanding this data within exploring sentiment in the online educational environment. Although this method presents a combination of text and assessment advocating the use of sentiment analysis techniques to focus on the equivalence of opinions (positive versus negative), it will provide a richer exploration of student experiences related to the emotional aspects of students in an online environment.

The purpose of this study is to find a method and approach that can effectively present best practices from a future perspective by analyzing students' emotions toward the online education environment. Analytical techniques obtain a list of terms related to some topics in learning and visualization that connect and visualize relationships based on sentiment classification in an interactive way that can be illustrated within the online environment of teaching.

The following proposed methods and approaches are presented in the paper:

- 1) Introduce the hippocampal analysis method to analyze and extract potential topics in the online education environment.
- 2) Based on the observations of university students, a new methodology was developed to determine the emotions felt by measuring the negative and positive in the online educational environment.
- 3) In addition, relationships are hierarchical and interconnected to obtain the accuracy of emotional information in an online educational environment.

II. STATE OF THE ART

Online education in the online environment contains a huge amount of information and can be divided into two parts: learning materials and student review information [12]. However, you need to explain how to properly elicit the topic

*Corresponding Author.

of 'attention and performance' from your students; interviews in an online educational environment. Improving emotions based on the sentiment of student feedback, which has become a key factor in improving the quality of community service and improving student learning efficiency. Many scholars have conducted extensive practice and in-depth research, which can be summarized into three main steps: the concept of topic discovery [8], sentiment analysis [11], and sentiment aggregation. In this regard, various investigations and studies have been conducted to improve the quality of data extraction in the online education environment.

In a previous study, an analysis of students' sentiments about online education in Jordan was not covered by all universities, most were a small sample of one university. Our study covered analyzing students' emotions at all universities in Jordan and included many samples without being limited to one university. This article comprehensively explains the proposed method, and focuses on how to find problems and problems in the educational environment of online communities by analyzing the distribution of various emotions and observations on the positive and negative aspects.

III. SENTIMENT ANALYSIS FOR ONLINE STUDENTS

In the process of researching a topic, in addition to analyzing feelings, one can identify emotional changes from online students participating in the online topics within the online educational environment. Therefore, it is imperative to define the distribution of emotions according to the subject in question and the activities conducted in the online education environment platforms.

Sentiment analysis, also known as opinion mining, is the process of analyzing, processing, and classifying subjective texts using sentiment techniques. The methods of analyzing dominant emotions today can be divided into three aspects.

The first aspect is to analyze the text by building a sentiment dictionary that relies primarily on the characteristics of the symbol dictionary with specific semantic rules. PMI (Pointwise Mutual Information) and LDA (Latent Dirichlet Allocation) are frequently used to construct emotional vocabulary, among which PMI is used to determine the emotional disposition of words, and LDA is used to extract emotional words from the corpus. [6, 20]. We developed the PMI algorithm for vocabulary expansion, and propose a semantic polarity algorithm to analyze the emotional tendency of texts to improve the classification accuracy of text data [15]. The author of [18] proposes an LDA-based method to create a domain-specific sentiment dictionary based on the current general sentiment dictionary, which extracts the subject words with the group's prior knowledge. The second aspect focuses on finding emotions in machine learning (ML) based classes such as support vector machines (SVMs) [7] nave bases (NB) [14, 21]. Vinodhini develops a hybrid formulation of SVM and core component PCA analysis to improve the accuracy of sentiment classification by reducing the complexity of the sentiment retrieval model. [13] [16]. We extract the seeds of the term sentiment from Wikipedia using probabilistic latent semantic analysis used as the input matrix for the ME model. Meanwhile, to classify emotions, we use entropy classification theory to determine the properties of

emotions. Also, the last aspect is an approach that relies on focused learning by sending words contained in text vectors to remove the deep emotional features that are mainly associated with confounding neural networks (CNNs) and recurrent neural networks (RNNs). [13] Combines CNN's wedding and meditation techniques to analyze emotions in less loud words. Ethem et. egg. [3] proposes a cross-linguistic sentiment analysis model that can achieve CNN-based sentiment analysis for small groups.

Although many researchers have made great efforts to improve the emotional classification of online communities for practical work, evaluation of the emotional unit composition, especially in the online educational environment, is still insufficient.

Since the emotional analysis of student learning is closely related to the context in which the subject is located, it is necessary to establish the rules of association with context awareness that can be established in the online education environment platform.

This study uses Nvivo tools and Python code to analyze Jordanian students' sentiment towards online education during 2020-2021 to improve the impact and effectiveness of the online education environment platform in higher education institutions.

IV. METHODOLOGICAL ASPECTS

In this section, we discuss how to conduct the fieldwork of this study, suggest methods to identify research problems, and provide a framework for solving these problems step by step. Each step is based on rules and guidelines. According to God et al. [1] research methods are comprehensive methods for studying questions of interest, including specific research methods and tools used to achieve fixed research goals. Al-Dajani [1] believes that this methodology is a procedure for collecting and analyzing the data needed to select appropriate research methods and determine data collection techniques, and the purpose and purpose of the research should be clear.

V. SENTIMENT ANALYSIS

As mentioned above, big data analytics performed on Facebook, students, universities, and active managers have provided insight into the discussion of data science and online learning in the online education environment. Whether its effectiveness and popularity will increase over the next few years. In other words, sentiment analysis allows us to gather information about what other people think [1].

Big data and sentiment analysis are effective ways to capture consumer sentiment. Unlike traditional marketing methods such as focus groups and face-to-face interviews, it has always been very difficult for marketing researchers to gain true consumer opinions, awareness, and preferences. We provide free sentiment analysis service using SNS big data. Also, consumer-generated data available on social media like Facebook doesn't have the bias interviewers might present in their case during a personal interview.

However, according to [2], taking big data out of context can lose its meaning or objectivity. In this case, the data

values can be corrupted as the data can be modeled and reduced to fit a mathematical model [17]. This is where cheating comes in. Netgraphy can be used to explore big data online, so it can be used as a tool to investigate sentiment analysis in an online educational environment, providing more context and deeper insight into the results of sentiment analysis environment, online social networks such as Facebook, Twitter and YouTube [1]. Research provides more information about symbols, meanings and patterns that big data approaches may not take into account [5]. Fig. 1 shows the sentiment analysis method.



Fig. 1. Method of Sentiment Analysis.

VI. DATA COLLECTION

Sentiment analysis was conducted using Facebook's university group data, including online education data. Data was extracted from Facebook pages using Face Pager data extraction software [22]. As mentioned above, analyzing big data trends is an effective way to understand consumer moods, perceptions and preferences. Free access to social media is easy. Additionally, the data is free from potential biases that group interviewers or test takers might encounter in the data [22].

Aggregated data sets extracted from each university group on Facebook were processed, filtered, and analyzed using Microsoft Office Excel. The raw data from this dataset is created in just a few steps [22]:

1) As mentioned above, this study used online sentiment analysis. Therefore, research ignores all other forms of behavior such as likes and reactions, and focuses on the content of posts and comments. This was done because of the size of the data set. No data will be applied unless you remove extraneous data.

2) All duplicate comments have been explicitly removed to prevent unwanted bias, data collection errors or bot activity.

3) This is an Excel file that converts data by date and comment into CSV format. Analyze students' emotions using Nvivo, a qualitative data processing and analysis application.

VII. DATA ANALYSIS

After cleaning and preparing the raw data extracted from the university's Facebook group, the entire dataset consisted of 10,000 text messages, which provided the advantages of big data analysis such as size, speed, and diversity in this study [9]. This study was conducted very recently and contains a large amount of data that can be used to integrate and use various sources of information, such as comments, posts, and responses from various stakeholders. That said datasets are very interesting for doing this type of analysis, i.e. sentiment analysis. Sentiment analysis is performed via CAQCAS, a qualitative content analysis software, a computing subsidiary of Nvivo [22]. CAQCAS uses computer linguistics and text

mining to identify verbal emotions, often in the form of positive, neutral, or negative emotions. In this sense, sentiment analysis can be viewed as an automated knowledge discovery method that aims to find hidden patterns in large amounts of data. When performing sentiment analysis, an important step in the analysis is word classification. There are two general methods available for determining the direction of emotion: the body-based method and the vocabulary-based method [10]. However, the body-based method is rarely used when analyzing emotions. However, both the Modana-based method and the vocabulary-based method require a predefined dictionary or a set of subjective words. Therefore, this research compares the relevant text with a dictionary or dictionary to determine the strength and degree of emotion corresponding to the emotion, so the proposed research compares the relevant text with a dictionary to calculate emotion to determine whether it is done, the degree of emotion, degree of strength and emotion. More specifically, this study uses Pages for nvivo, the Windows search engine, to analyze the collected data. Nvivo can be used to analyze sentiments and texts for online social networks such as Facebook, YouTube, and Twitter [1, 18, 19].

VIII. EXPERIMENTS AND RESULTS

The concerned sentiment about online education was analyzed for a full year, 2020-2021, where it was analyzed from March to December, the period that transformed the learning system in Jordan into a completely online learning system.

As discussed in previous sections, the integration of the resulting data with nvivo and Python code for Windows version 11 describes all the text messages present in the university's Facebook groups, which turned out to be accompanied by emotion whether it is negative, neutral, or with a positive sentiment.

Fig. 2 shows the consequences of emotions. Most text messages were rated negative, with more than a third of text messages rated positively. Relatively few, about 8 percent, text messages were rated as neutral. Overall, out of a total of 10,000 text messages, 3,970 received positive, 800 neutral, and 5,230 negative ratings in Table I. Relatively, this means that 39.7% of text messages were positive and 52.3% negative.

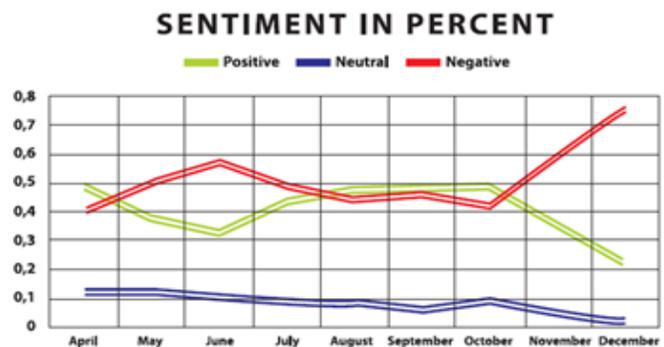


Fig. 2. The Share of the Text Messages Found on the Universities Facebook Group per Month is Either Labelled Positive, Negative, or Neutral.

TABLE I. SHOWS THE AGGREGATE NUMBERS FOR POSITIVE, NEGATIVE, AND NEUTRAL COMMENTS FOR EACH MONTH

	Positive	Neutral	Negative	Total
April	800	100	900	1800
May	500	70	700	1270
June	370	88	550	1008
July	400	60	850	1310
August	650	77	330	1057
September	280	90	500	870
October	450	100	250	800
November	320	65	550	935
December	200	150	600	950
	3,970	800	5,230	10,000
	0,397630831	0,079455154	0,522914015	1

Also, the portion of negative or positive text messages fluctuates a lot over time. For example, as shown in Fig. 2, between March and April, at least 50 percent of text messages are rated negatively. However, less than 50 percent of text messages between the months of May and June are rated negatively. However, the month of July again has a majority of negative comments. As shown, neutral text messages have relatively low volatility, staying within the 2.5 to 12.5 percent range. Positive texting ranges from 22 percent to 48.5 percent. Finally, negative text messages fluctuate between 39.8% and a maximum of 75.2%.

In a nutshell, Table II shows the three major mood swings found in college Facebook groups. First, from March to May, the percentage of negative text messages is increasing. However, a big change occurred in October. It is a sharp trend that turns negative. Texting is increasing rapidly, while Positive opponents are declining at a similar rate. As a result of analyzing the emotions of students in the 2020 school year who started using online education as a basic learning tool as the Corona 19 crisis started in Jordan in March of this year, the emotions of students about online education are contained here.

TABLE II. SHOWS THE OVERALL PERCENTAGE OF POSITIVE, NEGATIVE, AND NEUTRAL COMMENTS FOR EACH MONTH

Percent	Positive	Neutral	Negative
April	0.480812641	0.120767494	0.398419865
May	0.372336758	0.125422326	0.502240916
June	0.323345013	0.105890857	0.57076413
July	0.430826534	0.087619723	0.481553742
August	0.475581934	0.080878947	0.443539119
September	0.479839916	0.063509874	0.456650209
October	0.485078956	0.097711892	0.417209152
November	0.351778987	0.050816241	0.597404772
December	0.221909233	0.025456442	0.752634324

IX. CONCLUSION

This paper described a dataset of assessments and textual responses to student assessments for online education. Sentiment analysis techniques are used to automatically classify text responses as positive, negative, or neutral using student posts and comments.

The outcome of our study highlighted that 52.3% of students feel negative about online education, as one of the main reasons for the student's feeling was the poor connection of the Internet for some students, or the difficulty of electronic exams. Therefore, the reasons must be known by higher education decision makers and work to increase the effectiveness of education via the Internet.

Future work will include expanding the sample with more student assessments and this should provide more reliable results. And also increasing the number of university groups on Facebook to include the largest number of students. Analyzing the sentiment of faculty members and administrators about online education to include all members of the university community and take a sample of students on Twitter to also know how students sentiment about online education.

ACKNOWLEDGMENT

The researchers would like to express their sincerest gratitude for the Academic Alliance for Reconciliation in the Middle East and North Africa (AARMENA) Capacity Building in Higher Education Project (CBHE), Co-funded by the Erasmus+ Program of the European Union.

REFERENCES

- [1] AlDajani, I. M. (2020). Internet Communication Technology (ICT) for Reconciliation: Applied Phronesis Netnography in Internet Research Methodologies.
- [2] Boyd, D. & Crawford, K., 2012. Critical Questions for Big Data. *Information, Communication & Society*, 15(5), pp.662–679.
- [3] Ethem, F.C., Aysu, E.C., & Fazli, C. (2018). Multilingual sentiment analysis: An RNN-based framework for limited data. In *Proceedings of ACM SIGIR 2018 Workshop on Learning from Limited or Noisy Data*, July 12, Michigan, USA, pp 1–5.
- [4] Fariza, K. (2019). Students' identities and its relationships with their engagement in an Online Learning Community. *International Journal of Emerging Technologies in Learning*, 14(5), 4–19.
- [5] Kozinets, R., 2002. The Screen: Using Netnography Marketing Communities. *Journal of Marketing*, 39(1), pp.61–72.
- [6] Li, X.D., Ba, Z.C., & Huang, L. (2015). A text feature selection method based on weighted latent dirichlet allocation and multi-granularity. *New Technology of Library and Information Service*, 258, 42–49.
- [7] Liu, Y., Bi, J.W., & Fan, Z.P. (2017). A method for multi-class sentiment classification based on an improved one-vs-one (OVO) strategy and the support vector machine (SVM) algorithm. *information Sciences*, 394, 38–52.
- [8] Lu, Y., Zhang, P., Liu, J., Li, J., & Deng, S. (2013). Health-related hot topic detection in online communities using text clustering. *PLoS ONE*, 8(2), e56221.
- [9] McAfee, A. et al., 2012. Big Data: The Management Revolution. *Harvard Business Review*, 90, pp.60–68.
- [10] Miao, Q., Li, Q., & Zeng, D. 2010. Fine-grained opinion mining by integrating multiple review sources. *Journal of the Association for Information Science and Technology*, 61(11), 2288–2299.
- [11] Nan, L., & Wu, D.D. (2010). Using text mining and sentiment analysis for online forums hotspot detection and forecast. *Decision Support Systems*, 48(2), 354–368.

- [12] Shea, P., Li, C.S., & Pickett, A. (2006). A study of teaching presence and student sense of learning community in fully online and web-enhanced college courses. *Internet & Higher Education*, 9(3), 175–190.
- [13] Shin, B., Lee, T., & Choi, J.D. (2017). Lexicon integrated CNN models with attention for sentiment analysis. *Proceedings of the 8th Workshop on Computational Approaches to Subjectivity, Sentiment and Social Media Analysis*, September 7–11, Copenhagen, Denmark, pp 149–158.
- [14] Shirakawa, M., Nakayama, K., Hara, T., et al. (2017). Wikipedia-based semantic similarity measurements for noisy short texts using extended naive bayes. *IEEE Transactions on Emerging Topics in Computing*, 3(2), 205–219.
- [15] Turney, P.D., & Littman, M.L. (2003). Measuring praise and criticism: Inference of semantic orientation from association. *ACM Transactions on Information Systems*, 21(4), 315–346.
- [16] Vinodhini, G. (2014). Sentiment mining using SVM-based hybrid classification model. *Advances in Intelligent Systems & Computing*, 246, 155–162.
- [17] Xie, X., Ge, S., Hu, F., Xie, M., & Jiang, N. (2017). An improved algorithm for sentiment analysis based on maximum entropy. *Soft Computing*, 23(1), 599–611.
- [18] Alfayoumi B., Alshraideh M., Martin Leiner, Iyad Muhsen Aldajani. (2021). Machine Learning Predictions For The Advancement Of the Online Education in The Higher Education Institutions in Jordan, *Journal of Hunan University Natural Sciences*, 48(9).
- [19] Almanaseer, Waref, Mohammad Alshraideh, and Omar Alkadi. (2021). A Deep Belief Network Classification Approach for Automatic Diacritization of Arabic Text *Applied Sciences*. <https://doi.org/10.3390/app11115228>.
- [20] Al-Shaikh, A., Mahafzah, B.A. & Alshraideh, M. (2021). Hybrid harmony search algorithm for social network contact tracing of COVID-19. *Soft Comput* . <https://doi.org/10.1007/s00500-021-05948-2>.
- [21] Alshraideh M, Jawabreh E, Mahafzah BA, Al Harahsheh HM (2013). Applying genetic algorithms to test JUH DBs exceptions. *Int J Adv Comput Sci Appl* 4:8–20. <https://doi.org/10.14569/ijacsa.2013.040702>.
- [22] Ryrberg C., Akbar S, Vej J. (2017). Measuring the Effects of Airbnb's Growth on Consumer Brand Perception in the Hotel Industry: A Case Study of Best Western Hotels & Resorts, *Copenhagen Business School*.

Comparative Study of Flooding Area Detection with SAR Images based on Thresholding and Difference Images Acquired Before and After the Flooding

Kohei Arai

Faculty of Science and Engineering
Saga University, Saga City
Japan

Abstract—Comparative study of flooding area detection with Synthetic Aperture Radar (SAR) images based on thresholding and difference images acquired before and after the flooding is conducted. Method for flooding, landslide and sediment disaster area detections with SAR is proposed. The following two different methods for flooding detection are common. It is not so easy to determine a threshold for the thresholding method while subtraction method between before and after images of a disaster occurrence has the disadvantage that false disaster areas are detected due to a variation of ground cover targets. Therefore, a comparative study between both methods is required. Its application is demonstrated for the disaster which is occurred in Saga Prefecture, Japan due to a long term of heavy rain during from the begging of August to the middle of August in 2021. Through experiments with Sentinel-1 SAR imagery data, it is found that the proposed method works well for the detection of the disaster.

Keywords—Flooding; landslide; sediment disaster; heavy rain; image quality; Synthetic Aperture Radar; SAR; sentinel-1 SAR; thresholding; difference images between before and after disaster

I. INTRODUCTION

Sentinel Asia means "Asia Observer", which is an activity to utilize space technology, especially remote sensing technology, for disaster management in the Asia-Pacific region. This initiative is being promoted in cooperation with space agencies in the Asia-Pacific region, including Japan, and with disaster prevention agencies in this region, and has become an international framework.

Disaster information such as images of disaster-stricken areas observed by earth observation satellites is available on the Internet. It also has a function called Web-GIS (Geographic Information System), which allows satellite images to be superimposed and displayed on a map. Activities include observing the situation in the disaster area as soon as possible after a disaster occurs and providing related information for forest fires and floods as a regular monitoring activity. In addition, meteorological satellite (MTSAT-1R) images are available on Web-GIS.

Not only Sentinel Asia, but also, other remote sensing satellite data-based disaster area detection is getting more popular. There are some methods for the disaster area detection with SAR imagery data. One of those is based on thresholding of the SAR image which is acquired after disaster. This is a

straightforward method. The other method is based on difference images which are acquired before and after disaster. On the other hand, there is another method based on deep learning with training samples of input SAR images and truth data on disaster. In this paper, a comparative study is conducted between thresholding-based and difference image-based methods. These methods do not require truth data on disaster occurred areas.

Also, in this paper, some examples of disaster areas, flooding areas, land slide areas, sediment disaster areas detections with Sentinel-1 SAR data are demonstrated. The heavy rains in August 2021 are estimated to have damaged 3,000 houses, and more than 200 landslides such as slope collapses and landslides. According to the prefecture, four men and women in their 60s and 80s were injured in this heavy rain in Saga City and Kanzaki City. Both are minor injuries.

As for the damage to the houses, one building was completely destroyed and one was partially destroyed by the debris flow that occurred in the Shiwaya district of Kanzaki Town, Kanzaki City. Inundation above and below the floor has been confirmed in approximately 3000 buildings in 15 cities and towns.

In some areas, investigations are still ongoing, and the number of floods is expected to increase further. In addition, rivers and revetments in 155 locations throughout the prefecture have collapsed, and sediment-related disasters such as slopes, shoulder collapses, landslides, and landslides have been confirmed in approximately 220 locations. Even August 17, eight households in the Yamada area of Miyaki Town have been instructed to ensure emergency safety, and evacuation orders have been issued to some areas of Takeo City and Ureshino City, and as of 4:00 pm, 198 people from 95 households have been evacuated.

Record heavy rains continued, and on the 14th of August 2021, landslides and floods occurred one after another in Saga prefecture. In the mountains, the back mountains collapsed and knocked down the huts, and in the flatlands, floods were seen here and there, stopping the flow of people and goods. With the issuance of a heavy rain special warning for the fourth consecutive year in the prefecture, some people are confused by the repeated warnings of "heavy rain once every few decades."

In the next section, related research works are described followed by research background and theoretical background. Then, the proposed method is described followed by some experiments are described together with conclusion and some discussions.

II. RELATED RESEARCH WORK

There are the following disaster related papers:

Present status for disaster observation systems working group is reported [1]. Also, four dimensional GIS and its application to disaster monitoring with satellite remote sensing data is proposed [2].

An expectation to remote sensing for disaster management is reported [3]. Meanwhile, the conference on GIS and application of remote sensing to disaster management four dimensional GIS and its application to disaster monitoring with satellite remote sensing data is discussed [4].

The current status on disaster monitoring with satellites in Japan is reported [5]. Meantime, the joint symposium on disaster management between United Nation and Japan-US Science/Technology and Space Application Program is reported [6].

An expectation on remote sensing technology for disaster management and response is announced [7]. On the other hand, Virtual Center for Disaster Management is proposed [8]. Meanwhile, opening remarks of satellite-based disaster management is made [9].

Disaster related activities are reported [10]. Meanwhile, internet GIS and disaster information clearing house is proposed [11].

Opening address of the disaster management symposium is made [12]. Also, virtual center for disaster management is proposed [13]. Meantime, joint research on disaster management is proposed [14].

URL search engine with text search tools for disaster mitigation is created [15]. Meanwhile, four-dimensional GIS system through internet is proposed [16]. Visualization of disaster information derived from Earth observation data is proposed [17].

Java based image processing and analysis software package is created [18]. On the other hand, internet Geographic Information System (GIS) is created [19]. Meanwhile, disaster related URL search engine with queries in a natural language is proposed [20].

Disaster monitoring with ASTER onboard Terra satellite is conducted [21]. Also, clearing house for disaster management is created [22]. In the meantime, ICT technology for disaster mitigation (Tsunami warning system) is proposed [23].

Cellular automata-based approach for prediction of hot mudflow disaster area is proposed [24]. Meanwhile, simulation of hot mudflow disaster with cellular automata and verification with satellite imagery data is conducted [25].

Backup communication routing through Internet Satellite, WINDS, for transmission of disaster relief data is proposed

[26] together with backup communication routing through Internet satellite WINDS for transmission of disaster relief data [27].

Two-dimensional cellular automata approach for disaster spreading proposed [28]. Also, disaster mitigation is overviewed as a Visiting Scholar, World Class University [29].

Micro traffic simulation with unpredictable disturbance based on Monte Carlo simulation: effectiveness of the proposed agent cars of Sidoarjo hot mudflow disaster is conducted [30] together with probabilistic cellular automata-based approach for prediction of hot mudflow disaster area and volume is proposed [31].

Two-dimensional CA approach for disaster spreading is proposed [32]. On the other hand, deceleration in the micro traffic model and its application to simulation for evacuation from disaster area is proposed [33].

Cellular automata approach for disaster propagation prediction and required data system in GIS representations is proposed [34] together with cellular automata for traffic modelling and simulation in a situation of evacuation from disaster areas [35].

New approach of prediction of Sidoarjo hot mudflow disaster area based on probabilistic Cellular Automata (CA) is proposed [36] together with cellular automata for traffic modeling and simulation in a situation of evacuation from disaster areas for cellular automata simplicity behind complexity [37].

Back-up communication routing through Internet satellite WINDS for transmitting of disaster relief data is proposed [38]. Also, sensor network for landslide monitoring with laser ranging system avoiding rainfall influence on laser ranging by means of time diversity and satellite imagery data-based landslide disaster relief is created [39].

Task allocation model for rescue disable persons in disaster area with help of volunteers is proposed [40]. Also, cell-based GIS as Cellular Automata (CA) for disaster spreading prediction and required data systems is created [41].

Deceleration in the evacuation from disaster area is modeled and validated [42]. On the other hand, cell-based GIS as cellular automata for disaster spreading predictions and required data systems is created [43].

Visualization of 5D assimilation data for meteorological forecasting and its related disaster mitigation utilizing VIS5D of software tool is attempted [44]. Meanwhile, vital sign and location/attitude monitoring with sensor networks for the proposed rescue system for disabled and elderly persons who need some help in evacuation from disaster areas is proposed [45].

Method and system for human action detection with acceleration sensors for the proposed rescue system for disabled and elderly persons who need some help in evacuation from disaster areas is created [46]. Meanwhile, method and system for human action detection with acceleration sensors for the proposed rescue system for disabled and elderly persons

who need a help in evacuation from disaster areas is proposed [47].

Disaster relief with satellite based Synthetic Aperture Radar data is proposed [48]. Meanwhile, Sentinel 1A SAR data analysis for disaster mitigation in Kyushu is presented [49].

Flooding and oil spill disaster relief using Sentinel of remote sensing satellite data is reported [50]. Convolutional neural network considering physical processes and its application to disaster detection is proposed [51].

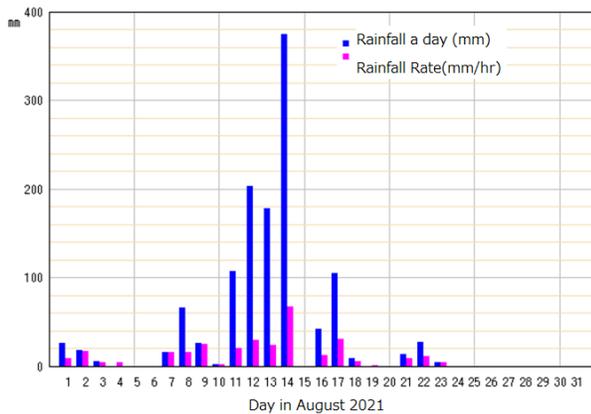
Method for rainfall rate estimation with satellite-based microwave radiometer data is proposed for detection of flooding area [52]. On the other hand, flood damage area detection method by means of coherency derived from interferometric SAR analysis with Sentinel-1A SAR is proposed and validated with the truth data of flooding which occurred in Oita, Kyushu, Japan [53].

III. RESEARCH BACKGROUND AND PROPOSED METHOD

A. Intensive Study Areas and Weather Condition

Heavy rains started from 11 August 2021 and are continued for a week and ended on 17 August 2021. In more detail, Fig. 1(a) shows rainfall a day (mm) and maximum rainfall rate an hour (mm/hr) in a day in the intensive study area of the Saga prefectural areas in Japan (Fig. 1(b)). Much 1000 mm of rainfall is observed within the week. Due to the rainfall, more than 3000 houses are damaged and more than 200 landslides such as slope collapses and landslides.

Fig. 2(a), (b), (c) shows the Sentinel-1 SAR imagery data which are acquired on 3 (before the rainfall), 15 (middle of the rainfall) and 28 (after the rainfall) August in 2021, respectively.



(a) Rainfall a Day (mm) and Maximum Rainfall Rate an Hour (mm/hr) in a Day



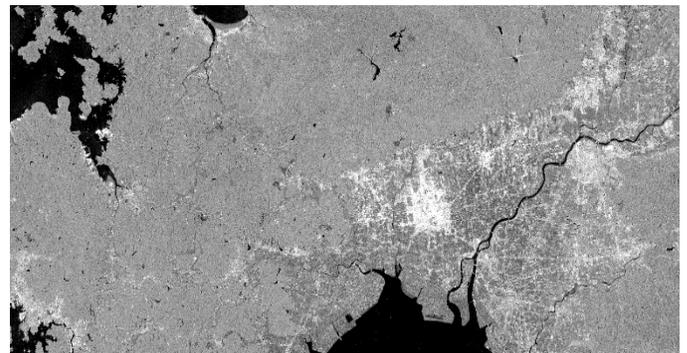
(b) Intensive Study Area of the Saga Prefectural Areas in Japan

Fig. 1. Intensive Study Area and Weather Condition (Heavy Rainfall in the Area).

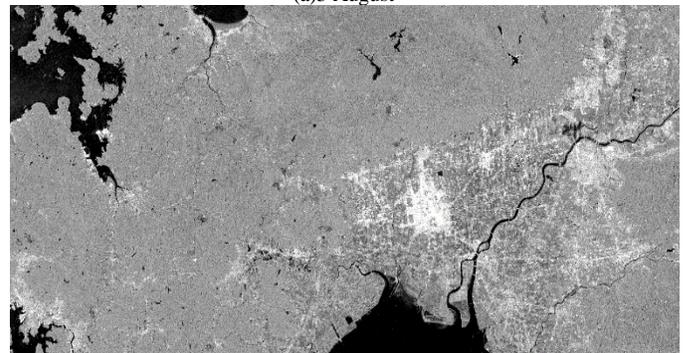
B. Methods for Disaster Detection

1) *Flooding area detection*: It is possible to detect flooding areas to compare between Sentinel-1 SAR imagery data which are acquired before and after the rainfall. Backscattering coefficient of Sentinel-1 SAR imagery data is going down due to dielectric loss at the surface of the rainfall areas. Also, it is possible to detect the flooding areas by means of thresholding of the Sentinel-1 SAR imagery data which is acquired after the rainfall with the appropriate threshold.

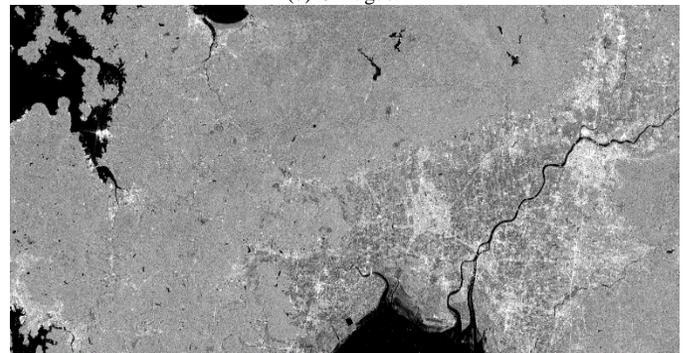
2) *Landslide, sediment disaster detection*: On the other hand, it is possible to detect landslide, sediment disaster areas to compare between Sentinel-1 SAR imagery data which are acquired before and after the rainfall. Backscattering coefficient of Sentinel-1 SAR imagery data is going up because ground cover trees and grasses are disappeared at the surface of the landslide, sediment disaster areas.



(a) 3 August



(b) 15 August



(c) 28 August

Fig. 2. Sentinel-1 SAR Imagery Data which are Acquired on 3 (before the Rainfall), 15 (Middle of the Rainfall) and 28 (after the Rainfall) August in 2021.

IV. EXPERIMENT

A. Flooded Area Detection in Saga Prefecture

Sentinel-1 SAR of 3 August (Fig. 2(a)) is subtracted from the Sentinel-1 SAR of 15 August (Fig. 2(b)). Then, the flooded areas are extracted. Fig. 3 shows the resultant image of the flooded areas. Dark portions of Fig. 3 image show the flooded areas and lakes, ponds. The flooded areas are situated almost everywhere in Saga prefecture.

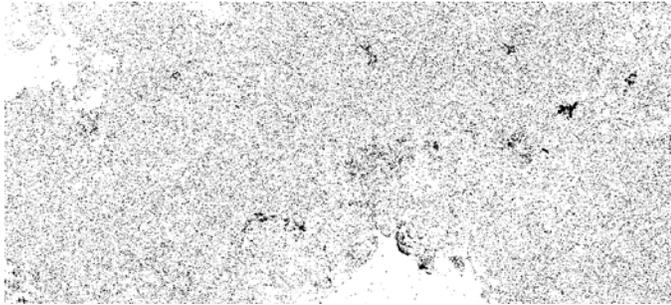
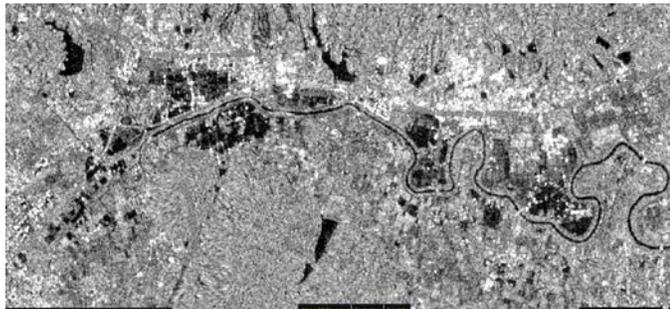


Fig. 3. Extracted Flooding Areas in Saga Prefecture due to Heavy Rainfall in August 2021.

B. Flooded Area Detection in Omachi-Cho in Saga Prefecture

Also, the flooded areas can be detected through thresholding of the Sentinel-1 SAR imagery data. Fig. 4(a) shows original Sentinel-1 SAR image of Omachi-Cho in Saga prefecture is acquired on 15 August 2021. The resultant image of detected flooding areas is shown in Fig. 4(b) while the Google map of the Omachi-Cho is shown in Fig. 4(c).

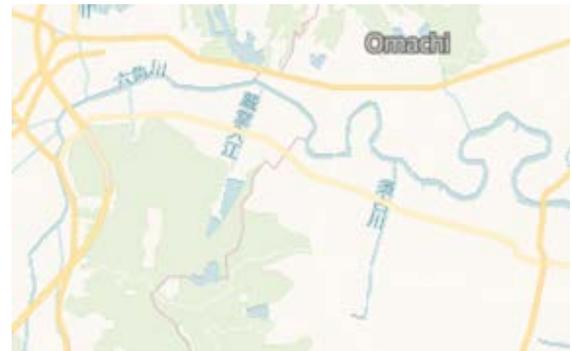
In 2019, some portions of Omachi-Cho are flooded due to relatively heavy rainfall. Fig. 5(a) shows Sentinel-1 SAR image of Omachi-Cho which is acquired on 15 August 2019.



(a) Sentinel-1 SAR

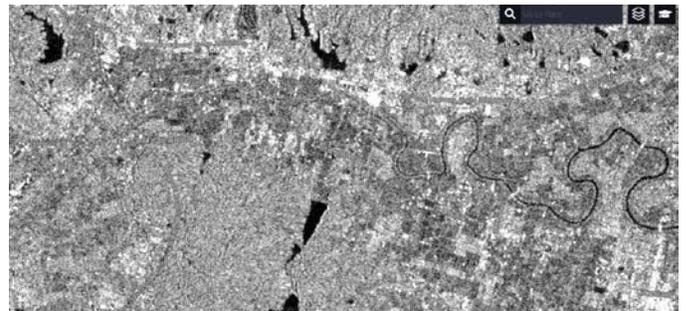


(b) Detected flooding areas

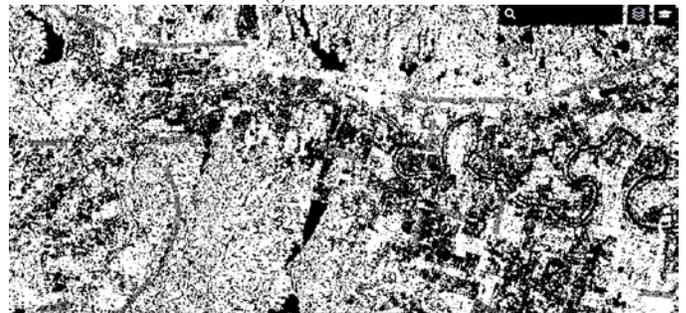


(c) Google Map

Fig. 4. Detection of Flooding Areas of Omachi-Cho, in Saga Prefecture due to the Heavy Rainfall in August 2021.



(a) Sentinel-1 SAR



(b) Detected flooding areas

Fig. 5. Detection of Flooding Areas of Omachi-Cho in Saga Prefecture due to the Relatively Heavy Rainfall in August 2019.

On the other hand, Fig. 5(b) shows the flooding areas of Omachi-Cho detected through thresholding with the appropriate threshold. Through a comparison between Fig. 4(b) and Fig. 5(b), it is found that the flooding areas are almost coincident. Most of these matches the location of the old river channel. Also, it is found that the flooding areas of 2021 are larger than that of 2019. Furthermore, the depth of flooding is deeper in 2021 than that of 2019.

C. Trend of Moisture in Omachi-Cho in 2021

By using Sentinel-2 of optical sensor data, it is possible to estimate moisture. Trend analysis is made for moisture due to the heavy rainfall in August 2021. This moisture trend relates to the flooding closely. Fig. 6(a) shows the moisture index derived from Sentinel-2 of optical sensor data which is acquired on 23 June 2021. From the beginning of August 2021, rainfall started so that moisture index of 2 August 2021 shows a lot of clouds as shown in Fig. 6(b). Fig. 6(c), (d), (e) shows moisture index of 7, 9, 19 August 2021.

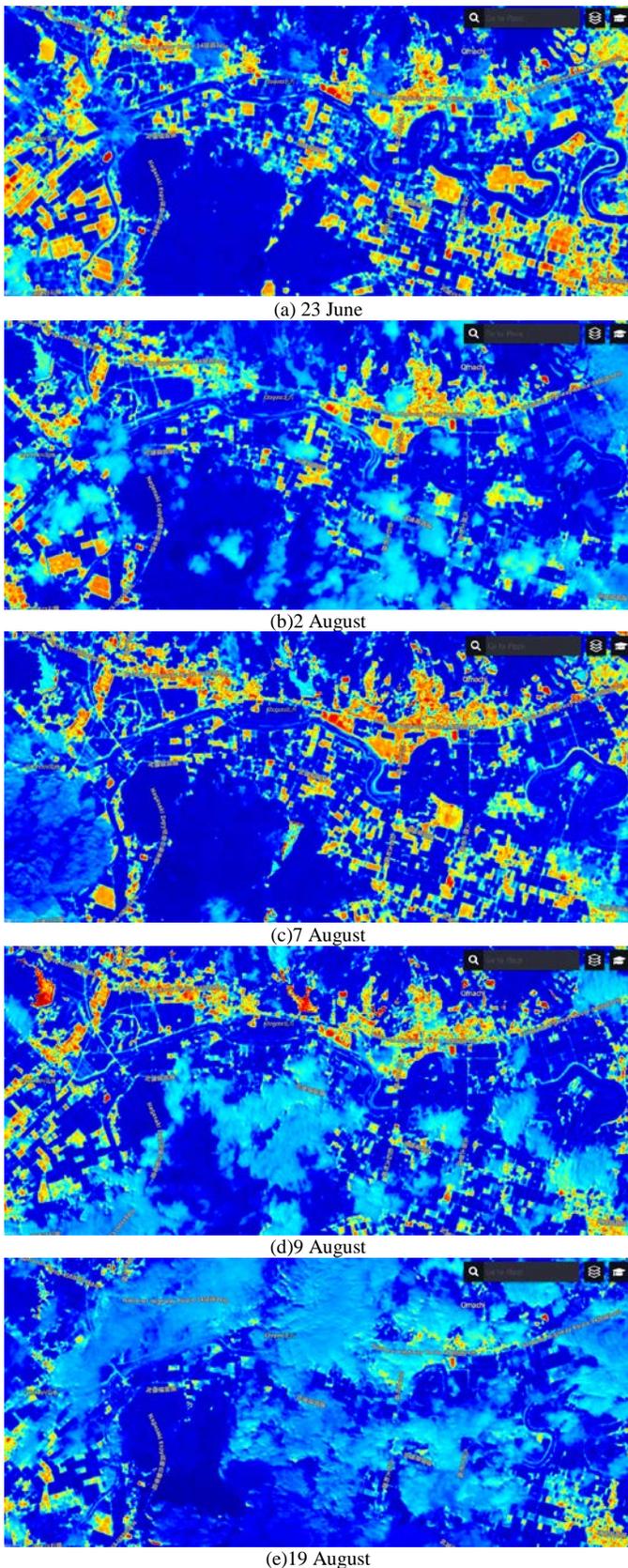


Fig. 6. Moisture Index Trend of Omachi-Cho Derived from Sentinel-2 Optical Sensor of Imagery Data which is acquired in August 2021.

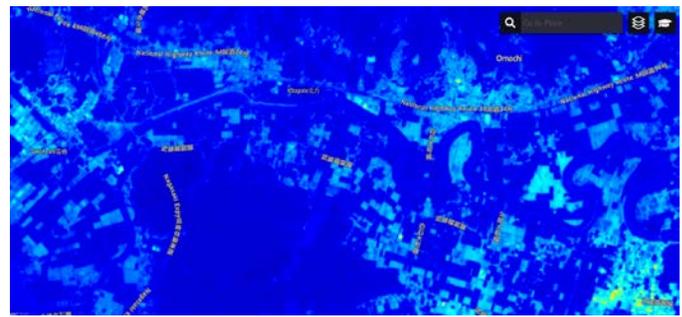


Fig. 7. Moisture Index of Omachi-Cho Areas in August 2019.

It is found that the Omachi-Cho areas are moisturized due to heavy rainfall in 2021. This is one of causes of the flooding and landslide as well as sediment disasters. Meanwhile, moisture index of Omachi-Cho areas derived from Sentinel-2 optical sensor which is acquired on 10 August 2019 is shown in Fig. 7. It is found that the Omachi-Cho areas are almost covered with clouds on 10 August 2019.

D. Miyaki-Cho Minobaru Yamada, Saga Landslide

The Yamada district of Miyaki-cho, Miyaki-gun, where "emergency safety assurance" has been issued for 25 people in 8 households because there is a risk of debris flow in the cold water (Shozu) river that flows through the Minobaru-Yamada district of Miyaki-cho. The evacuation shelter life will reach its fourth day on the 18th, and while the residents look tired, there is no prospect of cancellation because the weather will not recover. Residents are worried about when they can go home.

According to the Civil Engineering Office in the eastern part of the prefecture, the mountain surface on the right bank of the Kansui River, about 1.5 km upstream from the area, collapsed to block the river over a height of about 100 meters and a width of about 50 meters. Since the amount of water is large and heavy machinery cannot enter, staff members are walking into the site to prepare for surveying. The office says, "We are aiming for an early recovery, but the weather has not recovered, and we cannot predict the time."

Fig. 8(a) shows the location of collapsed area in Miyaki-cho, Minobaru Yamada, Saga on Google map due to the heavy rain in August 2021 while Fig. 8(b) shows the photo of the collapsed area.

On the other hand, Fig. 9(a) shows Sentinel-1 SAR image of the collapsed area of the Miyaki-Cho Minobaru Yamada, Saga Landslide which is acquired on 10 August 2021 while Fig. 9(b) shows that which is acquired on 16 August 2021. The longitude and latitude are 33.38762N, 130.42950E. The Sentinel-1 SAR images are VV polarization of decibel gamma0 data and is radiometric terrain corrected data. Yellow marks in Fig. 9 indicate the collapsed locations. Digital Number: DN of 10 August is 169 (255 in Maximum) while that of 16 August is 189. This implies that the backscattered coefficient of the collapsed area is raised from 169 to 189 due to the collapsing.

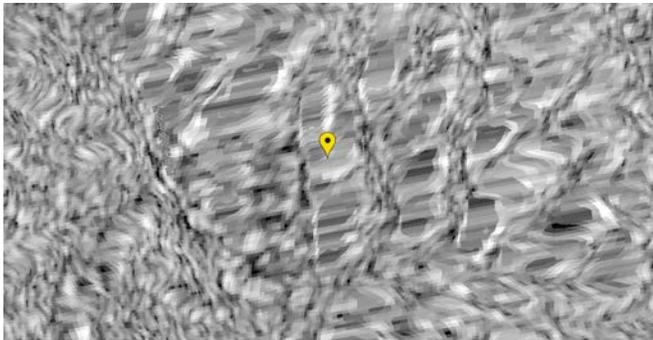


(a) Location of Collapsed Area

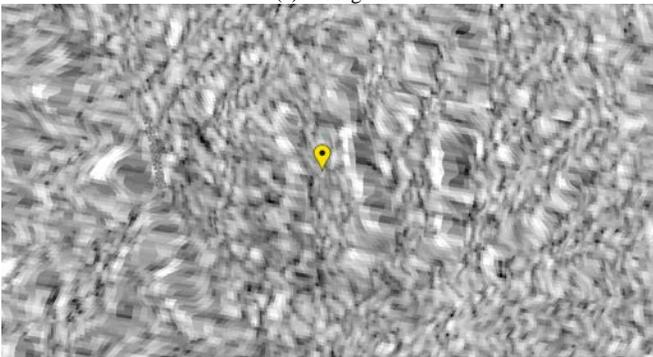


(b) Photo of Collapsed Area

Fig. 8. Miyaki-Cho Minobaru Yamada, Saga Landslide.



(a) 10 August



(b) 16 August

Fig. 9. Sentinel-1 SAR Images which is acquired before and after the Collapsing Occurred at the Miyaki-Cho Minobaru Yamada, Saga in August 2021.

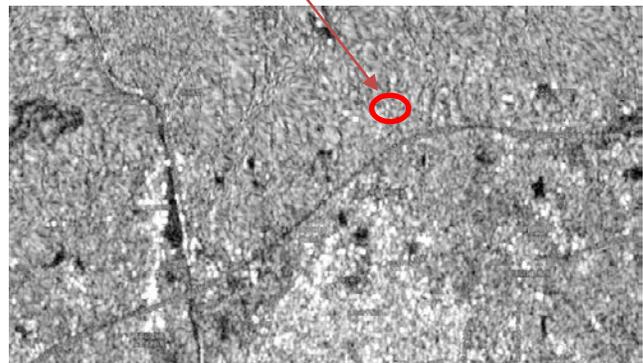
E. Landslide which is Occurred at Yamato-Cho in Saga

Regarding the record heavy rain that continued in Saga Prefecture from the 11 August 2021, the prefecture reported at the disaster countermeasures headquarters meeting held on the 18 August 2021 that a debris flow of about 1500 meters was occurring in Kuikei, Yamato-cho, Saga City. No human damage has occurred.

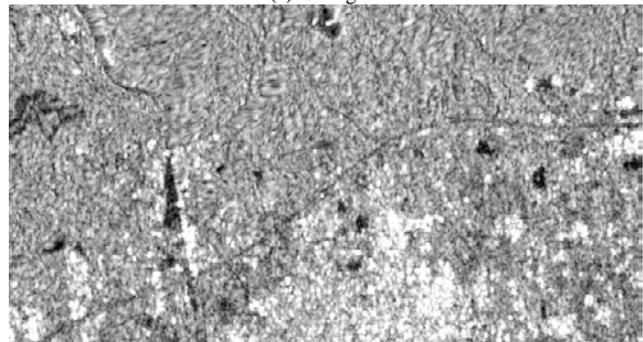
According to the Prefectural Forest Maintenance Division, debris flow from the forest flows into the agricultural land due to heavy rain and reaches under the elevated Nagasaki Expressway.

Fig. 10(a) shows the landslide area of Sentinel-1 SAR image which is acquired on 28 August 2021 (After the rainfall) which is occurred at Yamato-Cho in Saga due to the heavy rain in August 2021. Meanwhile, Fig. 10(b) and (c) shows that of 15 August (during the rainfall) and of 3 August (before the rainfall), respectively.

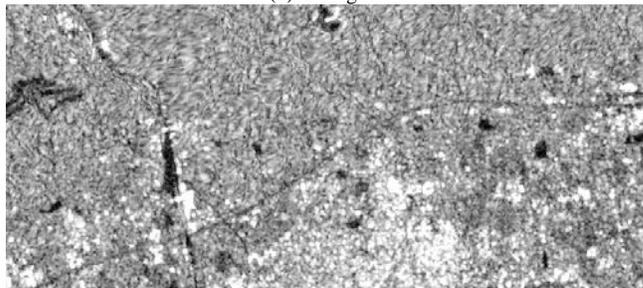
Landslide at Yamato-Town in Saga City



(a) 28 August



(b) 15 August



(c) 28 August

Fig. 10. Landslide which is occurred at Yamato-Cho in Saga due to Heavy Rain in August 2021.

Red circle shows the location of landslide area which is relatively high back scattering coefficients along with the line (white line in the red circle). There is no such high backscattering coefficient on 3 August as shown in Fig. 10(c). The white line of high back scattering coefficient pixels are increased as shown in Fig. 10(b).

Therefore, it is found that the landslide, collapsing, sediment disaster can be estimated with SAR imagery data onboard remote sensing satellites.

The result from this comparative study is summarized in the following Table I.

TABLE I. FEATURE OF THE DISASTER AREA DETECTION METHODS FOR THE COMPARATIVE STUDY

Method	Advantage	Disadvantage
Thresholding with appropriate threshold	Only an appropriate threshold is needed	It is hard to determine the appropriate threshold
Subtraction of after image from before image of a disaster occurrence	Just two imagery data are required	Non disaster areas are sometime detected due to ground cover targets changes

V. CONCLUSION

Comparative study of flooding area detection with Synthetic Aperture Radar (SAR) images based on thresholding and difference images acquired before and after the flooding is conducted. It is concluded that the difference images-based method which are acquired before and after the disaster is superior to the thresholding-based method. Because the disaster situations are different by the areas in concern, single thresholding is not adequate for all the disaster areas. On the other hand, difference images-based method takes into account the different disaster situations by different areas.

Method for flooding, landslide and sediment disaster area detections with SAR is proposed. Such disaster which was occurred in Saga Prefecture, Japan due to a long term of heavy rain during from the begging of August to the middle of August in 2021 is analyzed with the proposed method. Through experiments with Sentinel-1 SAR imagery data, it is found that the proposed method works well for the detection of the disaster. It is also found that the landslide, collapsing, sediment disaster can be estimated with SAR imagery data onboard remote sensing satellites.

Moisture trend analysis can be done with Sentinel-2 optical sensor data. This is one of causes of flooding, landslide and sediment disasters. It is also confirmed that the proposed two methods for flooding, landslide and sediment disaster detection (before disaster occurred image subtracted by after disaster occurred image, and thresholding of after disaster occurred image with appropriate threshold) works well.

VI. FUTURE RESEARCH WORK

In the future, it will be demonstrated for frequent observation of SAR imagery data. Sentinel-1 SAR imagery data can be acquired within 5 days (Revisit cycle of the one Sentinel-1 satellite is 10 days and there are two Sentinel-1

satellites, a and b). There are on-going projects of SAR constellations such as QPS/SAR-x.

ACKNOWLEDGMENT

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

REFERENCES

- [1] Kohei Arai, Present Status for Disaster Observation Systems Working Group, Proceedings of the 5th Japan-US Space Research Cooperation Conference, Hawaii, Nov. 1995.
- [2] Kohei Arai, Four Dimensional GIS and Its Application to Disaster Monitoring with Satellite Remote Sensing Data, Proceedings of the Conference on GIS and Application of Remote Sensing to Disaster Management, 132-137(1997).
- [3] Kohei Arai, An Expectation to Remote Sensing for Disaster Management, Proceedings of the United nation and Japan-US Science/Technology and Space Application Program Joint Symposium on Disaster Management, (1997).
- [4] Kohei Arai, The Conference on GIS and Application of Remote Sensing to Disaster Management Four Dimensional GIS and Its Application to Disaster Monitoring with Satellite Remote Sensing Data, Proceedings of the Conference on GIS and Application of Remote Sensing to Disaster Management, 132-137 Greenbelt, Maryland, U.S.A., 1997.
- [5] Kohei Arai, The Current Status on Disaster Monitoring with Satellites in Japan, Proc. of the Committee on Earth Observation Satellites/Working Group on Information Systems and Services/Task Team 19 Meeting, Greenbelt, Maryland, U.S.A., 1997.
- [6] Kohei Arai, Proc. of the Joint Symposium on Disaster Management Between United Nation and Japan-US Science/Technology and Space Application Program, Hawaii, U.S.A., 1997.
- [7] Kohei Arai, An Expectation on Remote Sensing Technology for Disaster Management and Response, United Nations Proceedings Series, Edt.Y.Ogawa and Kohei Arai, No.28, p.11, 1998.
- [8] Kohei Arai, Virtual Center for Disaster Management, Proc. of the 2nd United Nation and JUSTSAP Joint Symposium, 1998.
- [9] Kohei Arai, Opening Remarks of Satellite Based Disaster Management, Proc. of the Disaster Management Workshop in Ihilani Hotel, Hawaii USA, Invited Speech, 1998.
- [10] Kohei Arai, Disaster related activities, Proceedings of the 1st JUSTSAP-ADRC Joint Symposium on Disaster Management, (1999).
- [11] Kohei Arai, Internet GIS and Disaster Information Clearing House, Proceedings of the 1st JUSTSAP-ADRC Joint Symposium on Disaster Management, (1999).
- [12] Kohei Arai, Opening address of the disaster management symposium, United nations Center for Regional Development Proceedings, No.34, pp.9-12, (1999).
- [13] Kohei Arai, Virtual center for disaster management, United nations Center for Regional Development Proceedings, No.34, pp.33-38, (1999).
- [14] Kohei Arai, Joint Research on Disaster Management, Proceedings of the United Nations, Center for Regional Development, UNCRD Headquarter, Nagoya, 7 Jan., 1999.
- [15] Kohei Arai, URL search engine with text search tools for disaster mitigation, Proceedings of the Asian Disaster Reduction Center R&D Project Workshop, Mar.3, (2000).
- [16] Kohei Arai, Four-dimensional GIS system through internet, Proceedings of the Asian Disaster Reduction Center R&D Project Workshop, Mar.4, (2000).
- [17] Kohei Arai, Visualization of disaster information derived from Earth observation data, Proceedings of the Asian Disaster Reduction Center R&D Project Workshop, Aug.31, (2000).
- [18] Kohei Arai, Java based image processing and analysis software package, Proceedings of the Japan-US Science, Technology and Space Application Program Workshop, Hiro, Hawaii, (2000).

- [19] Kohei Arai, Internet Geographic Information System (GIS), Proceedings of the Japan-US Science, Technology and Space Application Program Workshop, Hiro, Hawaii, (2000).
- [20] Kohei Arai, Disaster related URL search engine with queries in a natural language, Proceedings of the Japan-US Science, Technology and Space Application Program Workshop, Hiro, Hawaii, (2000).
- [21] Kohei Arai, Disaster monitoring with ASTER onboard Terra satellite, Proceedings of the Japan-US Science, Technology and Space Application Program Workshop, Hiro, Hawaii, (2000).
- [22] Kohei Arai, Clearing house for disaster management, Proceedings of the Japan-US Science, Technology and Space Application Program Workshop, Hiro, Hawaii, Nov.15, (2000).
- [23] Kohei Arai, ICT technology for disaster mitigation (Tsunami warning system), Proceedings of the 1st International Workshop on Knowledge Cluster Systems, 2007.
- [24] Kohei Arai and Achmad Basuki, Cellular automata-based approach for prediction of hot mudflow disaster area, Proceedings of the International Conference on Computational Science and Its Applications (ICCSA2010), LNCS part-II, 87-98, 2010.
- [25] Kohei Arai and Achmad Basuki, Simulation of hot mudflow disaster with cellular automata and verification with satellite imagery data, Proceedings of the ISPRS WG VIII/1 TS-19, 2010.
- [26] Kohei Arai, Kiyotaka Fujisaki, Hiroaki Ikemi, Masato Masuya, Terumasa Miyahara, Backup communication routing through Internet Satellite, WINDS, for transmission of disaster relief data, Proceedings of the International Symposium on WINDS Application Experiments, 2010.
- [27] Kohei Arai, Backup communication routing through Internet satellite WINDS for transmission of disaster relief data, Proceedings of the International Symposium on WINDS, 2010.
- [28] Kohei Arai and Achmad Basuki, Two-dimensional cellular automata approach for disaster spreading, Proceedings of the 18th Indonesian Scientific Meeting, 2010.
- [29] Kohei Arai, Disaster Mitigation, Visiting Scholar, World Class University, The Program of Sebelas Maret University, Invited Speaker, 2010.
- [30] Kohei Arai, Tri Harsono, Achmad Basuki, Micro traffic simulation with unpredictable disturbance based on Monte Carlo simulation: effectiveness of the proposed agent cars of Sidoarjo hot mudflow disaster, Journal of Emitter, 1, 1, 1-10, 2010.
- [31] Achmad Basuki, Tri Harsono and Kohei Arai, Probabilistic cellular automata-based approach for prediction of hot mudflow disaster area and volume, Journal of EMITTER1, 1, 11-20, 2010.
- [32] Achmad Basuki and Kohei Arai, Two dimensional CA approach for disaster spreading, Innovation Online (INOVASI), 18,12,19-26, 2010.
- [33] Tri Harsono, Kohei Arai, Deceleration in the micro traffic model and its application to simulation for evacuation from disaster area, Proceedings of the IES: Industrial Electronics Seminar, at EEPIS, 1-8, 2011.
- [34] Kohei Arai, Cellular automata approach for disaster propagation prediction and required data system in GIS representations, Proceedings of the 1st ICSU/WDS Conference - Global Data for Global Science, 2011.
- [35] Kohei Arai, Tri Harsono, Achmad Basuki, Cellular automata for traffic modelling and simulation in a situation of evacuation from disaster areas, Cellular Automata-Simplicity Behind Complexity, Edt. Aiejandro Salcido, ISDN: 978-953-307-230-2, In Tech Publishing Co. Ltd., 193-218, 2011.
- [36] Kohei Arai, Achmad Basuki, New Approach of Prediction of Sidoarjo Hot Mudflow Disaster Area Based on Probabilistic Cellular Automata, Geo-informatica - An International Journal (GIJ), 1, 1, 1-11, 2011.
- [37] Kohei Arai, Tri Harsono, Achmad Basuki, Cellular automata for traffic modeling and simulation in a situation of evacuation from disaster areas -Cellular automata Simplicity behind Complexity-, Edt. Aiejandro Salcido, ISBN:978-953-307-230-2, In Tech Publishing Co. Ltd., 193-218, 2011.
- [38] Kohei Arai, Back-up communication routing through Internet satellite WINDS for transmitting of disaster relief data, International Journal of Advanced Computer Science and Applications, 2, 9, 21-26, 2011.
- [39] Kohei Arai, Sensor network for landslide monitoring with laser ranging system avoiding rainfall influence on laser ranging by means of time diversity and satellite imagery data-based landslide disaster relief, International Journal of Applied Sciences, 3, 1, 1-12, 2012.
- [40] Kohei Arai, T.X.Sang, N.T.Uyen, Task allocation model for rescue disable persons in disaster area with help of volunteers, International Journal of Advanced Computer Science and Applications, 3, 7, 96-101, 2012.
- [41] Kohei Arai, Cell based GIS as Cellular Automata for disaster spreading prediction and required data systems, CODATA Data Science Journal, 137-141, 2012.
- [42] T.Harsono, Kohei Arai, Deceleration in the evacuation from disaster area, Journal of Electronics, Mechanics & Robotics, Informatics & Computer, Telecommunications (EMITTER), 2, 2, 203-210, 2012.
- [43] Kohei Arai, Cell based GIS as cellular automata for disaster spreading predictions and required data systems, Advanced Publication, Data Science Journal, Vol.12, WDS 154-158, 2013.
- [44] Kohei Arai, Visualization of 5D assimilation data for meteorological forecasting and its related disaster mitigation utilizing VIS5D of software tool, International Journal of Advanced Research in Artificial Intelligence, 2, 9, 24-29, 2013.
- [45] Kohei Arai, Vital sign and location/attitude monitoring with sensor networks for the proposed rescue system for disabled and elderly persons who need a help in evacuation from disaster areas, International Journal of Advanced Research in Artificial Intelligence, 3, 1, 24-33, 2014.
- [46] Kohei Arai, Method and system for human action detection with acceleration sensors for the proposed rescue system for disabled and elderly persons who need a help in evacuation from disaster areas, International Journal of Advanced Research in Artificial Intelligence, 3, 1, 34-40, 2014.
- [47] Kohei Arai, Method and system for human action detection with acceleration sensors for the proposed rescue system for disabled and elderly persons who need a help in evacuation from disaster areas, International Journal of Advanced Research in Artificial Intelligence, 3, 1, 34-40, 2014.
- [48] Kohei Arai, Hiroshi Okumura, Shogo Kajiki, Disaster relief with satellite based synthetic aperture radar data, Proceedings of the SAI Future Technology Conference 2017, No.521, 1026-1029, in Vancouver, 2017.
- [49] Kohei Arai, Sentinel 1A SAR Data Analysis for Disaster Mitigation in Kyushu, Kyushu Brunch of the Japanese Society on Remote Sensing, Special Lecture for Young Engineers on Remote Sensing, Nagasaki University, 2018.
- [50] Kohei Arai, Flooding and oil spill disaster relief using Sentinel of remote sensing satellite data, International Journal of Advanced Computer Science and Applications IJACSA, 10, 12, 290-297, 2019.
- [51] Kohei Arai, Convolutional neural network considering physical processes and its application to disaster detection, International Journal of Advanced Computer Science and Applications IJACSA, 10, 12, 105-111, 2019.
- [52] Kohei Arai, Method for rainfall rate estimation with satellite based microwave radiometer data, International Journal of Advanced Computer Science and Applications IJACSA, 11, 3, 82-91, 2020.
- [53] Kohei Arai, Hiroshi Okumura, Shogo Kajiki, Flood Damage Area Detection Method by Means of Coherency Derived from Interferometric SAR Analysis with Sentinel-1A SAR, International Journal of Advanced Computer Science and Applications IJACSA, 11, 7, 88-94, 2020.

AUTHORS' 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 in April 1990. He is now an Emeritus Professor of Saga University since 2014. He was a council member 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 and is an Adjunct Professor of Nishi-Kyushu University as well as Kurume Institute of Technology/AI Application Laboratory since 2021. 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 60 books and published 640 journal papers as well as 460 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>

Developing of Middleware and Cross Platform Chat Application

Study Case: Telegram, LINE

Danny Sebastian¹, Restyandito², Kristian Adi Nugraha³

Fakultas Teknologi Informasi, Universitas Kristen Duta Wacana, Yogyakarta, Indonesia

Abstract—The rapid development of technology has resulted in many new innovations on social media platforms. Now-a-days, there are many chat applications available, namely Whatsapp, Telegram, LINE, Viber, and many others. This in turn forces users to juggle between many chat applications as different applications can't communicate with each other. This research aims to develop a chat application which serves as a middleware to make communication between developed chat application and two conventional chat applications possible (Telegram and LINE). Several tests are done to ensure that the message exchange process (in text, picture, video, and file type) works well between the developed chat application as well as Telegram or LINE.

Keywords—Telegram API; line API; chat application; flutter; middleware

I. INTRODUCTION

The rapid development of technology has invented many new innovations on social media platforms. There are so many social media applications available, yet this doesn't stop the emergence of new social media applications. In Indonesia, there are so many social media platforms available, with Line, Telegram, Whatsapp, and Viber being some of the most notorious social media platforms offering its service in Indonesia. Social media platforms generally offer messages, pictures, voice message, file exchanges, and other things [1]. Every chatting application offers different features available for the users to use. For instance, Telegram offers the file upload feature, a feature that LINE has yet to offer [2] [3].

Every user has their own preferences in choosing which social media platforms they want to use. Oftentimes, the amount of acquaintances using a certain social media platform being the main consideration on which social media platform they are going to use. This happens because of the limitation in which users can only exchange messages within the same social media platforms. To this day, message exchanges between different social media platforms are still impossible.

Usually, each user has their own preferences in choosing chat apps. In fact, usually the selection of chat apps depends on the community group, each community group has their own favorite chat apps. This condition makes it difficult when someone joins several community groups, and each community group uses different chat apps. Different features offered by each social media platform provider and limitations on communicating using different platforms forced the users to choose which platforms they are going to use. Oftentimes,

often users have to use a lot of social media and have an account in each chat application.

The writer feels the need to research and develop a custom chat application and middleware which will connect several social media platforms. In this research, LINE and Telegram chatting applications are used. This article is divided into five parts, namely, introduction, literature review, research methods, results and findings, and conclusions.

II. LITERATURE REVIEW

Chatting in Indonesian means communication between a person with another person or people [4]. In the computing world, chatting means communication between 2 or more people using computer devices [4]. Nowadays, chatting applications are growing rapidly, with many chatting applications being developed to fulfill the users' communication needs. There are so many features offered by social media platforms nowadays, namely files transfer, auto response/bot [5] [6], business features, gaming features [7], and many more. Chatting application providers aren't always big companies such as Whatsapp, Telegram, Viber, LINE, but also small developers. Hence, several chatting applications made it possible to communicate with other applications using Application Programming Interface (API) [2] [3].

Middleware is a software application which can connect a system with another system [7]. Middleware can be used to connect several systems within the same device or even on different devices connected to the internet [8] [9]. Middleware can also be used to connect applications on the same type of device or different types of devices, such as mobile device - mobile phone, mobile phone - television, mobile phone - computer, computer - computer, et cetera [10]. In developing a middleware application, there are a few solutions/methods, namely message oriented middleware [11], object-oriented middleware [12], Remote procedure call, database middleware, transactional middleware, portals, embedded middleware [13], and content-centric middleware [14].

Middleware development was also done to bridge a chatting application with other application. Several researchers have developed middleware for chatting applications to add features, such as Artificial Intelligence [15]. Some researchers developed middleware from scratch and some other used API provided by the chatting applications provider [16]. Other than API, webhook method also used to send messages between chat bots.

Several researches and development on custom chatting applications has been done. A custom chatting application equipped with Natural Language Processing was developed in one research [17]. In this research the system will automatically do sentiment analysis towards the message being sent. If the analyzed message has negative context, then the message will not be sent. In another research, a custom location based chatting application was developed [18], in which the application allows the users to find friends and communicate with other users within a certain distance. Another research was also done, intending to help the communication between faculty members (lecturer, assistant lecturer) and the students [19]. The custom chatting application developed was able to automatically create a group chat based on the subjects' registration done every semester.

Several researches on chatting application development using the API offered by big chatting application providers, namely Telegram, LINE, et cetera was also done. Some developed a smart home system using NodeMCU Microcontroller combined with Telegram API [20]. By using the application developed in this research, users are able to monitor and command their Internet of Things devices using Telegram. Telegram Bot API was used to send messages from Telegram to the Internet of Things devices. Other than that, the Telegram BOT API was also used to create an e-complaint application for a college [21]. In this application, the Telegram Bot API was used to receive complaints and calculate the complaints statistics based on the divisions being complained to.

In summary, custom chatting applications that were developed are Android based [1] [17] [18], iOS based [1] [22], website applications [4] [23], and desktop application [24]. Android based mobile applications can be developed using either Java or Kotlin, while iOS based mobile applications are developed using either objective-C or Swift. In the application development community, there is a new trend which is a cross-platform application, in which the developed applications can be compiled and create both an Android and iOS based application using a single code base. One of the frameworks used to create this cross-platform device is the Flutter Framework. Flutter Framework itself is an open source cross platform development framework developed by Google [25]. Flutter itself is based on the Dart Programming Language. Several technology company giants were using Flutter Framework to develop their products, namely, Alibaba and Google Ads.

A. Chat API

Application Programming Interface (API) is used by an application to exchange information with other applications [26]. API success relies on the API documentation provided by API for software development needs. Many chat applications have provided API which allows other application to access the chat applications' services.

Telegram provides API for software developers to connect their applications to Telegram's system. This API allows Telegram Bot creation [2]. Telegram Bot itself acts as an interface to run code from a server. Telegram API uses text in JSON format in passing data with other systems. This JSON

formatted text allows developers to develop application using many different programming languages.

Line Messaging API is a service provided by LINE to exchange data between Line Platform and other application [3]. Just like Telegram Bot API, LINE Messaging API uses JSON to communicate with other applications. LINE Messaging API uses webhook method to pass data to the server.

B. NoSQL Database

NoSQL database are databases that don't use SQL command in which data was saved in an unstructured format and often time don't have relations with other table like SQL databases [27] [28]. NoSQL database was intended to save data in a flexible way in modern application development. In many cases, NoSQL databases used in real-time application development.

In general there are four types of NoSQL Database [29]:

- Graph databases: These databases uses graph theory concept. Example: Neo4j and Titan.
- Key-Value store databases: In these databases, data are stored in two parts, which are key and value. Example: Redis, DyanmoDB, Riak.
- Column Store databases: In these databases, data are stored in column of data. Example: BigTable, Cassandra.
- Document Databases: These databases are more extensive database than the key-value store. The value are saved in document type and stored in a ore complex format, like JSON. Example: MongoDB, CouchDB.

C. Flutter

Flutter is an open source mobile application development made by Google [30]. Flutter allows Android and iOS based application development using only one source code base [31]. Flutter uses Dart Programming Language. Flutter Framework uses widget concept in interface creation. There are many widgets provided, namely Column, Row, Icon, and many other widgets. The widget in Flutter acts are either visual component or as a container for other widgets [32].

III. RESEARCH METHOD

A. System Design

The system developed consists of two main applications, namely mobile chatting application and middleware application. The chatting application is used as an interface for the user to test the system. This chatting application was developed using Dart programming Language with Flutter Framework. While the middleware acts as a connector to connect the chatting application developed with Telegram API, LINE API.

Architecture of the system developed can be seen on Fig. 1. Message exchange process starts on one of the Conventional Chat Application/CCA (Telegram/LINE/Signal) to the CCA's chat API (step 1). Then the CCA's API will pass the message to the middleware to be received by the webhook

prepared (step 2). The middleware will then process the message fetched by saving the message’s metadata, saving the file, image, video, our sound data to Firebase. The middleware developed uses 3 Firebase service, namely Firestore, Firebase Cloud Storage, and Firebase Cloud Messaging. Firestore is used to save the messages’ metadata and content, such as the message’s recipient, message’s sender, chatting application, etc. Example of data stored in Firestore can be seen on Fig. 2 for text data and Fig. 3 for non-text data. Firebase Cloud Storage is used to store video, image, voice, and file message data. Example of data stored in Firebase Cloud Storage can be seen on Fig. 4. After being processed, the middleware will then pass the message to Flutter Chat Application/FCA (step 3).

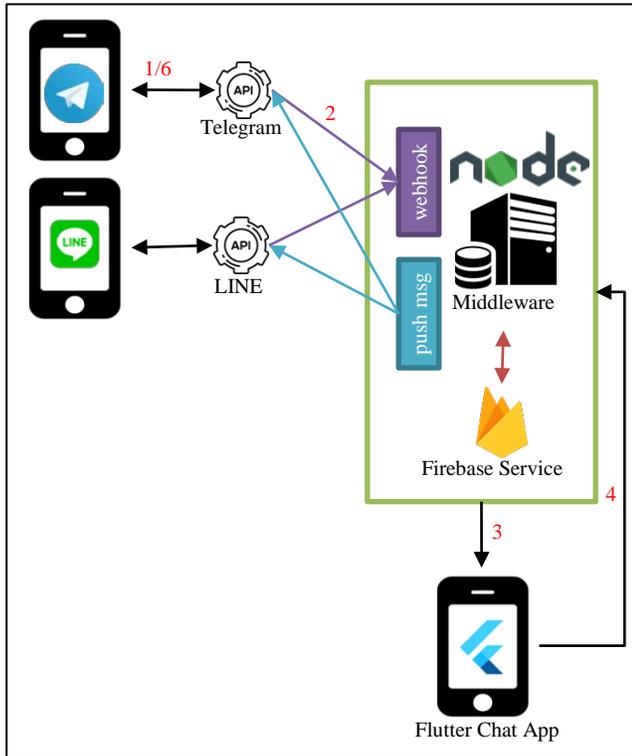


Fig. 1. Whole System Application Architecture.

```
content: "tess"
idFrom: "-467753380"
idTo: "v8LWQosYDaY5THmOObGziZ1orXs2"
timestamp: "1623169064892"
type: "text"
```

Fig. 2. Example of Data Stored in Firestore, Type:Text Message.

```
content: "https://storage.googleapis.com/chatbridge.appspot.com/162330659543
GoogleAccessId=chatbridge%40appspot.gserviceaccount.com&Expires=
idFrom: "Cb78748d9442797c5617263235e745a1b"
idTo: "Rc6LkPslVgTSBILC3Z44ELn6Bb2"
timestamp: "1623306630431"
type: "video"
```

Fig. 3. Example of Data Stored in Firestore, Type:Video.

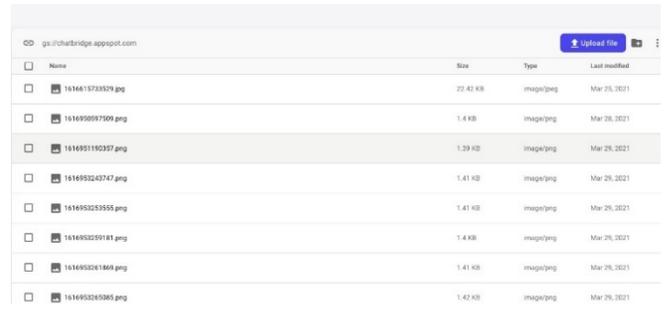


Fig. 4. Example of Data Stored in Firebase Cloud Storage.

Meanwhile, messages passed from FCA to CCA starts from (step 4), where FCA forward messages to the middleware. Messages from FCA will then be processed on the middleware and stored in Firebase services. After that, messages will then be forwarded to the recipient’s CCA through Chat Application API using Push Message (step 5/6). Available API could be seen at Table I.

After the application has been developed, system test was done. This system test was done to make sure that the application has successfully work as expected. The system test scenario can be found on Table II. System test was done on Text, Image, Video, Sound and File type. For each message type, testing was done from CCA to FCA, and vice versa.

B. System Test

Performance testing was done to measure the time needed by the middleware to forward and receive messages. The performance testing scenario can be seen on Table III. In general, the testing was done using four types of data, namely, Text, Image, Video and File. For text data type, size of the data forwarded was classified based on the number of characters. As for the Image, Video and File data type, data was classified based on the file size (in megabyte). Testing for the Text, Image, and Video data was done on Telegram, and LINE. However, File data wasn’t tested on LINE as the chatting application doesn’t have file sharing feature.

TABLE I. APPLICATION PROGRAMMING INTERFACE (API) MIDDLEWARE

Method	URI	Description
POST	/telegram/webhook	Receive messages from telegram bot and forward it to the FCA
POST	/telegram/push	Receive messages from the FCA and forward them to Telegram API
POST	/line/webhook	Receive message from LINE bot and forward them to the FCA
POST	/line/push	Receive messages from the FCA and forward it to LINE API

TABLE II. SYSTEM TEST SCENARIO

Method	URI	Description
CCA-FCA, FCA-CCA	Text	Telegram, LINE
CCA-FCA, FCA-CCA	Image	Telegram, LINE
CCA-FCA, FCA-CCA	Video	Telegram, LINE
CCA-FCA, FCA-CCA	Sound	Telegram, LINE
CCA-FCA, FCA-CCA	File	Telegram

TABLE III. PERFORMANCE TEST SCENARIO

Type	Chat Application	Measurement	Size
Text	Telegram, LINE	Characters	400, 800, 1200, 1600, 2000, 2400, 2800, 3200, 3600, 4000
Image	Telegram, LINE	MB	1, 2, 3, 4, 5
Video	Telegram, LINE	MB	1, 2, 3, 4, 5
File	Telegram	MB	1, 2, 3, 4, 5

TABLE IV. SYSTEM TEST RESULT

From-To	Message Type	CCA	Result
CCA-FCA	Text	Telegram	Pass
		LINE	Pass
FCA-CCA		Telegram	Pass
LINE		Pass	
CCA-FCA	Image	Telegram	Pass
		LINE	Pass
FCA-CCA		Telegram	Pass
LINE		Pass	
CCA-FCA	Video	Telegram	Pass
		LINE	Pass
FCA-CCA		Telegram	Pass
LINE		Pass	
CCA-FCA	File	Telegram	Pass
		FCA-CCA	Telegram

The system developed has start and end timer. In the FCA to CCA testing, the start timer was invoked when the “Send” button on the FCA is clicked, while the stop timer was invoked when the middleware sends out push message to the Chat API. As for the CCA to FCA testing, the start tier was invoked when the middleware webhook receive request, while the stop timer was invoked when the message has been forwarded by the middleware to FCA.

$$process_time = \frac{(t_1+t_2+t_3+t_4+t_5)}{5} \quad (1)$$

In this testing, the possibility of unstable internet connection may be a problem. To tackle this problem, every test scenario was done 5 times and average processing time will be calculated to then be used as a final result. Average process tie formula can be seen on equation (1). For example, Telegram Text data type testing for 400 characters processing time was measured on 0.5 second, 0.7 second, and 0.63 second. Thus, the processing time for this test case is 0.61 second. Each test case will be carried out for testing from CCA to FCA and vice versa. Performance time result will be compared for CCA to FCA and FCA to CCA data.

IV. RESULT AND FINDINGS

A. System Test

System testing has been done and the result can be seen on Table IV. All system testing scenario can be done by the chat application’s middleware and Flutter Chat Application (FCA). Captures of the Flutter Chat Application can be seen on Fig. 5. Based on the testing result, the middleware application developed has successfully able to forward messages from the Flutter Chat Application (FCA) to the Conventional Chat Application (CCA) and vice versa. This success also applies for all message types tested.

Currently the architecture and communication process starts by creating a chat group on Telegram/LINE, then an OTP request is made to be able to start communication between the custom chat app and the Telegram/LINE chat app. Currently, the architecture and communication processes in the middleware that are built are still unable to communicate between LINE and Telegram. This is because there is an OTP request that must be made so that communication can be carried out. Due to this limitation, it is necessary to adjust the add contact process. On the other hand, when chatting, the middleware needs to add fields recording where the message was sent from and where the message was sent.

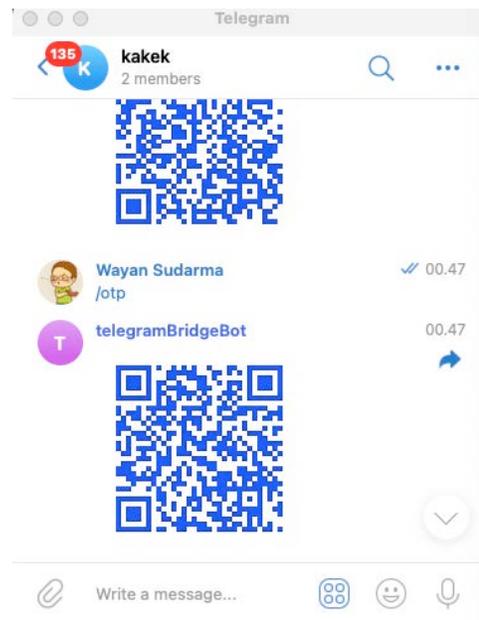


Fig. 5. Screenshot user Interface Application Flutter Chat Application.

B. System Performance Evaluation

System Performance Test was performed on each of the message type sent. The message types tested were text, picture, video, and file messages. Testing result for text data can be seen on Table V and Fig. 6. The results show that the messages sent from the CCA to the FCA took longer than the messages sent from the FCA to the CCA. As seen in Fig. 6 there was a significant increase in time needed to forward a message containing 2800 characters from FCA to Telegram (represented by the orange line).

This increase in time may be caused by the mobile network used for testing. However, in general there were no significant increases in time when the character-count is increased.

TABLE V. SYSTEM PERFORMANCE TEST (TEXT)

Char length	Telegram		LINE	
	Tele-FCA	FCA-Tele	LINE-FCA	FCA-LINE
400	144	1070.6	121.4	706
800	163.8	728.8	118	822
1200	164.4	721.8	156	667.2
1600	166.4	817	139.2	711.4
2000	281.4	972	122.6	669.4
2400	126.8	809	126.6	731.2
2800	150.8	1476.2	147	754
3200	289.8	762.4	216.2	1120.6
3600	194.8	766	232.2	783.6
4000	185.8	830.4	106.2	925.8

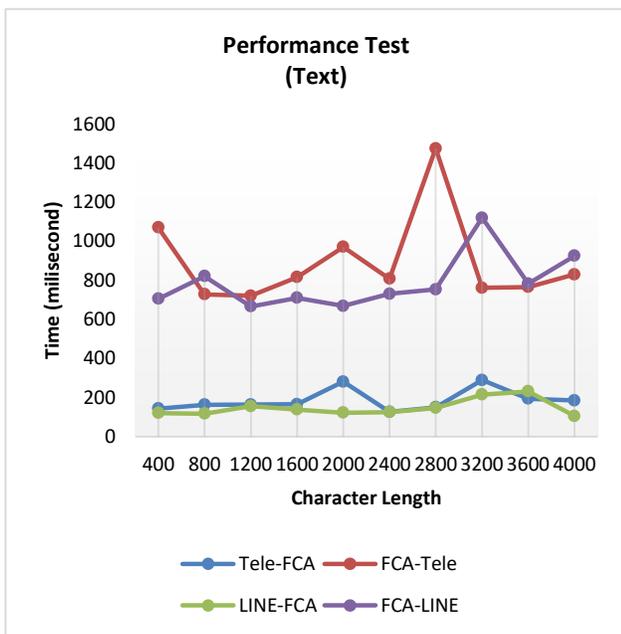


Fig. 6. System Performance Test (Text).

The second testing was done on image messages. The test result can be seen on Table VI and Fig. 7. It can be seen that there is a significant time increase on messages sent from the FCA to Telegram (displayed in orange line) and from FCA to LINE (displayed in yellow line) for image with 5MB in size. Based on the testing, there is no significant time difference between messages sent from the FCA to the CCA and from the CCA to the FCA.

The third testing was done on video messages. The test result can be found on Table VII and Fig. 8. Based on the testing done, it can be seen that there is a significant increase in time aligned with the increase of file size for all scenarios. However, a significant increase in time was most noticeable on messages sent from the CCA to the FCA (displayed in blue and grey line). In general, it can be seen that messages sent from the CCA to the FCA (displayed in blue and grey line) require more time than messages sent from the FCA to the CCA (displayed in orange and yellow line).

TABLE VI. SYSTEM PERFORMANCE TEST (IMAGE)

Size (MB)	Telegram		LINE	
	Tele-FCA	FCA-Tele	LINE-FCA	FCA-LINE
1	5939.6	8217	10526.2	5164.4
2	4592.8	10162	8015.4	5383.6
3	5426.2	6477.2	8793.2	5379.2
4	5979.6	5059.2	8945.4	4903.2
5	5629.4	21017.6	8009.2	21473.2

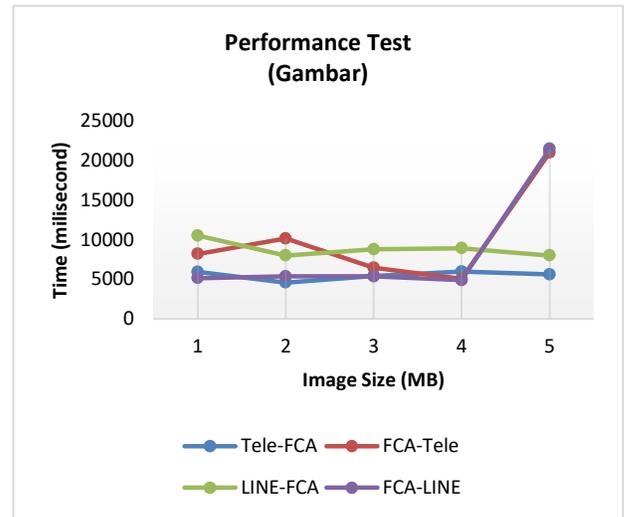


Fig. 7. System Performance Test (Image).

TABLE VII. SYSTEM PERFORMANCE TEST (VIDEO)

Size (MB)	Telegram		LINE	
	Tele-FCA	FCA-Tele	LINE-FCA	FCA-LINE
1	10294.75	6816.2	24761	8083.8
2	20547.6	9381.4	32932.6	10983.8
3	23186.6	8190.6	47755.4	12659.2
4	34914.2	10264.4	51798.8	17165.6
5	48456	10883.6	58812.6	20204

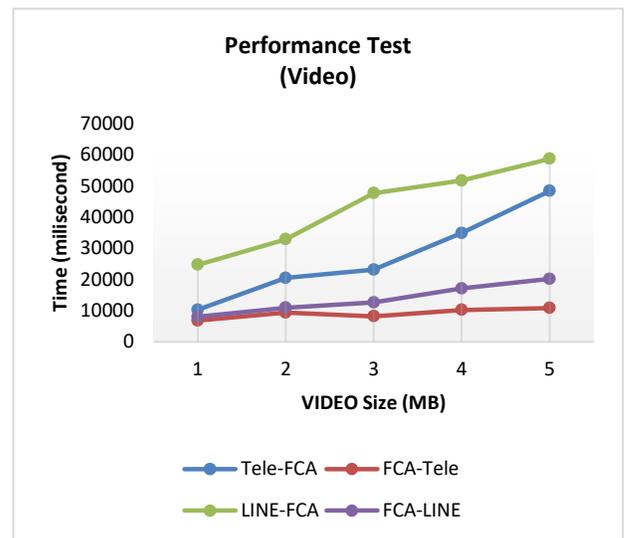


Fig. 8. System Performance Test (Video).

The fourth testing was done on file type messages. This testing was created specifically for Telegram as LINE does not yet offer this message type. The testing result can be seen on Table VIII and Fig. 9. Based on the testing done, it can be seen that there is a significant increase in processing time as the file size increases.

TABLE VIII. SYSTEM PERFORMANCE TEST (FILE)

Size (MB)	Telegram	
	Tele-FCA	FCA-Tele
1	15183.6	9957
2	21697	12236
3	25806.4	15778.6
4	35879.4	17901.8
5	40866.8	22704.6

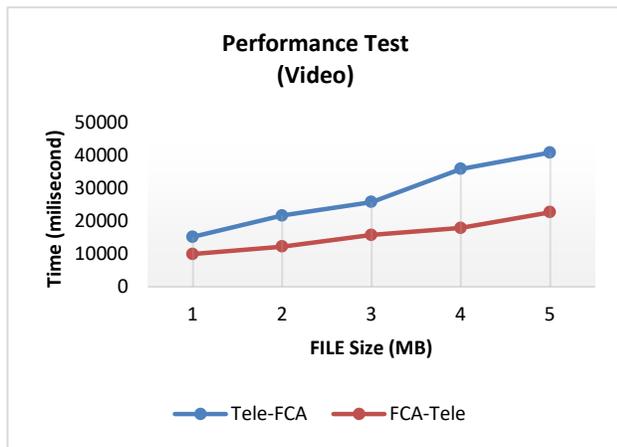


Fig. 9. System Performance Test (File).

V. CONCLUSION

Based on this research, it is concluded that:

- Middleware application was able to exchange messages between the developed chatting application based on Flutter and Conventional Chatting Application (Telegram and LINE), with text, pictures, videos, voice, and file being the type of messages exchanged.
- For video and file messages, there is a correlation between file size and the time needed to forward the message. The bigger the file, the longer it takes to send the file.

Suggestion for future research,

- Adding other conventional chatting application which can be served by the middleware.

ACKNOWLEDGMENT

The writers would like to thank Duta Wacana Christian University and Indonesian Ministry of Research and Technology. This research was funded by Indonesian Ministry of Research and Technology with contract number: 311/E4.1/AK.04.PT/2021 dated 12 July 2021, 3281.5/LL5/PG/2021/22 July 2021 and 264/D.01/LPPM/2021/23 Juli 2021.

REFERENCES

- [1] N. Sabah, J. M. Kadhim and B. N. Dhannoon, "Developing an End-to-End Secure Chat Application," *IJCSNS*, vol. 17, no. 11, p. 108, 2017.
- [2] Telegram, "Telegram APIs," Telegram, [Online]. Available: <https://core.telegram.org/>. [Accessed 12 08 2020].
- [3] LINE Corp, "LINE Messaging API," LINE Corp, 2021. [Online]. [Accessed 20 06 2021].
- [4] D. Henriyani, D. P. Subiyanti, R. Fauzian, D. Anggraini, M. V. G. Aziz and A. S. Prihatmanto, "Design and implementation of web based real time chat interfacing server," in 2016 6th International Conference on System Engineering and Technology (ICSET), Bandung, Indonesia, 2016.
- [5] R. Parlika, S. I. Pradika, A. M. Hakim and K. R. NM, "BOT Whatsapp Sebagai Pemberi Data Statistik Covid-19 Menggunakan PHP, Flask, dan MySQL," *Jurnal Informatika dan Sistem Informasi (JIFoSI)*, vol. 1, no. 2, pp. 282-293, 2020.
- [6] M. Vorontsov and S. I. Radmir, "Automation of Message Sending Processes Using Specialized Software," in 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia, 2021.
- [7] A. N. Wulanjani, "Discord Application: Turning a Voice Chat Application for Gamers into a Virtual Listening Class," in *Education 4.0: Trends and Future Perspectives in English Education, Linguistics, Literature, and Translation*, Semarang, Indonesia, 2018.
- [8] K. Geihs, "Middleware challenges ahead," *Computer*, vol. 34, no. 6, pp. 24-31, 2001.
- [9] M. Saranya and A. A. Priya, "A Study on Middleware Technologies in Cloud Computing," *International Journal for Innovative Research in Science & Technology (IJIRST)*, vol. 4, no. 3, pp. 31-36, 2017.
- [10] L. F. Meloni, G. C. Costa, G. Kobayashi and C. S. Kurashima, "Implementation of chat application for ginga middleware technology using second screen," in 2016 IEEE international symposium on consumer electronics (ISCE), Sao Paulo, Brazil, 2016.
- [11] J. Yongguo, L. Qiang, Q. Changshuai, S. Jian and L. Qianqian, "Message-oriented Middleware: A Review," in 2019 5th International Conference on Big Data Computing and Communications (BIGCOM), QingDao, China, 2019.
- [12] M. Henning, "A new approach to object-oriented middleware," *IEEE Internet Computing*, vol. 8, no. 1, pp. 66-75, 2004.
- [13] J. Zhang, M. Ma, P. Wang and X.-d. Sun, "Middleware for the Internet of Things: A survey on requirements, enabling technologies, and solutions," *Journal of Systems Architecture*, vol. 117, 2021.
- [14] G. S. Wedpathak, "An Approach of Software Engineering through Middleware," *International Journal of Engineering and Management Research (IJEMR)*, vol. 5, no. 1, pp. 127-138, 2015.
- [15] P. Thosani, M. Sinkar, J. Vaghasiya and R. Shankarmani, "A Self Learning Chat-Bot From User Interactions and Preferences," in 2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS), Madurai, India, 2020.
- [16] C. E. Swandi, K. A. Nugraha, D. Sebastian and Restyandito, "Middleware Development to Connect Telegram Messenger and Instant Messenger for the Elderly," in *The 5th International Conference on Information Technology and Digital Applications (ICITDA 2020)*, Yogyakarta, Indonesia, 2021.
- [17] S. Karthick, R. J. Victor, S. Manikandan and B. Goswami, "Professional chat application based on natural language processing," in 2018 IEEE International Conference on Current Trends in Advanced Computing (ICCTAC), Bangalore, India, 2018.
- [18] M. Kamruzzaman, "Localized Chat Application," *Daffodil International University*, 2018.
- [19] V. Efendy, K. A. Nugraha and D. Sebastian, "Implementasi Chat Room dan Push Notification pada e-Class Berbasis Mobile," *Jurnal Teknik Informatika dan Sistem Informasi*, vol. 5, no. 2, pp. 267-282, 2019.
- [20] Y. Findawati, A. Idris, Y. Rachmawati and E. A. Suprayitno, "IoT-Based Smart Home Controller Using NodeMCU Lua V3 Microcontroller and Telegram Chat Application," in *International Conference on Engineering, Technologies, and Applied Sciences (ICETSAS)*, Bengkulu, Indonesia, 2020.

- [21] N. Rosid, A. Rachmadany, M. Multazam, A. Nandiyanto, A. Abdullah and I. Widiaty, "Integration telegram bot on e-complaint applications in college," in The 2nd Annual Applied Science and Engineering Conference (AASEC 2017), Bandung, Indonesia, 2018.
- [22] H. Engoren and E. Zorn, "Bridgr: An iOS Application for Organizing and Discussing Long-Distance Carpooling," 2019.
- [23] E. Kho, V. C. Mawardi and N. J. Perdana, "Web-based Live Chat Application uses Advanced Encryption Standard Methods and Rivest Shamir Adleman," in 3rd Tarumanagara International Conference of the Applications of Technology and Engineering (TICATE), Jakarta, Indonesia, 2020.
- [24] N. V. Vukadinovic, "WhatsApp Forensics: Locating Artifacts in Web and Desktop Clients," Purdue University Graduate School, West Lafayette, 2019.
- [25] M. Szczepanik and M. Kedziora, "State Management and Software Architecture Approaches in Cross-platform Flutter Applications," in 15th International Conference on Evaluation of Novel Approaches to Software Engineering (ENASE 2020), 2020.
- [26] M. Meng, S. Steinhardt and A. Schubert, "Application programming interface documentation: what do software developers want?," Journal of Technical Writing and Communication, vol. 48, no. 3, pp. 295-330, 2018.
- [27] A. Davoudian, L. Chen and M. Liu, "A survey on NoSQL stores," ACM Computing Surveys (CSUR), vol. 51, no. 2, pp. 1-43, 2018.
- [28] A. Moniruzzaman and S. A. Hossain, "Nosql database: New era of databases for big data analytics-classification, characteristics and comparison," International Journal of Database Theory and Application, vol. 6, no. 4, 2013.
- [29] A. Gupta, S. Tyagi, N. Panwar, S. Sachdeva and U. Saxena, "NoSQL Databases: Critical Analysis and Comparison," in 2017 International Conference on Computing and Communication Technologies for Smart Nation (IC3TSN), Gurgaon, India, 2017.
- [30] Flutter Dev, "Flutter Documentation," Google, 2017. [Online]. Available: <https://flutter.dev/docs>. [Accessed 26 06 2021].
- [31] K. Wasilewski and W. Zabierowski, "A Comparison of Java, Flutter and Kotlin/Native Technologies for Sensor Data-Driven Applications," Sensors, vol. 21, no. 10, 2021.
- [32] S. Santoso, D. J. Surjawan and E. D. Handoyo, "Pengembangan Sistem Informasi Tukar Barang Untuk Pemanfaatan Barang tidak Terpakai dengan Flutter Framework," Jurnal Teknik Informatika dan Sistem Informasi (JuTISI), vol. 6, no. 3, pp. 589-598, 2020.

A Survey on Deep Learning Face Age Estimation Model: Method and Ethnicity

Hadi A. Dahlan

Faculty of Information Science and Technology
National University of Malaysia
43600 UKM Bangi, Selangor, Malaysia

Abstract—Face age estimation is a type of study in computer vision and pattern recognition. Designing an age estimation or classification model requires data as training samples for the machine to learn. Deep learning method has improved estimation accuracy and the number of deep learning age estimation models developed. Furthermore, numerous datasets availability is making the method an increasingly attractive approach. However, face age databases mostly have limited ethnic subjects, only one or two ethnicities and may result in ethnic bias during age estimation, thus impeding progress in understanding face age estimation. This paper reviewed available face age databases, deep learning age estimation models, and discussed issues related to ethnicity when estimating age. The review revealed changes in deep learning architectural designs from 2015 to 2020, frequently used face databases, and the number of different ethnicities considered. Although model performance has improved, the widespread use of specific few multi-races databases, such as the MORPH and FG-NET databases, suggests that most age estimation studies are biased against non-Caucasians/non-white subjects. Two primary reasons for face age research's failure to further discover and understand ethnic traits effects on a person's facial aging process: lack of multi-race databases and ethnic traits exclusion. Additionally, this study presented a framework for accounting ethnic in face age estimation research and several suggestions on collecting and expanding multi-race databases. The given framework and suggestions are also applicable for other secondary factors (e.g. gender) that affect face age progression and may help further improve future face age estimation research.

Keywords—Deep learning; face age estimation; face database; ethnicity bias

I. INTRODUCTION

Facial aging is a complex biological process. Most researchers in the computer vision and the pattern recognition fields have already found multiple ways to extract information from the face for age estimation/classification. However, not all information extracted can help the system learn. When the system learned from only a specific ethnic sample, it may not estimate/classify the age of other ethnic subjects correctly, even after the face age estimation system improved.

Earlier face aging models combined extractors and classifiers to extract specific aging features and accurately classify the facial image into its correct age. The downside of this approach is that the data needed for learning are usually structured and quantitatively limited; too little or too much data could lead to models learning incorrect patterns, resulting in

inaccurate age classification. Meanwhile, deep learning is another approach that could help algorithms improve the computer's ability to discover common facial aging traits (e.g. aging wrinkles) within vast amounts of data and classify the facial image into its correct age. However, face age databases mostly have limited ethnic subjects, only one or two ethnicities and may result in ethnic bias during age estimation, thus impeding progress in understanding face age estimation.

In this study, the review on face age estimation/classification/distribution examined problems regarding:

- 1) What face databases are frequently used in the age estimation study, and how many different ethnics are in those databases?
- 2) What deep learning technique is used in facial aging research? How did the technique change through time? And do they account for different ethnicities in their studies?
- 3) What are the most used deep learning network architecture and what are their strengths and weaknesses?
- 4) How to obtain more face images of people of different ethnicities in the time of restrictions (e.g. due to quarantine)?

Accordingly, this study surveyed the available face age databases, the most used database in this type of research, and the deep learning techniques used for the face age estimation (or distribution; or classification) model design. More than 50 papers (2015-2020) that used the deep learning method for face age studies were reviewed in this study. The aim of this paper is to survey the different deep learning face age estimation methods and how they account for different ethnicities. By understanding the different deep learning face age estimation methods and the problem related to ethnic bias in their face age estimation, we can discover significant racial traits that could help distinguish unique aging patterns used to solve racial face age estimation problems in real-life applications. Moreover, a framework for studying CNN face age estimation while considering the ethnicities of the subjects is included in this paper to help guide future face age estimation studies that use either the deep learning approach or the standard machine learning approach.

The remainder of this paper is structured as follows: Section 2 mention several related works regarding deep learning and early face age estimation; Section 3 explains the human facial aging and differences in process between several races; Section 4 surveys the face age image databases that can be used for facial age estimation studies and shows the quantities of

each race in each database (if any); Section 5 explains the face age estimation model and reviews the different deep learning techniques proposed between 2015-2020 as well as the databases used. The importance of ethnic traits in age estimation is also highlighted; Section 6 discusses the relevant open issues regarding ethnic characteristics; Section 7 discusses several possible solutions to solve the problems, Section 8 presents the conclusions and Section 9 mentions the future directions.

II. RELATED WORK

The deep learning model has two primary processes: 1) training and 2) inferring. The training phase is the process of labelling large quantities of data (i.e. identifying and memorising the data matching characteristics). Meanwhile, in the inferring phase, the deep learning model decides on the label for the new data using the knowledge gained from the earlier training phase. Manual feature extraction on the data is unnecessary because the model's neural network architecture can learn the feature directly from the data, eliminating the need for data labelling. This learning feature is advantageous when working on large quantities of unstructured data (multiple formats like text and pictures). Recently, deep learning, such as convolutional neural network (CNN), has become well-known in the image processing and pattern recognition fields for its capability to 'learn' from a large number of images and perform specific tasks accurately. The deep learning method can fit the parameters of multi-layered networks of nodes to the vast amounts of data before extrapolating outputs from new inputs. Knowing the commonly used network designs in face age estimation studies and their strengths and weaknesses would be interesting enough.

Recently, face age estimation studies using the deep learning approach to estimate a person's age based on aging features, such as the facial skull shape and aging wrinkle, have increased. These aging features are a person's regular facial aging changes that occur through the years. Nevertheless, considering ethnicity in age estimation can pose a different problem since each ethnicity/race has been confirmed to have a different rate of facial aging [1, 2, 3, 4]. For example, a 20-year-old White subject would look older than a 20-year-old Asian because of their facial bones and skin structures differences [2]. For the CNN model to learn correctly, many datasets containing multiple races with equal ratios are needed.

Although many face databases are available for age estimation, most are racially biased and have just only one or two significant ethnicities. Unbalanced ethnic samples can create problems as age estimation models depend solely on these databases. A bias might occur, for example, when estimating the age of an Asian subject if the majority of ethnicities available in a database are Caucasians/White due to the differences in facial structure and rate of skin aging [1, 2]. In most previous face age estimation/classification/ distribution studies, all sample databases were used for training and testing while utilising different deep learning methods that match their research aim(s) and main objective(s). However, ethnic traits are usually ignored, resulting in very few analyses of racial traits' effects on the face age estimation process. A few reasons for this exclusion: researchers mainly consider racial traits as

age-invariant features, difficulties in capturing a person's face aging progression in a controlled/uncontrolled environment, and capturing >100 face images of different ethnic people in equal quantities can be time-consuming and costly. Nonetheless, it is undeniable that the facial aging process differs between races; therefore, ethnicities should be considered in future research when experimenting with the next CNN age estimation model. Moreover, analyses on the ethnic age difference can contribute to a better understanding of human facial aging.

III. HUMAN FACIAL AGING – ETHNICITIES

Face features and expression are fundamental ways of human communication. Many studies have observed the facial appearance and examined ways to apply the knowledge to real-world applications. One of these studies is face age estimation, which is research on estimating a person's age based on facial appearance observations. Over the years, multiple facial traits help determine a person's age, including the shape of the face, skin texture, skin features, and skin colour contrast [5, 6]. The two predetermined features are as follows: 1) face shape change, particularly the cranium bones that grow with time. This process predominately occurs during childhood to adulthood transition; 2) development of wrinkles or face texture as facial muscle weakens due to decreased elasticity. This process occurs during the transition from adulthood to the senior stage [7, 8].



Fig. 1. Different Ethnic Facial Aging Features for Four Women Aged Over 60 Years Old. from Left to Right: Caucasian, East Asian, Latino/Hispanic, and African (All Images were Taken from [13]).



Fig. 2. Facial Feature and Aging Difference for Adult Caucasian (Top Left) and Asian (Bottom left), while the Baby's Face for the Caucasian is on the Top Right and Bottom right for the Asian (Images were taken from [2], Except for the Caucasian Baby, from [14]).

Internal and external forces act upon the outer and inner skin as a person age, causing some level of damage and changing the skin's appearance. As demonstrated in [9, 10], the older skin was perceived to have a different colour contrast and luminosity than the younger skin. Healthy young skin, which is plumper and emits radiant colour, has a smooth and uniformly fine texture that reflects light evenly. Meanwhile, aged skin tends to be rough and dry with more wrinkles, freckles, and age spots and emits dull colour [11, 12]. However, ethnicities can affect these aging rates because of differences in skull structure and skin type [1] (see Fig. 1). For instance, the skin of a Caucasian subject will gradually have more aging wrinkles when compared to an Asian subject as the age increases from 20 to 39 years old. This phenomenon is due to the different skull and skin structures of each ethnic. Caucasians have a significant angular face, while Asians tend to be broader and less angular, similar to a baby's broad face [2] (see Fig. 2). Due to this broader facial structure, soft-tissue loss in Asians is seen and felt to a lesser extent. Another example is between the Caucasians and the African-Americans' skin. Black skin's epidermis contains a thicker stratum corneum with more active fibroblasts than the Caucasians, making them less affected by photo aging [3, 4]. Although black skin does not tend to get fine lines like white skin, it does get folded when getting older. Such information should be considered to design a more accurate age estimation model which can specify proper age estimation/classification knowledge when dealing with specific ethnic subjects.

IV. FACE AGE DATABASE

Designing face age estimation models require many samples for training and testing. Several studies collected face samples and then made them available to the public so that others might use them in their research. Furthermore, the shared database may serve as a benchmark against which other models can be compared and improved. Table I shows the face databases with age information or labels (henceforth, called Face Age Database). Only two databases captured face images in a controlled environment (MORPH and FACES). In contrast, the rest captured the face image in either a partially controlled or uncontrolled environment. Meanwhile, the FG-NET database has the most undersized samples and subjects, while the IMDB+WIKI database offers the most samples and subjects.

Table I reveals that most of the subjects in the databases are Caucasian/White, whereas Table II provides the ethnic count. Correspondingly, the ethnic percentage is shown in Fig. 3, which reveals very few databases with non-Caucasians/non-White ethnic (White = 80%; Black = 3%; Asian = 8%; and Others = 9%). This gap creates an imbalance in the databases when ethnicity is considered to estimate the age of non-Caucasian/non-White races. Moreover, not all the databases have ethnic information (e.g. IMDB+WIKI, FERET, and Webface). The lack of ethnic labels can make it difficult for face age model researchers to divide samples into their appropriate ethnicity, eventually treated as one of their research limitations.

TABLE I. SUMMARY OF FACE DATABASES WITH AVAILABLE INFORMATION

Year	Database	Samples	Environment		Age Range	Ethnic
			C	UC		
1998	FERET [21]	14,126 samples; 1,199 subjects	√	√	Not mentioned (real age)	Not mentioned
2002	FG-NET [22]	1,002 samples; 82 subjects		√	0-69 (real age)	All White/Caucasian
2004	LIFESPAN [23]	1, 142 samples; 575 subjects	√	√	18-93 (age group)	African-American:89; Caucasian:435; Others:52
2005	FRGC [24]	44,278 samples; 568 subjects	√	√	16-77 (real age)	White:386; Asian:125; Others:57
2006	MORPH [25]	55,134 samples; 13,618 subjects	√		16-77 (real age)	White-Black ratios 4:1; Others-very small
2008	YGA [26]	8,000 samples; 1,600 subjects		√	0-93 (real age)	Not mentioned
2009	GROUPS [27]	28,231 samples; 28,231 subjects		√	0-66+ (age group)	Not mentioned
2010	FACES [28]	2, 052 samples; 171 subjects	√		19-80 (age group)	All White/Caucasian
2012	Webface [29]	59, 930 samples		√	1-80 (real age)	Not mentioned
2014	Adience [30]	26,580 images; 2,284 subjects		√	0-60 (age group)	Not mentioned
2014	CACD [31]	160,000 samples; 2,000 subjects		√	16-62 (real age)	Not mentioned
2015	Chalearn 2015 [32]	4, 699 samples		√	Not mentioned (real age)	Not mentioned
2016	Chalearn 2016 [33]	7, 591 samples		√	Not mentioned (real age)	Not mentioned
2017	AgeDB [34]	16,516 samples; 570 subjects		√	1-101 (real age)	Not mentioned
2018	IMDB+WIKI [35]	523,051 samples; 20,284+		√	0-100 (real age)	Not mentioned
2007	Iranian face [15]	3,600 samples; 616 subjects		√	2-85 (real age)	All Iranian
2013	IMFDB [16]	34,512 samples; 100 subjects		√	Not mentioned (age group)	All Indian
2016	AFAD [17]	164,432 samples		√	15-40 (real age)	All Asian
2017	APPA-REAL [36]	7,591 samples; 7,000+ subjects		√	0-95 (real age)	Caucasian: 6,686; Asian: 674; Afro-American: 231

(C – captured or collected in a controlled environment; UC – captured or collected in an uncontrolled environment)

TABLE II. ETHNIC COUNT (BASED ON TABLE I)

Ethnic Count	Subjects (Approx. ≈)
White	7760
Black	320
Asian	799
Others	825

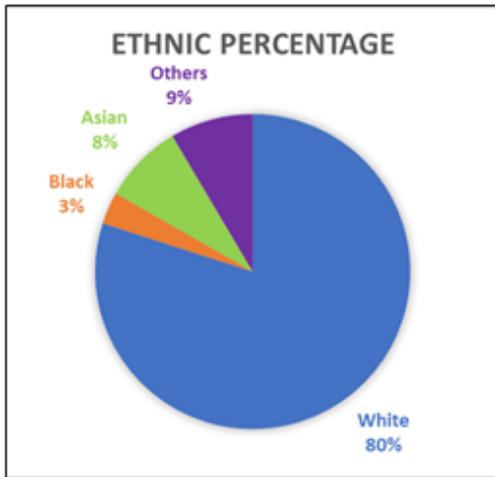


Fig. 3. Ethnic Percentage from All Databases (Based on known Data from Table I).

Some studies, however, have collected particular ethnic subjects with age information, such as Bastanfard A. et al. (Iranian face database) [15]; Setty S. et al. (Indian Movie Face database - IMFDB) [16]; and Niu Z. et al. (Asian Face Age Dataset - AFAD) [17]. Furthermore, there are ethnic-specific databases that can be used for face age research (see Table I coloured in grey). However, no studies have used these databases for deep learning age estimation research in the past six years; these databases are either not considered benchmark databases or less known by the face age estimation community.

V. FACE AGE DATABASE ESTIMATION MODEL

In one of the earliest face age model studies, Kwon and Lobo [18] classified age into three categories: infant, adult, and senior, and used simple feature extraction and machine learning for face age classification. Subsequently, computer science and pattern recognition researchers introduced various age classification/estimation methods [19, 20]. Earlier machine learning methods typically included one (or more) feature extractor and one (or more) age classifier (or estimator). The feature extractors can be holistic (e.g. whole facial shape), local (e.g. aging wrinkle), or both. The selection of feature extractors is influenced by the database used, with most of the sample quantity used by these methods being less than that of the deep learning approach.

Previous machine learning approaches can produce precise estimation (or classification) using just one or two databases, but are confined to those databases and could give an erroneous estimation if a wild sample is used for testing instead. Moreover, it is difficult for most machine learning approaches

to analyse unstructured data; they require additional tasks to divide the problem and later recombine the results to form a conclusion, which takes time and resources. Nevertheless, the deep learning method's known capability and strength have shifted the face aging system approach.

A. Deep Learning Approach

The rise of deep learning in image processing and machine learning has also impacted face age estimation. Better age estimation performance is strictly associated with the depth of the used network in the deep learning method, and it has become the generalist network adopted for feature extraction, including deep architectures that require a considerable amount of image samples, such as AlexNet, VGG-Net, VGG-Face, GoogLeNet, and Residual Networks (ResNet) [37]. VGG-Net has been reported to be one of the most effective deep learning architectures for age estimation. Notwithstanding, new studies continue to propose deep architecture designs for improving model accuracy when processing a sample of subjects' faces captured in an uncontrolled environment.

Deep learning face age research can be classified into three types: 1) classification age (CA) - classify the face age with several classes equal to the number of the considered age groups; 2) estimation age (EA) - estimate age using a regressor; and 3) distribution age (DA) - a modified CA strategy obtained by substituting the one-hot encoding vector with a statistical distribution centred on the estimated age [37]. Furthermore, the deep learning approach is much more accurate than other older machine learning methods at estimating age from sample images captured in the wild (uncontrolled environment). Nevertheless, if the subject's ethnicity in the dataset is not considered, the ethnic bias will persist.

B. Deep Learning Model Method and Ethnicity Bias in Database

When searching for papers on face age research, this study focused on research that used the deep learning method from 2015-2020. Deep learning has the potential to revolutionise computer science and machine learning. Furthermore, data biases are becoming more important with the rise of more powerful machine learning, which deep learning takes advantage of when dealing with large amounts of data. The search was conducted using a variety of web search engines, including Google Scholar and Web of Science.

Table III displays the search results, which include the following information: publisher, year of publication, network architecture, domain area, selected databases, and ethnicity consideration. From 2015-2016, the most commonly used network architectures were well-known general architectures such as GoogleNet, VGG-Net, and DCNN (or Deep-CNN). As the year progressed, an increasing number of studies began to design the architectural network or modify the general CNN network architecture to fit their research objectives. As a result, the network design became more complex to produce a more accurate novel model (e.g. by combining multiple CNN networks to create a hybrid network). In the research domain area, there have been 33 EA studies, 20 CA studies, and only 8 DA studies. However, there is no significant preference between the research domain and databases used in the studies.

Therefore, it can be inferred that most of these databases can be used in all deep learning areas: EA, CA, and DA.

TABLE III. DEEP LEARNING FACE AGE RESEARCH AREA AND AGE DATABASES USED FOR TRAINING AND TESTING (FROM 2015-2020)

Ref.	Publisher	Year	Network Architecture	Domain Area			Database Model										Account Ethnic
				CA	DA	EA	M	C15	I	A	F	C16	W	G	P	O	
[38]	IEEE	2015	GoogLeNet		√	√	√	√					√			√	No
[39]	IEEE	2015	VGG-Net	√				√	√								No
[40]	IEEE	2015	GoogLeNet			√	√	√		√	√		√			√	No
[41]	IEEE	2015	VGG-Net & GoogleNet			√		√									No
[42]	IEEE	2015	VGG-Net & Novel arch.		√		√	√		√	√				√		No
[43]	IEEE	2015	DLA			√	√				√						No
[44]	IEEE	2015	Tree kernel adaptive CNN			√	√					√					No
[45]	Elsevier	2015	LeNet			√	√								√		No
[46]	IEEE	2015	Novel arch.	√						√							No
[47]	IEEE	2015	DCNN-H-3NNR			√	√	√		√							No
[48]	IEEE	2016	DCNN			√		√		√	√			√			No
[49]	IEEE	2016	VGG-Net			√						√					No
[50]	IEEE	2016	Novel arch.	√			√									√	No
[51]	IEEE	2016	VGG-Net			√	√										No
[52]	IEEE	2016	Compact-CNN			√	√								√	√	Yes
[53]	Elsevier	2016	DCNN	√										√			No
[54]	IEEE	2016	GilNet; AlexNet; VGG-Net	√						√							No
[55]	IEEE	2016	VGG-Net	√	√			√	√							√	No
[56]	IEEE	2016	DADL		√			√*	√			√**					No
[57]	IEEE	2016	VGG-Net	√				√	√			√					No
[58]	IEEE	2016	VGG-Net	√					√			√					No
[59]	IEEE	2016	DCNN	√						√						√	No
[60]	IEEE	2016	Novel arch.		√		√				√					√	No
[61]	IEEE	2017	AGEn & MO-CNN	√			√	√	√		√	√				√	No
[62]	IEEE	2017	Multitask CNN			√	√	√	√	√	√						No
[63]	IEEE	2017	ODFL & ODL	√			√	√			√						No
[64]	Elsevier	2017	GA-DFL	√			√	√			√						No
[65]	Elsevier	2017	VGG-Net CNN+LDAE		√		√		√		√	√			√		No
[66]	Elsevier	2017	Novel arch.	√	√	√	√						√				Yes
[67]	Elsevier	2017	D2C			√	√					√					No
[68]	PMLR	2017	R-SAAFc2			√		√*	√	√	√			√			No
[69]	IEEE	2017	Deep-ROR	√					√	√							No
[70]	IEEE	2017	DMTL			√	√									√	Yes
[71]	IEEE	2017	M-LSDFL	√			√	√	√	√	√		√	√			No
[72]	IEEE	2017	DMTL			√	√	√	√							√	Yes
[35]	Springer	2018	VGG-Net	√			√	√	√	√	√					√	No
[73]	IEEE	2018	VGG-Net-GPR			√	√	√	√							√	Yes
[74]	IEEE	2018	ELM			√	√		√	√		√					Yes
[75]	ALM-DL	2018	ScatNet	√												√	No
[76]	IEEE	2018	CMT-deep network			√	√				√		√				No
[77]	Elsevier	2018	DAG-CNNs			√	√		√		√						No
[78]	Springer	2019	CNN+triplet ranking	√		√	√			√						√	No
[79]	Elsevier	2019	DeepAge			√	√			√							No
[80]	IEEE	2019	SADAL			√	√			√							No
[81]	IEEE	2019	Novel Arch.			√		√									No
[82]	IEEE	2019	Multitasks-AlexNet			√			√							√	No
[83]	IEEE	2019	ODFL & ODL			√	√	√			√					√	No
[84]	IEEE	2020	SADAL & VDAL			√	√	√			√						No
[85]	Elsevier	2020	LRN		√	√	√	√								√	Yes
[86]	IEEE	2020	CR-MT	√		√	√						√			√	No
[87]	SYMMETRY	2020	MA-SFV2	√		√	√				√						No
[88]	IEEE	2020	DOEL-groups			√	√	√	√		√					√	No
[89]	IEEE	2020	MSFCL			√	√	√		√	√					√	No

(CA – Classification Age; DA – Distribution Age; EA – Estimation Age; M – MORPH; C15 - ChaLearn2015; I – IMDB+WKI; A – Adience; F – FG-NET; C16 - ChaLearn2016; W – Webface; G – GROUP; P – Private DB; O – Others; *√* - variation of ChaLearn2015; **√** - variation of chalearn2016).

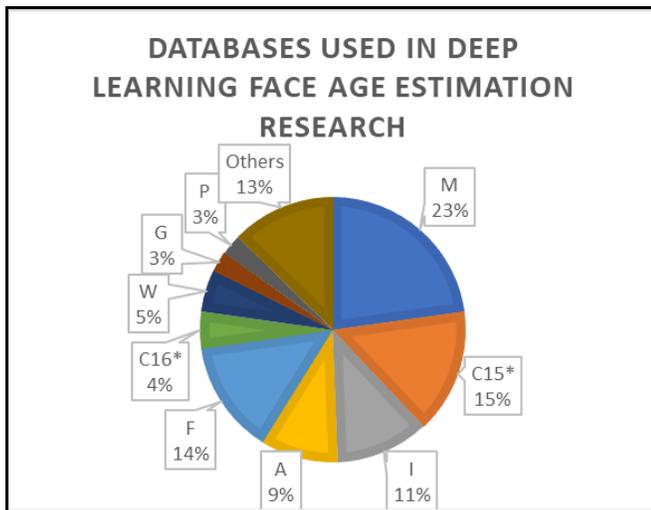


Fig. 4. Breakdown of Databases used in Deep Learning Face Age Estimation Research (based on Table III). ‘*’ Means that there are Multiple Versions of the Databases Included in the Count (M – MORPH; C15 - ChaLearn2015; I – IMDB+WIKI; A – Adience; F – FG-NET; C16 - ChaLearn2016; W – Webface; G – GROUP; P – Private DB)

Meanwhile, Fig. 4 depicts the most commonly used databases for face age research (derived from Table III), indicating that MORPH [25] is the most commonly used database because it has the highest sample count (55,134 samples) captured in a controlled environment. Because of this advantage, the MORPH database is the best benchmark database for comparing the CNN model performance with other models since it can lessen the influence of unwanted factors that may affect the overall estimation results. The MORPH database, on the other hand, has an unbalanced ratio of races in its dataset (refer to Table I), which can lead to ethnic bias when estimating age.

The second most used face age database is ChaLearn2015 [32], which was explicitly developed for the ICCV 2015 ChaLearn Looking at People Apparent Age Estimation Challenge [32]. This challenge event was a competition to build the best appearance age estimation model, and most of the authors of the research surveyed in this study competed in it. ChaLearn2016 [33], the fifth most used database, is the second/expanded version of the ChaLearn2015 database. The lack of ethnicity records for subjects in both ChaLearn databases makes analysing the effect of ethnicity on a model's overall performance difficult, even though both databases have a diverse set of races.

The FG-NET [22] database comes in third place, with images captured in uncontrolled real-life conditions that are not equally distributed across age groups and has the lowest

samples (1,002 samples) compared to other databases. FG-NET has been used in face age research since around 2005 [5], making it one of the most well-known databases used primarily for comparing model performance in the face age research community. Despite this, the majority of its subjects are Caucasians/Whites. When used in the CNN model, a small dataset should be fine-tuned or pre-trained with another database with large sample size, such as IMDB+WIKI. The IMDB+WIKI [35] dataset contains images with one or more people in them, as well as annotations for researchers' reference when there are multiple people in one image. However, there is no proper explanation for which annotation refers to which person in the image of multiple people. Therefore, studies primarily use this database for pre-training deep networks due to its large sample size. Because of the lack of annotation, no model performance results for IMDB+WIKI are shown in Table IV, which reveals the model performance on studies based on their selected databases. Although the IMDB+WIKI database samples contain multiple ethnicities, no annotation for a subject's ethnicity is available.

Adience [30], a database for gender and age group classification, comes in fourth place, with subjects drawn from real-world conditions. Its sources are mostly Flickr albums uploaded from smartphone devices. This database was made available to the general public under the Creative Commons (CC) licence. Meanwhile, in fifth place is Webface [29], a database collected for the experiments of a PhD thesis, and in sixth place is GROUP [27], a collection of images of people captured in a group (hence the name) that includes age group and gender information. Nevertheless, none of these three databases has a record of the subject's ethnicity.

Although some studies used/included their own database, these private databases [42, 52, 55, 65] contain no information about the subject's ethnicity. Furthermore, some of them were only used to fine-tune network models [55], [65]. CACD [31], LIFESPAN [23], LFW [90], FACES [28], FRGC [24], AFAD [17], and FERET [21] are the remaining databases used in the age model. Only a few of these were used in the face age deep learning research (categorised as 'Others' in Table III).

Meanwhile, some of the studies used a different database for pre-training their models (e.g. face detection in images) than the one used for age estimation, such as the CelebFaces Attributes (CelebA) [91] and ImageNet databases [92]. The CelebA database was built using the CelebFaces [91] face verification database with face attribute annotations. ImageNet, on the other hand, is a database for object classification and detection. Both databases lack age information and were primarily used for pre-training/fine-tuning the network model in these studies [39, 52, 57, 69, 70, 74].

TABLE IV. SUMMARY OF BEST CNN MODEL PERFORMANCE ON SELECTED DATABASES (FROM 2015-2020)

Ref.	Year	Best CNN Model Performance on Selected Databases <i>Database_used(performance_measurement)</i>	Account Ethnic
[38]	2015	C15(MAE = 3.33); C15-testset(e-error = 0.27)	No
[39]	2015	C15-validset(MAE = 3.22); C15-testset(e-error = 0.260)	No
[40]	2015	C15-validset(e-error = 0.309); C15-testset(e-error = 0.290)	No
[41]	2015	C15-validset(MAE = 3.29; e-error = 0.285); C15-testset(e-error = 0.287)	No
[42]	2015	C15-validset(e-error = 0.338); C15-testset(e-error = 0.306)	No

[43]	2015	M(MAE = 4.77); F(MAE = 4.26)	No
[44]	2015	M(MAE = 3.61); W(MAE = 7.27)	No
[45]	2015	M(MAE = 3.88); FRGC(MAE = 3.31)	No
[46]	2015	A(AEM = 50.7±5.1, AEO = 84.7±2.2)	No
[47]	2015	C15-validset(e-error = 0.359); C15-testset(e-error = 0.373)	No
[48]	2016	A(AEM = 52.88±6%, AEO = 88.45±2.2); C15-validset(e-error = 0.297)	No
[49]	2016	C16-validset(MAE = 3.85, e-error = 0.330); C16-testset(e-error = 0.370)	No
[50]	2016	M(MAE = 3.27); AFAD(MAE = 3.34)	No
[51]	2016	M(MAE = 3.45)	No
[52]	2016	M(MAE = 3.23); P(acc. = 88%)	Yes
[53]	2016	G(AEM = 56%, AEO = 92%)	No
[54]	2016	A(mean AEM = 57.9%)	No
[55]	2016	C15-validset(e-error = 0.261); C15-testset(e-error = 0.241)	No
[56]	2016	C15-validset(MAE = 1.76, e-error = 0.134); C15-testset(e-error = 0.321)	No
[57]	2016	C16-validset(e-error = 0.240); C16-testset(e-error = 0.336)	No
[58]	2016	C16-testset(e-error = 0.367)	No
[59]	2016	A(acc. = 42%); FERET(acc. = 86.4%)	No
[60]	2016	M(MAE = 2.78); F(MAE = 2.80)	No
[61]	2017	M(MAE = 2.52); F(MAE = 2.96); CACD (ave. MAE = 4.68); C15-validset(MAE = 3.21, e-error = 0.28); C15-testset(MAE = 2.94, e-error = 0.264); C16-testset(MAE = 3.82, e-error = 0.310)	No
[62]	2017	F(MAE = 2.00); C15-validset(e-error = 0.293)	No
[63]	2017	M(MAE = 2.92); F(MAE = 3.71); C15-validset(MAE = 3.95, e-error = 0.312)	No
[64]	2017	M(MAE = 3.25); F(MAE = 3.93); C15-validset(MAE = 4.21, e-error = 0.369)	No
[65]	2017	F(MAE = 2.84); M(MAE = 2.35); P(MAE = 4.33); C16 (e-error = 0.241)	No
[66]	2017	M(ave. MAE = 2.96); W(ave. MAE = 5.75)	Yes
[67]	2017	M(ave. MAE = 3.06); W(ave. MAE = 6.104)	No
[68]	2017	F(MAE = 3.01 MAE); A(AEM = 67.3, AEO = 97.4)	No
[69]	2017	A(AEM = 67.34 ± 3.56%, AEO = 97.51 ± 0.67%)	No
[70]	2017	M(acc. = 85.30 ± 0.6%)	Yes
[71]	2017	M(MAE = 2.89); F(MAE = 3.31); A(AEM = 60.20±5.3%, AEO = 93.70± 2.3%); C15-validset(e-error = 0.315)	No
[72]	2017	M(MAE = 3.00); LFW(MAE = 4.50)	Yes
[35]	2018	M(MAE = 2.68); F(MAE = 3.09); CACD(MAE = 4.79); A(AEM = 64.00±4.2%, AEO = 96.60±0.9%)	No
[73]	2018	M(MAE = 2.93); CACD (MAE = 5.22); C15-validset(MAE = 3.30, e-error = 0.290)	Yes
[74]	2018	M(MAE = 2.61); A(AEM = 66.49 ± 5.08%); C16-validset(MAE = 3.67, e-error = 0.325); C16-testset(e-error = 0.368)	Yes
[75]	2018	LIFESPAN(MAE = 4.01); FACES (MAE = 5.95)	No
[76]	2018	M(MAE = 2.89); F(MAE = 3.43)	No
[77]	2018	M(MAE = 2.81); F(MAE = 3.05)	No
[78]	2019	M(MAE = 2.87); A(AEM = 63.10 ± 1%, AEO = 96.7 ± 0.4%)	No
[79]	2019	M(MAE = 2.87); F(MAE = 7.08)	No
[80]	2019	M(MAE = 2.75); F(MAE = 3.67)	No
[81]	2019	C15-testset(MAE = 6.031, e-error = 0.441)	No
[82]	2019	Wiki(MAE = 5.47); UTKFace(MAE = 9.54); AgeDB(MAE = 10.01)	No
[83]	2019	M(MAE = 2.92); F(MAE = 3.71); APPARENT-AGE(MAE = 3.95)	No
[84]	2020	M(MAE = 2.57); F(MAE = 2.98); C15(MAE = 3.58, e-error = 0.285)	No
[85]	2020	M(MAE = 1.90); C15-validset(MAE = 3.05, e-error = 0.274); MegaAge-Asian(CA(7) = 91.64)	Yes
[86]	2020	M(ave. MAE = 2.36); CACD(MAE = 4.48); Webface(MAE = 5.67)	No
[87]	2020	M(MAE = 2.68); F(MAE = 3.81)	No
[88]	2020	M(MAE = 2.75), F(MAE = 3.44); AgeDB(MAE = 5.69); C15-validset(MAE = 2.93, e-error = 0.258); C15-testset(MAE = 2.71, e-error = 0.247)	No
[89]	2020	M(MAE = 2.73); F(MAE = 2.71); A(AEM = 65.3%, AEO = 96.3%); MEGAAGE-ASIAN(MAE = 2.81, CA(3)(62.89%), CA(5)(82.46%))	No

M – MORPH; C15 – ChaLearn2015; A – Adience; F – FG-NET; C16 – ChaLearn2016; W – Webface; G – GROUPS. Note that other databases that are not shown in this table but shown in Table III (e.g. I – IMDB+WIKI) were used for pre-training by the studies.

C. Deep Learning Technique Strengths and Weaknesses

A review of the different deep learning architectural networks used in previous studies revealed several techniques that are frequently used for face age estimation. Table V summarises the network architectures frequently used in the age estimation studies reviewed, as well as their strengths and weaknesses. As previously stated, the main goal of deep learning face age estimation is to find the best method for learning the face aging features from a large sample of data and then use the information to distinguish the different ages of test subjects. Each study's architecture was chosen based on its

research aim and objectives, such as the problem(s) to solve that can help improve face age classification/estimation/distribution. The problems include face detection, landmark localisation, optimisation, regression, classification, feature extraction, residual learning part, sampling technique, layer size (depth and width), discriminative distance, learning speed, training and/or testing process and others. This study identified several known network architectures that were frequently used in comparison to the others [93]. Among these network architectures are the following:

TABLE V. SUMMARY OF NETWORK ARCHITECTURES MOSTLY USED BY AGE ESTIMATION STUDIES IN THIS SURVEY

Architecture	Background (referred from [93])	Learning Methodology	Strength	Weakness	Author(s) that Used the Architecture
LeNet	<ul style="list-style-type: none"> - Invented in 1998 by Yann Lecun. - First popular CNN architecture. 	Spatial exploitation	<ul style="list-style-type: none"> - Small and simple design. - A good introduction to neural networks for beginners. 	<ul style="list-style-type: none"> - Problem to detect all aging features. Require extensive training. - Speed and accuracy are outperformed by newer network architecture. 	[45]
AlexNet	<ul style="list-style-type: none"> - Introduced in 2012 at the ImageNet Large Scale Visual Recognition Challenge. - Uses ReLu, dropout and overlap pooling. - First major CNN model that used GPUs for training. 	Spatial exploitation	<ul style="list-style-type: none"> - Using GPUs for training leads to faster training of models. - ReLu helps lessen the loss of features and improve model training speed. 	<ul style="list-style-type: none"> - Authors require to find design solutions on how to compete with other newer network architectures that are more accurate and faster. 	[54, 82]
VGG-Net	<ul style="list-style-type: none"> - Visual geometric group (VGG) was introduced in 2014. - It groups multiple convolution layers with smaller kernel sizes. 	Spatial exploitation	<ul style="list-style-type: none"> - Homogenous topology. - Smaller kernels. - Good architecture for benchmarking face age estimation - Pre-trained networks for VGG-Net are freely available. 	<ul style="list-style-type: none"> - Computationally expensive as more layer increases. - Face age estimation studies need to consider the vanishing gradient problem to improve the estimation performance. 	[35, 39, 42, 49, 51, 54, 55, 57, 58, 65, 73]
GoogleNet	<ul style="list-style-type: none"> - Researchers at Google introduced GoogleNet in 2014. - Introduced block concept. - Split transform and merge idea. - In a single layer, multiple types of 'feature extractors' are present to help the network perform better. 	Spatial exploitation	<ul style="list-style-type: none"> - Trains faster than VGG-Net. - Smaller pre-trained size than VGG-Net. - Training network has many options to solve tasks. 	<ul style="list-style-type: none"> - Heterogeneous topology design require face age estimation studies to make thorough customisation - from module to module. 	[38, 41, 43]
ResNet	<ul style="list-style-type: none"> - Introduced in 2015. - Residual learning. - Identity mapping-based skip connections. 	Depth + multi-path	<ul style="list-style-type: none"> - Capable of skipping learned feature(s), reducing training time and improve accuracy. - Solve the vanishing gradient problem faced by VGG-Net. - Possible to train very deep networks and generalise well. 	<ul style="list-style-type: none"> - Computationally expensive as more layer increases. 	[69, 71]
Novel Arch.	<p>Most designs were expanded/modified/or built from scratch based on the previously available architectures (e.g. AlexNet, VGG-Net, etc.)</p>	-	<ul style="list-style-type: none"> - Specialise in learning face representation for different ages. - Improving several parts of the network based on the study's aim and objectives. 	<ul style="list-style-type: none"> - Cater to a very specific problem(s). - Time-consuming when building from scratch. 	[42, 43, 44, 46, 47, 48, 50, 52, 53, 54, 56, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 71, 72, 73, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 84, 85, 86, 87, 88, 89]

1) *LeNet*: Yann Lecun invented the LeNet architecture in 1998 to perform optical character recognition (OCR), and its design is smaller and simpler than the rest of the network architectures. For beginners, this network is a good way to learn neural networks and can be used for face age estimation studies, such as in [45]. However, due to its simple design, the network requires additional improvement that the designer must build from scratch if used for face age estimation. It is also outclassed by newer models in terms of speed and accuracy when used as is, with no modifications.

2) *AlexNet*: Alex Krizhevsky introduced the AlexNet architecture in 2012, and it was the first major CNN model to use graphics processing units (GPUs) for training, which aided in training speed. Meanwhile, ReLU, dropout and overlap pooling were used to reduce feature loss and improve training speed. This architecture design was used in [54], [82] for face age classification and estimation, respectively. Their accuracy performance, however, was inferior to that of the model that used the LeNet network design [45] (see Table IV). This implies that, even though AlexNet is a newer network than LeNet, proper modification, structuring, and organisation of the AlexNet network are still required to achieve the best face age estimation (or classification) performance.

3) *VGG-Net*: Introduced in 2014, the VGG model improves training accuracy by improving its depth structure. The addition of more layers with smaller kernels increases nonlinearity, which is good for deep learning. This study discovered that VGG-Net is the most commonly used network model among the many available (11 papers). One of the possible explanations is that the VGG pre-trained networks are freely available online. Although it is the best architecture for benchmarking on the face age estimation task, the performance obtained by studies that used this model is not the best, but it is also not the worst. This could be due to the vanishing gradient problem, one of the main challenges faced when using VGG-Net, which occurs when the number of layers exceeds 20, causing the model to fail to converge to the minimum error percentage. When this happens, the learning rate slows to the point where no changes are made to the model's weights. Furthermore, using VGG-Net can be time-consuming because the training process can exceed a week, especially if it was built from scratch. As a result, when using the VGG-Net network for face age estimation, users must address the vanishing gradient problem as well as the training time.

4) *GoogleNet*: A class of architecture designed by Google researchers that won ImageNet 2014. Instead of a sequential architecture design, GoogleNet opted for a split transform and merge design, in which a single layer can have multiple types of "feature extractors". In addition, GoogleNet has a smaller pre-trained size and trains faster than VGG-Net [93]. One drawback of GoogleNet is that almost every module must be customised. As a result, when designing a face age estimation using GoogleNet, users must customise from module to

module. This study discovered that only [38, 40, 41] used this network architecture.

5) *ResNet*: ResNet was introduced in 2015 and provides residual learning to help solve the vanishing gradient problem (from the VGG-Net architecture). Furthermore, ResNet can have a deeper network (more layers) than VGG-Net while avoiding performance degradation. ResNet is a concept in which if a feature has already been learned, it can be skipped and focus can be given to newer features, thereby improving training time and accuracy. On the other hand, the ResNet structure design is primarily concerned with how deep the structure should be. If ResNet is chosen for face age estimation, the designer must consider how the network should be structured to learn multiple aging features. Adding more layers is one of the common ideas. However, this could result in a longer learning time for the model (it can take several weeks); therefore, the designer must also account for this. This study discovered that only a few face age estimation studies used Resnet architecture/concept in their design [69, 71].

6) *New Arch*: Is a network architecture created by expanding previous architectures, modifying them, or building the network from scratch. These architectures were created specifically to find the best network approach for learning how to best estimate age. For example, a facial image with a specific age can be affected by facial variations caused by external factors, such as lighting, which can lead to a neighbouring age category being predicted as the final bias. The study in [80] attempted to address this problem by proposing a network composed of a generator that could generate discriminative hard-examples (taken from extracted features done by a deep CNN) to complement the training space for robust feature learning and a discriminator that could determine the authenticity of the generated sample using a pre-trained age ranker [80]. This approach offers designers the 'freedom' to create the best solution to a given problem. The designs can be based on available networks and further modified to their preferences, rather than being limited to the original design architecture. This study found that most of the previous studies, particularly those conducted in 2020, tend to propose their own architectural network design. However, one major drawback of this design approach is that the designer may take a long time to modify/create networks when compared to using available networks.

D. Model Performance Evaluation

Multiple protocols and performance calculations were used in the studies to evaluate model performance. Table IV shows the performance of the CNN models used in the studies on the databases that they were tested on. The evaluation protocol is a method for studies to determine the optimal number of training and testing datasets for their chosen databases. Meanwhile, the performance calculation allows studies to compare the estimation/classification/ distribution accuracy of their own model to that of others. Because of the numerous ways for designing protocols and performance calculations, problems

arise when performance is compared on the same database but using different evaluation methods, resulting in a unanimous 'agreement' from most of the studies that specific performance calculation(s) should be used for comparison's sake for a specific database. Among the performance calculations used to evaluate the accuracy of the face age deep learning model are:

1) *Mean absolute error (MAE)*: a widely used performance evaluation for age estimation studies that measures the error between the predicted and actual ages. MORPH, FG-NET, ChaLearn2015, and ChaLearn2016 are examples of databases that used this evaluation method. The model performance improves as the MAE value decreases.

2) *E-Error*: is the performance calculation used in apparent age estimation. This evaluation metric was used to compare the performance of studies that used ChaLearn2015 [32] and ChaLearn2016 [33] datasets. The lower the e-Error, the better the performance.

3) *Accuracy of an exact match (AEM)*: a method of calculating accuracy that calculates the percentage of correctly estimated/classified age per the total number of test images used. This type of evaluation metric was used by the Adience database. The higher the AEM value, the better the performance. Some studies went so far as to include the standard deviation value in their evaluation.

4) *Accuracy error of one age category (AEO)*: Is another type of evaluation metric used on the Adience database, in which errors of one age group are also included as correct age classifications. The higher the AEO value obtained, the better the overall model performance.

5) *Cumulative score (CS)*: is defined as the percentage of images with an error of no more than a certain number of years. The evaluation is usually shown as a curve on a graph (which is not depicted in this paper), with the x-axis representing the error level in years and the y-axis representing the cumulative score (in percentage value). This type of evaluation performance was sometimes combined with the MAE evaluation method in studies that used MORPH, FG-NET, and other earlier year databases. Meanwhile, studies that used the MegaAge-Asian database present some of their results in terms of $CA(\theta)$, where θ is the allowable age error corresponding to the cumulative accuracy, which several of them are shown in Table IV.

Because the studies reviewed from 2015-2020 (see Table IV) used different databases, analysing and comparing their performance progress was difficult. Therefore, only the most frequently used databases were chosen and averaged to create a line chart depicting the performance progress of face age research from 2015-2020. Fig. 5 illustrates the average yearly performance for two different databases: MORPH and FG-NET. As shown in Fig. 5, the MAE values for the MORPH database decreased from 2015-2020, but not for FG-NET. The chart may imply that models applied to the MORPH database improved over six years, whereas FG-NET did not. Table VI shows the average MAE and its standard deviation for each

year; the improvement might be valid for MORPH since most of the standard deviation obtained is low (< 0.3). However, the implication for FG-NET may be invalid because only a few studies used this database in 2015-2016. Most of the standard deviation for 2017-2020 is high (> 0.4), meaning that the MAE results obtained by the different studies are too wide apart. Among other databases, the performance of the MOPRH database appears to be the best. The samples captured in a controlled environment help the models to better identify aging features because unwanted factors are absent (e.g occlusion). Meanwhile, the low quantity (1,002 images) and low quality (old images captured in an uncontrolled environment) samples of FG-NET might hinder the CNN model learning process in the studies. Nonetheless, some studies were able to obtain low MAE values using the FG-NET database: [62] MAE = 2.00 and [89] MAE = 2.71.

Regarding publishers, from 2015-2020 (see Fig. 6), IEEE is the publisher with the highest reviewed papers in this study. Elsevier is in second place, and Springer is in third. The bar chart in Fig. 6 shows that the number of published papers increased in 2016, but then declined until 2018, and then remained relatively low until 2020. The figure seems to imply that the deep learning approach is becoming less attractive to the face age research community, but this is most likely not the case. When a more robust, advanced, and practical deep learning technique becomes available, a resurgence may occur.

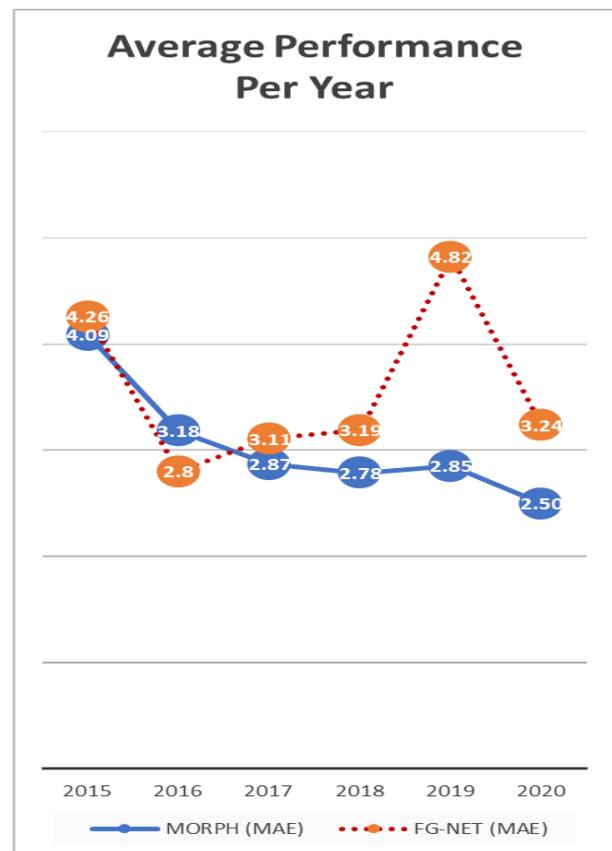


Fig. 5. Line Chart Shows Face Age Research's Performance Progress from 2015-2020 for MORPH and FG-NET (based on Table VI).

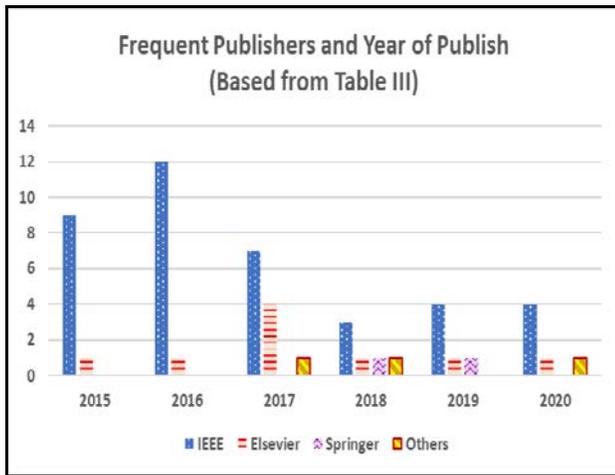


Fig. 6. Publishers and Frequency of Publication of Deep Learning Face Age Estimation Papers, Including Publication Year (based on Table III).

TABLE VI. PERFORMANCE PROGRESS OF FACE AGE RESEARCH FROM 2015-2020 FOR MORPH AND FG-NET DATABASES

Year	MORPH	FG-NET
	MAE (std. deviation)	MAE (std. deviation)
2015	4.09 (0.61)	4.26 (-)
2016	3.18 (0.28)	2.8 (-)
2017	2.87 (0.29)	3.11 (0.63)
2018	2.78 (0.14)	3.19 (0.21)
2019	2.85 (0.07)	4.82 (1.96)
2020	2.50 (0.33)	3.24 (0.49)

VI. OPEN ISSUES

As mentioned in the facial aging section, different ethnic subjects age differently, which means that a 20-year-old White subject would look older than a 20-year-old Asian. More research into the effects of ethnicity on face age estimation is needed. However, most studies focus only on primary aging features, such as face shape and aging wrinkles, and ignore secondary ones, such as racial facing aging traits. There are two possible reasons why studies did not take ethnic traits into account. The first is the perception that secondary aging features are non-essential for better model performance. A few CNN face age estimation studies have disproved the perception that race is unimportant. The second possible reason is that the lack of race variety in most databases causes researchers to overlook racial traits as one of the aging estimation problems in the first place.

Among papers reviewed, only seven considered ethnicity traits in the face age estimation experiment [52, 66, 70, 72, 73, 74, 85]. Studies in [52, 66, 70] considered ethnicity in the model learning performance and discovered that it does improve age estimation. However, these studies did not investigate the influence of racial traits on effectiveness in facial age estimation. Meanwhile, the study in [73] inferred that performance would improve if both gender and race information were included. Another study [74] discovered that gender and race could easily affect its age estimation model. Combining all of the age, gender, and race features further improved the age estimation performance of the model. Lastly, [85] explored the impact of ethnicity and gender on age

estimation, stating that having more samples for a specific ethnic can increase age estimation accuracy. These studies suggest that the CNN model can be further improved if the overall framework takes ethnicity into account first. When a large number of samples are available, CNN models perform better at discovering significant aging features, as this also improves the learning of racial aging traits.

Meanwhile, other studies on face age estimation that used machine learning rather than CNN have demonstrated the importance of ethnic aging traits. Ricanek et al. [94], for example, investigated the ethnicity of the subject and introduced the least angle regression (LAR) method, which was conducted on three databases: MORPH, FG-NET, and PAL, with five races included (African-American, Asian, Caucasian, Hispanic, and Indian). In another study, Akinyemi and Onifade [95] improved the performance of their model by incorporating ethnic parameters for African and Caucasian people into the GroupWise age ranking model. The FG-NET and FAGE databases were used in their experiment. FAGE is a locally collected dataset of 238 images of 209 black (African) individuals aged 0 to 41 years.

Shin et al. [96] presented an age estimation system that considered ethnic differences for Asians and Non-Asians using CNN and support vector machine (SVM). The proposed age estimation system outperformed the standard system when trained on an ethnicity-biased database. The study relied on LFW [90] and its samples, with Asians in the datasets consisting of Korean, Japanese, and Chinese web celebrities [96]. Several other studies, however, were unable to investigate their approach further due to a lack of multiple races in their datasets [94, 95, 96]. Hence, the importance of having more race variety in databases is demonstrated.

Table III shows that the databases in the deep learning age estimation model mostly favour Caucasian subjects. The race variety in the databases is imbalanced; in most databases, the Caucasian/White subjects are always the majority, while other races are either underrepresented or missing. Moreover, some of the databases with large samples and multiple races have no information on the subjects' ethnicity. There are only a few ethnic-specific databases, such as AFAD, IMFDB, and Iranian Face available. It would be beneficial to have more multiple ethnic databases with large samples and races that are evenly distributed.

VII. DISCUSSION AND SUGGESTION

The first problem to address is the negative perception that ethnicity is not a critical aging factor. Researchers should be informed more about the importance of ethnic traits in the aging face; thus, this paper aimed to raise awareness on this to others. Moreover, face age estimation research should be expanded; more researchers should consider the secondary aging traits when building CNN face age estimation models. The research scope should not be limited to primary aging features (face shape and aging wrinkles) but also expanded to secondary features that can help distinguish unique aging traits that occur only in specific races. One suggestion is to create a framework for organising different racial samples in a database before being used for a CNN model. The steps of the framework are as follow:

1) First, decide on the number of races to be included in the study and then collect as many samples as possible for each race while ensuring the samples are similar in quantity. This may require the creation of multiple databases with various ethnicities (e.g. using MORPH [25], IMFDB [16], Iranian face [15], and MEGAAGE-ASIAN [89] databases together). Because CNN would be the model approach, having a large sample size would not be an issue for the CNN learning process - it is required. The study must also decide whether to use all samples or specific ones based on the research aim and objective(s).

2) Next, apply the necessary image processing to the sample images, such as face detection, face landmark, and face alignment.

3) Each database's estimation performance is evaluated using an evaluation protocol. Multiple ethnic subjects from chosen databases are mixed and segregated into specific training and test sets when accounting for ethnicity in age estimation. The ethnic effect analysis requires two protocols: one that considers ethnicity and one that does not. The first protocol requires different ethnic subjects within these sets to be divided equally in quantity. Training and testing, for example, take up 80% and 20% of the total samples, respectively. When the samples are made up of two races (e.g. Caucasian and Asian), half of the training samples should be Caucasian and the other half should be Asian. Similarly with the test samples – half is Caucasian, and another half is Asian. The second protocol is similar to the first, except that the different ethnic subjects are split randomly rather than equally.

4) Afterwards, run the samples into the CNN model and analyse the result in terms of the ethnicity's effect on the overall age estimation. Search for any significant finding regarding the ethnicities traits that can be exploited in future age estimation studies.

Fig. 7 shows the proposed framework for studying CNN face age estimation while considering the ethnicities of the subjects. This framework can guide future face age estimation studies that use either the deep learning approach or the standard machine learning approach.

The review of the papers revealed that most studies did not consider using other ethnic-specific databases (e.g. Iranian [15], Indian [16]), even though these databases are available for use (see Table I). Benchmark databases like MORPH and FG-NET are more preferred because it is safer since these databases are frequently used and have long been used for comparison; thus, making it easy to perform comparative analysis. Nevertheless, using only the same benchmark databases and ignoring other available ethnic-specific databases can pose a risk, which will hinder the face age estimation research's progress in understanding the overall ethnic factor in facial aging process. Suppose various databases are continuously and increasingly used throughout the years. There will be enough results to allow meaningful comparison between studies, resulting in new benchmark databases that can be used and compared in the future.

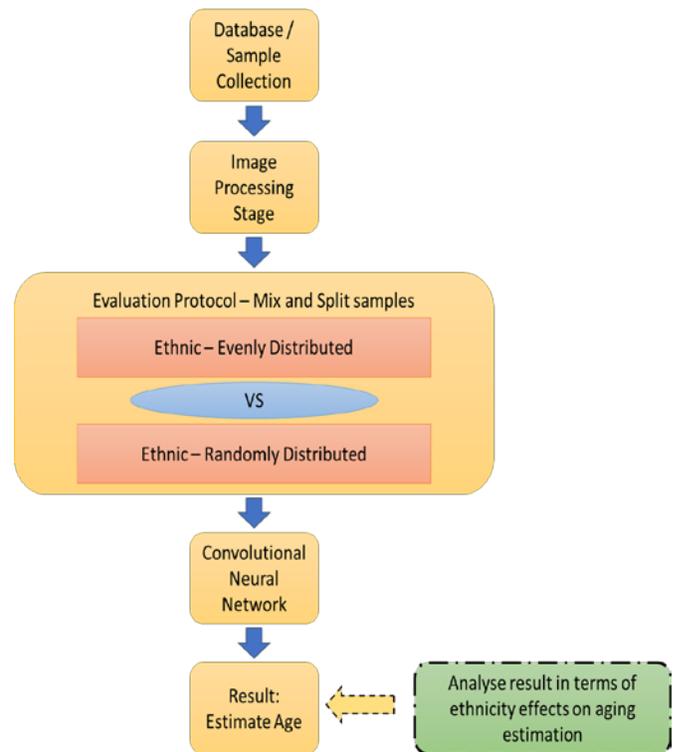


Fig. 7. Framework for Organising Different Racial Samples for CNN Face Age Estimation Study - Subject's Ethnicity Accounted for.

Although many public databases are available for face age estimation studies, very few are non-Caucasian/non-White databases. Accordingly, two suggestions could enable the collection of more ethnic-specific samples; either for private or public use:

1) Organise an ethnic-biased age estimation contest and develop an ethnic-specific dataset like how it was done for the ICCV 2015 ChaLearn [32] challenge dataset. This approach can help increase ethnic-biased age estimation studies from contestants and ethnic-specific database usage (e.g. AFAD, IMFDB, and Iranian database). These databases may become benchmark databases themselves later on.

2) In dangerous times, such as the current COVID-19 pandemic, most work and communication are now done online. Governments, businesses, educational institutions, medical institutions, and others are now using communication platforms for videoconferencing, online meetings, workspace chat, online classes, and even file sharing. One of the communication platform's primary functions is video streaming, which can accommodate up to nine people (or more) concurrently. This video streaming function allows researchers to organise a video conference for a group of volunteers to collect ethnic-specific samples for face age studies by capturing volunteers' face images during video streaming. Researchers must first decide whether to collect samples in a controlled/uncontrolled environment, for example, by requesting volunteers to standardise their background colours (use one colour) and stand still while researchers prepare to capture their faces (controlled

environment). Researchers must also decide whether to capture a single face image or multiple faces at once. However, the size and quality of the faces in the video may differ between users. Therefore, this should be taken into account when trying to use this approach to collect samples from volunteers, which can be co-workers or students (if the researcher is also an educator). Moreover, additional information about volunteers, such as their age and ethnicity, can be directly requested and recorded for research purposes. Microsoft Teams, Zoom, and Google Meet are some of the communication platforms that are available for use. Fig. 8 shows an example of captured face images using Microsoft Teams (single face or multiple faces).

When collecting samples, likely, some people would not be willing to help or give any personal information. Therefore, proper planning on target subjects selection before collecting their face images is required.



Fig. 8. Samples of Face Images - Captured using Microsoft Teams (Images taken from [97]).

It would be interesting to develop the suggested model framework with different ethnic races for face age recognition. Significant racial traits might be discovered, which can further distinguish the aging processes between different ethnic people. This discovery could further improve the understanding of racial aging traits, particularly concerning the face and the development of a model that can learn and identify those traits. Additionally, using the suggested sample collection method to collect and capture own samples may help ease the collection process. Aside from face age studies, the collected face images/samples can also be used for other facial image studies, such as emotion recognition and ethnic recognition. These suggestions, however, are beyond the scope of this study and will be considered in future research.

VIII. CONCLUSION

The analysis in this paper focused on ethnic consideration in the dataset used for the last six years for accurate age estimation using the deep learning approach. This paper specifically analysed 53 papers on deep learning face age estimation, model performance, selected databases, and whether or not any face ethnicity traits analysis was performed when estimating age. This paper also highlighted 19 database papers that promote the use of publicly available databases for age estimation research, as well as information on multiple database ethnicities. Although the deep learning approach improves face age estimation over time, it can be further enhanced by understanding how ethnicity affects face age estimation and designing an evaluation protocol that takes the subjects' ethnic traits into account. Moreover, a sizeable multi-racial database is needed for the investigation of aging in different ethnic groups. Therefore, it is crucial to collect the necessary information to create an extensive database with well-distributed age and ethnic labels. Suggestions for capturing samples were also provided to help researchers in increasing their ethnic-specific samples for private or public use.

IX. FUTURE DIRECTION

Making the collected ethnic-specific samples public and sharing them via web image collection sites can increase interest in conducting more ethnicity-based face age estimation research. More robust deep learning face age estimation models can be developed by performing more such studies, sample collection, and analyses in the future. Future research could also discover significant racial traits that could help distinguish unique aging patterns used to solve racial face age estimation problems in real-life applications. Proper planning and key considerations must be made when collecting samples, such as ensuring personal data privacy or a subject's consent. Additionally, it would be good to reiterate the benefit of having more samples for studies beyond facial age recognition.

ACKNOWLEDGMENT

The authors are grateful to the Faculty of Information Science and Technology, The National University of Malaysia, for supporting and contributing to this study; under the grant code GGPM-2019-038.

REFERENCES

- [1] N. A. Vashi, M. B. D. C. Maymone, & R. V. Kundu, "Aging differences in ethnic skin," *The Journal of clinical and aesthetic dermatology*, vol. 9, no. 1, pp. 31, 2016.
- [2] Y. Shirakabe, Y. Suzuki, & S. M. Lam, "A new paradigm for the aging Asian face," *Aesthetic plastic surgery*, vol. 27, no. 5, pp. 397-402, 2003.
- [3] A. E. Brissett, & M. C. Naylor, "The aging african-american face," *Facial Plastic Surgery*, vol. 26, no. 2, pp. 154-163, 2010.
- [4] M. O. Harris, "The aging face in patients of color: Minimally invasive surgical facial rejuvenation—A targeted approach," *Dermatologic therapy*, vol. 17, no. 2, pp. 206-211, 2004.
- [5] M. G. Rhodes, "Age estimation of faces: A review," *Applied Cognitive Psychology: The Official Journal of the Society for Applied Research in Memory and Cognition*, vol. 23, no. 1, pp. 1-12, 2009.
- [6] M. S. Zimble, M. S. Kokoska, & J. R. Thomas, "Anatomy and pathophysiology of facial aging," *Facial plastic surgery clinics of North America*, vol. 9, no. 2, pp. 179-87, 2001.
- [7] N. Ramanathan, R. Chellappa, & S. Biswas, "Age progression in human faces: A survey," *Journal of Visual Languages and Computing*, vol. 15, 3349-3361, 2009.
- [8] G. Y., Guo, & T. S. Huang, "Age synthesis and estimation via faces: A survey," *IEEE transactions on pattern analysis and machine intelligence*, vol. 32, no. 11, pp. 1955-1976, 2010.
- [9] R. Russell, et al. "Facial contrast is a cue for perceiving health from the face," in *Journal of Experimental Psychology: Human Perception and Performance*, vol. 42, no. 9, pp. 1354, 2016.
- [10] C. Trojahn, G. Dobos, A. Lichterfeld, U. Blume-Peytavi, & J. Kottner, "Characterizing facial skin aging in humans: disentangling extrinsic from intrinsic biological phenomena," in *BioMed research international*, 2015.
- [11] M. S. Zimble, M. S. Kokoska, & J. R. Thomas, "Anatomy and pathophysiology of facial aging," *Facial plastic surgery clinics of North America*, vol. 9, no. 2, pp. 179-87, 2001.
- [12] T. Igarashi, K. Nishino, & S. K. Nayar, "The appearance of human skin: A survey," *Foundations and Trends® in Computer Graphics and Vision*, vol. 3, no. 1, pp. 1-95, 2007.
- [13] N. A. Vashi, M. B. D. C. Maymone, & R. V. Kundu, "Aging differences in ethnic skin," *The Journal of clinical and aesthetic dermatology*, vol. 9, no. 1, pp. 31, 2016.
- [14] Stock photo caucasian baby. 2021. Crello. [online] Available at: <<https://crello.com/unlimited/stock-photos/166742418/stock-photo-caucasian-baby/>> [Accessed 22 July 2021].
- [15] A. Bastanfard, M. A. Nik, & M. M. Dehshibi, "Iranian face database with age, pose and expression," in *Machine Vision*, pp. 50-55, 2007.
- [16] S. Setty, et al., "Indian movie face database: a benchmark for face recognition under wide variations," in *2013 Fourth National Conference on Computer Vision, Pattern Recognition, Image Processing and Graphics (NCVPRIPG)*, pp. 1-5, December, 2013.
- [17] Z. Niu, M. Zhou, L. Wang, X. Gao, & G. Hua, "Ordinal regression with multiple output cnn for age estimation," in *Proceedings of the IEEE conference on computer vision and pattern recognition*, pp. 4920-4928, 2016.
- [18] Y. H. Kwon & N. da Vitoria Lobo. "Age classification from facial images," *Computer vision and image understanding*, vol. 74, no. 1, pp. 1-21, 1999.
- [19] R. Angulu, J. R. Tapamo, & A. O. Adewumi. "Age estimation via face images: a survey," *EURASIP Journal on Image and Video Processing*, 2018, no. 1, pp. 42, 2018.
- [20] O. F. Osman, & M. H. Yap. "Computational intelligence in automatic face age estimation: A survey," *IEEE Transactions on Emerging Topics in Computational Intelligence*, vol. 3, no. 3, pp. 271-285, 2018.
- [21] P. J. Phillips, H. Wechsler, J. Huang, & P. J. Rauss, "The FERET database and evaluation procedure for face-recognition algorithms," *Image and vision computing*, vol. 16, no. 5, pp. 295-306, 1998.
- [22] A. Lanitis, C. J. Taylor, & T. F. Cootes, "Toward automatic simulation of aging effects on face images," in *IEEE Transactions on pattern analysis and machine intelligence*, vol. 24, no. 4, pp. 442-455, 2002.
- [23] M. Minear, & D. C. Park, "A lifespan database of adult facial stimuli," *Behavior Research Methods, Instruments, & Computers*, vol. 36, no. 4, pp. 630-633, 2004.
- [24] P. J. Phillips, et al., "Overview of the face recognition grand challenge," in *2005 IEEE computer society conference on computer vision and pattern recognition (CVPR'05)*, Vol. 1, pp. 947-954, June, 2005.
- [25] K. Ricanek, & T. Tesafaye, "Morph: A longitudinal image database of normal adult age-progression," in *IEEE 7th International Conference on Automatic Face and Gesture Recognition (FGR06)*, pp. 341-345, April, 2006.
- [26] Y. Fu & T. S. Huang, "Human age estimation with regression on discriminative aging manifold," in *IEEE Transactions on Multimedia*, vol. 10 no. 4, pp. 578-584, 2008.
- [27] A. C. Gallagher, & T. Chen, "Understanding images of groups of people," in *2009 IEEE Conference on Computer Vision and Pattern Recognition*, pp. 256-263, June, 2009.
- [28] N. C. Ebner, M. Riediger, & U. Lindenberger, "FACES—A database of facial expressions in young, middle-aged, and older women and men: Development and validation," *Behavior research methods*, vol. 42, no. 1, pp. 351-362, 2010.
- [29] S. Zheng, "Visual image recognition system with object-level image representation," *Doctoral dissertation*, 2012.
- [30] E. Eiding, R. Enbar, & T. Hassner, "Age and gender estimation of unfiltered faces," in *IEEE Transactions on Information Forensics and Security*, vol. 9, no. 12, pp. 2170-2179, 2014.
- [31] B. C. Chen, C. S. Chen, & W. H. Hsu, "Cross-age reference coding for age-invariant face recognition and retrieval," in *European conference on computer vision*, Springer, Cham, pp. 768-783, September, 2014.
- [32] S. Escalera, et al., "Chalearn looking at people 2015: Apparent age and cultural event recognition datasets and results," in *Proceedings of the IEEE International Conference on Computer Vision Workshops*, pp. 1-9, 2015.
- [33] S. Escalera, et al., "Chalearn looking at people and faces of the world: Face analysis workshop and challenge 2016," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 1-8, 2016.
- [34] S. Moschoglou, A. Papaioannou, C. Sagonas, J. Deng, I. Kotsia, & S. Zafeiriou, "Agedb: the first manually collected, in-the-wild age database," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops*, pp. 51-59, 2017.
- [35] R. Rothe, R. Timofte, & L. Van Gool, "Deep expectation of real and apparent age from a single image without facial landmarks," in *International Journal of Computer Vision*, vol. 126, no. 2-4, pp. 144-157, 2018.
- [36] E. Agustsson, et al., "Apparent and real age estimation in still images with deep residual regressors on appereal database," in *2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017)*, pp. 87-94, May, 2017.
- [37] V. Carletti, A. Greco, G. Percannella, & M. Vento, "Age from faces in the deep learning revolution," in *IEEE transactions on pattern analysis and machine intelligence*, 2019.
- [38] X. Liu, et al. "Agenet: Deeply learned regressor and classifier for robust apparent age estimation," in *Proceedings of the IEEE International Conference on Computer Vision Workshops*, pp. 16-24, 2015.
- [39] R. Rothe, R. Timofte, & L. Van Gool, "Dex: Deep expectation of apparent age from a single image," in *Proceedings of the IEEE International Conference on Computer Vision Workshops*, pp. 10-15, 2015.
- [40] Y. Zhu, Y. Li, G. Mu, & G. Guo, "A study on apparent age estimation," in *Proceedings of the IEEE International Conference on Computer Vision Workshops*, pp. 25-31, 2015.
- [41] Z. Kuang, C. Huang, & W. Zhang, "Deeply learned rich coding for cross-dataset facial age estimation," in *Proceedings of the IEEE International Conference on Computer Vision Workshops*, pp. 96-101, 2015.
- [42] X. Yang, et al. "Deep label distribution learning for apparent age estimation," in *Proceedings of the IEEE international conference on computer vision workshops*, pp. 102-108, 2015.

- [43] X. Wang, R. Guo, & C. Kambhampettu, "Deeply-learned feature for age estimation," in 2015 IEEE Winter Conference on Applications of Computer Vision, pp. 534-541, January, 2015.
- [44] S. Li, J. Xing, Z. Niu, S. Shan, & S. Yan, "Shape driven kernel adaptation in convolutional neural network for robust facial traits recognition," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition, pp. 222-230, 2015.
- [45] I. Huerta, C. Fernández, C. Segura, J. Hernando, & A. Prati, "A deep analysis on age estimation," Pattern Recognition Letters, vol. 68, pp. 239-249, 2015.
- [46] G. Levi, & T. Hassner, "Age and gender classification using convolutional neural networks," in Proceedings of the IEEE conference on computer vision and pattern recognition workshops, pp. 34-42, 2015.
- [47] R. Ranjan, S. Zhou, J. Cheng Chen, A. Kumar, A. Alavi, V. M. Patel, & R. Chellappa, "Unconstrained age estimation with deep convolutional neural networks," in Proceedings of the IEEE International Conference on Computer Vision Workshops, pp. 109-117, 2015.
- [48] J. C. Chen, A. Kumar, R. Ranjan, V. M. Patel, A. Alavi, & R. Chellappa, "A cascaded convolutional neural network for age estimation of unconstrained faces," in 2016 IEEE 8th International Conference on Biometrics Theory, Applications and Systems (BTAS), pp. 1-8, September, 2016.
- [49] F. Gurpinar, H. Kaya, H. Dibeklioglu, & A. Salah, "Kernel ELM and CNN based facial age estimation," in Proceedings of the IEEE conference on computer vision and pattern recognition workshops, pp. 80-86, 2016.
- [50] Z. Niu, M. Zhou, L. Wang, X. Gao, & G. Hua, "Ordinal regression with multiple output cnn for age estimation," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 4920-4928, 2016.
- [51] R. Rothe, R. Timofte, & L. Van Gool, "Some like it hot-visual guidance for preference prediction," in Proceedings of the IEEE conference on computer vision and pattern recognition, pp. 5553-5561, 2016.
- [52] Y. Yang, F. Chen, X. Chen, Y. Dai, Z. Chen, J. Ji, & T. Zhao, "Video system for human attribute analysis using compact convolutional neural network," in 2016 IEEE International Conference on Image Processing (ICIP), pp. 584-588, September, 2016.
- [53] Y. Dong, Y. Liu, & S. Lian, "Automatic age estimation based on deep learning algorithm," Neurocomputing, vol. 187, pp. 4-10, 2016.
- [54] G. Ozbulak, Y. Aytar, & H. K. Ekenel, "How transferable are CNN-based features for age and gender classification?" in 2016 International Conference of the Biometrics Special Interest Group (BIOSIG), pp. 1-6, September, 2016.
- [55] G. Antipov, M. Baccouche, S. A. Berrani, & J. L. Dugelay, "Apparent age estimation from face images combining general and children-specialized deep learning models," in Proceedings of the IEEE conference on computer vision and pattern recognition workshops, pp. 96-104, 2016.
- [56] Z. Huo, X. Yang, C. Xing, Y. Zhou, P. Hou, J. Lv, & X. Geng, "Deep age distribution learning for apparent age estimation," in Proceedings of the IEEE conference on computer vision and pattern recognition workshops, pp. 17-24, 2016.
- [57] M. Uricár, R. Timofte, R. Rothe, J. Matas, & L. Van Gool, "Structured output svm prediction of apparent age, gender and smile from deep features," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 25-33, 2016.
- [58] R. Can Malli, M. Aygun, & H. Kemal Ekenel, "Apparent age estimation using ensemble of deep learning models," in Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition Workshops, pp. 9-16, 2016.
- [59] B. Hebda, & T. Kryjak, "A compact deep convolutional neural network architecture for video based age and gender estimation," in 2016 Federated Conference on Computer Science and Information Systems (FedCSIS), pp. 787-790, September, 2016.
- [60] Z. Hu, Y. Wen, J. Wang, M. Wang, R. Hong, & S. Yan, "Facial age estimation with age difference," in IEEE Transactions on Image Processing, vol. 26, no. 7, pp. 3087-3097, 2016.
- [61] Z. Tan, J. Wan, Z. Lei, R. Zhi, G. Guo, & S. Z. Li, "Efficient group-n encoding and decoding for facial age estimation," in IEEE transactions on pattern analysis and machine intelligence, vol. 40, no. 11, pp. 2610-2623, 2017.
- [62] R. Ranjan, S. Sankaranarayanan, C. D. Castillo, & R. Chellappa, "An all-in-one convolutional neural network for face analysis," in 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), pp. 17-24, May, 2017.
- [63] H. Liu, J. Lu, J. Feng, & J. Zhou, "Ordinal deep learning for facial age estimation," in IEEE Transactions on Circuits and Systems for Video Technology, vol. 29, no. 2, pp. 486-501, 2017.
- [64] H. Liu, J. Lu, J. Feng, & J. Zhou, "Group-aware deep feature learning for facial age estimation," in Pattern Recognition, vol. 66, pp. 82-94, 2017.
- [65] G. Antipov, M. Baccouche, S. A. Berrani, & J. L. Dugelay, "Effective training of convolutional neural networks for face-based gender and age prediction," in Pattern Recognition, vol. 72, pp. 15-26, 2017.
- [66] J. Xing, K. Li, W. Hu, C. Yuan, & H. Ling, "Diagnosing deep learning models for high accuracy age estimation from a single image," in Pattern Recognition, vol. 66, pp. 106-116, 2017.
- [67] K. Li, J. Xing, W. Hu, & S. J. Maybank, "D2C: Deep cumulatively and comparatively learning for human age estimation," in Pattern Recognition, vol. 66, pp. 95-105, 2017.
- [68] L. Hou, D. Samaras, T. M. Kurc, Y. Gao, & J. H. Saltz, "Convnets with smooth adaptive activation functions for regression," in Proceedings of machine learning research, vol. 54, pp. 430, 2017.
- [69] K. Zhang, et al., "Age group and gender estimation in the wild with deep ror architecture," IEEE Access, vol. 5, pp. 22492-22503, 2017.
- [70] F. Wang, H. Han, S. Shan, & X. Chen, "Deep multitask learning for joint prediction of heterogeneous face attributes," in 2017 12th IEEE International Conference on Automatic Face & Gesture Recognition (FG 2017), pp. 173-179, May, 2017.
- [71] H. Liu, J. Lu, J. Feng, & J. Zhou, "Label-sensitive deep metric learning for facial age estimation," IEEE Transactions on Information Forensics and Security, vol. 13, no. 2, pp. 292-305, 2017.
- [72] H. Han, A. K. Jain, F. Wang, S. Shan, & X. Chen, "Heterogeneous face attribute estimation: A deep multitask learning approach," IEEE transactions on pattern analysis and machine intelligence, vol. 40, no. 11, pp. 2597-2609, 2017.
- [73] J. Wan, Z. Tan, Z. Lei, G. Guo, & S. Z. Li, "Auxiliary demographic information assisted age estimation with cascaded structure," IEEE transactions on cybernetics, vol. 48, no. 9, pp. 2531-2541, 2018.
- [74] M. Duan, K. Li, & K. Li, "An Ensemble CNN2ELM for Age Estimation," IEEE Transactions On Information Forensics And Security, vol. 13, no. 3, 2018.
- [75] H. F. Yang, B. Y. Lin, K. Y. Chang, & C. S. Chen, "Joint estimation of age and expression by combining scattering and convolutional networks," ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM), vol. 14, no. 1, pp. 9, 2018.
- [76] B. Yoo, Y. Kwak, Y. Kim, C. Choi, & J. Kim, "Deep facial age estimation using conditional multitask learning with weak label expansion," IEEE Signal Processing Letters, vol. 25, no. 6, pp. 808-812, 2018.
- [77] S. Taheri, & Ö. Toygar, "On the use of DAG-CNN architecture for age estimation with multi-stage features fusion," Neurocomputing, vol. 329, pp. 300-310, 2019.
- [78] W. Im, S. Hong, S. E. Yoon, & H. S. Yang, "Scale-Varying Triplet Ranking with Classification Loss for Facial Age Estimation," in Computer Vision – ACCV 2018. Lecture Notes in Computer Science, vol. 11365. Springer, Cham, 2018.
- [79] O. Sendik, and Y. Keller. "DeepAge: Deep Learning of face-based age estimation," in Signal Processing: Image Communication, vol. 78, pp. 368-375, 2019.
- [80] S. Penghui, L. Hao, W. Xin, Y. Zhenhua, & S. Wu. "Similarity-aware deep adversarial learning for facial age estimation," in 2019 IEEE International Conference on Multimedia and Expo (ICME), pp. 260-265, July, 2019.
- [81] C. Miron, V. Manta, R. Timofte, A. Pasarica, & R. I. Ciucu, "Efficient convolutional neural network for apparent age prediction," in 2019 IEEE

- 15th International Conference on Intelligent Computer Communication and Processing (ICCP), pp. 259-262, September, 2019.
- [82] N. Savov, M. Ngo, S. Karaoglu, H. Dibeklioglu, & T. Gevers, "Pose and Expression Robust Age Estimation via 3D Face Reconstruction from a Single Image," in Proceedings of the IEEE International Conference on Computer Vision Workshops, pp. 0-0, 2019.
- [83] H. Liu, J. Lu, J. Feng, & J. Zhou. "Ordinal Deep Learning for Facial Age Estimation," IEEE Transactions on Circuits and Systems for Video Technology, vol. 29, no. 2, pp. 486-501, 2019.
- [84] H. Liu, P. Sun, J. Zhang, S. Wu, Z. Yu, & X. Sun. "Similarity-Aware and Variational Deep Adversarial Learning for Robust Facial Age Estimation," IEEE Transactions on Multimedia, 2020.
- [85] P. Li, Y. Hu, X. Wu, R. He, & Z. Sun. "Deep label refinement for age estimation," Pattern Recognition, vol. 100, p. 107178, 2020.
- [86] N. Liu, F. Zhang, & F. Duan. "Facial Age Estimation Using a Multitask Network Combining Classification and Regression," IEEE Access, vol. 8, pp. 92441-92451, 2020.
- [87] X. Liu, Y. Zou, H. Kuang, & X. Ma. "Face Image Age Estimation Based on Data Augmentation and Lightweight Convolutional Neural Network," Symmetry, vol. 12, no. 1, pp. 146, 2020.
- [88] J. C. Xie, & C. M. Pun. "Deep and Ordinal Ensemble Learning for Human Age Estimation From Facial Images," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2361-2374, 2020.
- [89] M. Xia, X. Zhang, L. Weng, & Y. Xu. "Multi-Stage Feature Constraints Learning for Age Estimation," IEEE Transactions on Information Forensics and Security, vol. 15, pp. 2417-2428, 2020.
- [90] G. B. Huang, M. Mattar, T. Berg, & E. Learned-Miller, "Labeled faces in the wild: A database for studying face recognition in unconstrained environments," Workshop on Faces in 'Real-Life' Images: Detection, Alignment, and Recognition, October, 2008.
- [91] Z. Liu, P. Luo, X. Wang, & X. Tang, "Deep learning face attributes in the wild," in Proceedings of the IEEE international conference on computer vision, pp. 3730-3738, 2015.
- [92] O. Russakovsky, et al., "Imagenet large scale visual recognition challenge," International journal of computer vision, vol. 115, no. 3, pp. 211-252, 2015.
- [93] A. Khan, A. Sohail, U. Zahoora, & A. S. Qureshi. "A survey of the recent architectures of deep convolutional neural networks," Artificial Intelligence Review, vol. 53, no. 8, 5455-5516, 2020.
- [94] K. Ricanek, Y. Wang, C. Chen, & S. J. Simmons, "Generalized multi-ethnic face age-estimation," in 2009 IEEE 3rd International Conference on Biometrics: Theory, Applications, and Systems, pp. 1-6, September, 2009.
- [95] J. D. Akinyemi, & O. F. Onifade, "An ethnic-specific age group ranking approach to facial age estimation using raw pixel features," in 2016 IEEE Symposium on Technologies for Homeland Security (HST), pp. 1-6, May, 2016.
- [96] M. Shin, J. H. Seo, & D. S. Kwon, "Face image-based age and gender estimation with consideration of ethnic difference," in 2017 26th IEEE International Symposium on Robot and Human Interactive Communication (RO-MAN), pp. 567-572, 2017.
- [97] Microsoft.com. 2021. Online Meeting Software, Video Conferencing | Microsoft Teams. [online] Available at: <<https://www.microsoft.com/en-my/microsoft-teams/online-meetings>> [Accessed 3 May 2021].

Comparative Analysis of Supervised Machine Learning Techniques for Sales Forecasting

Stuti Raizada, Jatinderkumar R. Saini*
Symbiosis Institute of Computer Studies and Research
Symbiosis International (Deemed University)
Pune, India

Abstract—This study talks about how data mining can be used for sales forecasting in retail sales and demand prediction. Prediction of sales is a crucial task which determines the success of any organization in the long run. There are various techniques available for predicting the sales of a supermarket such as Time Series Algorithm, Regression Techniques, Association rule etc. In this paper, a comparative analysis of some of the Supervised Machine Learning Techniques have been done such as Multiple Linear Regression Algorithm, Random Forest Regression Algorithm, K-NN Algorithm, Support Vector Machine (SVM) Algorithm and Extra Tree Regression to build a prediction model and precisely estimate possible sales of 45 retail outlets of Walmart store which are at different geographical locations. Walmart is one of the foremost stores across the world and thus authors would like to predict the sales accurately. Certain events and holidays affect the sales periodically, which sometimes can also be on a daily basis. The forecast of probable sales is based on a combination of features such as previous sales data, promotional events, holiday week, temperature, fuel price, CPI i.e., Consumer Price Index and Unemployment rate in the state. The data is collected from 45 outlets of Walmart and the prediction about the sales of Walmart was done using various Supervised Machine Learning Techniques. The contribution of this paper is to help the business owners decide which approach to follow while trying to predict the sales of their Supermarket taken into account different scenarios including temperature, holidays, fuel price, etc. This will help them in deciding the promotional and marketing strategy for their products.

Keywords—Sales forecasting; linear regression; random forest regression; KNN regression algorithm; SVM algorithm; supervised machine learning techniques

I. INTRODUCTION

Retail is considered as one of the most significant and fast-growing business domains in data science field because of its high-volume data and abundant optimization challenges for example, ideal prices, recommendations, discounts, stock levels which can be resolved by using different data analysis methods. When it comes to predicting the sales of commodities, it gets quite challenging in today's stimulating and ever-changing business environment. Only a few enhancements while sales prediction could help retailers in depressing operational costs and improving sales. And it could result in more customer satisfaction [1]. Prediction of correct sales at every outlet of retail is important for the accomplishment of each retailing company as it aids in management of inventory, results in right distribution of products across various stores, solves the problem of over and

under stocking at each store in order to minimize losses, and maximize sales and satisfaction of customers [2]. Since there are many factors that come into play when one has to predict the sales, it has become a challenging issue to solve for all retail companies [3]. To add on, sales can also depend on a diversity of external factors such as weather, seasonal trends happening in a place where the store is located, competition from other retail stores and online shopping etc. It may include internal actions for example, promotions, discounts, pricing etc., which add to the intricacy of the problem.

There are various Machine Learning techniques which could be used for forecasting the sales of a Supermarket. Random Forest Regression is a supervised learning algorithm which incorporates ensemble learning method in it which helps in doing forecasting. A Random Forest works by constructing several decision trees first during the course of training and using the mean of the classes as the output for prediction of all the trees. A prediction from Random Forest Regressor is generated by taking an average of all the predictions produced by trees in the forest, which will increase the accuracy of the prediction. K-NN Regression is a technique that uses feature similarity to predict the value of a new data point. The new value is predicted based on how closely it lies to the points in the training dataset. SVR is a Supervised learning algorithm and works on the principle of Support Vector Machine. It is used in determining the best line of fit which has maximum no. of points lying on it. Extra Tree Regression is also an ensemble learning model with very minor difference to Random Forest Technique. Random Forest uses the replica of bootstrap i.e., doing the sub-sample of input data with replacement whereas Extra Tree Regressor takes into account the entire original sample of data. One for difference between the two techniques is selection of cut point. Extra Tree techniques choose the cut points randomly; however, Random Forest selects the optimum split.

After studying the literature related to Sales Forecasting, the methodology adopted has been defined. The model has been trained on various ML Algorithms such as Linear Regression, Random Forest Regression, KNN Regression, SVR and Extra Tree Regression. The Results obtained from each of the model have been discussed and finally the conclusion is obtained.

II. LITERATURE REVIEW

Microsoft Time Series Algorithm [4] provides regression algorithms that are optimized for forecasting of continuous

*Corresponding Author.

values such as product sales or demand over time. If one has to forecast for continuous variables like product sales, demand over time using regression algorithms Microsoft time series algorithm will help in that. It will not need any new additional columns to predict trends unlike decision tree algorithm, which can be considered as one of the significant advantages of Time Series Algorithm. It is capable of predicting any anomalies that we can face in the sales/demand based on the source data set that is fed into the model. As data keeps growing, one can simply update the data that is being used as input to the model, and the model will incorporate that and predicts accordingly. Cross Prediction can be performed using the Microsoft Time Series algorithm which is one of its unique features. The algorithm can be trained with two different, but related data sets or series, and the resulting model will be able to predict the outcome of one series based on the behavior of the other series by understanding the co-relation existing between them. For example, let's consider the problem statement as observed sales of one car can influence the forecasted sales of another car. Working of the Algorithm: When data related this problem, statement is given to the time series, it will be using Autoregressive Tree Models with Cross Prediction (ARTXP) and also Autoregressive Integrated Moving Average (ARIMA) and then combines the output of both algorithms which will help in improving the prediction accuracy. When it comes to predicting something for short-term, ARTXP algorithm will be used and for long-term predictions ARIMA.

Linear Regression [5] is a technique to model the relationships between two variables by fitting a linear equation to observed data. One variable is termed as explanatory variable (predictor) and the other variable is the dependent variable (target). It is about finding the best line of fit for training as well as testing data. This technique has been used in predicting the demand of commodities by analyzing the sales of the stores. Sales Forecasting is an important aspect in Production and Supply Chain Management [6]. KNN Regression is a regression technique uses the similarity measure to predict the values after analyzing the past cases data. It extracts the features from the data and uses 'feature similarity' in order to predict the values of new data points. The value of new data is assigned by calculating the average of the nearest neighbors of the new data point. The other approach to KNN is by calculating an inverse distance weighted average of the K-nearest neighbors. It uses same distance functions as used for Classification – Euclidean, Minkowski and Manhattan. Association Rule Discovery [7]; because of its wide application, Association Rule Discovery has become a trending topic in Data Mining. It finds the frequent patterns among the datasets. The aim of Association rule mining is to extract interesting relations, common patterns, and correlations among sets of items in the data repositories. For Example, it can be seen that 80% of the customers in India who buy Mobile Phones also buy Headsets for better music quality. Shelke et al. [8] has discussed various Machine Learning algorithms which can be applied in multiple sectors of industry such as retail, marketing, logistics etc. based on the requirement. It concluded the study by indicating that Rule Induction (RI) is the most frequently used ML technique in data mining [9] [10]. The previous study on sales prediction have been performed using regression techniques as well as

boosting techniques and boosting algorithms have resulted in better results as compared to regression techniques [11]. Zhan-Li Sun et.al [12] has used a neural network technique known as Extreme Learning Machine (ELM) to find out the relationship between sales amount and few crucial factors which affect demand using a real time dataset and found that their model outperform over the other sales forecasting methods using back propagation neural networks. Non-linear models are compared with linear model for sales forecasting and it was observed that neural networks perform well with de-seasonalized time series data whereas Regression models are effective with seasonal dummy variables [13]. Fashion Retail Industry has been considered as the most difficult in terms of predicting the sales due to shorter life span of products as the taste of the customer keeps changing. Statistical techniques have been applied to predict the sales such as Bayesian analysis, Exponential smoothing etc. Also, forecasting has been done using AI Methods of Artificial Neural Networks (ANN) and Evolutionary Neural Networks (ENN) [14]. Thomassey et al. [15] has proposed a forecasting model based on hybrid approach of combining fuzzy logic, neural networks, and evolutionary procedures. Manpreet et al. [16] have considered big data perspective while predicting the sales of Walmart. He has used the technologies such as Python API and Scala of the Spark framework.

Data is of no use if it cannot be examined, understood and applied in some context [17]. Harsoor and Patil et al. [18] have predicted the sales of Walmart stores using Big data applications such as Hadoop, MapReduce and Hive. For the purpose of analyses and visualizing of data, tools such as Hadoop Distributed File Systems (HDFS) [19], Hadoop Map Reduce Framework [20] and Apache Spark along with Scala, Python high level programming environments are used. Katal, Wazid and Goudar et al. [21] proposed Parallel programming like Distributed File System, Map Reduce and Spark as the prominent tools for dealing with Big Data. Sharma, Chauhan and Kishore did a comparative study between Hadoop, MapReduce and Spark and concluded that Spark is much better option for analyzing Big Data [22]. Spark has proven to be 100 times faster than other techniques of data analysis [23]. Omar et al. [24] has inspected the Back Propagation Neural Network for forecasting the sales of Walmart.

After studying the literature available for Sales Forecasting in various industries, it was identified that various algorithms have been used and the choice of algorithm is extremely crucial based on the dataset on which forecasting has to be made. For the data of short time period, statistical models could be used but they may not perform well with Big Data and thus, technologies such as Hadoop Distributed File System or Map Reduce is a better choice. This paper will help the retailers to decide which Machine Learning Algorithm will serve their purpose of sales forecasting without involving into the complexities of first choosing the algorithm and then implementing it.

III. METHODOLOGY

Here, the aim is to predict the sales of Walmart store using various Supervised ML Algorithms. The algorithms used are Linear Regression, Random Forest Regression, K-NN

Regression, Support Vector Machine and Extra Tree Regression as shown in Fig. 1. Linear Regression has been used for predicting the sales of several commodities in Walmart taking in consideration factors such as previous sales, Holiday week, Fuel price in that week, Unemployment rate etc. Considered the dataset of 45 retail outlets of Walmart store and did cleaning of data using Python. Further the dataset was divided into Training Data and Testing Data in the ratio of

80:20. Post that, Data Pre processing techniques have been applied in order make the data ready for feeding into the models. After feature selection, the model was trained and then the test data was given as an input and feature measurement has been performed. Lastly, the input was given to different model built for various algorithms and accuracy scores were obtained.

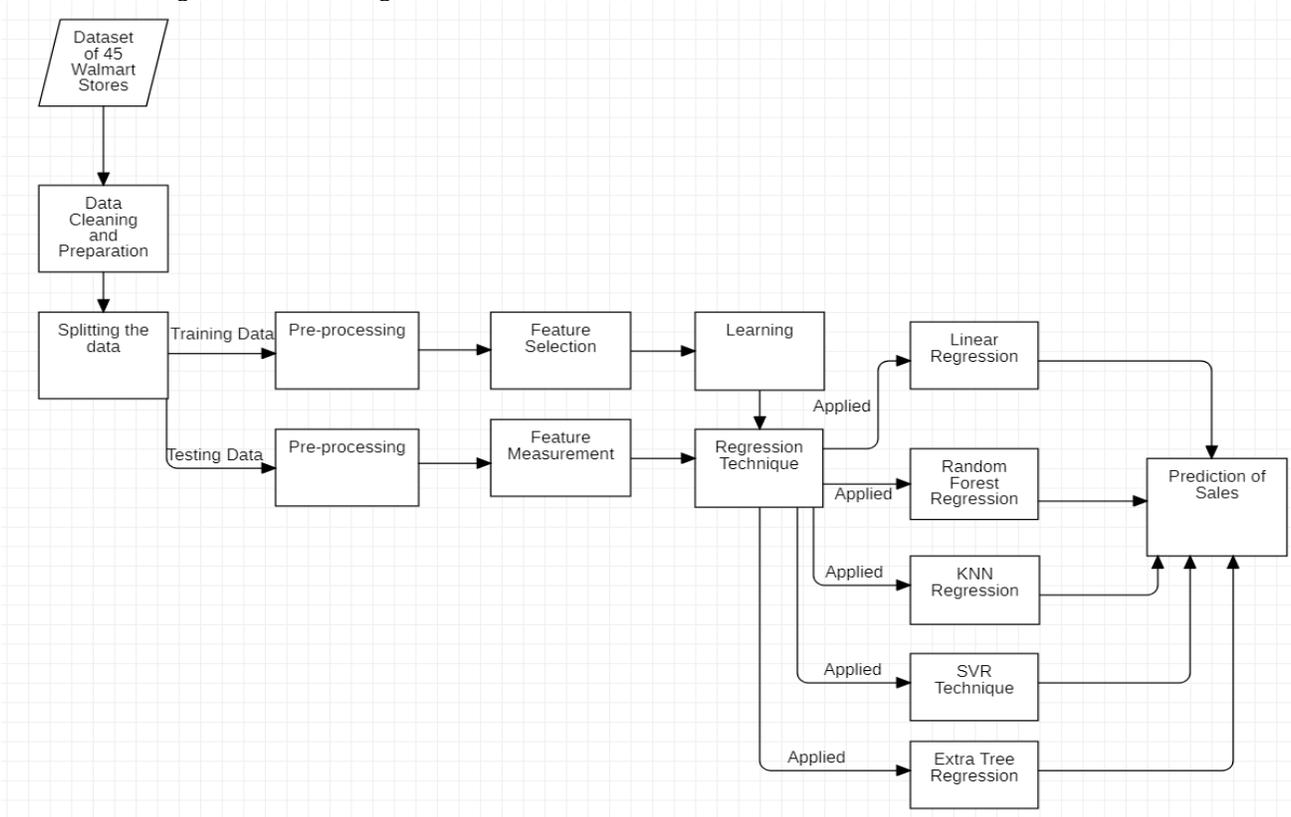


Fig. 1. Proposed Methodology.

Store	Date	Weekly_Sales	Holiday_Flag	Temperature	Fuel_Price	CPI	Unemployment
1	05-02-2010	1643690.9	0	42.31	2.572	211.0963582	8.106
1	12-02-2010	1641957.44	1	38.51	2.548	211.2421698	8.106
1	19-02-2010	1611968.17	0	39.93	2.514	211.2891429	8.106
1	26-02-2010	1409727.59	0	46.63	2.561	211.3196429	8.106
1	05-03-2010	1554806.68	0	46.5	2.625	211.3501429	8.106
1	12-03-2010	1439541.59	0	57.79	2.667	211.3806429	8.106
1	19-03-2010	1472515.79	0	54.58	2.72	211.215635	8.106
1	26-03-2010	1404429.92	0	51.45	2.732	211.0180424	8.106
1	02-04-2010	1594968.28	0	62.27	2.719	210.8204499	7.808
1	09-04-2010	1545418.53	0	65.86	2.77	210.6228574	7.808
1	16-04-2010	1466058.28	0	66.32	2.808	210.4887	7.808
1	23-04-2010	1391256.12	0	64.84	2.795	210.4391228	7.808
1	30-04-2010	1425100.71	0	67.41	2.78	210.3895456	7.808
1	07-05-2010	1603955.12	0	72.55	2.835	210.3399684	7.808
1	14-05-2010	1494251.5	0	74.78	2.854	210.3374261	7.808
1	21-05-2010	1399662.07	0	76.44	2.826	210.6170934	7.808
1	28-05-2010	1432069.95	0	80.44	2.759	210.8967606	7.808
1	04-06-2010	1615524.71	0	80.69	2.705	211.1764278	7.808
1	11-06-2010	1542561.09	0	80.43	2.668	211.4560951	7.808
1	18-06-2010	1503284.06	0	84.11	2.637	211.4537719	7.808

Fig. 2. Walmart Data Set for 45 Stores.

A. Dataset and Experiment Discussion

The sales data which is considered for prediction model has been taken from 45 stores of Walmart. The historical data taken for prediction covers sales from February 5, 2010 to November 1, 2012 [25]. There are 3 separate data files corresponding to each year and the accuracy of models has been calculated accordingly.

The data set which is considered for the study contains the following fields:

- 1) Store - the number of stores as 45 stores are considered.
- 2) Date – We have considered date as the first date of the week of sales for time series forecasting.
- 3) Weekly Sales – Weekly sales for the given store.
- 4) Holiday Flag – to determine if the week is a special holiday week. It shows 1 for Holiday week and 0 for Non-holiday week. This will help in understanding the trends during the holidays.
- 5) Temperature – Temperature recorded on the day of sale.
- 6) Fuel Price – Cost of fuel in the region where the store is located.
- 7) CPI – Dominant consumer price index.
- 8) Unemployment – Dominant unemployment rate in the region where store is present.

Fig. 2 shows the snapshot of the dataset of Walmart store.

Following are the steps which are followed for experimentation:

- 1) The first step is importing the necessary libraries which would be used for building the model such as numpy, pandas, matplotlib, seaborn.
- 2) After that, loaded the dataset for every year 2010, 2011 and 2012 respectively to the IDE.

- 3) Once data has been loaded, prepared the data for experiment by converting date to datetime format.
- 4) Checked if there are any missing or null values.
- 5) Then, splitted the date column and created 3 columns namely day, month and year.
- 6) For building the prediction model, found outliers in the data by plotting Temperature, Fuel Price, CPI and Unemployment on X- axis.
- 7) The next step was to drop the outliers and considered the range in which outliers does not fall.
- 8) Then, again checked if the plot looks fine without outliers.
- 9) Imported sklearn library for building the model and selected features and target for X and Y axis to predict the sales.
- 10) Splitted the data into training and testing set in the ratio of 80:20.
- 11) Used Linear Regression, Random Forest Regressor, KNN Regressor, SVR, Extra Tree Regressor to predict the sales of Walmart store along Y-axis to do comparative analysis of Prediction Model.
- 12) Calculated the errors in the Prediction Model by finding Mean Absolute Error, Mean Squared Error and Root Mean Squared Error.

IV. RESULT

The results obtained from the prediction models fed with datasets of three years 2010, 2011 and 2012 have been summarized below in Tables I, II and III, respectively.

From the Tables I, II and III, it has been observed that the Mean Absolute Error is highest in case of Support Vector Regression for all the three years and minimum in case of Extra Tree Regression. Mean Absolute Error is the average magnitude of the error in prediction set. It is the average over the test sample of absolute difference between prediction and actual observation.

TABLE I. STATISTICAL MEASURES FOR DATASET OF YEAR 2010

Algorithms	Mean Absolute Error	Mean Squared Error	Root Mean Squared Error
Linear Regression	424421.93	251400879887.53	501398.92
Random Forest Regression	80396.14	25126954749.18	158514.84
KNN Regression	281135.23	131980791838.85	363291.60
Support Vector Regressor	470857.85	320200129812.73	565862.28
Extra Tree Regression	48281.35	5534368506.39	74393.33

TABLE II. STATISTICAL MEASURES FOR DATASET OF YEAR 2011

Algorithms	Mean Absolute Error	Mean Squared Error	Root Mean Squared Error
Linear Regression	409909.51	235782880216.47	485574.79
Random Forest Regression	43811.57	4031635222.35	63495.15
KNN Regression	272092.75	123596844025.18	351563.42
Support Vector Regressor	430737.43	267243666430.57	516956.15
Extra Tree Regression	42752.07	3840250218.75	61969.75

TABLE III. STATISTICAL MEASURES FOR DATASET OF YEAR 2012

Algorithms	Mean Absolute Error	Mean Squared Error	Root Mean Squared Error
Linear Regression	447155.52	269282898979.58	518924.75
Random Forest Regression	50487.45	9118432907.22	95490.48
KNN Regression	272433.64	122911201809.44	350586.93
Support Vector Regressor	474953.02	311212134485.71	557863.90
Extra Tree Regression	42218.75	3952869757.58	62871.85

Root Mean Squared error is the square root of the average of squared differences between predicted and actual observation. It is least in case of Extra Tree Regression as compared to other Regression Techniques.

Before building the prediction model, the outliers in the dataset have been identified and removed. Fig. 3 to Fig. 6 visualizes outlier detection for the datasets of year 2010, 2011 and 2012. Among these, Fig. 3, Fig. 4 and Fig. 6 depict the presence of outliers in Temperature data, Fuel Price data and Unemployment data respectively. Fig. 5 depicts that there is no outlier in Consumer Price Index.

After finding out the outliers, the next step was to remove the outliers for feeding the input to the Prediction model.

Fig. 7, 12 and 17 are obtained after performing Linear Regression on the data for the year 2010, 2011 and 2012 respectively. However, it has been observed that for all the three datasets the graph looks scattered and thus it is not advisable to predict the sales using Linear Regression Model.

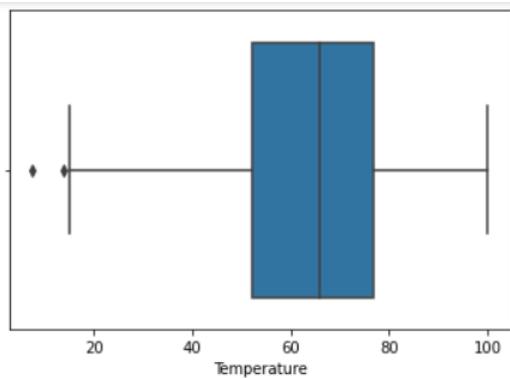


Fig. 3. Outlier in Temperature.

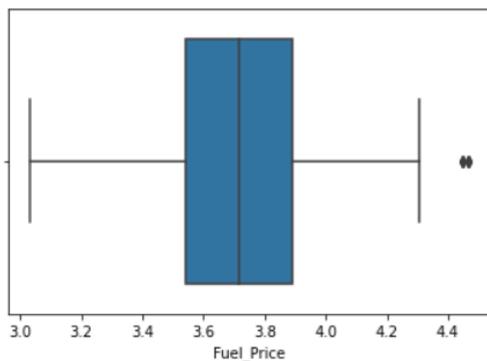


Fig. 4. Outliers Present in Fuel Price.

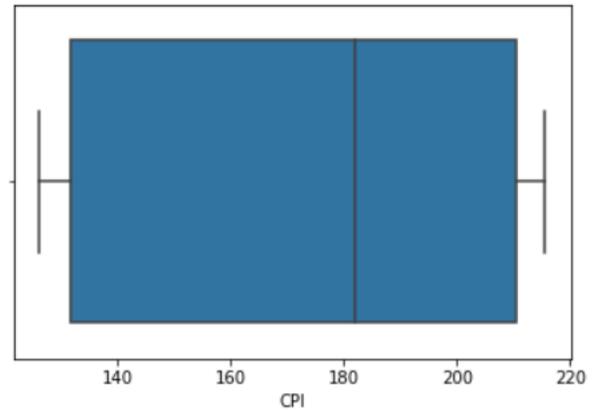


Fig. 5. No Outliers in CPI.

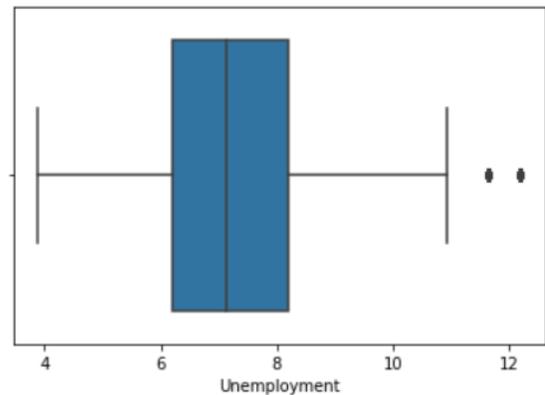


Fig. 6. Outliers Present in Unemployment.

Fig. 8, 13 and 18 forecasts the sales of the products in Walmart Store using Random Forest Technique against the weekly sales of the stores. Various factors taken into consideration on X-axis are Store number, Fuel Price, Unemployment, CPI, day, month and year. The graph in this case is almost concentrated on the best line of it and Random Forest provides good accuracy scores for all 3 datasets.

Fig. 9, 14 and 19 forecasts the sales using KNN Regression Technique. The graph is not much concentrated but it performs better than Linear Regression and provides the accuracy of around 50 to 60%.

Fig. 10, 15 and 20 are obtained after applying Support Vector Regression technique and it clearly demonstrate the worst performance amongst all other techniques used for predicting the sales of Walmart store.

Fig. 11, 16 and 21 are obtained after predicting the sales from Extra Tree Regressor Model and it performed best amongst all the models discussed so far. The graph looks somewhat similar to Random Forest Technique however, it is more accurate and all the data points are almost falling on the best of fir providing the accuracy of 98% in all three cases. This is because both these techniques use ensemble model of learning and averages the output obtained from several decision trees to provide better performance.

Results obtained for 2010 year dataset are shown below.

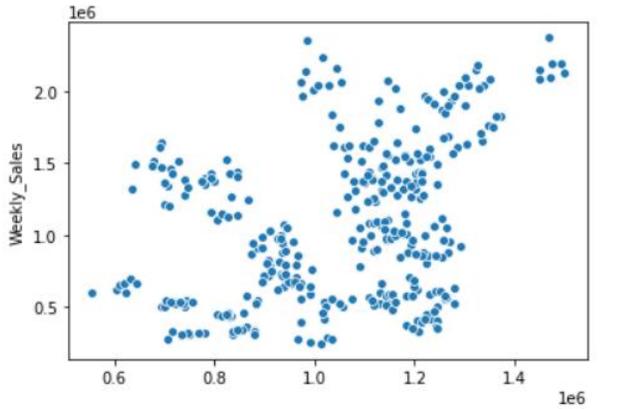


Fig. 7. Sales Prediction using Linear Regression Model (2010).

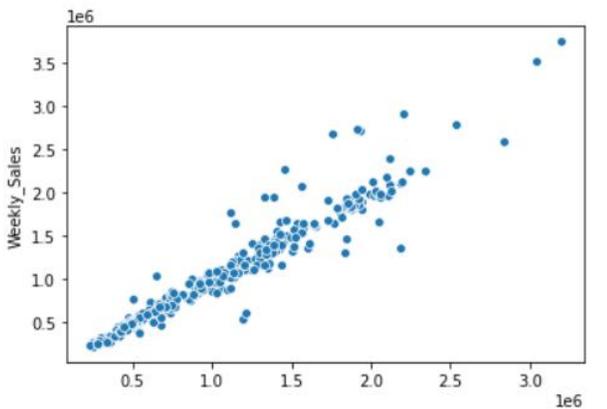


Fig. 8. Sales Prediction using Random Forest Regression Model (2010).

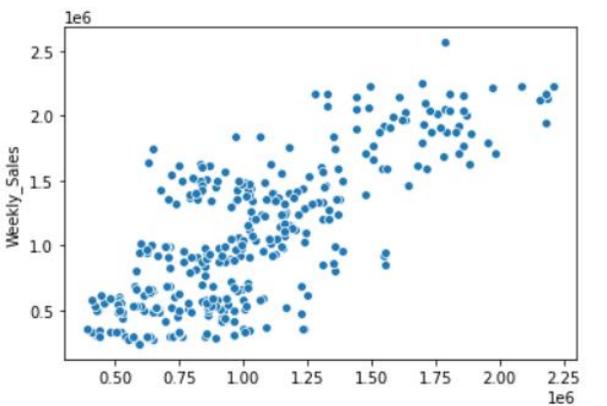


Fig. 9. Sales Prediction using KNN Regression Model (2010).

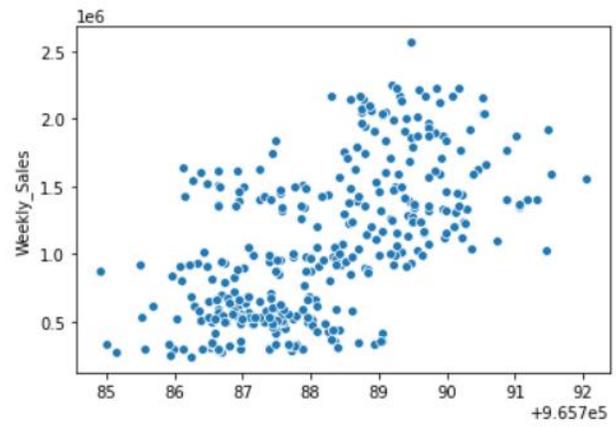


Fig. 10. Sales Prediction using SVR Model (2010).

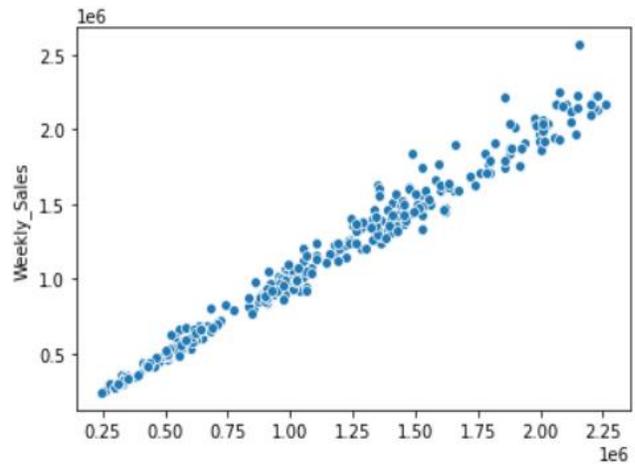


Fig. 11. Sales Prediction using Extra Tree (2010).

The results obtained for the dataset of year 2011 are as follows:

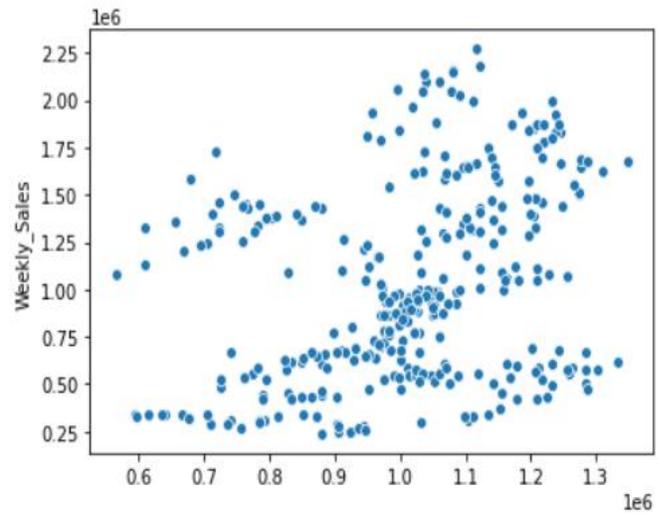


Fig. 12. Sales Prediction using Linear Regression Model (2011).

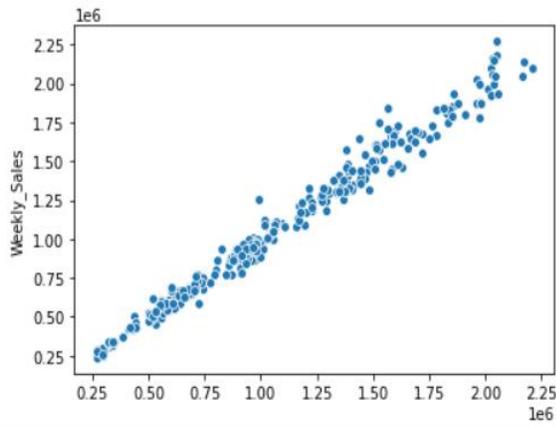


Fig. 13. Sales Prediction using Random Forest Regression Model (2011).

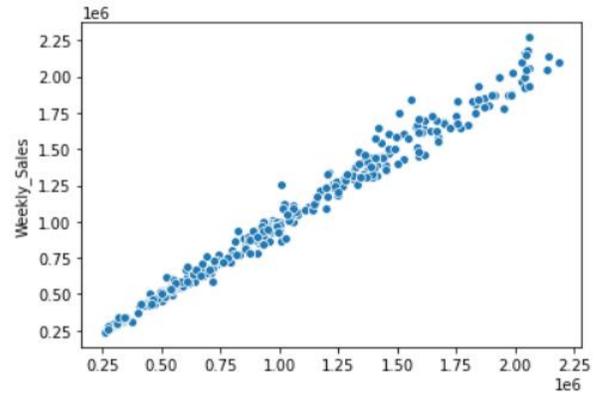


Fig. 16. Sales Prediction using Extra Tree (2011).

The below graphs are obtained for the data of year 2012:

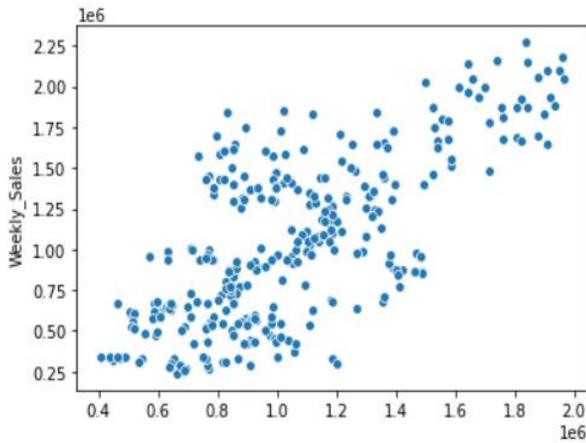


Fig. 14. Sales Prediction using KNN Regression Model (2011).

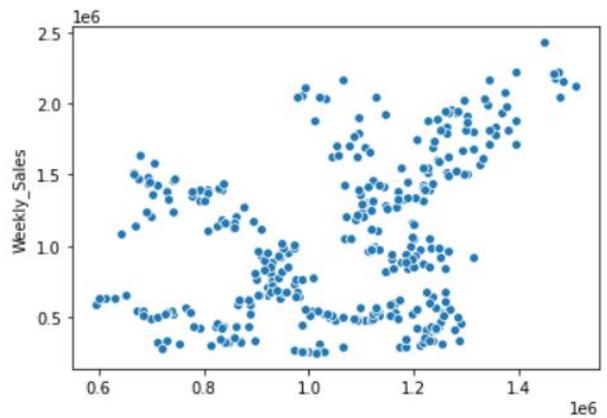


Fig. 17. Sales Prediction using Linear Regression Model (2012).

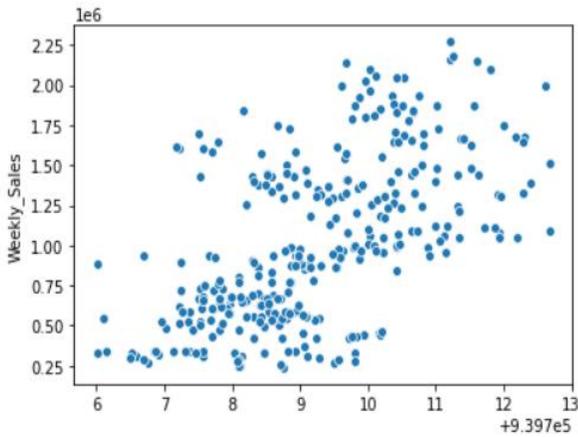


Fig. 15. Sales Prediction using SVR Model (2011).

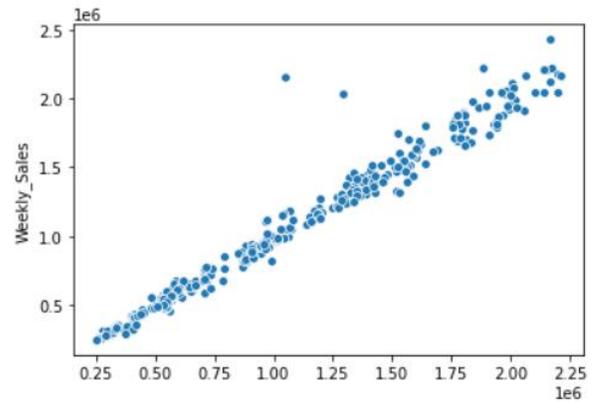


Fig. 18. Sales Prediction using Random Forest Regression Model (2012).

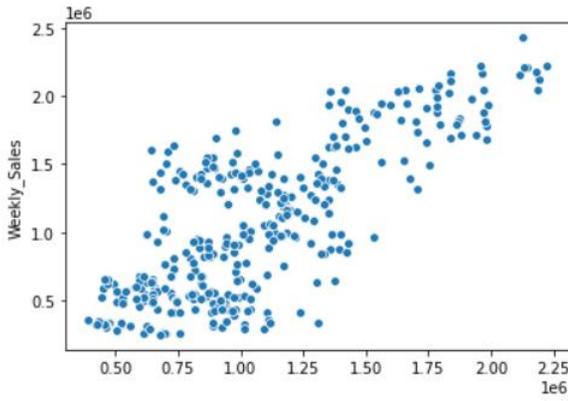


Fig. 19. Sales Prediction using KNN Regression Model (2012).

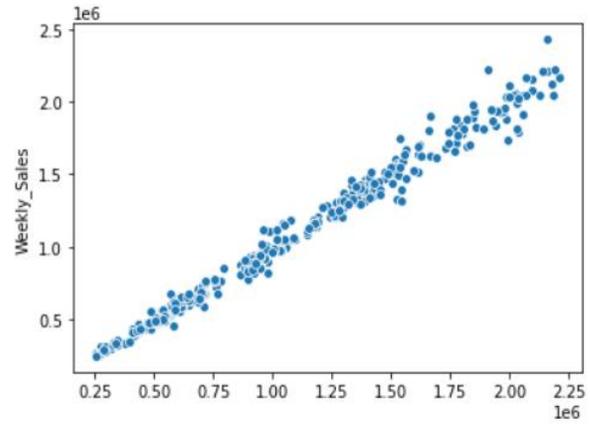


Fig. 21. Sales Prediction using Extra Tree (2012).

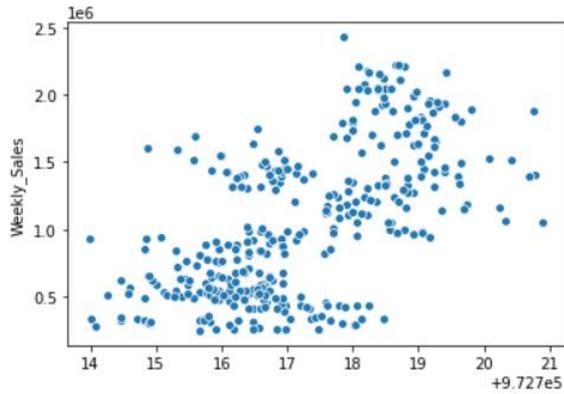


Fig. 20. Sales Prediction using SVR Model (2012).

From the Tables IV, V and VI, it is evident that Support Vector Regression model is the poorest and could not predict the sales of Walmart stores correctly. However, Extra Tree Regression Model performs best on the data for all three years when compared to other supervised Machine Learning techniques and predicts the sales with 98% accuracy and thus could be relied upon for Sales forecasting when the parameters considered are Fuel Price, Unemployment, Holiday and CPI.

TABLE IV. PERFORMANCE METRICS FOR YEAR 2010

Performance Metric Name	Linear Regression Score	Random Forest Score	KNN Regression Score	SVR Score	Extra Tree Regression Score
Accuracy	13.95%	92.73%	57.00%	- 4.32%	98.20%

TABLE V. PERFORMANCE METRICS FOR YEAR 2011

Performance Metric Name	Linear Regression Score	Random Forest Score	KNN Regression Score	SVR Score	Extra Tree Regression Score
Accuracy	10.23%	98.45%	52.71%	- 2.24%	98.53%

TABLE VI. PERFORMANCE METRICS FOR YEAR 2012

Performance Metric Name	Linear Regression Score	Random Forest Score	KNN Regression Score	SVR Score	Extra Tree Regression Score
Accuracy	14.15%	97.01%	59.77%	- 1.85%	98.70%

V. DISCUSSION

Based on the above experimentation, it has been observed that Simple Regression techniques for building the prediction models may not be the best choice for sales prediction if the management is trying to predict the sales for lesser duration and have historical data only for few years. This is because the accuracy is good only for ensemble learning techniques which involves averaging of results obtained from multiple decision trees. Therefore, the business owner should choose Ensemble Learning Models.

One limitation of this study is that based on the variance in training data, the predictions obtained from a specific algorithm may vary. So, the owner has to decide the algorithm effectively given his requirements.

VI. CONCLUSION

Based on the dataset used, it can be said that Extra Tree Regression Technique is the best to predict the sales of Walmart Store in future followed by Random Forest Regression Technique. This result could be useful for other retail store owners as well in order to determine their sales and they could directly opt for Sales Prediction using Extra Tree Regression Technique or Random Forest Approach rather than spending time in doing analysis using other Supervised Machine Learning Algorithms. The other retailers could also be benefitted by doing the demand analysis on the similar grounds. This study contributed in understanding the fact that external factors, such as Unemployment rate, Holiday Week, CPI, etc. also plays a vital role while predicting the sales of any retail store.

REFERENCES

- [1] Jain, A., Menon, M. N., & Chandra, S. (2015). Sales forecasting for retail chains. San Diego, California: UC San Diego Jacobs School of Engineering.
- [2] Linoff, G. S., & Berry, M. J. (2011). Data mining techniques: for marketing, sales, and customer relationship management. John Wiley & Sons.
- [3] Wayne, L. (2014). Winston. Analytics for an Online Retailer: Demand Forecasting and Price Optimization.
- [4] Mekala, P., & Srinivasan, B. (2014). Time series data prediction on shopping mall. *Int. J. Res. Comput. Appl. Robot*, 2(8), 92-97.
- [5] Sohrabpour, V., Oghazi, P., Toorajipour, R., & Nazarpour, A. (2021). Export sales forecasting using artificial intelligence. *Technological Forecasting and Social Change*, 163, 120480.
- [6] Vahid Sohrabpour, Pejvak Oghazi, Reza Toorajipour, Ali Nazarpour. (2021). Export sales forecasting using artificial intelligence, *Technological Forecasting and Social Change*, Volume 163.
- [7] Jannach, D., Zanker, M., Felfernig, A., & Friedrich, G. (2010). *Recommender systems: an introduction*. Cambridge University Press.
- [8] Shelke, R. R., Dharaskar, R. V., & Thakare, V. M. (2017). Data mining for supermarket sale analysis using association rule. *Int. J. Trend Sci. Res. Dev*, 1(4).
- [9] Bose, I., & Mahapatra, R. K. (2001). Business data mining—a machine learning perspective. *Information & management*, 39(3), 211-225.
- [10] Punam, K., Pamula, R., & Jain, P. K. (2018, September). A two-level statistical model for big mart sales prediction. In 2018 International Conference on Computing, Power and Communication Technologies (GUCON) (pp. 617-620). IEEE.
- [11] Krishna, A., Akhilesh, V., Aich, A., & Hegde, C. (2018, December). Sales-forecasting of retail stores using machine learning techniques. In 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS) (pp. 160-166). IEEE.
- [12] Zhan-Li Sun, Tsan-Ming Choi, Kin-Fan Au, Yong Yu. (2008). Sales forecasting using extreme learning machine with applications in fashion retailing, *Decision Support Systems*, Volume 46, Issue 1.
- [13] Ching-Wu Chu, Guoqiang Peter Zhang. (2003). A comparative study of linear and nonlinear models for aggregate retail sales forecasting, *International Journal of Production Economics*, Volume 86, Issue 3.
- [14] Govindan, Kannan, Liu, Na, Ren, Shuyun, Choi, Tsan-Ming, Hui, Chi-Leung, Ng, Sau-Fun. (2013). Sales Forecasting for Fashion Retailing Service Industry: A Review, *Mathematical Problems in Engineering*, Hindawi Publishing Corporation.
- [15] S. Thomassey, M. Happiette, and J.-M. Castelain. (2005). "A global forecasting support system adapted to textile distribution," *International Journal of Production Economics*, vol. 96, no. 1, pp. 81–95, 2005.
- [16] M. Singh, B. Ghutla, R. Lilo Jnr, A. F. S. Mohammed and M. A. Rashid, "Walmart's Sales Data Analysis - A Big Data Analytics Perspective," 2017 4th Asia-Pacific World Congress on Computer Science and Engineering (APWC on CSE), 2017.
- [17] D. Silverman, "Interpreting Qualitative Data: Methods for Analyzing Talk Text and Interaction", Text and Interaction, Sage Publications Ltd: Methods for Analyzing Talk, 2006.
- [18] A. S. Harsoor and A. Patil, "Forecast of sales of walmart store using Big Data application", *International Journal of Research in Engineering and Technology*, vol. 4, pp. 6, June 2015.
- [19] M. Zaharia, M. Chowdhury, T. Das, A. Dave, J. Ma, M. Mccauley, et al., "Fast and interactive analytics over Hadoop data with Spark", U senix - The Advanced Computing Systems Association, 2012.
- [20] J. Dean and S. Ghemawat, "MapReduce: simplified data processing on large clusters", *Association for Computing Machinery*, 2008.
- [21] A. Katal, M. Wazid and R. H. Goudar, *Big Data: Issues Challenges Tools and Good Practices*, 2013.
- [22] M. Sharma, V. Chauhan and K. Kishore, "A review: MapReduce and Spark for Big Data analysis", 5th International Conference on Recent Innovations in Science. 5: Engineering and Management, June 2016.
- [23] H. Pandey, Is Spark really 100 times faster on stream or its hype?, vol. 2, Sept 2016.
- [24] Omar, H. A., & Liu, D. R. (2012, January). "Enhancing sales forecasting by using neuro networks and the popularity of magazine article titles." *Sixth International Conference on Genetic and Evolutionary Computing (ICGEC)* (pp. 577-580).
- [25] <https://www.kaggle.com/input/retail-analysis-with-walmart-data> - Dataset used for modelling .

Machine Learning for Diagnosing Drug Users and Types of Drugs Used

Anthony Anggrawan¹, Ni Gusti Ayu Dasriani⁵, Mayadi⁶
Computer Science Study Program
Bumigora University, Mataram, Indonesia

Christofer Satria²
Visual Communication Design Study Program
Bumigora University, Mataram, Indonesia

Che Ku Nuraini³
Department of Centre of Research and Innovation
Management, Universiti Teknikal Malaysia Melaka, Malaysia

Lusiana⁴
Technical Information Study Program
STMIK AMIK Riau, Riau, Indonesia

Abstract—Drug use is very detrimental to the physical and psychological health of users. Drug abuse also causes addiction and is a global epidemic. Therefore it is not surprising that scientific research related to drugs has attracted attention for research. However, many factors become obstacles in the medical services of the drug user, including cost, flexibility, and a slow process. Meanwhile, electronic systems can speed up handling time, improve work efficiency, save costs and reduce inspection errors. It means that a breakthrough is needed in developing a platform that can identify drug users. Therefore, this research aims to build machine learning with expertise like an expert who can diagnose drug users and distinguish the types of drugs used by drug users. The expert system on machine learning was developed using the Forward Chaining and Certainty Factor methods. This study concludes that the expert system on machine learning developed can be used to diagnose drug users and distinguish the types of drugs used with an accuracy of up to 80%. The implications of the expert system on machine learning are an alternative method for narcotics officers and medical doctors in diagnosing drug users and the types of drugs used.

Keywords—Machine learning; drug; expert system; forward chaining; certainty factor

I. INTRODUCTION

Social environment factors have influenced others to engage in drug use [1] [2]. Adult figures who are addicted to drugs have a great influence on the behavior of others to become addicted [3]. Poor, low skills, life pressure, anxiety, and deviant behavior are factors that also lead to drug use [3]. Relaxing, drinking, staying up late, increasing enthusiasm, and relieving stress are other triggering factors for many drug use among young people [4]. Drug use, including amphetamines, marijuana, cocaine, heroin, and the like, are a major public health problem in physiological symptoms, resulting in behavioral changes, cognitive problems, and mental health [5]. Drug use also affects the physiology and behavior of future generations [2].

Drug abuse causes physical dependence (addiction) or relapse to continuously consume [6], although it has resulted in physical and psychological problems [6]. The previous research shows that drug users are very high [7] [1] and increasing globally [8]. Drug abuse has become a global

epidemic that affects human behavior [9]. Because drug use is very detrimental to the physical and psychological harm of the user, it is not surprising that this research related to drugs has attracted attention for scientific research [10].

Another factor that is often considered in medical services is the cost factor and its inflexibility (Bevan & Patel, 2016). Processes that are done manually tend to cause delays in medical diagnosis [11]. Using an electronic system can speed up handling time, improve work efficiency, and save costs [11]. Using an electronic system allows lower errors and eliminates omissions in deciding the test results and achieving the results [12]. However, the success of curing drug abuse and dependence is still limited; this includes the lack of success in the early identification of at-risk populations, resulting in increased death rates due to overdose [13]. In other words, not paying attention to the early symptoms of consuming drugs will be disastrous and make people who are loved suffer the destructive effects of the substance [14].

Meanwhile, if it turns out to be able to identify it early, it can prevent harmful consequences in the future that are sure to occur [14]. It means that there is a need for breakthroughs in developing platforms that can identify and screen patients susceptible to addiction after using opioid drugs [13]. Therefore, this research aims to develop a machine learning that has expertise like an expert. The expert system created can identify and screen or diagnose early drug users and the types of drugs used by using the Certainty Factor and Forward Chaining methods. The certainty factor method measures the certainty of the type of drug used by the user or patient who conducts consultations. On the other hand, forward chaining plays a role in the flow of the reasoning process from beginning to end based on data mining of physical symptoms of drug users and the types of drugs used (collected or explored previously).

Medical data is helpful as the knowledge that helps make scientific decisions regarding drug use [15]. Electronic medical use based on doctor's notes is useful for an effective treatment medium [10]. In the meantime, data mining is capable of electronic checks based on the patient's medical record [10].

Besides, the machine learning methods are a technique that can be useful for finding correlations based on the case for prediction purposes [16]. Unfortunately, machine learning is still few in the medical field due to technical problems [17]. Therefore, the simple machine learning method built in this research by imitating (studying) human knowledge in analyzing the physical symptoms of drug users and then implementing it in predicting drug users and identifying drug types used by users. It means that the expert system in machine learning has intelligence like an expert in diagnosing users and the types of drugs used from the physical symptoms that arise from drug users. Taking into account that the current use of information and communication technology (ICT) is growing or expanding very quickly or booming [18]. Therefore, the embodiment of the machine learning system in this research is website-based. So, anyone (the public) can access it from anywhere and has flexibility because it can work on various devices and operating systems. Therefore, a machine learning system in this research is helpful for early diagnosis without having to examine a narcotics laboratory and without a doctor or expert.

It is necessary to know the percentage of machine learning efficacy in identifying drug users and the type of drug used. It means that further testing to determine the actual percentage of machine learning efficacy still needs to be done. This study makes this happen by comparing the test results achieved by machine learning based on symptoms of drug users compared to the test results achieved from laboratory tests of drug users' urine in identifying drug users and the type of drug used. If machine learning has high efficacy, it can save time and cost of drug testing for suspects or drug users by using machine learning compared to testing drugs on urine or blood for suspects and drug users.

Some recent works related to this research:

- Zhongheng Zhang (2016) introduced the k-nearest neighbor (kNN) method as a simple machine learning method for modeling [17]. The similarity between the research in this article and the previous one is that they both use a simple approach to machine learning. While the difference is that the research uses the certainty factor method and forward chaining for machine learning, while previous research uses the kNN method for machine learning. Another difference is that the previous research was focus on predicting the class from the new dataset to the most similar class. In contrast, the research in this article focuses on machine learning to diagnose drug users and the types of drugs used.
- Anthony Anggrawan, Khasnur Hidjah, and Jihadil Qudsi S. (2017) implement intelligent application programs to detect kidney failure [19]. The previous research and the research in this article have similarities in developing web application programs with the PHP programming language and MySQL database. In addition, the last analysis used medical data on failure cases to diagnose new renal illness issues using CBR (Case-Based Reasoning method). In contrast, the articles in this study use the expertise of

drug experts (specialists) as knowledge of the application system for early diagnosis of drug users and the types of drugs used by drug users using the Forward Chaining and Certainty Factor methods.

- Kurnia Muludi, Radix Suharjo, Admi Syarif, and Fitri Ramadhani (2018) identified tomato plant diseases [20]. This previous research and the research in this article both implements forward chaining and certainty factor methods. However, the difference in the last research is to build an expert system to identify plant diseases based on android [20]. In contrast, the research in the article builds an expert system to identify users of drugs and the types of drugs used based on the website.
- Munaiseche, Kaparang, and Rompas (2018) built an expert system to assist doctors in diagnosing eye diseases [21]. In contrast to the research in this article, it is to create an expert system to diagnose drug users and the types of drugs used. Furthermore, this previous research used the forward chaining method, while the research in this article uses the forward chaining method and certainty factor. The similarities between the previous study and the research in this article are that both use PHP and MySQL in building an expert system.
- Ninive Von Greiff and Lisa Skogens (2021) investigated a drug user recovery program for drug addiction [22]. The research method is the interview or qualitative approach [22]. The similarity of the research in this article with previous studies is that they both study drug users. The difference is in previous studies examining the results of addiction recovery on drugs with the interview method. Meanwhile, the research in this article builds machine learning that has an intelligent system to detect drug users and the types of drugs used.

The latest related work identifies that the article in this study has a novelty that no previous researcher has researched. Another strength of this research is conducting a comparative test to determine the efficacy of machine learning or expert systems developed in identifying users and the types of drugs used by users that have not been studied before.

The systematics of writing this paper is as follows: the following sub-section discusses the research methodology, which includes research data and research methods used. The next subsection discusses the results and discussion of the research. Finally, the conclusions obtained from the study results and suggestions for further research are narrated in the Conclusions subsection.

II. RESEARCH METHODOLOGY

This study is a case study at the Indonesian National Narcotics Agency (Badan Narkotika Nasional or BNN) in Mataram, Indonesia. The number of drug users used as samples to test the expertise and accuracy of the machine learning built in this study was 30. The selection of data samples in this study was random. This research's

development of machine learning expertise consists of stages: knowledge acquisition, expert system design (programming), machine learning/expert system testing, and accuracy test (see Fig. 1).

A. Knowledge Acquisition

For the system development stage, the effort made is to obtain knowledge from drug experts, which is used as a knowledge base to build the machine learning or expert systems. The method used in obtaining knowledge related to narcotics is the interview method. The knowledge gained is the knowledge about the types of drugs and their symptoms. Based on the knowledge obtained, there are ten types of drugs that drug users dominantly use, and there are 27 types of drug symptoms.

In the knowledge acquisition stage, an expert from the Indonesian National Narcotics Agency (in Mataram, Indonesia) shares knowledge about drug use, including those related to symptoms and the types of drugs used by drug users. The knowledge gained at this stage serves as a knowledge base in building expertise from machine learning.

B. Expert System Design

The expert system design stage is a process for modeling the data that has been collected and designing an application system that is planned according to programming problems and the acquisition of knowledge obtained. This stage in computer science is known as planning the use case diagram design, data flow diagram (DFD) design, database design, and flowchart to be built on the application program. The programming stage is the implementation stage of the system design plan into a computer programming language [23]. This research uses the PHP and MySQL programming languages. The computer application program that is built is a cloud application program. Application development with PHP programming language and MYSQL database makes application programs can run via the web. By being stored on the server computer, the application program is ubiquitous. The ubiquitous application program means that the application program can be accessed from anywhere and at any time [24].

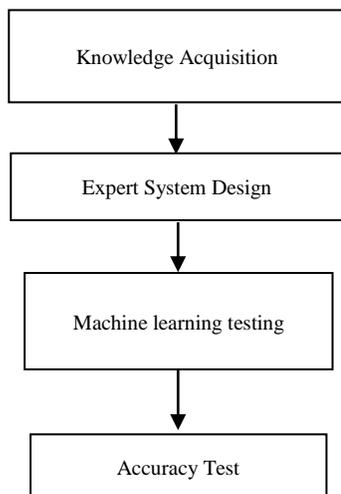


Fig. 1. Stages in the Development of an Expert System on Machine Learning.

C. Machine Learning Testing

The machine learning testing phase is the functional testing phase of the built application or black-box testing. Black-box testing is a test that no longer involves programming code or programming languages. In short, black-box testing on the expert system in this study is to determine whether the expert system built is under the list of desired system requirements.

D. Accuracy Test

Testing accuracy in machine learning is to determine the level of expertise of the expert system built in this study. It means that it is known how much accuracy the expert system has built-in diagnosing users' types of narcotics.

III. RESULT AND DISCUSSION

A. Knowledge Acquisition

The knowledge acquisition stage is the stage of acquiring the required knowledge data. The acquired knowledge acquisition data is useful in solving programming logic in diagnosing users and the types of drugs used by drug users. Table I shows the code for the type of drug used by drug users. Meanwhile, Table II presents the code of symptoms caused by drug users.

TABLE I. LIST OF TYPES OF DRUGS

No.	Drug Type Code	Drug Name
1	P01	Cocaine
2	P02	Marijuana
3	P03	Ecstasy
4	P04	Heroin
5	P05	Methamphetamine
6	P06	Hallucinogen
7	P07	Amphetamine
8	P08	Pethidine
9	P09	Codeine
10	P10	Morphine

TABLE II. LIST OF SYMPTOM OF DRUG USER

Symptoms of Drug User			
Code	Symptom	Code	Symptom
G01	Out of breath	G15	Difficult to focus
G02	Anxious and restless	G16	Difficult to rest
G03	Nausea and vomiting	G17	Weight loss
G04	Diarrhea	G18	Dry mouth
G05	Convulsions	G19	Blurred vision
G06	Easy to get angry	G20	Changes in skin color
G07	Depression	G21	Constipation
G08	Changes in sleep patterns	G22	Stomachache
G09	Sweating	G23	Drowsiness
G10	Chills (Hot cold)	G24	Itching
G11	Shaking	G25	Difficulty urinating
G12	Insomnia	G26	Mood swings
G13	Fast heart rate	G27	Dizziness
G14	Increased blood pressure		

TABLE III. RULE BASE OF TYPES AND SYMPTOMS OF BASIC DIAGNOSIS

Rule Base	
Drug Type	Symptom
P01	G01 and G02 and G03 and G04 and G05
P02	G06 and G02 and G07 and G08 and G09 and G10
P03	G05 and G11 and G12 and G13 and G14
P04	G15 and G02 and G07 and G16
P05	G11 and G01 and G16 and G17 and G18
P06	G09 and G11 and G18 and G19 and G10 and G14
P07	G18 and G03 and G04 and G05 and G01 and G20
P08	G07 and G13 and G05 and G03
P09	G27 and G03 and G18 and G21 and G22
P10	G023 and G24 and G09 and G25 and G26

After modeling the acquired knowledge acquisition data or knowledge representation (as shown in Table III) the next step is to implement it into the certainty factor algorithm. The certainty factor uses a value between 0.2 and 1.0 to assume a level of confidence in the data. A simulation of the calculation of the certainty factor was carried out based on the weight of symptoms arising from the type of drug used by drug users with weights of 0.8 and 1.0 according to the opinion of the drug expert (see Table IV).

TABLE IV. DETERMINATION OF DRUG SYMPTOM WEIGHT SCORE ACCORDING TO THE DECISION OF DRUG EXPERTS

No	Symptom	Weight Score
1	Very often	1
2	Often	0,8
3	Never	0

So, on the drug symptom weighted score given to the certainty factor, a score of 0 indicates that drug users do not experience these symptoms. If a drug user experiences symptoms, then the weighted score given for the frequently experienced symptoms is 0.8 and the most frequently experienced is 1.0, according to the drug expert's decision.

This study's knowledge base of machine learning expertise is the symptoms, types of drugs, and CF rules obtained from drug experts (see Table V). The knowledge base is an essential component that contains the knowledge possessed by competent experts in the related field (i.e., narcotics in this study). Furthermore, the knowledge base is the basis for decision-making in an expert system, where this decision-making is related to the process of retrieving previously collected and stored knowledge.

B. Expert System Design

Fig. 2 shows the interactions that occur between system users and the developed expert system.

This study has a database that stores records of users, patients, symptoms, and types of drugs, including diagnostic data, so it is necessary to design a data workflow model to realize a structured program.

TABLE V. KNOWLEDGE BASE

Symptom	J-001	J-002	J-003	J-004	J-005	J-006	J-007	J-008	J-009	J-010
	C F	C F	C F	C F	C F	C F	C F	C F	C F	C F
Out of breath					0.8		1			
Anxious and restless	0.8	0.8		1						
Nausea and vomiting	0.8						0.8	0.8	0.8	
Diarrhea	1						0.8			
Convulsions	0.8		0.8				0.8	0.8		
Easy to get angry		1								
Depression		0.8		0.8				1		
Changes in sleep patterns		0.8		0.8						
Sweating		0.8				0.8				0.8
Chills		0.8				0.8				
Shaking			0.8		0.8	0.8				
Insomnia			0.8							
Fast heart rate			0.8					0.8		
Increased blood pressure			0.8			1				
Difficult to focus				1						
Difficult to rest					0.8					
Weight loss					0.8					
Dry mouth					1	0.8	0.8		1	
Blurred vision						0.8				
Changes in skin color							0.8			
Constipation									0.8	
Stomachache									0.8	
Drowsiness										1
Itching										0.8
Difficulty urinating										0.8
Mood swings										1
Dizziness									0.8	

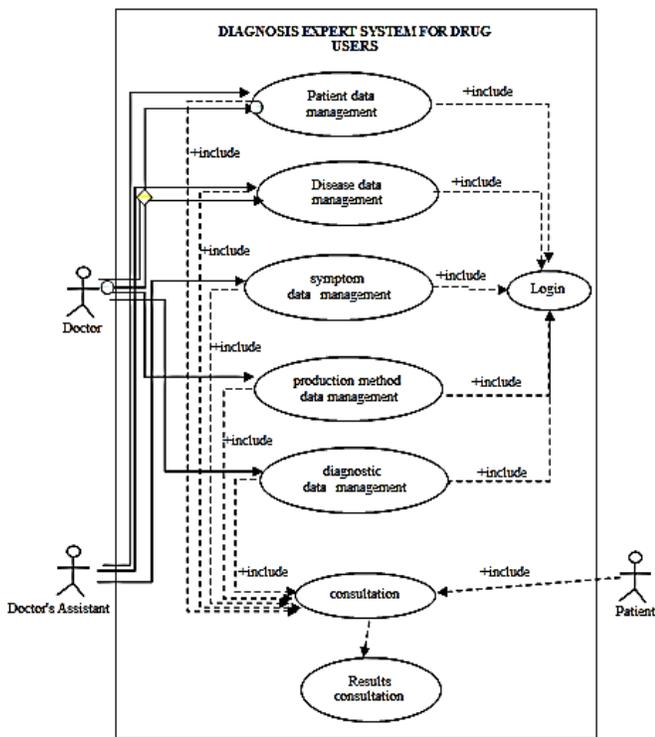


Fig. 2. Use Case Diagram on Machine Learning.

The Data Flow Diagram (DFD) in Fig. 3 and Fig. 4 illustrates where the data flow comes from and where the data processing on the expert system is built.

The context diagram in Fig. 3 shows the data flow of the system globally. In contrast, the overview diagram in Fig. 4 shows a more detailed data flow that the system performs and its engagement with external data.

The flow diagram in Fig. 5 shows a series of flow relationships in the expert system built in this study or shows the overall process sequence in building an expert system in this study.

The flow diagram contains a more detailed description of how each step of the procedure is actually carried out in building an expert system on machine learning that can diagnose users and the types of drugs used by users.

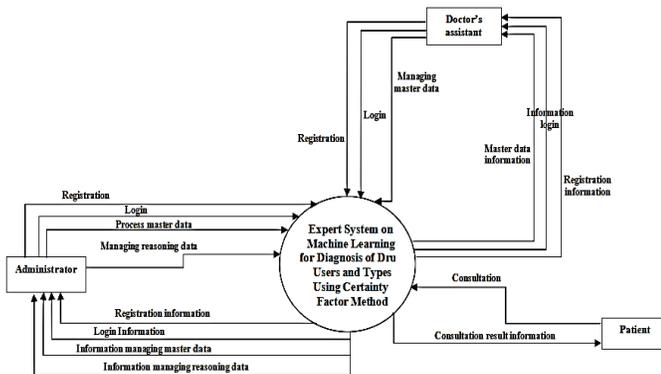


Fig. 3. Context Diagram of Data Flow on Machine Learning.

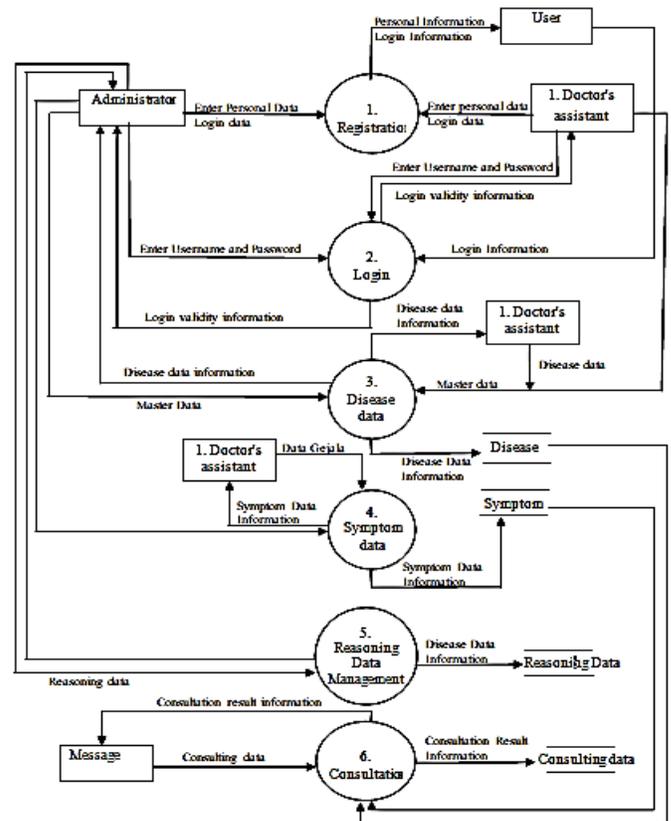


Fig. 4. Overview Diagram of Data Flow on Machine Learning.

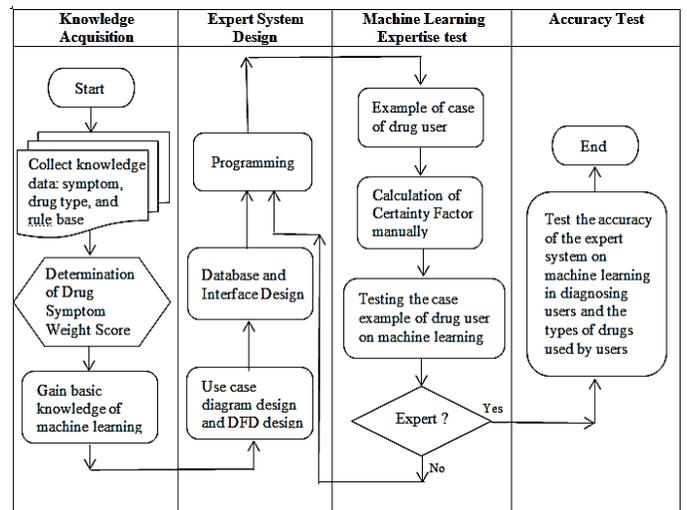


Fig. 5. Flow Diagram of the whole Process of Building an Expert System on the Machine Learning.

C. Machine Learning Testing

Expertise testing of machine learning is carried out using case samples from a patient. For example, in one case, a drug patient had symptoms of shortness of breath, depression, chills, anxiety and restlessness, and irritability. Symptoms of drug patients who have symptoms of shortness of breath, depression, chills, anxiety and restlessness, and irritability are symptoms of drug users: (1) Cocaine, (2) Cannabis, (3) Heroin, and (4) Amphetamine.

The formula for CF is:

$$CF[H,E] = CF[H] * CF[E]$$

$$CF \text{ Combine } CF[H,E]1 = CF[H,E]1 + CF[H,E]2 * (1 - CF[H,E]1)$$

$$CF \text{ Combine } CF[H,E] \text{ old}3 = CF[H,E] \text{ old} + CF[H,E] * (1 - CF[H,E] \text{ old})$$

Based on manual calculations, the results are as follows:

1. For J-001 = Cocaine

$$G01 = \text{Out of breath (0.8)}$$

$$CF[H,E] = CF[H] * CF[E]$$

$$= (0.8 * 0.8)$$

$$= 0.64$$

G02 = Anxious and restless (0.8)

$$CF[H,E] = CF[H] * CF[E]$$

$$= (0.8 * 0.8)$$

$$= 0.64$$

$$CFk1 = CF[H,E]1 + CF[H,E]2 * (1 - CF[H,E]1)$$

$$= 0.64 + 0.64 * (1 - 0.64)$$

$$= 0.870$$

So the expert CF from the symptoms entered by the user for the type of drug Cocaine is probably 0.870 or 87%.

2. For J-002 = Marijuana

$$G07 = \text{Depression (0,8)}$$

$$CF[H,E] = CF[H] * CF[E]$$

$$= (0.8 * 0.8)$$

$$= 0.64$$

G10 = Chills (0.8)

$$CF[H,E] = CF[H] * CF[E]$$

$$= (0.8 * 0.8)$$

$$= 0.64$$

G02 = Anxious and restless (0.8)

$$CF[H,E] = CF[H] * CF[E]$$

$$= (0.8 * 0.8)$$

$$= 0.64$$

G06 = Easy to get angry (1)

$$CF[H,E] = CF[H] * CF[E]$$

$$= (0 * 1)$$

$$= 0$$

$$CFk1 = CF[H,E]1 + CF[H,E]2 * (1 - CF[H,E]1)$$

$$= 0.64 + 0.64 * (1 - 0.64)$$

$$= 0.870$$

$$CFk2 = CFk1 + CF[H,E]3 * (1 - CFk1)$$

$$= 0.870 + 0.64 * (1 - 0.870)$$

$$= 0.953$$

$$CFk3 = CFk2 + CF[H,E]4 * (1 - CFk2)$$

$$= 0.953 + 0 * (1 - 0.953)$$

$$= 0.953$$

So the CF of the symptoms entered by the user for the type of marijuana drug is likely to be 0.953 or 95%.

3. For J-004 = Heroin

$$G07 = \text{Depression (0.8)}$$

$$CF[H,E] = CF[H] * CF[E]$$

$$= (0.8 * 0.8)$$

$$= 0.64$$

G02 = Anxious and restless (1)

$$CF[H,E] = CF[H] * CF[E]$$

$$= (0 * 1)$$

$$= 0$$

$$CFk1 = CF[H,E]1 + CF[H,E]2 * (1 - CF[H,E]1)$$

$$= 0.64 + 0 * (1 - 0.64)$$

$$= 0.64$$

So the CF of the symptoms entered by the user for the type of heroin drug is most likely 0.64 or 64%.

4. For J-007 = Amphetamine

G01 = Out of breath (1)

$$CF[H,E]1 = CF[H]1 * CF[E]2$$

$$= (0.8 * 1) = 0.8$$

So the CF of the symptoms entered by the user for the type of Amphetamine is most likely 0.8 or 80%.

Based on the value of manual calculations, the largest CF value is taken, which is 0.953 or 95% with the type of marijuana drug. It means the patient is using a type of marijuana drug. A case example is tested on an expert system application program (or on machine learning). If the patient's symptoms in the case sample (with the same symptoms) are entered into the expert system built in this study, the result of the process is as shown in Fig. 6.

Expert system testing on machine learning shows that the expert system has succeeded in correctly identifying the user and the type of drug used by the user. In order to know how accurate the machine learning expertise is, this study also tested several other patients by comparing the results with the urine test results at the Indonesian National Narcotic Agency laboratory in Mataram, Indonesia.

HASIL KONSULTASI		
Nama	:	Andi
Umur	:	24
Jenis Kelamin	:	Laki-laki
Pekerjaan	:	PHS
Alamat	:	ampenan
No	Pertanyaan	Jawaban
1	Sesak Nafas	TIDAK
2	Cemas dan Gelisah	IYA
3	Mual dan Muntah	TIDAK
4	Diare	TIDAK
5	Kejang-kejang	TIDAK
6	Mudah Marah	TIDAK
7	Depresi	IYA

Fig. 6. Screenshot of Expert System Questions about Drug Symptoms Experienced by Patients.

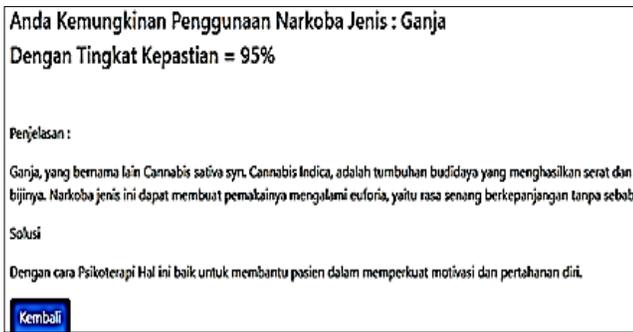


Fig. 7. Screenshot of the Expert System Test Results on the Type of Drug used by the Patient.

Fig. 7 describes it as follows: You are probably using a type of drug with a 95% certainty. Another narrative in Fig. 7 is: another name for cannabis is cannabis sativa. Cannabis sativa is a cultivated plant that contains fiber and narcotic substances in its seeds. This drug makes user experience euphoria, namely a prolonged feeling of pleasure for no reason. The cure is psychotherapy, which helps the patient strengthen the motivation to stop using it.

Expert system testing on machine learning shows that the expert system has succeeded in correctly identifying the user and the type of drug used by the user. In order to know how accurate the machine learning expertise is, this study also

tested several other patients by comparing the results with the urine test results at the Indonesian National Narcotic Agency laboratory.

D. Accuracy Test of Machine Learning

The accuracy test of machine learning in this study is to determine the expert performance of the application system built-in diagnosing users and the types of drugs used.

Testing the level of accuracy of machine learning expertise is to compare the suitability of the results with the urine test results from patients at the Indonesian National Narcotics Agency. In a trial of 30 times on 30 patients, there were 30 results of machine learning tests that can correctly identify drug users and as many as 24 machine learning test results that can detect the types of drugs used by drug users. It means that the test results on the data of 30 drug patients show that an expert system on machine learning built using the Certainty Factor method has expertise in diagnosing drug users up to 80 percent. The accuracy rate of up to 80 percent is obtained from the calculation results of 24 divided by 30 and multiplied by 100%.

The details of the machine learning accuracy test results are as described in Table VI. Table VI shows the comparison between the results of the expert system and the results of drug experts on the diagnosis of the types of drugs used by drug users.

TABLE VI. MACHINE LEARNING EXPERTISE ACCURACY TEST RESULT

Number	Case	System Result	Expert Result	Suitability
1	G01, G02, G03, G04, G05	Cocaine	Cocaine	Suitable
2	G06, G02, G07, G08, G09, G10	Marijuana	Marijuana	Suitable
3	G05, G11, G12, G13, G14	Ecstasy	Ecstasy	Suitable
4	G15, G02, G07, G16	Heroin	Heroin	Suitable
5	G11, G01, G16, G17, G18	Methamphetamine	Methamphetamine	Suitable
6	G09, G11, G18, G19, G10, G14	Hallucinogen	Hallucinogen	Suitable
7	G18, G03, G04, G05, G01, G20	Amphetamines	Amphetamines	Suitable
8	G07, G13, G05, G03	Pethidine	Pethidine	Suitable
9	G27, G03, G18, G21, G22	Codeine	Codeine	Suitable
10	G23, G24, G09, G25, G26	Morphine	Morphine	Suitable
11	G03, G06, G07, G15	Pethidine	Pethidine	Suitable
12	G01, G08, G09, G18	Codeine	Codeine	Suitable
13	G01, G02, G05, G09, G11, G15, G18	Codeine	Hallucinogen	Not suitable
14	G04, G12, G13, G17	Ecstasy	Ecstasy	Suitable
15	G08, G11, G17, G18, G19	Methamphetamine	Methamphetamine	Suitable
16	G01, G13, G15, G20, G22	Amphetamines	Amphetamines	Suitable
17	G17, G20, G21, G22, G23, G25, G27	Codeine	Morphine	Not suitable
18	G02, G07, G11, G15, G16	Pethidine	Heroin	Not suitable
19	G03, G07, G10, G14, G19	Pethidine	Pethidine	Suitable
20	G08, G11, G15, G18, G19, G20, G22, G23	Codeine	Amphetamines	Not suitable
21	G02, G06, G07, G08, G09, G10, G19, G27	Marijuana	Marijuana	Suitable
22	G05, G11, G12, G14, G19, G20	Hallucinogen	Ecstasy	Not suitable
23	G01, G06, G07, G10, G24	Pethidine	Marijuana	Not suitable
24	G03, G07, G09, G21	Morphine	Morphine	Suitable
25	G05, G12, G17, G22	Ecstasy	Ecstasy	Suitable
26	G07, G12, G15, G26	Heroin	Heroin	Suitable
27	G02, G08, G15, G23	Heroin	Heroin	Suitable
28	G06, G09, G15, G26	Morphine	Morphine	Suitable
29	G07, G11, G18, G23, G27	Codeine	Codeine	Suitable
30	G08, G15, G25, G26	Morphine	Morphine	Suitable

IV. CONCLUSION

The results of this study found that: (a) Machine learning in this study can predict drug users and types of drugs based on the symptoms that drug users complain about. (b) This study machine learning acquired knowledge about the symptoms of drug users, types of drugs, and basic knowledge related to the weight of the certainty factor of each type of drug and the symptoms caused so that it can diagnose drug users and the types of drugs used by users. (c) The accuracy of machine learning in this study in predicting the types of drugs used by users and the types of drugs used by users reached 80%. (d) The expert system in this research is website-based so that the expert system from this research can be used by various parties and in different places to identify users and the types of drugs used by users.

The implication of this research result is that the expert system built in this study can be a tool (choice) to replace or complete the testing system for drug users through urine testing in the laboratory.

The drawback of the results of this study is that machine learning expertise in this study is only limited to simple machine learning, as is the case with simple machine learning which was built on previous research by Zhongheng Zhang (2016), which used the KNN method in building learning machines. Furthermore, the machine learning expertise generated from this research is only limited to the expertise possessed in accordance with the knowledge obtained (symptoms, types of drug abuse, rule base, and calculation of certainty factor) under study. Therefore, further research needs to build machine learning that can increase its expertise based on more new data and use another method.

REFERENCES

- [1] R. Jiménez, J. Anupol, B. Cajal, and E. Gervilla, "Data mining techniques for drug use research," *Addict. Behav. Reports*, vol. 8, pp. 128–135, 2018.
- [2] F. M. Vassoler, E. M. Byrnes, and R. C. Pierce, "The impact of exposure to addictive drugs on future generations: Physiological and behavioral effects," *Neuropharmacology*, vol. 76, no. PART B, pp. 269–275, 2014.
- [3] P. K. Shanmugam, "The Influence of Social Factors in Drug Addiction—A Mini Review of Work by Miller & Carroll (2006)," *J. Alcohol. Drug Depend.*, vol. 05, no. 04, pp. 4–6, 2017.
- [4] A. Boys, J. Marsden, and J. Strang, "Understanding reasons for drug use amongst young people: A functional perspective," *Health Educ. Res.*, vol. 16, no. 4, pp. 457–469, 2001.
- [5] G. López, L. M. Orchowski, M. K. Reddy, J. Nargiso, and J. E. Johnson, "A review of research-supported group treatments for drug use disorders," *BMC Public Health*, vol. 16, no. 51, pp. 1–21, 2021.
- [6] Z. Justinova, L. V. Panlilio, and S. R. Goldberg, "Drug Addiction," *Natl. Libr. Medicine*, vol. 1, no. 1, pp. 310–335, 2009.
- [7] T. Saah, "The evolutionary origins and significance of drug addiction," *Harm Reduct. J.*, vol. 2, pp. 1–7, 2005.
- [8] G. Leshner, E. M. Stevens, S. Kim, N. Kim, T. L. Wagener, and A. C. Villantie, "Cognitive and affective responses to marijuana prevention and educational messaging," *Drug Alcohol Depend.*, vol. 225, no. August, pp. 1–3, 2021.
- [9] M. Zaman et al., "Drug abuse among the students," *Pakistan J. Pharm. Res.*, vol. 1, no. 1, p. 41, 2015.
- [10] L. W. Chou, K. M. Chang, and I. Puspitasari, "Drug Abuse Research Trend Investigation with Text Mining," *Comput. Math. Methods Med.*, vol. 2020, pp. 1–8, 2020.
- [11] A. Bevan and N. Patel, "An Electronic Prescription Alerting System—Improving the Discharge Medicines Process," *Arch. Dis. Child.*, vol. 101, no. 9, p. e2.55–e2, 2016.
- [12] A. Tsyben, N. Gooding, and W. Kelsall, "Assessing the Impact of a Newly Introduced Electronic Prescribing System Across a Paediatric Department – Lessons Learned," *Arch. Dis. Child.*, vol. 101, no. 9, p. e2.13–e2, 2016.
- [13] M. Mahmoudi, S. Pakpour, and G. Perry, "Drug-Abuse Nanotechnology: Opportunities and Challenges," *ACS Chem. Neurosci.*, vol. 9, no. 10, pp. 2288–2298, 2018.
- [14] J. Redman, "Recognizing the Warning Signs of Drug Addiction : What You Need to Know," *Mental Health and Counseling Studies*. pp. 1–7, 2021.
- [15] N. Jojen, "A Survey Paper on Data Mining Techniques in Drug Industry," *Int. J. Eng. Res. Technol.*, vol. 3, no. 30, pp. 296–299, 2015.
- [16] A. Yosipof, R. C. Guedes, and A. T. García-Sosa, "Data mining and machine learning models for predicting drug likeness and their disease or organ category," *Front. Chem.*, vol. 6, no. May, pp. 1–11, 2018.
- [17] Z. Zhang, "Introduction to machine learning: K-nearest neighbors," *Ann. Transl. Med.*, vol. 4, no. 11, pp. 1–7, 2016.
- [18] A. Anggrawan, "Interaction between learning preferences and methods in face-to-face and online learning," *ICIC Express Lett.*, vol. 15, no. 4, pp. 319–326, 2021.
- [19] A. Anggrawan, K. Hidjah, and Q. S. Jihadi, "Kidney failure diagnosis based on case-based reasoning (CBR) method and statistical analysis," in *2016 International Conference on Informatics and Computing, ICIC 2016, 2017*, pp. 298–303.
- [20] K. Muludi, R. Suharjo, A. Syarif, and F. Ramadhani, "Implementation of forward chaining and certainty factor method on android-based expert system of tomato diseases identification," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 9, pp. 451–456, 2018.
- [21] C. P. C. Munaiseche, D. R. Kaparang, and P. T. D. Rompas, "An Expert System for Diagnosing Eye Diseases using Forward Chaining Method," in *IOP Conference Series: Materials Science and Engineering, 2018*, vol. 306, no. 1, pp. 1–8.
- [22] N. Von Greiff and L. Skogens, "Recovery and identity: a five-year follow-up of persons treated in 12-step-related programs," *Drugs Educ. Prev. Policy*, pp. 1–10, 2021.
- [23] A. Anggrawan, "Percentage of Effect of Blended Learning Madel on Learning Outcome," in *Proceedings of 2019 4th International Conference on Informatics and Computing, ICIC 2019, 2019*.
- [24] A. Anggrawan, N. Ibrahim, S. Muslim, and C. Satria, "Interaction between Learning Style and Gender in Mixed Learning with 40 % Face-to-face Learning and 60 % Online Learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, pp. 407–413, 2019.

Insights on Deep Learning based Segmentation Schemes Towards Analyzing Satellite Imageries

Natya S¹, Ramya K², Dr. Seema Singh³

Research Scholar, Department of Electronics and Telecommunication Engineering, BMS Institute of Technology & Management, Bengaluru, Karnataka, India¹

(Also, Assistant Professor, Department of Electronics and Communication Engineering, Presidency University, Bengaluru, Karnataka, India)¹

Assistant Professor, Department of Electrical and Electronics Engineering, Presidency University, Bengaluru, Karnataka, India²

Professor and Dean (External Relations), Electronics and Telecommunication Engineering Department, BMS Institute of Technology & Management, Bengaluru, Karnataka, India³

Abstract—Satellite imageries are essentially a complex form of an image when subjected to critical analytical operation. The analytical process applied on remotely sensed satellite imageries are utilized for generating the land cover map. With an abundance of traditional techniques evolved to date, deep learning-based schemes are progressively gaining pace for identifying and classifying a terrestrial object in satellite images. However, different variants of deep learning approaches have different operations, and so are the consequences. At the same time, there is no reported literature to highlight the issues, trends, and effectiveness much on a generalized scale concerning segmentation. Therefore, this paper reviews some of the recent segmentation approaches using deep learning to contribute towards review findings in the form of research trends, research gaps, and essential learning outcomes. The paper offers a compact and distinct picture of deep learning approaches used to boost segmentation for satellite images.

Keywords—Deep learning; landcover; map generation; remotely sense image; satellite image; segmentation

I. INTRODUCTION

The satellite images of various resolutions are used for generating maps for land cover [1]. Analysis of satellite images potentially assists in developing multiple classes of landcover, e.g., water, impervious surface, vegetation surface, residential area, etc. [2]. To construct an accurate landcover map, it is essential to classify various elements, e.g., trees, individual buildings, roads, cars, etc. In this process of building a landcover map, spatial resolution is proven more efficient than spectral resolution [3][4]. It will also mean that image pixels with finer resolution are more beneficial than the maximized number of spectral bands [5]. This is the prime justification behind the increased usage of remote sensing satellite images to enhance the terrestrial object's visibility [6]. In this direction towards generating an accurate landcover map of the satellite image, most existing studies are now emphasized towards pixel-based analysis where segmentation plays a significant role. This is also boosted by applying a deep learning approach towards land cover map generation and classification of objects [7]-[9]. With the availability of various wireless technologies, satellite images are transmitted from a satellite to the earth receiving center, where processing

is carried out [10][11]. However, the problem surfaces towards the quality of received signal where signal fluctuations are witnessed due to electrical signals in wireless transmission systems [12]-[14]. This finally leads to various errors and artifacts within the received satellite images [15][16]. Most of these artifacts are in the form of noises, while it is challenging to eliminate coupled noises. Existing filters are not capable of controlling these forms of noises [17]-[19].

The available processing algorithms for satellite images are required to be proven for their efficiencies concerning computational complexities (space and time) that are significantly missing from literature towards wireless image transmission. The pixel-based analysis approach also leads to issues with the increase of spatial resolution; the complex patterns start to surface for spectral response originated from multiple objects of much smaller dimension in an urban region. The prime reason is using a similar object to develop various structures in landcover while emission of similar spectral response is continued. In object-based analysis, multiple segments are generated from an image indexed with different attributes, followed by subjecting it to rules of classification operation (e.g., texture, size, area, length, etc.). However, both pixel and object-based analyses have inefficiencies towards classification, making way for the deep learning approach to contribute to the segmentation process. However, deep learning cannot be fully considered an end solution, although it shows potential progress in analyzing satellite images. Despite some dedicated research approaches towards segmentation problems, deep learning has shown promising results, as well as there are also pitfalls associated with this approach.

The paper presents a discussion of existing deep learning approaches towards improving segmentation mechanism of satellite images. With an increasing proliferation towards adopting deep learning techniques, it is essential to understand its rate of success for analyzing satellite imageries, which itself is one complex form of signal. The significant problem under consideration is that there is no standard reporting for implementation effectiveness of using deep learning methods towards addressing segmentation problem, which is one of the

essential steps in analyzing satellite images. In spite of availability of different variants of deep learning, the research question arises are i) what are the identified advantages and limitation of different deep learning schemes towards segmentation problem in satellite images? ii) which is the most preferred dataset of satellite imageries considered for existing evaluation, iii) what is the existing direction of research trend of exploiting the potential of deep learning over analyzing satellite images?. Hence, based on the above stated research question.

Hence, this paper studies the effectiveness of existing deep learning schemes for the segmentation of satellite images. The contribution of this review paper are multi-fold viz. i) a compact briefing of satellite imageries concerning conventional segmentation and its associated challenges, ii) exhaustive recent reviews of frequently adopted deep learning segmentation schemes on satellite images, iii) compact briefing of the frequently adopted dataset by the existing researcher, iv) Discussion of research trends of existing deep learning segmentation methods, v) exclusive highlights of research gap and essential findings of this review study of recent papers. The paper's organization is: Section II discusses satellite imageries while existing literature of different deep learning approaches is discussed in Section III. Section IV discusses data adoption while Section V highlights research trends with various perspectives. Section VI discusses review contribution, while Section VII outlines the paper's conclusion.

II. SATELLITE IMAGERIES

Satellite imageries are considered one of the meteorologists' primary sets of information to predict the atmosphere's behavior. Satellite images are of three types, as shown in Fig. 1 viz. water-vapor images, infrared images, and visible images [20][21]. Some of the actual applications of remotely-sensed ideas are viz. i) tracking cloud for weather prediction, ii) monitoring growth of city area, iii) identifying changes in forest and farmland over some time, iv) Mapping and exploring the topography of ocean bed, v) forest fire, etc. Apart from this, satellite images have broader applications, e.g., anomaly hunting, regional planning, cartography, geology, oceanography, agriculture, forestry, etc. [22]. With the modernization, there has been a change in the forms and types of satellite images based on capturing it. Visual sensors play a significant role in this regard, integrated into modern-day satellites to generate remote sensing images [24]. This is a process of identifying different physical characteristics specific to a monitoring region based on emitted radiation from the air-borne vehicle or the satellite. This paper has discussed the case of satellite images in remote sensing, which is characterized by five types of resolution, i.e., geometric, radiometric, temporal, spectral, and spatial [25].

The resolution of satellite images largely depends upon the orbit altitude and types of the instrument being used. This manuscript will not illustrate fundamental theories of satellite images, as information can be easily accessed from various online articles, e.g. [26][27]. Instead, the proposed study will emphasize the challenges of processing it and understanding the existing literature's effectiveness. A series of image

processing is carried out to process satellite images, e.g., enhancement, feature extraction, segmentation, fusion, detection of changes, compression, classification, and feature detection [28]. Out of all these processes, the most critical function that significantly contributes to accuracy in prediction is the segmentation process. The process of segmenting satellite images targets to obtain a distinct segment of boundaries and their objects.

Some of the conventional methods of satellite image segmentation are briefed in Table I which exhibits conventional approaches of segmentation over satellite images e.g. Gabor filter and graph-based [29], firefly algorithm [30], deep learning [31], Markov Random Field [32], and Cuckoo Search [33]. From the preliminary outcomes, it can be seen that performance (especially with respect to accuracy) is higher for deep learning compared to other conventional methods irrespective of any dataset being used. The segmentation techniques mentioned above in Table I are considered as a baseline by various research work; however, the segmentation approaches are still found not to exhibit better predictive accuracy as they should be. There is a reason for this trade-off which is complexities associated with segmenting satellite images which are as follows: i) limitation of coverage area of satellite images, ii) availability of limited information from current satellite data [34], iii) higher possibilities of degradation of image quality during retrieval process [35], and iv) possibilities of generation of artifact-data when aggregated from multi-instrument data. Hence, there are significant challenges in performing proper segmentation for any complex remote sensing satellite images in all the cases mentioned above.

Further, it is noticed that landcover classification is associated with various challenges viz. multitemporal images, presence of clouds, classification of the object, small scale benchmarks, etc. Landcover images of the satellite are considered to be massive, and hence the mining community has already started to utilize the Big Data concept towards mapping and classifying crops [36]. In this respect, deep learning is a potential player to contribute to classification. It is because. However, this is also another factor of motivation to take an interest in working on this topic in the current era. Hence, this paper explores the impact of existing deep learning on the segmentation of satellite images.

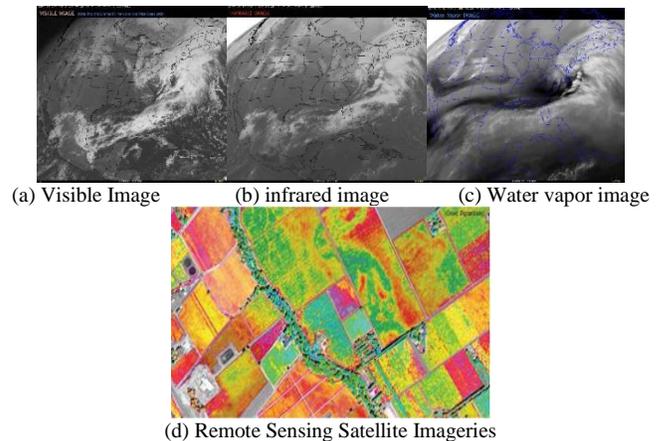


Fig. 1. Types of Satellite Images [23].

TABLE I. CONVENTIONAL SEGMENTATION METHODS

Segmentation Method	Test Image	Outcome
Gabor filter, graph-based [29]	QuickBird	Quality=85%, Correctness=92% Completeness=93%
Firefly Algorithm [30]	NASA satellite image (multiband)	SSIM=0.92448 MSE=3376.16 PSNR=13.71
Deep Learning [31]	Infrared Image	Accuracy=90%
Markov Random Field [32]	QuickBird	Recall= 0.77, Precision=0.71, F-Measure=0.74
Cuckoo Search [33]	Pleiades Satellite Image	FSIM=0.96, MSE=411.86, PSNR=21.99

III. DEEP LEARNING SCHEMES

Deep learning schemes are constructed based on the neural network that consists of neurons in the form of multiple layers capable of transforming the input of satellite images to an outcome image in the form of identified land covers. This is achieved by progressively learning the high-level features. This section discusses different taxonomies and approaches of deep learning schemes that have been used for image segmentation towards the satellite data as follows:

A. Convolution Neural Network

The generalized framework of Convolution Neural Network (CNN) consists of harnessing the softmax layer using different blocks with distinct architecture and ensemble of its outcome. The conventional practices of CNN comprise different layers, e.g., input, convolution, pooling, completely connected layer, and outcome of the soft-max layer. The computation of the filter adopted in the convolution layer is mathematically represented as follow:

$$\phi_n^l = g(\sum_{m \in M_n} \Delta a + b_m^l) \quad (1)$$

In the above expression (1), the outcome of the filter ϕ_n^l is dependent on multiple variables: The variable g represents nonlinear activation function while the first component Δa represents $(x_m^{l-1}, w_{m,n}^l)$ where variable x is input during the second component b_m^l Represents bias term considering weight w with m^{th} filter corresponding to l^{th} layer. Further feature maps are produced from progressive usage of pooling and convolution layer that is finally transformed into one-dimensional features leading to final prediction using soft-max layer. Fig. 2 highlights the sequence of the process mentioned above in CNN.

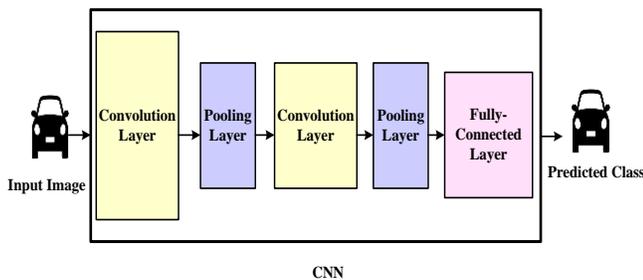


Fig. 2. Process Flow of CNN.

Further, the process of training in CNN can be boosted by using Adam Optimizer [37], stochastic gradient descent, batch normalization [38], dropout [39], parametric rectified linear unit [40], etc. At present, there are various approaches of CNN being applied towards image segmentation of satellite data.

One of the significant beneficial characteristics of the CNN model is that it doesn't have any dependencies towards tuning the parameters. This fact was investigated in the study of Wurm et al. [41]. The study also analyzes the capabilities of transferring a trained network to a different type of dataset. The idea of this implementation is to carry out semantic segmentation of landcover using CNN. The presented study emphasizes the transfer learning operation of fully CNN.

The study of segmentation carried out by Zhang et al. [42] has extracted road area of land from satellite images using CNN. A raster map is constructed from satellite signal trajectories, where the outcome shows better accuracy. A recent work carried out by Li et al. [43] used CNN for extracting features considering the case study of developing footprint maps of buildings. This mechanism also uses a graph model to consider the spatial correlation of data to retain boundary-related information. Preprocessing is carried out using co-registration and truncated signed distance labels. The CNN inputs satellite image and ground truth, leading to extracted feature where a segmentation probability is computed and pairwise potential extraction. This combined yields a new graph model that finally generates multi-class results emphasizing object detection. A similar category of work has also been carried out by Saetchnikov et al. [44]. Multiple deep neural networks of CNN have been used for comparative analysis to perform segmentation leading to object detection and tracking.

Wang et al. [45] have developed a unique segmentation process that is iterative in its operation to preprocess remote sensing images for detecting ships. The region detection of the ship is carried out using multivariate Gaussian distribution. The training is carried out using optical panchromatic data during a hardware synthesis of the model over a Field Programmable Gate Array. The work carried out by Jiang et al. [46] has captured geographic information of road using remote sensing technology of satellite imageries. This technique uses CNN to classify satellite images into two categories, i.e., road and non-road sections. Further optimization is carried out to address the inclusion issues of non-road noises owing to natural scene factors using wavelet packets. Another unique work was carried out by Persello et al. [47], where the identification of information settlement over a landcover has been investigated. The study has emphasized over-extraction of spatial feature and texture information. The authors have used a complete convolution network where labeling towards the pixel of satellite images has been carried out. The higher representation of the data is autonomously subjected to a learning algorithm considering six layers of convolution network. Different from conventional studies towards land cover, Wang et al. [48] have carried out the study using CNN to find the ice concentration.

TABLE II. SUMMARY OF EXISTING TECHNIQUES ON CNN

Authors	Problems	Segmentation Technique	Dataset	Advantages	Limitation
Wurm et al. [41].	Slum area segmentation	Fully CNN, transfer function	QuickBird dataset	Results in high-resolution image	Narrowed test cases with low scope
Zhang et al. [42]	Road extraction	CNN, trajectories of GPS	Google Earth Satellite Imageries	Simplified process	No benchmarking
Li et al. [43]	Building footprint map	CNN, graph model	-Inria Aerial image dataset -Kaggle -ISPRS -Planetscope satellite images	Optimal training time	Increased processing time
Jiang et al. [46]	Identification of road	CNN, wavelet packet filter	GIS data	Achieves >4% accuracy	computational intensive
Persello et al. [47]	Identification of informal settlement	Fully convolution neural network	Dar es Salaam	Low computational cost	Higher training time
Saetchnikov et al. [44]	Object detection	Multiple variants of CNN	DSTL Dataset	Supportive of practical application	Computational complexity not addressed.
Wang et al. [48]	Identification of ice concentration	CNN	RADARSAT-2	Simpler process	The lower scale of analysis
Wang et al. [45]	Identification of ship	CNN, multivariate Gaussian distribution, FPGA	Panchromatic data	Usage of few parameters, robust detection	Extensive test environment not adopted

Observation: From this discussion, it can be seen that CNN is used as a standalone and in combination with other schemes to boost the segmentation performance. For the majority of the implementation scheme, the performance of the CNN remains nearly similar with respect to method simplification and accuracy. It is also seen that the usage of CNN is found highly efficient for extracting potential features, classification of the scene, and detection of a specific form of land in satellite images. However, it is observed that features often tend to diminish while using the pooling layer. This will potentially affect the computational performance. In contrast, the outcome of the feature map and predictive resultants is not much improved during satellite image segmentation using CNN.

Table II highlights the strength and weaknesses of the existing segmentation approaches facilitated by CNN to understand the contribution of existing literature.

B. Recurrent Neural Network

Recurrent Neural Network (RNN) formulates a directed / undirected graph obtained from node connection in neural network considering temporal sequence. Input with variable length sequence is processed using internal state of RNN which is a network class for infinite impulse response. Used over wide variety of application in current time, RNN is another frequently used supervised learning model deployed towards segmentation of satellite images. Essentially meant to carry out analysis of discrete sequences, it is found that RNN can generate deep feedforward networks. The conventional architecture of RNN is shown in Fig. 2.

According to Fig. 3, the conventional RNN model usually connects the outcome of all the neurons to the input to construct a topology of the network. RNN is of different types, i.e., one-to-one, one-to-many, many-to-one, and many-to-many. The common activation function in RNN is sigmoid, Tanh, and relu. In this case, the outcome of the previous step

is considered an input for the existing step. One of the significant advantages of RNN in the segmentation process is its memory system, which retains information about all its calculations, thereby reducing the complexity of attributes not present in other neural networks. The discussion presented by Taberner et al. [49] gave a good insight into using deep learning over time-series datasets of satellite imageries. The most recent work carried out by Turkoglu et al. [50] has used RNN with multiple layers where gated cells were drawn. The most significant contribution of this study is findings that state a change in gradient magnitude when it moves through the cell over a deep lattice of RNN. The study has used MNIST dataset which is benchmarked dataset consisting of satellite imageries. The work carried out by Ienco et al. [51] has harnessed the potential of RNN to carry out the classification of landcover from satellite images. This technique has carried out segmentation using a multi-temporal stack to obtain information associated with multi-temporal layers of an object. The researcher has used a multiresolution segmentation approach followed by applying statistical evaluation over its features. Maggiori et al. [52] present a similar direction of work, where RNN has been used as an iterative and semantic segmentation process. Sun et al. [53] have implemented Long Short Term Memory RNN, which harnesses temporal factors of crops captured from satellite images over a time series.

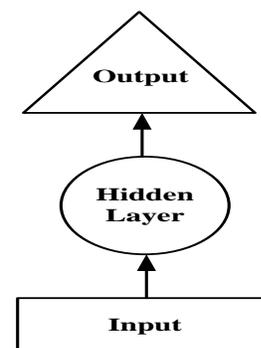


Fig. 3. Conventional Architecture of RNN.

TABLE III. SUMMARY OF EXISTING TECHNIQUES ON RNN

Authors	Problems	Segmentation Technique	Dataset	Advantages	Limitation
Turkoglu et al. [50]	Improving the performance of RNN	Gated RNN	MNIST dataset	Computationally improved performance, higher accuracy	Non-scalable performance
Ienco et al. [51]	Classification of landcover	RNN, multi-temporal stack	Pleiades VHSR, Corine Land Cover.	Very simplified approach	Don't consider complexities within the data.
Maggiori et al. [52]	Map classification	RNN, semantic segmentation	OpenStreetMap	Higher accuracy	Higher processing time
Sun et al. [53]	Land cover classification	Semantic segmentation	Cropland Data Layer	Higher accuracy	Resource intensive operation

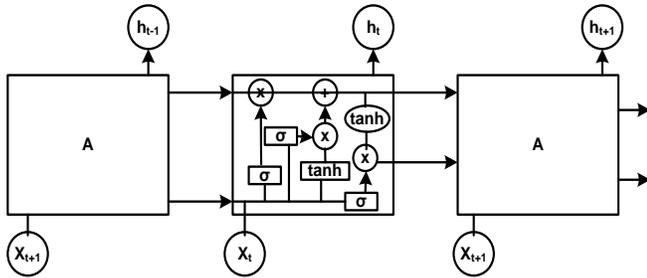


Fig. 4. Conventional Architecture of LSTM.

Observation: RNN is a good option for boosting segmentation performance; however, not much recent research has been carried out in this perspective. Table III highlights the summary.

C. Long Short Term Memory

Long Short Term Memory, also called LSTM, is a typical case of RNN to offer extensive dependencies of long-term learning. It is capable of recording information over a more extended period without much effort. It is noticed that RNN consists of iterative modules formed in the chain for the neural network. In conventional RNN, a single tanh layer is used as a simplified structure for the iterative module. A similar chain-based system also exists in LSTM; however, the structure slightly differs concerning iterative modules. LSTM offers four layers of the interactive structure instead of a single layer. Fig. 4 highlights the conventional architecture of LSTM with multiple blocks of operation, i.e., neural network layer, pointwise operator, vector transfer, concatenation, and copy function.

The prime notion of LSTM is basically about a cell state that linearly runs over the entire chain letting the network simplify the flow of information. A specialized structure is used in LSTM called gates, which can add or eliminate information over the cell state. Usually, conventional gates in LSTM consist of pointwise multiplication operations and use a sigmoid neural network. From the image processing viewpoint, LSTM can be applied to images only after anticipated features have been extracted from them. At present, the applicability of LSTM towards improving the segmentation process of satellite images has been researched

upon by various investigators. It has been noticed that although deep learning is preferred for classifying remote sensing images, simultaneous recognition of multiple objects and extracting their spatial relationship is yet a bigger problem in deep learning. This problem is addressed in Cui et al. [54], where a novel deep learning model is constructed by combining LSTM with fully CNN. The model has used natural language to define the spatial relationship of the remote objects using attention-based LSTM. The model has carried out semantic segmentation of multi-scale using CNN and U-Net entirely for object recognition of remotely sensed images. Nearly similar work is also carried out by Ghosh et al. [55]. A bidirectional LSTM is used along with UNet to extract temporal and spatial features of the satellite images for landcover mapping. The presented study has also used attention-based aggregation for all hidden representations of Spatio-temporal factors using a feedforward neural network followed by softmax normalization and spatial averaging. One of the significant advantages of this model is that it can perform segmentation even if different forms of atmospheric disturbances cover the images. Another recent work carried out by Kalinicheva et al. [56] has carried out a similar direction of study towards analyzing satellite images considering dynamic land cover changes. However, the authors have developed a better version of LSTM by introducing a unique unsupervised approach with an evolution graph. This technique makes use of image segmentation over the changed areas using the graph-based tree-merging method. Combined usage of LSTM and fully CNN has been reported in Sefrin et al. [57], which offers the benefit of using multi-temporal information. Apart from this, a better classification is presented due to adopted preprocessing techniques. Another work carried out by Zhu et al. [58] has developed a hybrid model where the semantic segmentation process is integrated with relearning of post classification. After feature extraction, the model performs an object-based voting system for controlling fluctuation in different classes. Table IV briefs of comparison of existing LSTM based approaches.

Observation: LSTM has been proven for better classification and segmentation performance for satellite images associated with landcover. However, the models don't emphasize its practicality as not many computing units can be used over a system with limited memory or channel capacity. This challenge remains unattended.

TABLE IV. SUMMARY OF EXISTING TECHNIQUES ON LSTM

Authors	Problems	Segmentation Technique	Dataset	Advantages	Limitation
Cui et al. [54]	Object recognition	Semantic segmentation, multi-scale	RSICD	The spatial relation of remote sensing image	Higher processing time
Ghosh et al. [55]	Mapping landcover	Spatiotemporal segmentation, bidirectional LSTM	-Sentinel-based crop mapping. -Planet-based Cashew tree mapping	Effectively mitigate noise	Doesn't consider correlation among a large number of land cover
Kalinicheva et al. [56]	Change detection in landcover	Graph-based tree-merging segmentation	SPOT-5, Sentinel-2	Simplified clustering	Complexity increases with hierarchies of graphs
Sefrin et al. [57]	Change detection in landcover	LSTM, semantic segmentation	Federal State of Saxony	Better classification performance	Studies are not emphasized, unknown classes
Zhu et al. [58]	Change detection in landcover	LSTM, semantic segmentation	QuickBird, WorldView-2	Higher accuracy of classification	Time consumption is still more

D. Staked Auto Encoders

An autoencoder is an unsupervised learning structure characterized by input, hidden, and output layers, while the training operation in autoencoders consists of encoding and decoding. The encoder carries out the mapping of the input data into hidden representation, while the decoder carries out the reconstruction of input data from the hidden representation. The dependable parameters for the encoding process are encoding function, weight matrix, and bias vector. In contrast, dependable parameters for the decoding process are still the same, i.e., decoding function, weight matrix of decoder, and bias vector. To control the reconstruction error, an objective function exists for optimizing it considering the loss function. So, stacked autoencoders are basically about stacking a specific number of n autoencoders into the same n number of hidden layers using a supervised learning approach, as shown in Fig. 5.

Further supervised learning scheme is used for fine-tuning it. At present, there is the evolution of specific schemes that use autoencoders to analyze satellite images. In most existing approaches, the first line of action is to train the initial autoencoders to extract the trained feature vector. The second step is to use that feature vector for the next layer as an input, and it's iterated till the completion of training. Finally, after all the hidden layers are trained, cost minimization is carried out, followed by updating weights. Existing approaches have reported the use of stacked auto encoders for change detection in landcover. The work carried out by Jing et al. [59] has used stacked auto encoders where multi-scale image segmentation is deployed over temporal images followed by the adoption of

CNN to obtain a change map. A stacked autoencoder is used for classification. Usage of a similar principle was also reported in the work of Protopapadakis et al. [60] to evaluate targets over massive unlabeled data. Further denoising auto encoders have been reported in the work of Zhang et al. [61], where a spanning tree has been used for segmentation. The model can extract texture, spatial, and spectral features for all the identified objects, contributing to higher accuracy. Table V summarizes the existing contribution of stacked autoencoders towards segmentation process.

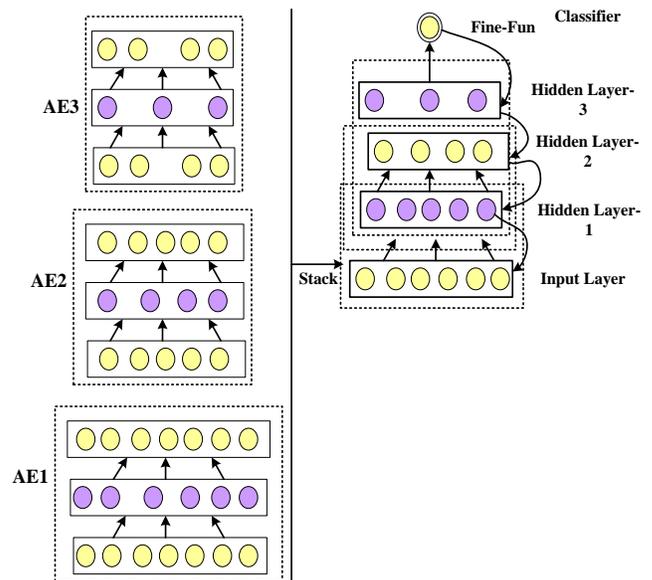


Fig. 5. Conventional Architecture of Stacked Autoencoders.

TABLE V. SUMMARY OF EXISTING TECHNIQUES ON STACKED AUTOENCODERS

Authors	Problems	Segmentation Technique	Dataset	Advantages	Limitation
Jin et al. [59]	Change detection	Multi-scale segmentation	ImageNet	Effective feature extraction	Induce computational complexity
Protopapadakis et al. [60]	Building extraction	Semantic segmentation	Vaihingen city in Germany	Redundancy reduction, Higher accuracy	Increased number of stacks
Zhang et al. [61]	Object classification	Spanning tree	UAV image of Anhui Province, China SPOT5	Higher accuracy	No assessment of computational complexity.

Observation: Deployment of stacked autoencoders is relatively a new scheme used for the segmentation of satellite images. Hence, there are few implementation studies towards stacked auto encoders to improve segmentation performance. Unfortunately, all the analyses using this approach don't find the appropriate number of stacks sufficient for encoding. The computational complexity raised towards maintaining the accumulation of information is not yet resolved in the existing system.

IV. ADOPTION OF DATASET

There are various types of a dataset of satellite images/remote sensing images used for analysis for landcover analysis. One of the essential datasets is the QuickBird dataset [62], which provides massive images of 0.60m Ground Sample Distance resolution and consists of four further multispectral bands with very high resolution ranging from 0.30-0.60m. The images were captured from 2001 to 2015 with an orbit height of 450 km. The following important dataset is Google Earth Satellite Imageries [63] which includes a raster dataset of satellites easier to be processed by any scripting environment. This is a massive dataset of satellite imageries consisting of a different crop type digital map, vegetation map, oil map, terrestrial field plots, elevation, human population, forest, water cover, etc. It also consists of Landsat satellite images with 30 meters resolution considered highly updated thermal and multispectral data [64]. MODIS [65] and Sentinel [66] is another dataset developed in collaboration with the Google dataset itself. MODIS dataset consists of satellite images ranging from 250m-1000m of snow cover, surface temperature, surface reflectance, leaf area index, and thermal anomalies, usually retrieved on 16days duration from Aqua and Terra spacecraft.

Further, the Sentinel dataset is a part of the European Space Agency consists of optimal high-resolution images (from Sentinel 1A/1B), land-ocean-climate images (Sentinel-3), and air quality images (from Sentinel-5P). They are frequently used in current research to analyze climatic change, emergency management, atmospheric monitoring, Marine monitoring, land monitoring. SPOT-5 dataset is another contribution for the European Space Agency [67], where the images were collected between 2002 and 2015 with an orbit height of 832 km and an orbit duration of 101 min. Similar organization of European Space Agency also offers RADARSAT-2 dataset whose resolution ranges from 9.0-160m [68]. This is the most updated dataset captured between 2008 and 2021, with both medium and very high resolution of wavelength between 5.2-7.7 cm. Inria Aerial image dataset consists of labeled remotely sensed images with 810 square kilometers [69]. With a spatial resolution of 0.3m, this dataset has color imageries with ground truth data and two semantics classes. This dataset consists of alpine towers, densely populated areas, and irregular urban settlements. A sample dataset for Inria is shown in Fig. 6, which exhibits sample Chicago landcover (Fig. 6(a)) and its reference as ground truth (Fig. 6(b)). The presence of reference/ground truth image assists in evaluating the correctness of analysis models, and hence this dataset is widely adopted.

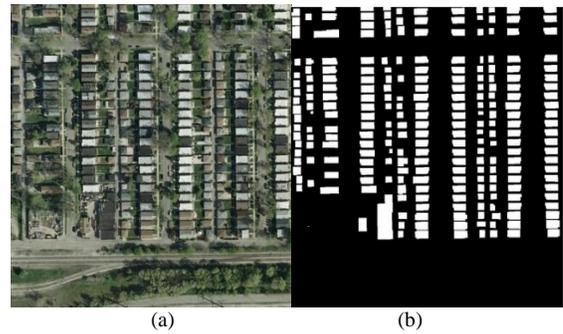


Fig. 6. Sample INRIA Dataset.

Existing studies have also been carried out considering the MNIST dataset, a benchmarked dataset for satellite images as a part of Kaggle [70]. This labeled dataset is managed in the form of images and CSV files. Kaggle dataset also consists of a DSTL dataset consisting of image identity with class type over its labeled area [71]. The dataset is maintained in 3/16-band satellite images with a resolution range of 0.31-7.5 m. The next dataset found in the current study is the ISPRS dataset, consisting of an indoor scene, old buildings, aerial images of specific locations, and satellite images of different parts of the earth [72]. Another dataset adopted in the current study is remote Sensing Image Captioning Dataset (RSICD) collected from the different applications of Google with all images with 224x224 pixels and 10921 remote sensing images [73]. Apart from the above-mentioned standard dataset, existing literature has also reported usage of another dataset too viz. Planetscope satellite images [74], GIS data [75], Pleiades VHSR, Corine Land Cover [76], OpenStreetMap [77], Cropland Data Layer [78], WorldView-2 [79], ImageNet [80]. It should be noted that all the dataset has the different characteristic of data of satellite images.

Fig. 7 showcases the adoption of different datasets towards the study of analyzing satellite images. The graphical trends shown in the above figure are obtained from filtering relevant research papers published between 2011 and 2021. It showcases that MODIS, Sentinel, and QuickBird are the most frequently adopted dataset by the researchers. Table VI highlights the comparative characteristic of different satellite image dataset with respect to spatial resolution. It should be noted that different dataset has different types of characteristic which is mainly based on the process of acquisition of signal. Hence, the proposed study considers highlighting spatial resolution of the images being captured to be mentioned in Table VI.

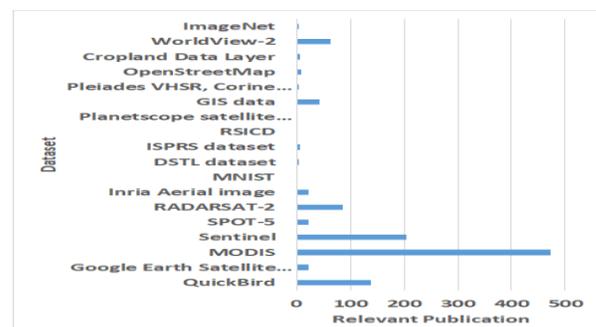


Fig. 7. Adoption of Dataset in Research Work.

TABLE VI. CHARACTERISTICS OF SATELLITE IMAGE DATASET

Satellite Image dataset	Resolution
QuickBird dataset [62]	0.30-0.60 m
Google Earth Satellite Imageries [63]	30 m
MODIS [65]	250-1000m
Sentinel [66]	10-60 m
SPOT-5	10 m-600 KM
RADARSAT-2	10-100m
Inria Aerial image dataset [69]	0.3 m
MNIST dataset [70]	0.3-0.7 m per pixel
DSTL dataset [71]	0.31-7.5 m
PlanetScope satellite images [74]	3.75m-50 cm
GIS data [75]	125 m
Pleiades VHSR, Corine Land Cover [76]	20 m
OpenStreetMap[77]	100 dpi
Cropland Data Layer [78]	30-56m
WorldView-2 [79]	0.46 m
ImageNet [80]	64x64 pixels

V. RESEARCH TRENDS

At present, various Deep Learning (DL) approaches are being implemented towards analyzing satellite images / remotely sensed images. Last five years, data from IEEE Xplore digital archives have been studied to arrive at the inevitable conclusion of research trends.

From Fig. 8, it can be seen that the number of adoption of deep learning has been spontaneously increasing in the last five years. There are more probabilities towards the continuation of similar trends in upcoming years.

From Fig. 9, it is noticed that CNN is the dominant DL approach compared to other DL variants, i.e., RNN, LSTM, Stacked Autoencoders, Fully Convolution Network (FCN), and Deep Belief Network (DBN). Also, there is increasing adoption of LSTM and FCN approaches; however, they are significantly less in numbers. Hence, chances are more for CNN to be dominant in coming years too.

From Fig. 10, it is noticed that urban-based application is more investigated, followed by a water-based application using DL methods. The urban-based application will include identifying land covers, mainly exhibiting that it will focus on the research area.

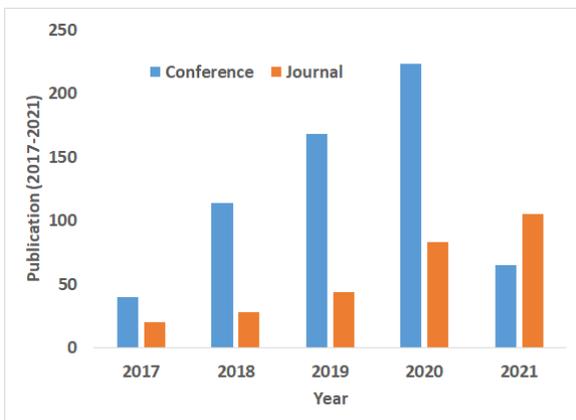


Fig. 8. Year-Wise Trends of DL-Approaches on Satellite Images.

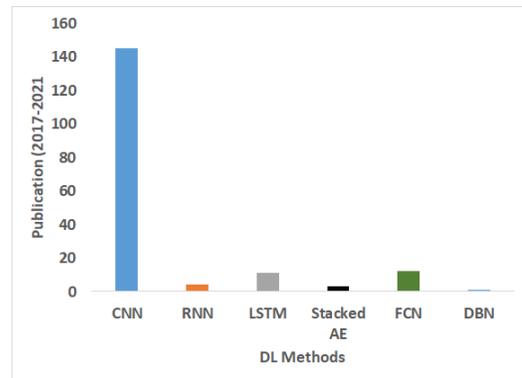


Fig. 9. Trends towards Taxonomies of DL-Approaches on Satellite Images.

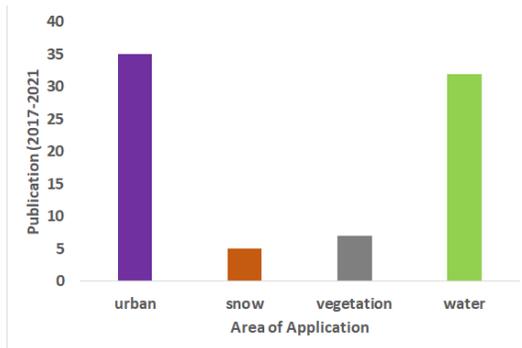


Fig. 10. Trends of Application Area Year-Wise Trends of DL-Approaches on Satellite Images.

This outcome eventually shows a higher scope of continued research work using DL methods towards satellite images in more progressive order. These findings of the research trend are one of the essential contributions of this manuscript.

VI. REVIEW CONTRIBUTION

From the prior section, it can be seen that various degree of research work is being carried out towards the segmentation of satellite images. It should be noted that not all deep learning mechanisms have implemented segmentation towards the input image. This paper has discussed only the research work where segmentation has been applied. The *scope* of this paper is i) the paper considers discussion of approaches published in last five years, ii) the paper emphasizes assessing the impact of different deep learning models towards segmentation. After reviewing different taxonomies of deep learning methods towards segmentation, different points of research gap are concluded that are briefed as follows:

A. Research Gap

The essential research gap explored after reviewing existing approaches are as follows:

- Unattended Computational Problems in Deep Learning: Despite the frequently adopted technique, the studies using deep learning have witnessed an evident trade-off between achieving simplification in learning (positive point) and poor computational performance (negative point). Almost all the CNN

approaches studied in this paper are witnessed with lower performance scalability or increased computational complexities. Unless lower computational complexities characterize the framework; it is eventually not feasible to prove its application over real-life resourced defined computing devices. This fact is also witnessed for almost all deep learning techniques.

- **Complexities of Satellite Images:** Irrespective of any dataset of satellite imageries, it is now known that such images are accompanied by various challenges, from analyzing the raw sensed image to obtaining higher accuracy by extracting essential features. Although, deep learning methods can only be applied if the preprocessing is effectively carried out, which is missing in the most implementations. Hence, it is essential to preprocess the satellite image before feature extraction because it consists of a large amount of information. The deep learning method can automate the process for better classification; however, it will still depend on practical preprocessing input images before training.
- **Biased Focused on Segmentation Approach:** A closer look into existing approaches shows a majority of semantic segmentation methods used over satellite images. Such a technique labels each pixel concerning the associated class of satellite images, further subjected to dense prediction. One of the pitfalls of such an approach is that instances of the same classes are not segmented, potentially affecting landcover applications. Apart from this, various methods reported in this paper using deep learning don't include object irregularity, illumination factor, poor contrast, noise, etc. The exclusion of these points will eventually affect the accuracy of classification using deep learning.
- **Less Emphasis towards Computational Performance:** Although there are more comprehensive deep learning approaches to analyze satellite images, it is essential to identify the proper model. Different models have different performance patterns, and there is no full-proof deep learning model generalized towards analyzing satellite images. Inappropriate selection of deep learning model towards segmentation is a complex task as segmentation operation to be applied wholly subjected and application-oriented. This eventually leads to computational complexities, evident from limiting points found in existing studies discussed in this paper. Without addressing computational performance, it is quite questionable to understand their applicability.

B. Discussion

A closer look into the deep learning approaches shows many methods for analyzing satellite images, but not much work is reported towards segmentation approaches. One interesting observation noted in all segmentation-based approaches is that almost every research work has adopted different datasets with different properties and implemented

them. Although Sentinel, MODIS, and QuickBird are frequently adopted datasets, they differ in addressing different problems. A better form of progressive work towards a deep learning approach is required considering a large scale similar dataset first, which can be compared with other existing datasets later. But this is not the case with existing methods. Another observation is that existing approaches are not witnessed much with scalable and consistent performance. LSTM, which is considered a better variant of RNN, is seen with time consumption and increased complexities in many cases. This is because architecture towards an extensive memory system is theoretically proven, and its performance doesn't scale up when exposed to a complex and challenging environment. Apart from this, CNN has implemented either individually or in combination with other training models. The standalone implementation of CNN towards the segmentation process is witnessed with various challenges that are not attended. The first challenge in standalone CNN implementation is associated with the drastically slower operation that consumes enough training time for the larger size of the satellite image. None of the existing studies has reported overcoming the dependencies of a resourceful graphical processing unit for supporting extensive layers of training in CNN. Apart from this, after the object is identified from satellite images using the CNN technique, it must be encoded for better accuracy. However, it is not feasible for CNN to encode pixel position and identify changes in object orientation. This will potentially affect the accuracy. Hence, there is a need to address the inherent issues of deep learning and attend to other matters.

VII. CONCLUSION

Remote sensing and satellite images have become essential applications for change detection and classification. With an increasing rise of deep learning-based approaches for analyzing satellite images, the idea of this paper is to review the existing approaches associated with segmentation. The novelty points of this paper are i) existing review papers has reviewed semantic segmentation, segmentation with specific application, whereas the proposed review paper has explicitly discussed all the recent segmentation approaches using deep learning with various application grounds offering more technical insights, ii) proposed review contributes to updated research trends to understand most dominant deep learning-based technique suitable for segmentation, iii) each study has been discussed concerning good points and limiting factors for offering more granularity in review findings, iv) the proposed review work contributes towards research gap followed by a discussion to know less spoken information about strength and weakness of existing schemes.

Future work will be further carried out to address the research gap identified in this paper. A computational framework can be designed to consider various artifact inclusion combined that has never been done before. This will offer a scope to introduce a novel preprocessing approach that can potentially contribute to the enriched feature extraction process. Further, a novel deep learning model can be framed, emphasizing reduced training demands, reduced processing time, and optimal computational performance.

REFERENCES

- [1] I.L.Turnera, M. D. Harleya, R. Almarb, E.W.J.Bergsma, "Satellite optical imagery in Coastal Engineering", Elsevier-ScienceDirect, Coastal Engineering, Vol.167, August 2021.
- [2] H. Zhang, H. Liu, Y. Wang, "A new scheme for urban impervious surface classification from SAR images", ISPRS Journal of Photogrammetry and Remote Sensing, vol.139, 2018.
- [3] K. Maurya, S. Mahajan, & N. Chaube, "Remote sensing techniques: mapping and monitoring of mangrove ecosystem—a review" Springer-Open Access-Journal for Complex and Intelligent System, 2021.
- [4] R. Pazur, B. Price, & P. M. Atkinson, "Fine temporal resolution satellite sensors with global coverage: an opportunity for landscape ecologists", Springer-Open Access, Research Article for Landscape Ecology, vol.36, pp.2199-2213, 2021
- [5] V. Yu. Ignatiev, I. A. Matveev, A. B. Murynin, A. A. Usmanova & V. I. Tsurkov, "Increasing the Spatial Resolution of Panchromatic Satellite Images Based on Generative Neural Networks", Springer, Journal of Computer and Systems Sciences International, Vol.60, pp.239-247, 2021.
- [6] C. Vallentin, K. Harfenmeister, S. Itzerott, B. Kleinschmit, C. Conrad & D. Spengler, "Suitability of satellite remote sensing data for yield estimation in northeast Germany", Springer-Open Access Journal for Precision Agriculture, 2021.
- [7] P. Gudžius, O. Kurasova, V. Darulis & E. Filatovas, "Deep learning-based object recognition in multispectral satellite imagery for real-time applications", Springer-Machine Vision and Application, vol.32, Article No.98, 2021.
- [8] S. Srivastava, A. V. Divekar, C. Anilkumar, I. Naik, V. Kulkarni & V. Pattabiraman, "Comparative analysis of deep learning image detection algorithms" Springer-Open Access Journal of Big Data, Vol.8, Article No.66, 2021.
- [9] J. Nalepa, M. Myller, M. Cwiek, L. Zak, T. Lakota, L. Tulczyjew, and M. Kawulo, "Towards On-Board Hyperspectral Satellite Image Segmentation: Understanding Robustness of Deep Learning through Simulating Acquisition Conditions", MDPI Journal of Remote Sensing, vol.13, Iss.1532, 2021.
- [10] El-Habib Bensikaddour, Y. Bentoutou, N. Taleb, "Embedded implementation of multispectral satellite image encryption using a chaos-based block cipher", ScienceDirect-Journal of King Saud University - Computer and Information Sciences, Vol.32, Iss.1, pp.50-56, 2020.
- [11] A. Hagag, I. Omara, S. Chaib, X. Fan, F. E. Abd El-Samie, "Distributed Coding and Transmission Scheme for Wireless Communication of Satellite Images", Springer- International Conference on Computer and Information Science, Computer and Information Science, pp 29-42, 2017.
- [12] D. Yan, H. Yi, D. He, K. Guan, B. Ai, Z. Zhong, J. Kim, H.Chung, "Channel Characterization for Satellite Link and Terrestrial Link of Vehicular Communication in the mmWave Band", IEEE-Open Access, vol.7, 2019.
- [13] A. M. Crisan, A. Martian, R. Cacoveanu, D. Coltuc, "Angle-of-Arrival Estimation in Formation Flying Satellites: Concept and Demonstration", IEEE-Access, vol.7, 2019.
- [14] I. F. Akyildiz, A. Kak, S.Nie, "6G and Beyond: The Future of Wireless Communications Systems", IEEE Access, vol.8, 2020.
- [15] J. Thrane, D. Zibar, H. L. Christiansen, "Model-Aided Deep Learning Method for Path Loss Prediction in Mobile Communication Systems at 2.6 GHz", IEEE Access, vol.8, 2020.
- [16] M. Ju, C. Ding, Y.J Guo, D. Zhang, "Remote Sensing Image Haze Removal Using Gamma-Correction-Based Dehazing Model", IEEE-Access, vol.7, 2019.
- [17] N. A. Golilarz, H. Gao, S. Pirasteh, M. Yazdi, J. Zhou, and Y. Fu, "Satellite Multispectral and Hyperspectral Image De-Noising with Enhanced Adaptive Generalized Gaussian Distribution Threshold in the Wavelet Domain", MDPI-Remote Sensing, vol.13, Iss.101, 2021.
- [18] B. Dhruv, N. Mittal and M. Modi, "Analysis of different filters for noise reduction in images," 2017 Recent Developments in Control, Automation & Power Engineering (RDCAPE), pp. 410-415, doi: 10.1109/RDCAPE.2017.8358306, 2017.
- [19] L. Fan, F. Zhang, H. Fan & C. Zhang, "Brief review of image denoising techniques", Springer-Open Access-Visual Computing for Industry, Biomedicine, and Art, Vol.2, Article No.7, 2019.
- [20] S. Mahajan & B. Fataniya, "Cloud detection methodologies: variants and development—a review", Springer-Open Access, Survey and State of the Art, vol.6, pp.251-261, 2020.
- [21] J-R Lee, C-Y Chung, & M-L Ou, "Fog detection using geostationary satellite data: Temporally continuous algorithm", Springer-Asia-Pacific Journal of Atmospheric Sciences, vol.47, pp.113-122, 2011.
- [22] G. P. Obi ReddyS. K. Singh, "Geospatial Technologies in Land Resources Mapping, Monitoring and Management", Springer-Geotechnologies and the Environment book series, vol.21, 2018.
- [23] https://cimss.ssec.wisc.edu/satmet/modules/5_sat_images/si-1.html. Retrieved on 17-November, 2021.
- [24] L. Zhu, J. Suomalainen, J. Liu, J. Hyyppa, H. Kaartinen and H. Haggren, "A Review: Remote Sensing Sensors", IEEE-Open access peer-reviewed chapter, IntechOpen, 2017.
- [25] N. Verde, G. Mallinis, M.T. Strati, C. Georgiadis, and P. Patias, "Assessment of Radiometric Resolution Impact on Remote Sensing Data Classification Accuracy", MDPI-Remote Sensing, vol.10, Iss.8, 2018.
- [26] Unsalan, Cem, Boyer, Kim L. "Multispectral Satellite Image Understanding", Springer-Advances in Computer Vision and Pattern Recognition, 2011.
- [27] Hemanth, D. Jude, "Artificial Intelligence Techniques for Satellite Image Analysis", Springer-Remote Sensing and Digital Image Processing, 2020.
- [28] A. Asokan, J. Anitha, M. Ciobanu, A. Gabor, A. Naaji, and D. Jude Hemanth, "Image Processing Techniques for Analysis of Satellite Images for Historical Maps Classification—An Overview", MDPI-Applied Science, vol.10, Iss.12, 2020.
- [29] Alshehhi, R.; Marpu, P.R. Hierarchical graph-based segmentation for extracting road networks from high-resolution satellite images. ISPRS J. Photogramm. Remote Sens. 126, 245–260, 2017.
- [30] S. Pare, A.K. Bhandari, A. Kumar, G.K. Singh, "A new technique for multilevel color image thresholding based on modified fuzzy entropy and Lévy flight firefly algorithm". ScienceDirect-Computers & Electrical Engineering, vol.70, pp.476–495, 2018.
- [31] D. Marmanis, K. Schindler, J.D. Wegner, S. Galliani, M. Datcu, U. Stilla, "Classification with an edge: Improving semantic image segmentation with boundary detection", ISPRS Journal of Photogramm. Remote Sensing, 135, 158–172, 2018.
- [32] I. Grinias, C. Panagiotakis, G. Tziritas, "MRF-based segmentation and unsupervised classification for building and road detection in peri-urban areas of high-resolution satellite images", ISPRS Journal of Photogramm. Remote Sens, 122, 145–166, 2016.
- [33] S. Suresh, S. Lal, "An efficient cuckoo search algorithm based multilevel thresholding for segmentation of satellite images using different objective functions". Expert System Application, 58, 184–209, 2016.
- [34] A. Sayer, Y. Govaerts, P. Kolmonen, A. Lipponen, M. Luffarelli, T. Mielonen, "A review and framework for the evaluation of pixel- level uncertainty estimates in satellite aerosol remote sensing". Atmos. Meas. Tech. 13, 373–404, 2020. doi:10.5194/amt-13-373-2020.
- [35] L. Liang, and L. Di Girolamo, L., "A global analysis on the view-angle dependence of plane-parallel oceanic liquid water cloud optical thickness using data synergy from MISR and MODIS". Journal of Geophysical Research Atmospheres vol.118, pp.2389–2403, 2013 doi:10.1029/2012JD018201.
- [36] A. Shelestov et al., "Cloud Approach to Automated Crop Classification Using Sentinel-1 Imagery," in IEEE Transactions on Big Data, vol. 6, no. 3, pp. 572-582, 1 Sept. 2020, doi: 10.1109/TBDATA.2019.2940237.
- [37] D.P. Kingma,; J.A. Ba, "A method for stochastic optimization". arXiv 2014, arXiv:1412.6980.
- [38] S. Ioffe, S. Szegedy, "Batch normalization: Accelerating deep network training by reducing internal covariate shift", arXiv 2015, arXiv:1502.03167.

- [39] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, R. Salakhutdinov, "Dropout: A simple way to prevent neural networks from overfitting". *Journal of Machine Learning Research*, vol. 15, pp. 1929–1958, 2014.
- [40] K. He, X. Zhang, S. Ren, J. Sun, "Delving deep into rectifiers: Surpassing human-level performance on imagenet classification". In *Proceedings of the IEEE International Conference on Computer Vision, Santiago, Chile, 7–13 December 2015*; pp. 1026–1034.
- [41] M. Wurma, T. Stark, X. X. Zhu, M. Weigand, H. Taubenböck, "Semantic segmentation of slums in satellite images using transfer learning on fully convolutional neural networks", *Elsevier-ISPRS Journal of Photogrammetry and Remote Sensing*, vol.150, pp.59-69, 2019.
- [42] J. Zhang, Q. Hu, J. Li and M. Ai, "Learning From GPS Trajectories of Floating Car for CNN-Based Urban Road Extraction With High-Resolution Satellite Imagery," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 59, no. 3, pp. 1836-1847, March 2021, doi: 10.1109/TGRS.2020.3003425.
- [43] Q. Li, Y. Shi, X. Huang and X. X. Zhu, "Building Footprint Generation by Integrating Convolution Neural Network With Feature Pairwise Conditional Random Field (FPCRF)," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 58, no. 11, pp. 7502-7519, Nov. 2020, doi: 10.1109/TGRS.2020.2973720.
- [44] I. V. Saetchnikov, E. A. Tcherniavskaia and V. V. Skakun, "Object Detection for Unmanned Aerial Vehicle Camera via Convolutional Neural Networks," in *IEEE Journal on Miniaturization for Air and Space Systems*, vol. 2, no. 2, pp. 98-103, June 2021, doi: 10.1109/JMASS.2020.3040976.
- [45] N. Wang, B. Li, X. Wei, Y. Wang and H. Yan, "Ship Detection in Spaceborne Infrared Image Based on Lightweight CNN and Multisource Feature Cascade Decision," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 59, no. 5, pp. 4324-4339, May 2021, doi: 10.1109/TGRS.2020.3008993.
- [46] Y. Jiang, "Research on road extraction of remote sensing image based on convolutional neural network", *Eurasip Journal on Image and Video processing*, 2019.
- [47] C. Persello and A. Stein, "Deep Fully Convolutional Networks for the Detection of Informal Settlements in VHR Images," in *IEEE Geoscience and Remote Sensing Letters*, vol. 14, no. 12, pp. 2325-2329, Dec. 2017, doi: 10.1109/LGRS.2017.2763738.
- [48] L. Wang, K. A. Scott, L. Xu and D. A. Clausi, "Sea Ice Concentration Estimation During Melt From Dual-Pol SAR Scenes Using Deep Convolutional Neural Networks: A Case Study," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 54, no. 8, pp. 4524-4533, Aug. 2016, doi: 10.1109/TGRS.2016.2543660.
- [49] M. C. Taberner, F. J. Garcia-Haro, B. Martínez, E. I. Verdiguier, C. Atzberger, G. C. Valls, & M. A. Gilabert, "Understanding deep learning in land use classification based on Sentinel-2 time series", *Open-Access-Scientific Reports*, vol.10, 2020.
- [50] M. O. Turkoglu, S. D'Aronco, J. D. Wegner, and K. Schindler, "Gating Revisited: Deep Multi-layer RNNs That Can Be Trained", *arXiv:1911.11033v4 [cs.CV]* 6 Mar 2021.
- [51] D. Ienco, R. Gaetano, C. Dupaquier and P. Maurel, "Land Cover Classification via Multi-temporal Spatial Data by Recurrent Neural Networks", *arXiv:1704.04055v1 [cs.CV]* 13 Apr 2017.
- [52] E. Maggiori, G. Charpiat, Y. Tarabalka and P. Alliez, "Recurrent Neural Networks to Correct Satellite Image Classification Maps," in *IEEE Transactions on Geoscience and Remote Sensing*, vol. 55, no. 9, pp. 4962-4971, Sept. 2017, doi: 10.1109/TGRS.2017.2697453.
- [53] Z. Sun, L. Di, "Using long short-term memory recurrent neural network in land cover classification on Landsat and Cropland data layer time series", *Taylor and Francis, International Journal of Remote Sensing*, vol.40, Iss.2, 2019.
- [54] W. Cui, F. Wang, X. He, D. Zhang, X. Xu, M. Yao, Z. Wang and J. Huang, "Multi-Scale Semantic Segmentation and Spatial Relationship Recognition of Remote Sensing Images Based on an Attention Model", *MDPI-Remote Sensing*, vol.11, 2019.
- [55] R. Ghosh, P. Ravirathinam, X. Jia, C. Lin, Z. Jin, V. Kumar, "Attention-augmented Spatio-Temporal Segmentation for Land Cover Mapping", *arXiv:2105.02963v2 [cs.CV]* 14 Sep 2021.
- [56] E. Kalinicheva, D. Ienco, J. Sublime, M. Trocan, "Unsupervised Change Detection Analysis in Satellite Image Time Series using Deep Learning Combined with Graph-Based Approaches". *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, IEEE, 2020, 13, pp.1450-1466.
- [57] O. Sefrin, F. M. Riese, and S. Keller, "Deep Learning for Land Cover Change Detection", *MDPI-Remote Sensing*, Vol.13, 2021.
- [58] Y. Zhu, C. Geiß, E. So and Y. Jin, "Multitemporal Relearning With Convolutional LSTM Models for Land Use Classification," in *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 14, pp. 3251-3265, 2021, doi: 10.1109/JSTARS.2021.3055784.
- [59] R. Jing, Z. Gong and H. Guan, "Land Cover Change Detection With VHR Satellite Imagery Based on Multi-Scale SLIC-CNN and SCAE Features," in *IEEE Access*, vol. 8, pp. 228070-228087, 2020, doi: 10.1109/ACCESS.2020.3045740.
- [60] E. Protopapadakis, A. Doulamis, N. Doulamis, and E. Maltezos, "Stacked Autoencoders Driven by Semi-Supervised Learning for Building Extraction from near Infrared Remote Sensing Imagery", *MDPI-Remote Sensing*, vol.13, 2021.
- [61] X. Zhang, G. Chen, W. Wang, Q. Wang and F. Dai, "Object-Based Land-Cover Supervised Classification for Very-High-Resolution UAV Images Using Stacked Denoising Autoencoders," in *IEEE Journal of Selected Topics in Applied Earth Observations and Remote Sensing*, vol. 10, no. 7, pp. 3373-3385, July 2017, doi: 10.1109/JSTARS.2017.2672736.
- [62] <https://earth.esa.int/eogateway/catalog/quickbird-full-archive>, Retrieved on 19 Sep-2021.
- [63] <https://developers.google.com/earth-engine/datasets/catalog>, Retrieved on 19 Sep-2021.
- [64] https://www.usgs.gov/core-science-systems/nli/landsat/landsat-data-access?qt-science_support_page_related_con=0#qt-science_support_page_related_con, Retrieved on 19 Sep-2021.
- [65] <https://modis.gsfc.nasa.gov/data/>, Retrieved on 19 Sep-2021.
- [66] <https://sentinel.esa.int/web/sentinel/sentinel-data-access>, Retrieved on 19 Sep-2021.
- [67] <https://earth.esa.int/eogateway/missions/spot-5>, Retrieved on 19 Sep-2021.
- [68] <https://earth.esa.int/eogateway/catalog/radarsat-2-esa-archive>, Retrieved on 19 Sep-2021.
- [69] <https://project.inria.fr/aerialimagelabeling/>, Retrieved on 19 Sep-2021.
- [70] <https://www.kaggle.com/datamunge/overheadmnist>, Retrieved on 19 Sep-2021.
- [71] <https://www.kaggle.com/c/dstl-satellite-imagery-feature-detection>, Retrieved on 19 Sep-2021.
- [72] <https://www.isprs.org/data/>, Retrieved on 19 Sep-2021.
- [73] https://github.com/201528014227051/RSICD_optimal, Retrieved on 19 Sep-2021.
- [74] <https://www.planet.com/products/planet-imagery/>, Retrieved on 19 Sep-2021.
- [75] <https://www.usgs.gov/products/data-and-tools/gis-data>, Retrieved on 19 Sep-2021.
- [76] <https://land.copernicus.eu/pan-european/corine-land-cover>, Retrieved on 19 Sep-2021.
- [77] <https://www.openstreetmap.org/#map=5/51.495/-0.088>, Retrieved on 19 Sep-2021.
- [78] <https://catalog.data.gov/dataset/cropscape-cropland-data-layer>, Retrieved on 19 Sep-2021.
- [79] <https://www.satimagingcorp.com/satellite-sensors/worldview-2/>, Retrieved on 19 Sep-2021.
- [80] <https://www.image-net.org/update-mar-11-2021.php>, Retrieved on 19 Sep-2021.

DNA Profiling: An Investigation of Six Machine Learning Algorithms for Estimating the Number of Contributors in DNA Mixtures

Hamdah Alotaibi¹, Fawaz Alsolami²

Department of Computer Science
Faculty of Computing and Information Technology
King Abdulaziz University
Jeddah 21589, Saudi Arabia

Rashid Mehmood³

High Performance Computing Center
King Abdulaziz University
Jeddah 21589, Saudi Arabia

Abstract—DNA (Deoxyribonucleic acid) profiling involves analysis of sequences of individual or mixed DNA profiles to identify persons these profiles belong to. DNA profiling is used in important applications such as for paternity tests, in forensic science for person identification on a crime scheme, etc. Finding the number of contributors in a DNA mixture is a major task in DNA profiling with challenges caused due to allele dropout, stutter, blobs, and noise. The existing methods for finding the number of unknowns in a DNA mixture suffer from issues including computational complexity and accuracy of estimating the number of unknowns. Machine learning has received attention recently in this area but with limited success. Many more efforts are needed for improving the robustness and accuracy of these methods. Our research aims to advance the state-of-the-art in this area. Specifically, in this paper, we investigate the performance of six machine learning algorithms -- Nearest Neighbors (KNN), Random Forest (RF), Support Vector Machine (SVM), Logistic Regression (LR), Stochastic Gradient Descent (SGD), and Gaussian Naïve-Bayes (GNB) -- applied to a publicly available dataset called PROVEDIt, containing mixtures with up to five contributors. We evaluate the algorithmic performance using confusion matrices and four performance metrics namely accuracy, F1-Score, Recall, and Precision. The results show that LR provides the highest Accuracy of 95% for mixtures with five contributors.

Keywords—Machine learning; DNA profiling; DNA mixtures; forensic science

I. INTRODUCTION

Between different individuals, most of the genome is the same. However, there are some differences, and here comes the science of Deoxyribonucleic acid (DNA) profiling. It is the process that takes benefit from these differences and gives the ability to distinguish between individuals [1]. DNA profiling analyzes DNA sequences that are referred to as genetic markers. The most commonly used genetic marker is Short Tandem Repeats (STRs) [1]. DNA profiling is used in important applications such as for paternity tests, in forensic science for person identification on a crime scheme, etc. [2]. Determining the number of contributors is one of the essential stages in DNA profiling. This task is often not straightforward because of the challenges that could appear, caused due to allele dropout, stutter, blobs, and noise [3], [4].

The current methods for finding the number of unknowns in DNA mixtures can be divided into three types [5]. The first type includes the basic methods which are compute-intensive, are slow, and have accuracy issues (e.g., [6]). The second type includes high-performance computing (HPC) methods, which are faster but highly compute-intensive, and their accuracy requires significant improvements (e.g., [7]). The third type includes machine learning methods that are faster but their classification accuracies and robustness need to be improved, requiring many more efforts in this direction (e.g., [8]).

Recent years have seen rapid and considerable growth in using machine learning in different fields, showing promising results [9]. However, when dealing with inferring the number of contributors in the DNA profile mixture, few researchers have addressed the effect of using machine learning to solve this challenge. To the best of our knowledge, there are three works to date [8], [10], [11], and each one deals with the problem from a different perspective. The research on machine learning based DNA profiling is in its infancy, many more works are needed to improve the diversity and accuracy of the machine learning methods. Our research aims to advance the state-of-the-art in the DNA profiling domain. Specifically, in this paper, we investigate the performance of six machine learning algorithms -- Nearest Neighbors (KNN), Random Forest (RF), Support Vector Machine (SVM), Logistic Regression (LR), Stochastic Gradient Descent (SGD), and Gaussian Naïve-Bayes (GNB) -- applied to a publicly available dataset called PROVEDIt. The dataset contains DNA mixtures with up to five contributors.

We have investigated the performance of these algorithms in detail using four performance metrics namely accuracy, F1-Score, Recall, and Precision. The performance of each algorithm has been analyzed using confusion matrices and graphs of the four matrices for each of the five classes, One-Person, Two-Person, Three-Person, Four-Person, and Five-Person.

For KNN, the highest values for the F1-Score, Recall, and Precision metrics were achieved, all for the Five-Persons class, at 68%, 62%, 75%, respectively. For the RF algorithm, the highest values for the F1-Score, Recall, and Precision metrics were achieved for the Five-Persons class at 86%, One-Person class at 88%, and the Five-Persons class at 90%, respectively.

For SVM, the highest values for the F1-Score, Recall, and Precision metrics were achieved, all for the Five-Persons class, at 96%, 96%, 95%, respectively. For SGD, the highest values for the F1-Score, Recall, and Precision metrics were achieved for the Five-Persons class at 93%, both One-Person and Five-Person classes at 100%, and the Five-Persons class at 88%, respectively. For LR, the highest values for the F1-Score, Recall, and Precision metrics were achieved for the One-Person class at 97%, Five-Persons class at 98%, and the One-Person class at 97%, respectively. For GNB, the highest values for the F1-Score, Recall, and Precision metrics were achieved for the Three-Persons class at 71%, Three-Persons class at 83%, and the Five-Persons class at 100%, respectively. The highest Accuracy over all the algorithms was achieved by the LR algorithm at 95% for mixtures with up to five contributors.

The rest of the paper is organized as follows. Section II briefly reviews the related works. Section III describes the methodology of the proposed work. Section IV presents results and their analyses for the six machine learning algorithms. Section V contains the conclusion and future work.

II. RELATED WORK

The methods for estimating the number of contributors in a DNA mixture can be divided into three types. These are basic methods, HPC methods, and machine learning-based methods. The basic methods and tools include, among others, Maximum Allele Count (MAC) [6], Total Allele Count (TAC) [11], MLE [12], DNA Mixtures [13], Lab Retriever [14] and DNA MIX [15]. The parallel or HPC methods include Euroformix [16], LikeLTD [17] and NOCI [4], [5], [18]. To the best of our knowledge, only three works have used machine learning to determine the number of contributors in a DNA profile. Since machine learning is the focus of our research, these three methods are reviewed below in some detail.

Marciano and Adelman [8] evaluated five machine learning algorithms, and finally, they chose the SVM that reached 98% accuracy in the training stage and 97% accuracy in the testing stage for four contributors. Note that the 97% accuracy is on a dataset with up to four contributors compared to five contributors where typically the accuracy will be lower due to a larger number of classes. The data that they have used consists of 1405 profiles from 20 individuals. Benschop et al. [11] examined ten machine learning algorithms, and finally, they chose the RFC model with 19 features. They used 590 profiles that range from a single person to five person mixtures. They removed both Amelgenin and Y-chromosomal markers. There were more than 250 features for each profile, but they chose only the best 50 features. In terms of Accuracy, they got (83%). Kruijver et al. [10] use decision trees in their work. They used 766 profiles from Global filer multiplex with a 25-second injection. In terms of Accuracy, they got from (77.9% - 85.2%).

The research on machine learning based DNA profiling is in its infancy, many more works are needed to improve the diversity and accuracy of the machine learning methods. Our research aims to advance the state-of-the-art in the DNA profiling domain. Specifically, in this paper, we investigate the performance of six machine learning algorithms.

III. METHODOLOGY AND DESIGN

This section presents the proposed methodology for this work, depicted in Fig. 1. Section A will give a short explanation of the dataset that has been used. Section B will explain the ML models used in this work, and finally, Section C will show the evaluation metrics used.

A. The Dataset

The data in terms of DNA profiles have been taken from the public dataset PROVEDIt [19]. This dataset contains more than 25,000 STR profiles containing DNA mixtures that range from one to five contributors. The dataset contains more than one kit with different cycles number and injection times. Fig. 2 shows the number of profiles that we have taken from this dataset. We took 156 profiles to represent each class among the five classes, and we ended with 780 DNA profile mixtures, which means that we have 18720 samples (780 profiles * 24 markers). When we collected the data, we made sure it contained different injection times and cycle numbers.

We encountered more than one challenge for the preprocessing stage, including dealing with empty cells, OL values and deleting the unwanted markers. All of these challenges were addressed during the pre-processing phase in order to prepare the dataset for the classification stage.

B. Machine Learning Methods

In this paper, we examined six different machine learning algorithms that are introduced below.

K-Nearest Neighbors (KNN) is considered one of the simplest algorithms in classifying tasks. This algorithm aims to find the samples that exist close to each other [8].

Random Forest (RF) is an algorithm that is used in both classification and regression. As the name implies, it is a set of multiple decision trees. The dataset will be divided into a batch of random datasets, then building a decision tree for each of them. Each decision tree will give a different decision, and the majority result will be taken [20].

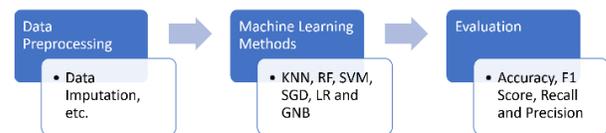


Fig. 1. A High-Level Depiction of our Methodology.

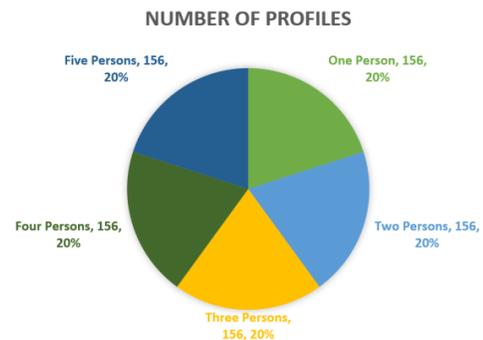


Fig. 2. PROVEDIt: Number and Distribution of DNA Mixtures with the Five Classes (Selected Profiles).

Support Vector Machine (SVM) is a very familiar algorithm when dealing with classification problems. When there is more than one way of drawing the line (boundary) to separate the data points (support vectors), one of the solutions is to measure the distance (margin) between the boundary and the data points. SVM will try to maximize this margin [8].

Stochastic Gradient Descent (SGD) is a suitable choice when having a significant dataset in terms of size and when there is not much computation. For forward pass, it uses a single sample at random and then changes weights [21].

Logistic Regression (LR) calculates the dependent variable based on the independent variable by calculating the errors between the actual data point and the predicted data point by the linear equation, then square the errors, sum them up, and minimize them [8].

Gaussian NB (GNB) comes from the Gaussian distributions that represent the dataset. It is suitable when the dimensionality of the inputs is complex and high. It used the Bayes theorem. It assumes that each feature is independent of other features [22].

C. Evaluation

In this work, we used four different performance metrics. Which are Accuracy that calculated as following $accuracy = (TP + TN)/(TP + FN + TN + FP)$, F1-Score that calculated as following $f1\ score = 2 * (recall * precision)/(recall + precision)$, Recall that calculated as following $recall = TP/(TP + FN)$, and Precision that calculated as following $precision = (TP/(TP + FP))$. Where TP is True Positive, TN is True Negative, FN is False Negative, and FP is False Positive.

IV. RESULTS AND ANALYSIS

This section presents the performance for the six algorithms. The six algorithms: KNN, RF, SVM, SGD, LR and GNB are analyzed respectively in Section IV.A to Section IV.F. Section IV.G will show a comparison between all the six algorithms. Section IV.H provides a brief descriptive comparison of our work in this paper with the earlier related works.

A. Nearest Neighbors (KNN)

Fig. 3 shows the confusion matrix for KNN model. There are five classes. The values vary from the minimum (zero) with purple color to the maximum (627) with dark yellow. The matrix could be read as follows. For Two number of unknowns, for instance, there are (502) correct predictions, (181) samples were misclassified as One-Person, (258) samples were misclassified as Three-Persons mixtures, (70) samples were misclassified as the Four-Persons mixtures and (16) samples were misclassified as the Five-Persons mixtures. The results show that One-Persons class have the highest number of correct predictions (627), then Five Persons class with (626), Three Persons class, Four Persons class and finally Two Person class. In terms of mischaracterization, Two Persons class has the highest number of misclassification (525), then Four Persons class (514), then Three Persons class (471), then One Person class (399) and finally Five Persons class (388).

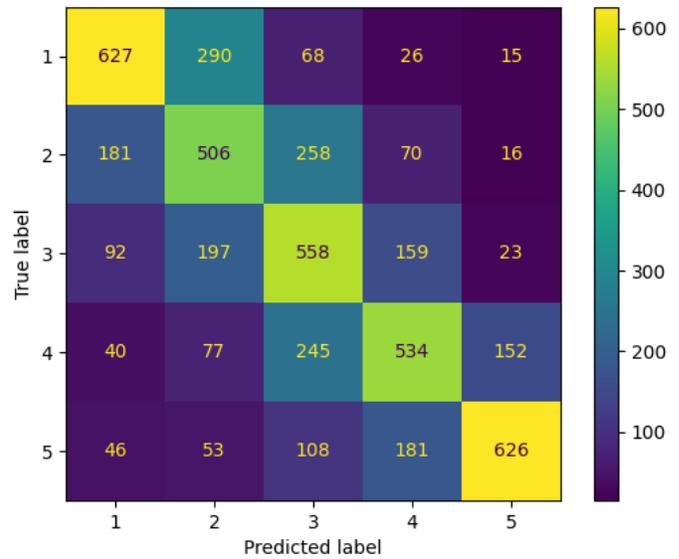


Fig. 3. The Confusion Matrix (KNN).

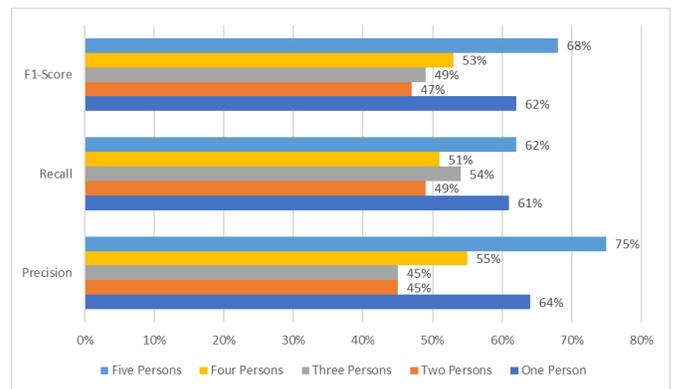


Fig. 4. F1-Score, Recall and Precision (KNN).

Fig. 4 shows F1-Score, Recall and Precision for the KNN model. The highest score is for Five Persons class Precision (75%) because referring to Fig. 3, we know that TP for Five Persons class is 626 and FP is 206, and the lowest is for both Three Persons and Two Persons classes Precision (45%) because as we know TP for Three Persons is (558) and FP is (679), and for Two Persons class TP is (506), and FP is (617). For F1-Score, the highest score is for Five Persons class (68%), and the lowest is for Two Persons class (47%). For Recall, the highest score is for Five Persons class (62%), and the lowest is for Two Persons class (49%). For Precision, the highest score is for Five Persons class (75%), and the lowest is for both Three Persons and Two Persons classes (45%).

B. Random Forest (RF)

Fig. 5 shows the confusion matrix for RF model. There are five classes. The values vary from the minimum (zero) with purple color to the maximum (902) with dark yellow. The matrix could be read as follows. For Three number of unknowns, for instance, there are (808) correct predictions, (41) samples were misclassified as One unknown, (138) samples were misclassified as Two unknown mixtures, (25) samples were misclassified as Four unknown mixtures and (17)

samples were misclassified as Five unknown mixtures. The results show that the One Person class have the highest number of correct predictions (902), then both Five Persons and Four Persons classes with (840), then Two Persons class with (822) and finally Three Persons class with (808). In terms of mischaracterization, Three Persons class has the highest number of misclassification (221), then Two Persons class (209), then Four Persons class (208), then Five Persons class (174) and finally One Person class (124).

Fig. 6 shows F1-Score, Recall and Precision for RF model. The highest score is for Five Persons class (90%) Precision because referring to Fig. 5, we know that TP for Five Persons class is (840) and FP is (96), and the lowest is for Two Persons class Precision (73%) because we know that TP for Two Persons class is (822) and FP is (302). For F1-Score, the highest score is for Five Persons class (86%), and the lowest is for Two Person class (76%). For Recall, the highest score is for One Person class (88%), and the lowest is for Three Persons class (79%). For Precision, the highest score is for Five Persons class (90%), and the lowest is for Two persons classes (73%).

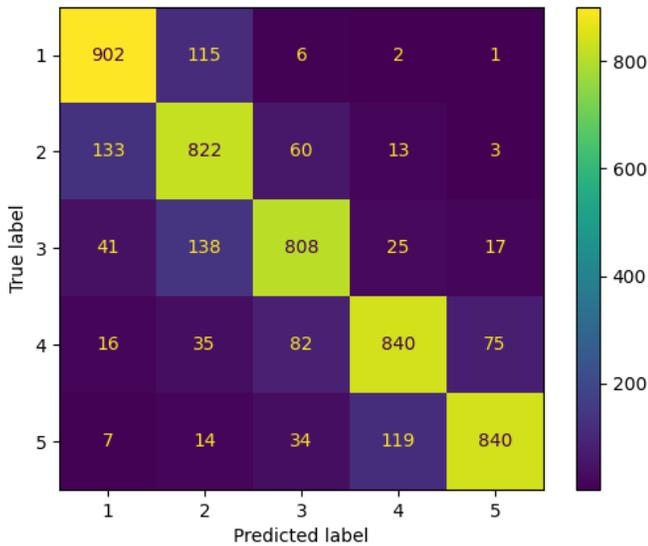


Fig. 5. The Confusion Matrix (RF).

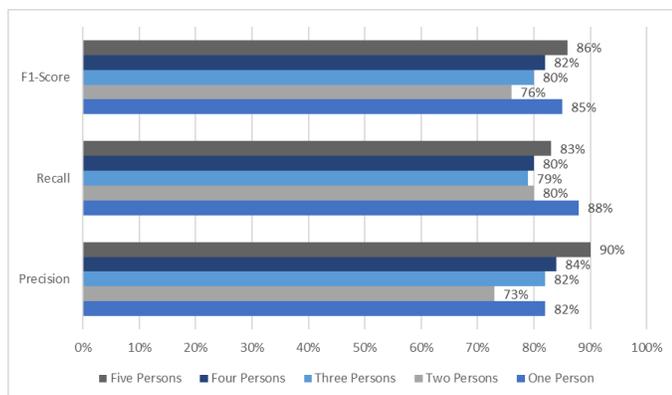


Fig. 6. F1-Score, Recall and Precision (RF).

C. Support Vector Machine (SVM)

Fig. 7 shows the confusion matrix for SVM model. There are five classes. The values vary from the minimum (zero) with purple color to the maximum (972) with dark yellow. The matrix could be read as follows. For Four unknowns, for instance, there are (911) correct predictions, (zero) samples were misclassified as One or Two unknown contributors, (88) samples were misclassified as Three Persons classes and (49) samples were misclassified as Five Persons class. The results show that Five Persons class have the highest number of correct predictions (972), then One Person class with (961), then Three Persons class with (932), then Two Persons class with (918) and finally Four Persons class with (911). In terms of mischaracterization, Four Persons class has the highest number of misclassification (137), then Two Persons class (113), then Three Persons class (97), then One Person class (65) and finally Five Persons class (42).

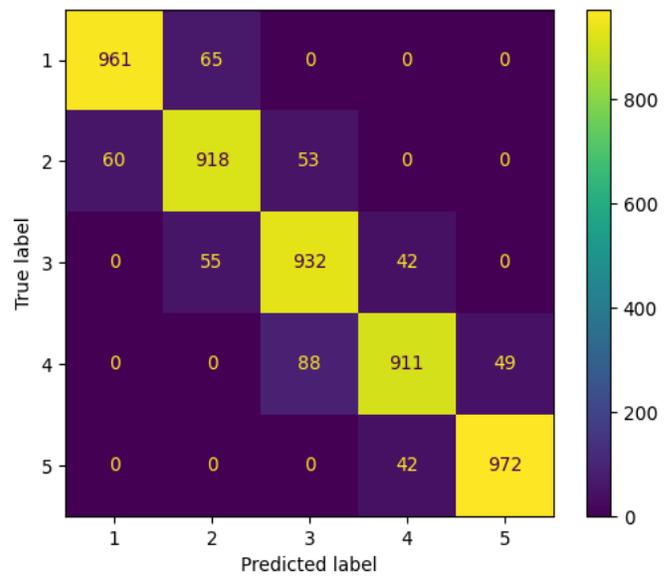


Fig. 7. The Confusion Matrix (SVM).

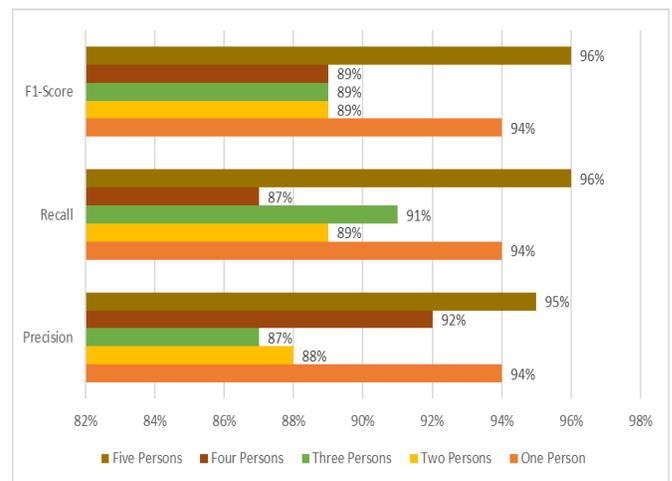


Fig. 8. F1-Score, Recall and Precision (SVM).

Fig. 8 shows F1-Score, Recall and Precision for RF model. The highest score is for both Five Persons class (96%) F1-Score and Five Persons class Recall because referring to Fig. 7 we know that TP for Five Persons class is (972), FP is (49), and FN is (42), and the lowest is for both Four Persons class Recall (87%) and Three Persons class Precision (87%) because we know that TP for Four Persons class is (911) and FN is (137), and TP for Three Persons class is (932), and FP is (141). For F1-Score, the highest score is for Five Persons class (96%), and the lowest is for Four Persons, Three Persons and Two Persons classes (89%). For Recall, the highest score is for Five Persons class (96%), and the lowest is for Four Persons class (87%). For Precision, the highest score is for Five Persons class (95%), and the lowest is for Three persons class (87%).

D. Stochastic Gradient Descent (SGD)

Fig. 9 shows the confusion matrix for SGD model. There are five classes. The values vary from the minimum (zero) with purple color to the maximum (1026) with dark yellow. The matrix could be read as follows. For Five unknowns, for instance, there are (1009) correct predictions, (zero) samples were misclassified as both One or Two unknown contributors, (1) samples were misclassified as Three Persons class and (4) samples were misclassified as Four Persons class. The results show that One Person class have the highest number of correct predictions (1026), then Five Persons class with (1009), then Three Persons class with (748), then Four Persons class with (436) and finally Two Persons class with (118). In terms of mischaracterization, Four Persons class has the highest number of misclassification (612), then Two Persons class (561), then Three Persons class (281), then Five Persons class (5) and finally One Person class (zero).

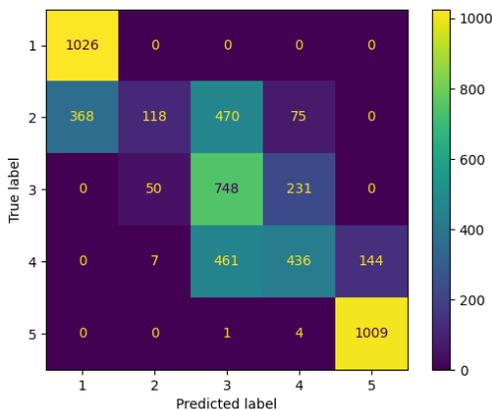


Fig. 9. The Confusion Matrix (SGD).

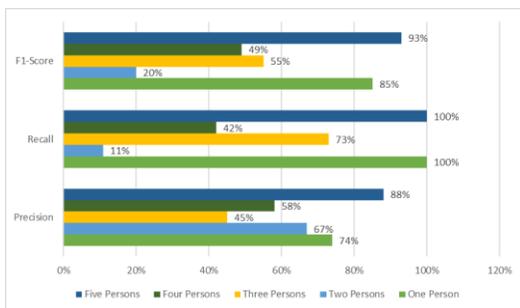


Fig. 10. F1-Score, Recall and Precision (SGD).

Fig. 10 shows F1-Score, Recall and Precision for SGD model. The highest score is for both Five Persons and One Person classes (100%) Recall because referring to Fig. 9, we know that TP for Five Persons class is (1009) and FN is (5), and TP for One Person class is (1026), and FN is (zero), and the lowest is for Two Persons class Precision (11%) because we know that TP for Two Persons class is (118) and FP is (913). For F1-Score, the highest score is for Five Persons class (93%), and the lowest is for Two Persons class (20%). For Recall, the highest score is for both Five Persons and Two Persons classes (100%), and the lowest is for Two Persons class (11%). For Precision, the highest score is for Five Persons class (88%), and the lowest is for Three persons class (45%).

E. Logistic Regression (LR)

Fig. 11 shows the confusion matrix for LR model. There are five classes. The values vary from the minimum (zero) with purple color to the maximum (990) with dark yellow. The matrix could be read as follows. For One number of unknowns, for instance, there are (990) correct predictions, (36) samples were misclassified as Two Persons class, (zero) samples were misclassified as Three, Four or Five unknown contributors. The results show that One Person class have the highest number of correct predictions (990), then Five Persons class with (989), then Three Persons class with (984), then Four Persons class with (958) and finally Two Persons class with (967). In terms of mischaracterization, Four Persons class has the highest number of misclassification (90), then Two Persons class (64), then Three Persons class (45), then Five Persons class (25) and finally One Person class (36).

Fig. 12 shows F1-Score, Recall and Precision for LR model. The highest score is for Five Persons class (98%) Recall because referring to Fig. 11, we know that TP for Five Persons class is (989) and FN is (25), and the lowest is for Four Persons class Recall (91%) because we know that TP for Four Persons class is (958) and FN is (90). For F1-Score, the highest score is for Five Persons class (96%), and the lowest is for Four Persons, Three Persons and Two Persons classes (94%). For Recall, the highest score is for Five Persons class (98%), and the lowest is for Four Persons class (91%). For Precision, the highest score is for One Person class (97%), and the lowest is for Three persons class (93%).

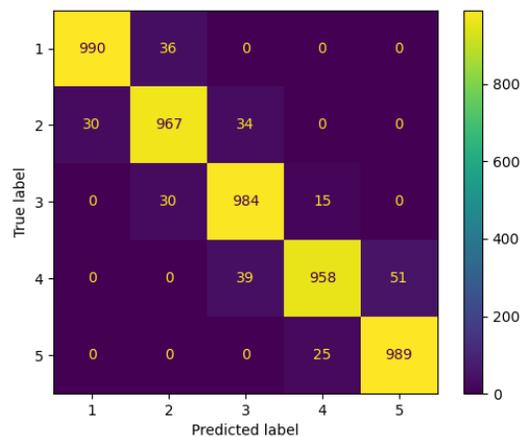


Fig. 11. The Confusion Matrix (LR).

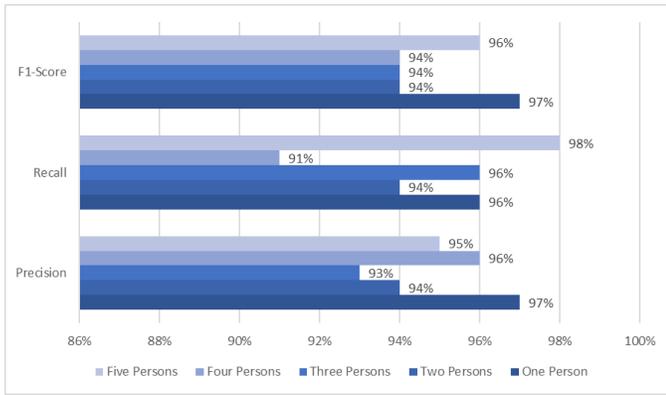


Fig. 12. F1-Score, Recall and Precision (LR).

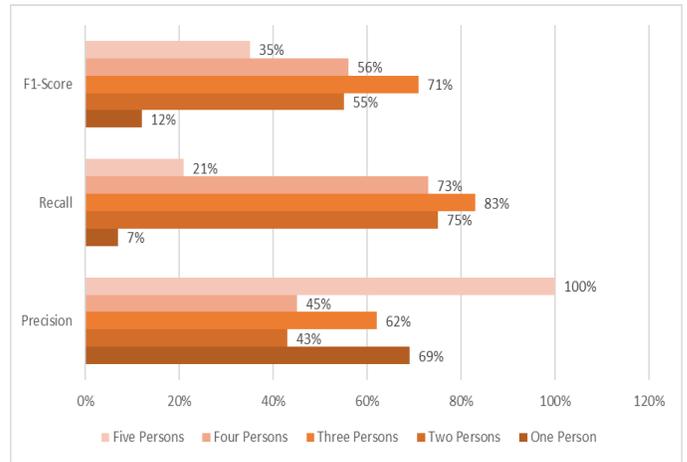


Fig. 14. F1-Score, Recall and Precision (GNB).

F. Gaussian NB (GNB)

Fig. 13 shows the confusion matrix for GNB model. There are five classes. The values vary from the minimum (zero) with purple color to the maximum (953) with dark yellow. The matrix could be read as follows. For the Two-Persons class, for instance, there are 772 correct predictions and 259 incorrect predictions. Among these misclassifications, ten samples were misclassified as the One-Person class. Moreover, 231 samples of these were misclassified as the Three-Persons class, 18 samples were misclassified as the Four-Persons class and none of the samples were misclassified as the Five-Persons class. The results show that Three Persons class have the highest number of correct predictions (858), then Two Persons class with (772), then Four Persons class with (760), then Five Persons class with (213) and finally One Person class with (70). In terms of mischaracterization, One Person class has the highest number of misclassification (956), then Five Persons class (801), then Four Persons class (288), then Two Persons class (259) and finally Three Persons class (171).

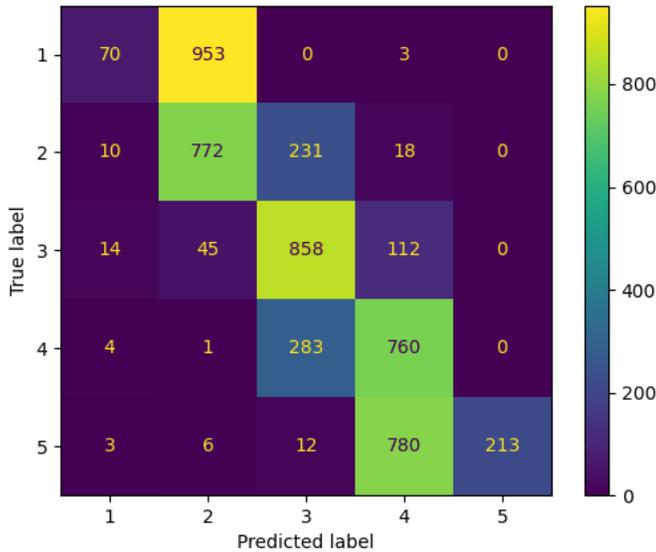


Fig. 13. The Confusion Matrix (GNB).

Fig. 14 shows F1-Score, Recall and Precision for GNB model. The highest score is for Five Persons class (100%) Precision because referring to Fig. 13, we know that TP for Five-Persons class is (213) and FP is (0), and the lowest is for One-Person class Recall (7%) because we know that TP for One Person class is (70) and FN is (31). For F1-Score, the highest score is for Three Persons class (71%), and the lowest is for One Person class (12%). For Recall, the highest score is for Three Persons class (83%), and the lowest is for One Person class (7%). For Precision, the highest score is for Five Persons class (100%), and the lowest is for Two persons class (43%).

G. Accuracy Comparison

Fig. 15 shows a comparison in terms of Accuracy between the proposed six ML algorithms. The x-axis shows the models names, and the y-axis shows the Accuracy percentage. The results show that LR has the highest score with (95%), then SVM with (91%), then RF with (82%), then SGD with (65%), then KNN with (55%) and finally GNB with (52%).

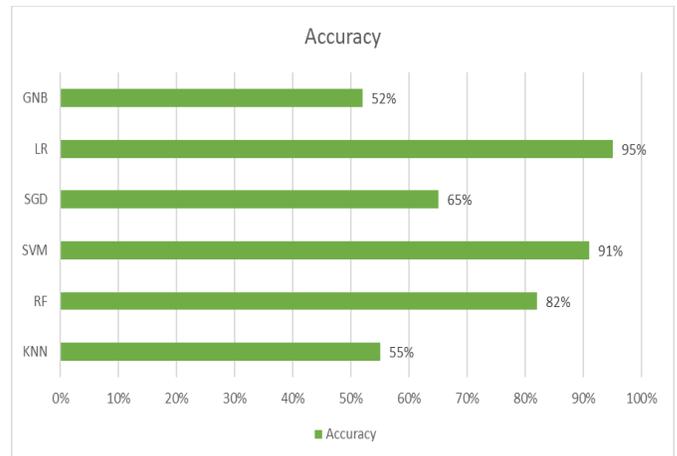


Fig. 15. Accuracy Comparison of the Six ML Algorithms.

H. Comparison with Related Works

Among all the earlier works in the literature on the use of machine or deep learning for estimating the number of unknowns, only Benschop et al. [11] and Kruijver et al. [10] estimated the number of unknowns for DNA mixtures with up to five contributors. The best Accuracy performance for Benschop et al. [11] was reported for the RF algorithm at 83%. The best Accuracy performance for Kruijver et al. [10] was reported for the Decision Trees algorithm at 85%. Comparing these results with our work presented in this paper, we have clearly achieved a better performance, i.e., for the LR algorithm at 95% Accuracy.

V. CONCLUSIONS AND FUTURE WORK

DNA profiling is considered one of the most challenging problems in forensic science. In the near future, the forensic science labs will have more profiles that could have many challenges to deal with, which shows the need for such tools that will help the analysts in their work. Within the next coming years, machine learning will become an essential component in many fields.

This study evaluated six machine learning algorithms with four performance metrics. These are F1-Score, Recall, Precision and Accuracy. The results show that the highest score for KNN is with Five Persons class Precision (75%), the highest score for RF is with Five Persons class Precision (90%), the highest score for SVM is with Five Persons class both F1-Score and Recall (96%), the highest score for SGD is with both Five Persons and One Person class Recall (100%), the highest score for LR is with the Five Persons class Recall (98%), and the highest score for GNB is with Five Persons class Precision (100%). The highest score for F1-Score is with the (LR) 97% One Person class. The highest score for Recall is with the (SGD) 100% One Person class and Five Persons class. The highest score for Precision is with the (GNB) 100% Five Persons class. In terms of Accuracy, the highest score is for the LR with (95%). Comparing with all other related works in the literature, we have clearly achieved a better performance, i.e., for the LR algorithm at 95% Accuracy.

This paper provides an investigation into the performance of machine learning methods for DNA profiling. Further evaluation of machine learning methods is needed and it will form our future work. We will use feature engineering methods to improve the performance of these machine learning methods. We will also investigate tuning the performance of the machine learning methods. Moreover, we will use deep learning to improve classification performance. A major theme of our research is smart cities and societies [23]–[25], big data [26]–[28], high performance computing [29], [30], healthcare [31]–[33], information systems [34], [35], system integration [36], [37], and artificial intelligence [38], [39]. Future work on DNA profiling will also look into developing new smart applications for DNA profiling and its integration with other smart city systems.

REFERENCES

- [1] J. M. Butler, "STR Genotyping and Data Interpretation," *Fundam. Forensic DNA Typing*, pp. 205–227, 2010, doi: 10.1016/b978-0-12-374999-4.00010-2.
- [2] J. M. Butler, "Applications of DNA Typing," *Fundam. Forensic DNA Typing*, pp. 397–421, 2010, doi: 10.1016/b978-0-12-374999-4.00017-5.
- [3] J. M. Butler, "Forensic Challenges," *Fundam. Forensic DNA Typing*, pp. 315–339, 2010, doi: 10.1016/b978-0-12-374999-4.00014-x.
- [4] E. Alamoudi, R. Mehmood, A. Albeshri, and T. Gojebori, "A Survey of Methods and Tools for Large-Scale DNA Mixture Profiling," *EAI/Springer Innov. Commun. Comput.*, pp. 217–248, 2020, doi: 10.1007/978-3-030-13705-2_9.
- [5] E. Alamoudi, R. Mehmood, A. Albeshri, and T. Gojebori, "DNA profiling methods and tools: A review," in *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST, Volume 224*, 2018, vol. 224, pp. 216–231, doi: 10.1007/978-3-319-94180-6_22.
- [6] T. M. Clayton, J. P. Whitaker, R. Sparkes, and P. Gill, "Analysis and interpretation of mixed forensic stains using DNA STR profiling," *Forensic Sci. Int.*, vol. 91, no. 1, pp. 55–70, 1998, doi: 10.1016/S0379-0738(97)00175-8.
- [7] E. M. Alamoudi, "Parallel Analysis of DNA Profile Mixtures with a Large Number of Contributors," p. 109, 2019.
- [8] M. A. Marciano and J. D. Adelman, "PACE: Probabilistic Assessment for Contributor Estimation—A machine learning-based assessment of the number of contributors in DNA mixtures," *Forensic Sci. Int. Genet.*, vol. 27, pp. 82–91, Mar. 2017, doi: 10.1016/j.fsigen.2016.11.006.
- [9] 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, doi: 10.1109/ACCESS.2017.2668840.
- [10] M. Kruijver et al., "Estimating the number of contributors to a DNA profile using decision trees," *Forensic Sci. Int. Genet.*, vol. 50, no. June 2020, p. 102407, 2021, doi: 10.1016/j.fsigen.2020.102407.
- [11] C. C. G. Benschop, J. van der Linden, J. Hoogenboom, R. Ypma, and H. Haned, "Automated estimation of the number of contributors in autosomal short tandem repeat profiles using a machine learning approach," *Forensic Sci. Int. Genet.*, vol. 43, Nov. 2019, doi: 10.1016/J.FSigen.2019.102150.
- [12] T. Egeland, I. Dalen, and P. F. Mostad, "Estimating the number of contributors to a DNA profile," *Int. J. Legal Med.*, vol. 117, no. 5, pp. 271–275, 2003, doi: 10.1007/s00414-003-0382-7.
- [13] T. Graversen, "Statistical and Computational Methodology for the Analysis of Forensic DNA Mixtures with Artefacts," p. 229, 2014.
- [14] K. Inman et al., "Lab Retriever: A software tool for calculating likelihood ratios incorporating a probability of drop-out for forensic DNA profiles," *BMC Bioinformatics*, vol. 16, no. 1, pp. 1–11, 2015, doi: 10.1186/s12859-015-0740-8.
- [15] T. Tvedebrink, P. S. Eriksen, H. S. Mogensen, and N. Morling, "Evaluating the weight of evidence by using quantitative short tandem repeat data in DNA mixtures," *J. R. Stat. Soc. Ser. C Appl. Stat.*, vol. 59, no. 5, pp. 855–874, 2010, doi: 10.1111/j.1467-9876.2010.00722.x.
- [16] Ø. Bleka, G. Storvik, and P. Gill, "EuroForMix: An open source software based on a continuous model to evaluate STR DNA profiles from a mixture of contributors with artefacts," *Forensic Sci. Int. Genet.*, vol. 21, pp. 35–44, 2016, doi: 10.1016/j.fsigen.2015.11.008.
- [17] D. J. Balding, C. D. Steele, D. Building, and G. Street, "likeLTD v6.3: an illustrative analysis, explanation of the model, results of validation tests and version history," 2016.
- [18] H. Swaminathan, C. M. Grgicak, M. Medard, and D. S. Lun, "NOCI: A computational method to infer the number of contributors to DNA samples analyzed by STR genotyping," *Forensic Sci. Int. Genet.*, vol. 16, pp. 172–180, 2015, doi: 10.1016/j.fsigen.2014.11.010.
- [19] L. E. Alfonse, A. D. Garrett, D. S. Lun, K. R. Duffy, and C. M. Grgicak, "A large-scale dataset of single and mixed-source short tandem repeat profiles to inform human identification strategies: PROVEDIt," *Forensic Sci. Int. Genet.*, vol. 32, no. July 2017, pp. 62–70, 2018, doi: 10.1016/j.fsigen.2017.10.006.
- [20] S. Kabiraj et al., "Breast Cancer Risk Prediction using XGBoost and Random Forest Algorithm," 2020 11th Int. Conf. Comput. Commun. Netw. Technol. ICCCNT 2020, pp. 11–14, 2020, doi: 10.1109/ICCCNT49239.2020.9225451.

- [21] “Stochastic Gradient Descent — Clearly Explained.” <https://towardsdatascience.com/stochastic-gradient-descent-clearly-explained-53d239905d31>.
- [22] “Naive Bayes.” https://scikit-learn.org/stable/modules/naive_bayes.html.
- [23] R. Mehmood, S. See, I. Katib, and I. Chlamtac, *Smart Infrastructure and Applications: foundations for smarter cities and societies*. Springer International Publishing, Springer Nature Switzerland AG, 2020.
- [24] 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, doi: 10.3390/s20102988.
- [25] 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,” *J. Open Innov. Technol. Mark. Complex.*, vol. 7, no. 1, p. 71, Feb. 2021, doi: 10.3390/joitmc7010071.
- [26] Y. Arfat, S. Suma, R. Mehmood, and A. Albeshri, “Parallel shortest path big data graph computations of us road network using apache spark: Survey, architecture, and evaluation,” in *Smart Infrastructure and Applications Foundations for Smarter Cities and Societies*, Springer Cham, 2020, pp. 185–214.
- [27] S. Usman, R. Mehmood, and I. Katib, “Big data and hpc convergence for smart infrastructures: A review and proposed architecture,” in *Smart Infrastructure and Applications Foundations for Smarter Cities and Societies*, Springer Cham, 2020, pp. 561–586.
- [28] E. Alomari, I. Katib, A. Albeshri, T. Yigitcanlar, R. Mehmood, and A. A. Sa, “Iktishaf+: A Big Data Tool with Automatic Labeling for Road Traffic Social Sensing and Event Detection Using Distributed Machine Learning,” *Sensors*, vol. 21, no. 9, p. 2993, Apr. 2021, doi: 10.3390/s21092993.
- [29] S. Alahmadi, T. Mohammed, A. Albeshri, I. Katib, and R. Mehmood, “Performance analysis of sparse matrix-vector multiplication (Spmv) on graphics processing units (gpus),” *Electron.*, vol. 9, no. 10, 2020, doi: 10.3390/electronics9101675.
- [30] T. Muhammed, R. Mehmood, A. Albeshri, and I. Katib, “SURAA: A Novel Method and Tool for Loadbalanced and Coalesced SpMV Computations on GPUs,” *Appl. Sci.*, vol. 9, no. 5, p. 947, Mar. 2019, doi: 10.3390/app9050947.
- [31] 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. 32258–32285, 2018, doi: 10.1109/ACCESS.2018.2846609.
- [32] 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,” *Int. J. Environ. Res. Public Health*, vol. 18, no. 1, pp. 1–36, Jan. 2021, doi: 10.3390/IJERPH18010282.
- [33] 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,” *Appl. Sci.*, vol. 10, no. 4, p. 1398, Feb. 2020, doi: 10.3390/app10041398.
- [34] N. Ahmad and R. Mehmood, “Enterprise systems and performance of future city logistics,” *Prod. Plan. Control*, vol. 27, no. 6, pp. 500–513, Apr. 2016, doi: 10.1080/09537287.2016.1147098.
- [35] N. Ahmad and R. Mehmood, “Enterprise systems: Are we ready for future sustainable cities,” *Supply Chain Manag.*, vol. 20, no. 3, pp. 264–283, May 2015, doi: 10.1108/SCM-11-2014-0370.
- [36] T. Mohammed, A. Albeshri, I. Katib, and R. Mehmood, “UbiPriSEQ— Deep reinforcement learning to manage privacy, security, energy, and QoS in 5G IoT hetnets,” *Appl. Sci.*, vol. 10, no. 20, 2020, doi: 10.3390/app10207120.
- [37] T. Muhammed, R. Mehmood, A. Albeshri, and A. Alzahrani, “HCDSR: A Hierarchical Clustered Fault Tolerant Routing Technique for IoT-Based Smart Societies,” 2020, pp. 609–628.
- [38] T. Yigitcanlar et al., “Artificial Intelligence Technologies and Related Urban Planning and Development Concepts: How Are They Perceived and Utilized in Australia?,” *J. Open Innov. Technol. Mark. Complex.*, vol. 6, no. 4, p. 187, Dec. 2020, doi: 10.3390/joitmc6040187.
- [39] T. Yigitcanlar, R. Mehmood, and J. M. Corchado, “Green Artificial Intelligence: Towards an Efficient, Sustainable and Equitable Technology for Smart Cities and Futures,” *Sustain.* 2021, Vol. 13, Page 8952, vol. 13, no. 16, p. 8952, Aug. 2021, doi: 10.3390/SU13168952.

Visualization of the Temporal Topic Model on Higher Education Preferences with Higher Education Ranking Indicators

Winda Widya Ariestya¹, Achmad Benny Mutiara², I Made Wiryana³, Setia Wirawan⁴
Gunadarma University, Faculty of Computer Science and Information Technology
Margonda Raya No. 100, Depok, Indonesia

Abstract—Private universities have devised a strategy to counteract the ongoing competition. Private universities can use the appropriate data analysis method to make higher education management decisions. The goal of this research is to find a new approach to data analysis methods in the form of visualization using the TTM (Temporal Topic Model) method to assist private university management. These findings are the two formulas used to generate time-based visualizations and the Temporal Topic Model per month to visually change news topics related to rankings so that management can decide on marketing strategies and policies that are in relation to public opinion.

Keywords—Management decisions; temporal topic model; university; visualization

I. INTRODUCTION

The number of private universities, in Indonesia is around 68 per cent of all universities, is one factor in the existence of competition for private universities in Indonesia. Private universities compete with each other to provide students as their consumers with the best educational services.

The challenge currently facing Indonesian universities is the implementation of the Outcome-Based Education method, where learning focuses not only on the teaching and learning process but also on output [1]. The Accreditation of National and International Higher Education requires a curriculum that is supported by an Outcome-Based Approach [2].

Furthermore, a proper marketing strategy is a requirement for all universities, one of which is to provide services of equal value to the expectations of students, particularly those of stakeholders [3].

News about tertiary education institutions may influence the community in determining the choice of tertiary institutions, as the information presented is one of the contents of the ranking news [4]. Higher education rankings are not widely known to the public, based on the results of research conducted by Gunarto [5] through a survey method with a descriptive analysis of people's perceptions and preferences of the reputation of higher education ratings.

A number of world university rankings, including Webometrics Rangking Of World University (WRWU), SCIMAGO Institutions Rankings (SIR), Academic Ranking of World Universities (ARWU), Taiwan Higher Education Evaluation and Accreditation Council (HEEACT), THE-QS

World Ranking of Universities, and 4 International Colleges & Universities (4ICU) [6]. Indonesia conducts a National Cluster of Higher Education through the Ministry of Research, Technology and Higher Education, which is released every semester with the objective of mapping Indonesian universities to enhance the standard of higher education under the auspices of the Ministry of Research, Technology and Higher Education, as well as being the basis for the Ministry of Research, Technology and Higher Education [7].

Advances in information technology are currently supporting the management of data needed for higher education management, which is used to obtain user preferences. Information technology can assist management in evaluating information that can offer decision-making options for management. It is not possible to distinguish data analysis from the presentation of enticing data in order to promote the process of analysis. Visual presentation of the data allows management to better understand the summary of the information presented. Information on tertiary institutions visually at a certain time can be used by management to determine policies for making competition decisions that take place.

Several studies on the Temporal Topic Model and the Use of Visualization, including Jeong [8], conducted a time analysis between three sources and two academic fields by conducting a text mining content analysis using LDA techniques. The resulting topic modeling has been declared effective in determining the content and trends of the time series of papers, patents and news articles. Jatmika [9] carried out a data mart visualization design to monitor the performance of the STIKOM Surabaya study programs. Visualization is designed to assist the Head of the Study Program in the academic performance of the Study Program. Ghosh et al [10] introduced a model of time-related issues in news articles to see trends in time-related issues. The time series regression technique in modeling has been found to be able to produce trendy topics efficiently.

This research differs from several previous studies in that it analyzes the community's tendency in choosing universities towards university ranking indicators with a new approach using the Temporal Topic Model and visualizing it in order to apply for higher education management. The resulting visualization is time-based, and the Temporal Topic Model is used once a month to produce shifts in news topics that are

visually related to university rankings, allowing management to make marketing strategies and policies that are in line with community opinions.

II. METHODS

Research commences with the process of collecting data in accordance with the subject under study. The next stage is the processing of data using text mining techniques. There are two stages in data processing, namely pre-processing and modeling using the LDA method and the Temporal Topic Model. Visualization was carried out as a tool for analyzing emerging topics from the results of data processing. The stages of this research can be seen in Fig. 1.

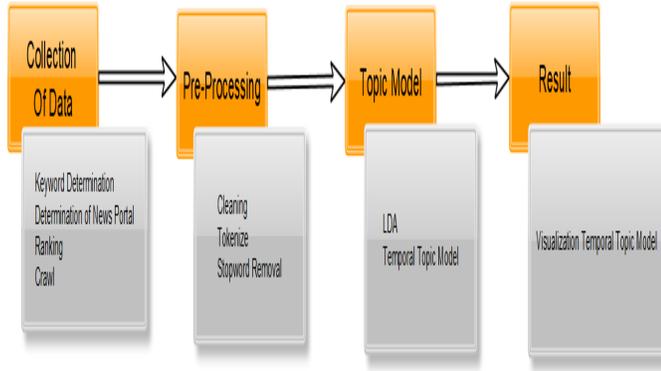


Fig. 1. Methods of Research.

A. Collection of Data

As a data source for this study, Indonesian news about universities was used. Text-only news content consists of text only. Before beginning the text mining process, keywords must be determined. Keywords are expressions that represent a concept, according to the KBBI Big Indonesian Dictionary [11]. The keywords used by Google Keyword Planner are listed in Table I [12].

Webometrics Ranking Of World University (WRWU), Times Higher Education Supplement (THES), Quacquarelli Symonds World University Rankings (QS WUR) are higher education rankings used on the basis of the IREG Ranking Audit [13] and Kemenristekdikti cluster ranking of universities in the world.

TABLE I. KEYWORDS FOR THE GOOGLE KEYWORD PLANNER

Keywords
Most prestigious private university
A private college
The best private university
A private university
There are private colleges
Telkom Institute of Technology
University Positioning
Kopertis-registered colleges
Private college list

In addition, there is a text crawling on the news portal. The news portals used are based on the results of eight national news portals with the highest level of access to alexa rank in 2020, namely the news portal tribunnews.com, detik.com, okezone.com, sindonews.com, kompas.com, liputan6.com, idntimes.com and merdeka.com. For understanding the temporal behaviour, the data is grouped monthly.

B. Text Pre-Processing

The news articles that have been obtained are unstructured text data and require pre-processing of text that is carried out sequentially and connected to each other in order to prepare the data to be more feasible than input in the next process [14]. The results of the preprocessing process become input for the modeling stage of the topic.

Grouped data requires pre-processing that includes the cleaning, tokenization and stopwords removal phases.

- Cleaning is the process of cleaning data, including the removal of links and dual spaces.
- Tokenize is the process of breaking sentences into words.
- Stopword deletion is a process of deleting words that are considered unimportant. This study is based on Sastrawi literary libraries.

C. Topic Model

The next stage is the topic of modeling using the Latent Dirichlet Allocation (LDA) technique introduced by Blei, et al. In the year 2003, this technique is an unsupervised machine learning technique that can be applied to generative probabilistic text data groups. Documents that make use of this technique can be seen as emerging themes from a number of documents [15].

In addition, the temporal subject model technique is used, a new approach to this technique where the subject of the model that has been generated is shown in a period of time per month by searching for relations in the ranking indicator with the formulation of equation 1.

This stage is the novelty of this research, which uses ranking indicators and visualizes with the Temporal Topic Model technique. The Temporal Topic Model (TTM) method is used to display the topic model generated within a certain time period. Each topic will be displayed in the TTM by linking to the ranking indicators.

$$TTM = < T_{k1}^1 \mapsto T_{k2}^2 \mapsto T_{kn}^n > \quad (1)$$

Where to:

TTM is a time-oriented set of consecutive times

$T_1 \dots T_n$ is a topic at times 1 to n

$K_1 \dots k_n$ is a list of topics

After obtaining the TTM, then visualization is carried out using the equation (1). The visualization on the left is a list of topics $T_1 \dots T_{20}$, 20 topics used refer to the research of Al-khairi, Wibisono and Putro [16] which states that the most

optimal number of topics is 20 topics. On the right is a ranking list of $R_1 \dots R_5$ in each month period $W_1 \dots W_n$ as shown in Fig. 2.

Topik	W1					W2					Wn				
	R1	R2	R3	R4	R5	R1	R2	R3	R4	R5	R1	R2	R3	R4	R5
T1															
T2															
T3															
⋮															
⋮															
⋮															
⋮															
⋮															
⋮															
Tn															

Where to:
 R1 is a rank 1.
 R2 is a rank 2.
 R3 is a rank 3.
 R4 is a rank 4.
 R5 is a rank 5.
 W1...Wn is a period of month.

Fig. 2. Design of TTM.

D. Visualization

Visualization is carried out after obtaining the results of the TTM in order to make it easier for the management of private tertiary institutions to see the preferences of individuals with the wording of equation 2.

$$V_i = \begin{cases} 1 & \text{if } i \in \{T_1, T_2, \dots, T_{20}\} \\ 0 & \text{if } i \notin \{T_1, T_2, \dots, T_{20}\} \end{cases} \quad (2)$$

Where to:

V_i is a TTM visualization

$T_1 \dots T_{20}$ is a topic 1 to top 20

1 is a topic related to the ranking indicator

0 is a topic unrelated to the ranking indicator

Each rating is represented by a color that represents each rating as in Fig. 3.

- The red color (W) represents the Webometrics ranking.
- Yellow color (T) represents Thes ranking.
- The green color (Q) represents the QS-WUR ranking.
- Purple (D) represents the Kemenristek Dikti clustering ranking.
- The blue color (O) represents if there are unrelated topics in the ranking.

The color will live if in a month there is a topic that is related to the ranking indicator. The color will not live if the topic is not related to the ranking indicator.



Fig. 3. Color Ranking.

III. RESULT AND DISCUSSION

The national news articles used in this study were 647 articles generated from crawling using predetermined keywords and news portals from 2016 to 2020. Fig. 4 depicts the crawling process for Indonesian-language university news data. They are also seen by time per month to generate data, as shown in Fig. 5.

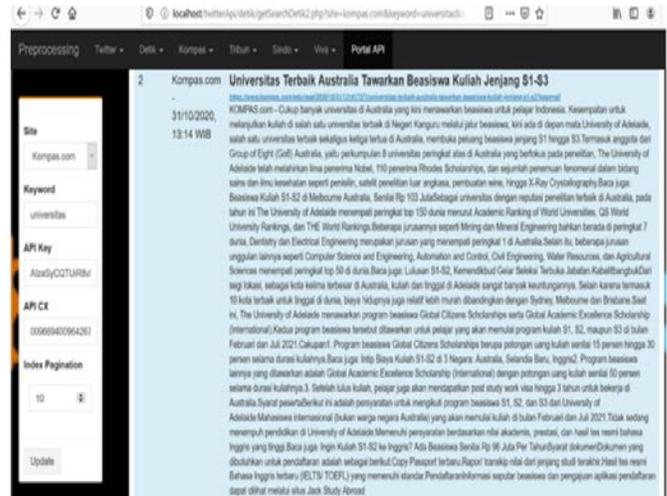


Fig. 4. Crawling Process.

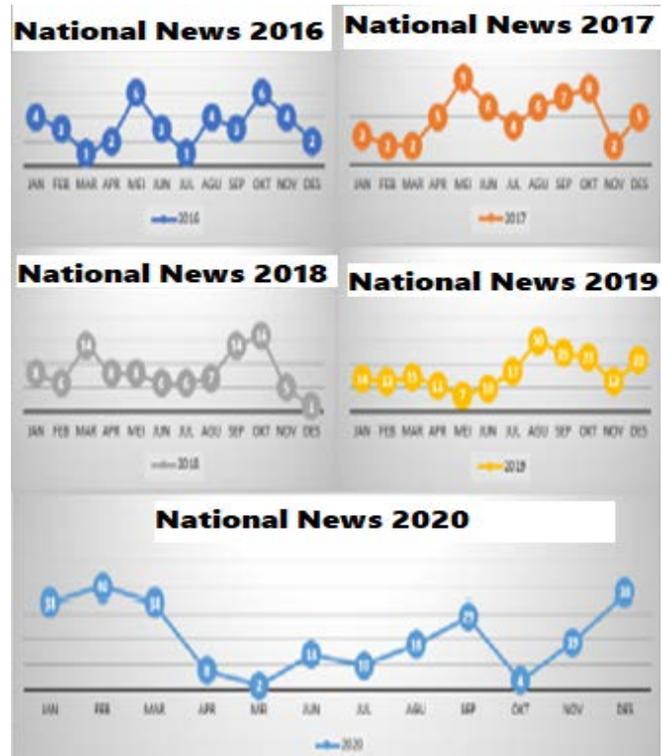


Fig. 5. National News per Month.

The data that has been grouped is then pre-processed to produce better data as input into the process stage of the model theme.

The number of topics to be displayed is determined in advance in the modeling process, and 10 topics are shown in this study. The following is an example of a topic that is produced in December 2020 as shown in Fig. 6.

```
[0,
'0.017*'universitas' + 0.016*'fakultas' + 0.015*'terbaik' + 0.013*'kampus' + '
'0.009*'swasta' + 0.009*'perguruan' + 0.008*'university' + '
'0.007*'pendidikan' + 0.006*'ilmu' + 0.006*'peringkat'),
(1,
'0.021*'universitas' + 0.018*'fakultas' + 0.016*'terbaik' + 0.013*'kampus' + '
'0.008*'perguruan' + 0.007*'university' + 0.007*'swasta' + 0.006*'peringkat' + '
+ 0.006*'kegiatan' + 0.006*'pendidikan'),
(2,
'0.018*'fakultas' + 0.015*'terbaik' + 0.015*'kampus' + 0.014*'universitas' + '
'0.009*'perguruan' + 0.006*'swasta' + 0.006*'pendidikan' + 0.006*'peringkat' + '
+ 0.005*'mahasiswa' + 0.005*'ilmu'),
(3,
'0.023*'fakultas' + 0.022*'terbaik' + 0.022*'universitas' + 0.021*'kampus' + '
'0.010*'swasta' + 0.009*'perguruan' + 0.008*'pendidikan' + 0.008*'ilmu' + '
'0.008*'mahasiswa' + 0.008*'peringkat'),
(4,
'0.017*'fakultas' + 0.015*'kampus' + 0.013*'universitas' + 0.011*'terbaik' + '
'0.009*'perguruan' + 0.008*'mahasiswa' + 0.007*'swasta' + 0.006*'mahasiswa' + '
+ 0.005*'ilmu' + 0.005*'pendidikan'),
(5,
'0.025*'universitas' + 0.021*'fakultas' + 0.019*'terbaik' + 0.017*'kampus' + '
'0.011*'perguruan' + 0.009*'mahasiswa' + 0.007*'pendidikan' + 0.007*'ilmu' + '
'0.007*'peringkat' + 0.006*'swasta'),
(6,
'0.019*'universitas' + 0.019*'fakultas' + 0.018*'kampus' + 0.017*'terbaik' + '
'0.009*'university' + 0.009*'mahasiswa' + 0.008*'perguruan' + 0.007*'swasta' + '
+ 0.007*'peringkat' + 0.006*'pendidikan'),
(7,
'0.026*'universitas' + 0.025*'fakultas' + 0.022*'kampus' + 0.016*'terbaik' + '
'0.009*'university' + 0.008*'swasta' + 0.007*'pendidikan' + '
'0.007*'perguruan' + 0.007*'ilmu' + 0.006*'peringkat'),
(8,
'0.013*'fakultas' + 0.013*'terbaik' + 0.013*'kampus' + 0.011*'universitas' + '
'0.007*'perguruan' + 0.007*'swasta' + 0.007*'peringkat' + 0.006*'university' + '
+ 0.006*'ilmu' + 0.006*'jaya'),
(9,
'0.030*'universitas' + 0.020*'fakultas' + 0.015*'kampus' + 0.015*'terbaik' + '
'0.012*'perguruan' + 0.008*'university' + 0.007*'swasta' + '
'0.007*'pendidikan' + 0.006*'kegiatan' + 0.006*'ilmu')]
```

Fig. 6. December 2020 Topic Model.

Topic 9, the ten words that appear at the highest frequency are 'universitas' with a weight of 0.030, followed by the words 'fakultas' with a weight of 0.020, followed by the words 'kampus,' 'terbaik,' 'perguruan,' 'university,' 'swasta,' 'pendidikan,' 'kegiatan' and 'ilmu.' The resulting weight shows the level of importance of the words on the subject.

Visually, words that contain a high frequency of occurrence in one subject are shown in Fig. 7. Using Wordcloud by showing that the word size is larger if the word weight has the highest frequency.

All data for 2020 are shown visually in Fig. 8. Where the left side describes the relationship between one subject and another, while the right side describes the frequency distribution of the word. In the 2020 data set, the top-frequency words are 'fakultas' and 'universitas.' In addition, the Twenty Topics with the highest frequency were used in the Temporal Topic Model process.

The topic model that has been produced only describes the emergence of subjects without knowing the topic shifts that occur every month. For this reason, a Temporary Topic Model and a visualization that is linked to a ranking indicator is needed so that the news topic can be identified as an input for higher education management every month.

Each topic generated per month is linked to the ranking indicator, the indicator is represented in color, so that if a relationship occurs, the color will live on the subject. This determination is based on Eq. 2, so that it is produced as shown in Fig. 9.

From the results of the Visualization of the Temporal Topic Model, it is found that there was a shift in the themes that occurred. For example, from January to May 2016, it is shown in Table II.

Table II shows that there is a shifting subject that happens every month, in January, to news about college scholarships, training, scientific research and scientific publications. February news on scientific research and scientific publications. In March and April, the news is about training, while in May it is about graduates, education and teaching, training and curriculum content.

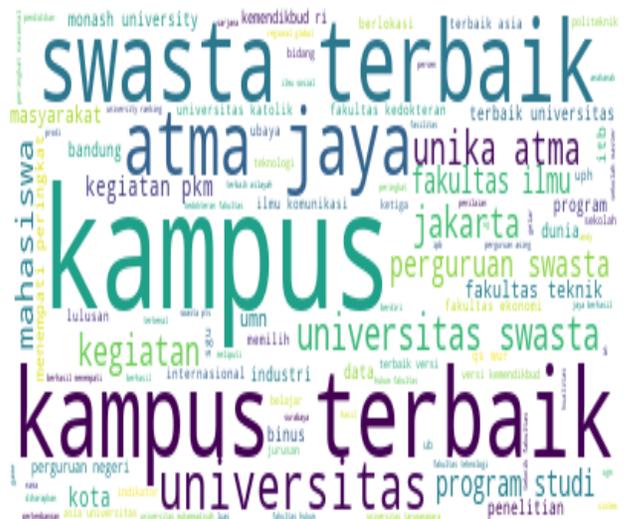


Fig. 7. Wordcloud News December 2020.

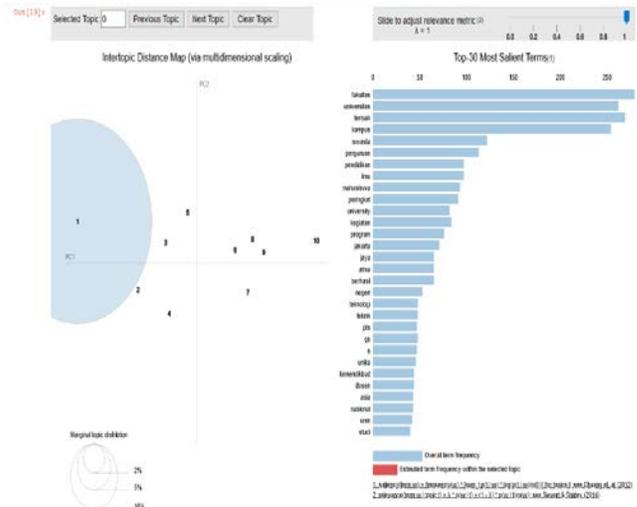


Fig. 8. Frequency of 2020 Data Words.

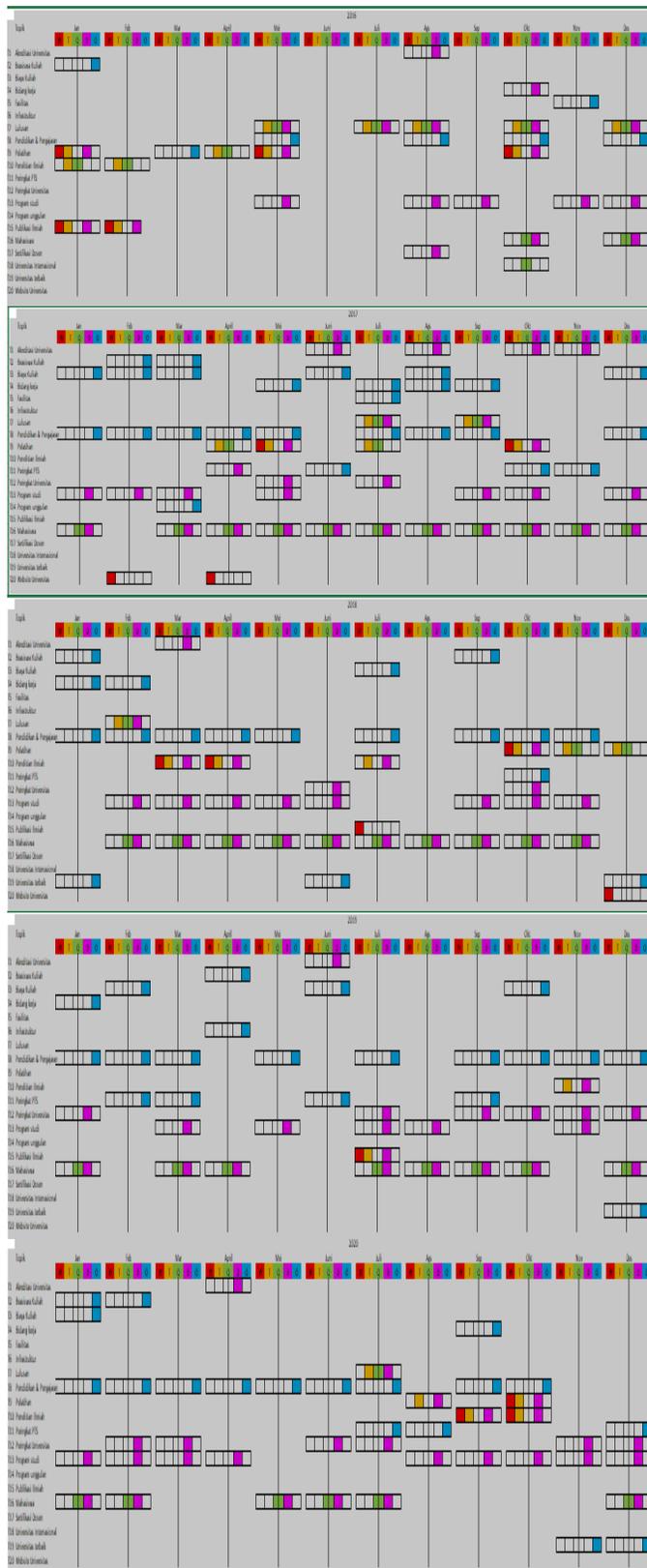


Fig. 9. Visualization of the Temporal Topic Model.

TABLE II. EXAMPLES OF SHIFT TOPIC

January	February	March	April	May
-	-	-	-	graduates
-	-	-	-	education and teaching
-	-	-	-	curriculum content
college scholarships,	-	-	-	-
training,	-	training,	training,	training,
scientific research	scientific research	-	-	-
scientific publications	scientific publications	-	-	-

IV. CONCLUSION

It can provide visual input to the management of private universities to facilitate the analysis of public preferences for higher education, before management decides on marketing strategies and policies that are in accordance with the views of the community, using the findings in the form of two equation formulas that are applied to produce a visualization of the Temporal Topic Model Technique. The resulting visualization is time-based and can be seen changing news topics visually.

The results of the visualization of the TTM obtained class parameters that can be used in the next stage, namely the classification process. The visualization function is carried out by calculating the topics connected to the ranking indicators, then the maximum value of each parameter will be searched, the parameter with the largest value that will be used as a parameter can be used as a feature of the assessment process which is part of the classification process.

ACKNOWLEDGMENT

This work is partially supported by Gunadarma University. The authors also gratefully acknowledge the helpful comments and suggestions of the reviewers, which have improved the presentation.

REFERENCES

- [1] H. Wahyudi and I.A. Wibowo, "Inovasi dan Implementasi Model Pembelajaran Berorientasi Lulusan (Outcome-Based Education, OBE) dan Washington Accord di Program Studi Teknik Mesin Universitas Mercu Buana", *J. Tek. Mesin*, 7(2), 50, 2018.
- [2] R. Belmawa, "Panduan Penyusunan Kurikulum Pendidikan Tinggi Di Era Industri 4.0", 2018.
- [3] A. Wahyuni, "Kajian Bauran Promosi Di Perguruan Tinggi "X"", *Liquidity*, 1(2), 175-182, 2012. doi: <https://doi.org/10.32546/lq.v1i2.148>
- [4] S. Sastropetro, "Pendapat Publik, Pendapat Umum, dan Pendapat Khalayak Dalam Komunikasi Sosial", Bandung: Remaja Rosdakarya, 1987, unpublished.
- [5] M. Gunarto, "Analisis Persepsi Dan Preferensi Masyarakat Terhadap Reputasi Pemingkat Perguruan Tinggi", *Journal Ilmu Manajemen*, 5(2), 2016.
- [6] O. Alaşehir, "University ranking by academic performance", Master's thesis, 2010. <http://etd.lib.metu.edu.tr/upload/12612484/index.pdf>.

- [7] Nizam, "Direktorat jenderal pendidikan tinggi umumkan klasterisasi perguruan tinggi Indonesia tahun 2020", <https://dikti.kemdikbud.go.id/kabar-dikti/kabar/direktorat-jenderal-pendidikan-tinggi-umumkan-klasterisasi-perguruan-tinggi-ind, 2020>.
- [8] D.H. Jeong and M. Song, "Time gap analysis by the topic model-based temporal technique", *Journal of informetrics*, 8(3), 776-790, 2014. doi: <https://doi.org/10.1016/j.joi.2014.07.005>.
- [9] K. Jatmika and A. Cahyono, "Rancang Bangun Data Mart dan Purwarupa Dashboard untuk Visualisasi Performa Akademik", *SISFO*, 5, 2015.
- [10] S. Ghosh, P. Chakraborty, E.O. Nsoesie, E. Cohn, S.R. Mekar, J.S. Brownstein and N. Ramakrishnan, "Temporal topic modeling to assess associations between news trends and infectious disease outbreaks", *Scientific reports*, 7(1), 1-12, 2017. doi: <https://doi.org/10.1038/srep40841>.
- [11] KBBI, Kamus Besar Bahasa Indonesia (KBBI), Online <https://kbbi.web.id/katakunci>, 2021.
- [12] G.K. Planner, "Google Keyword Planner Perguruan Tinggi", <https://ads.google.com/aw/keywordplanner>, 2020.
- [13] IREG, Ranking Audit, "Rank University", <https://web.archive.org/web/20161029232754/http://ireg-observatory.org/en/information>, 2016.
- [14] W.W. Ariestya, I. Astuti and I.M. Wiryana, "Preprocessing For Crawler Of Short Message Social Media", In 2018 Third International Conference on Informatics and Computing (ICIC) (pp. 1-6), IEEE, 2018, October. doi: 10.1109/IAC.2018.8780451. <https://ieeexplore.ieee.org/abstract/document/8780451>.
- [15] D. M. Blei, A.Y. Ng and M.I. Jordan, "Latent dirichlet allocation", *The Journal of Machine Learning Research*, 3, 993-1022, 2003.
- [16] Y.U. Al-khairi, Y. Wibisono, B.L. Putro, "Deteksi topik fashion pada twitter dengan latent dirichlet allocation". *JATIKOM: Jurnal Aplikasi dan Teori Ilmu Komputer*, 1(1):1-8, 2018. <http://jatikom.cs.upi.edu/index.php/jatikom/article/view/14>.

Sparse Distributed Memory Approach for Reinforcement Learning Driven Efficient Routing in Mobile Wireless Network System

Varshini Vidyadhar¹, Dr. Nagaraj R², Dr. G Sudha³

Research Scholar, Department of Computer Science and Engineering, Bangalore Institute of Technology, Bangalore, India¹
Professor, Department of Information Science and Engineering, Bangalore Institute of Technology, Bangalore, India²
Associate Professor, Department of Electrical and Electronics, Bangalore Institute of Technology, Bangalore, India³

Abstract—In recent years, researchers have explored the applicability of Q-learning, a model-free reinforcement learning technology towards designing QoS-aware, resource-efficiency, and reliable routing techniques in a dynamically changing network environment. However, Q-learning is based on tabular representation to characterize learned policies that frequently encounter a dimension disaster problem when introduced to the uncertain and dynamically changing network environment. In addition, the time required for agent learning in the training phase is too long, which makes it difficult for the agent to generalize the observation state efficiently. To this end, this paper attempts to overcome the overhead memory problems encountered in Q-learning-based routing techniques. In this paper, the study presents a novel memory-efficient intelligent routing mechanism based on adaptive Kanerva coding, which minimizes the storage cost required for storing large action and a state value. Unlike existing schemes, the proposed method optimizes memory requirements. Also, it enables better generalization by storing the learnable parameters of the function approximator present in the agent in a Kanerva-coding data structure. The Kanerva-coding is a sparse memory with distributed reading and writing mechanism which enables optimal compression and state abstractions for learning with fewer parameterized components making it highly memory efficient. The design and implementation of the proposed technique are done on the Anaconda tool. Simulation results demonstrate that the proposed technique can adaptively adjust the routing policy according to the varying network environment to meet the transmission requirements of different services with low memory requirements.

Keywords—Mobile wireless network; reinforcement learning; Q-learning; Kanerva coding; routing; memory optimization

I. INTRODUCTION

A. Background

A mobile wireless network can be regarded as a transient system that is inherently dynamic, decentralized, and formed via randomly deployed several wireless and mobile communicating sensor nodes to perform the distribution of the sensory information to the end node [1]. The ad-hoc feature in this transient system ensures fast and cost-effective network deployment. The sensory nodes operate as a router by receiving and forwarding the traffic of their nearby sensor nodes [2]. The salient features of mobile wireless networks are multi-hop communication, dynamic topology, bandwidth, and

resources constraints. Interruption due to uncertain and dynamic topology changes affects the efficiency of the node resources. It also compromises the transmission of data packets from the source to the end node. In this regard, efficient routing in wireless networks has been extensively studied in the literature [3-5]. Therefore, various routing mechanisms have been introduced, mainly divided into reactive, proactive, and location-based routing protocols. The routing scheme of proactive type is a table-driven approach where information regarding the entire network topology is maintained at each sensor node. However, updating the table introduces a huge overhead problem due to the large control traffic in the dynamic network. In the reactive routing mechanism, the route discovery executes on on-demand [6]. However, it requires collecting adjacent information, which is a costly procedure, and, in many instances, it may not be able to determine the end-to-end path. In location-based routing, the selection of the next-hop nodes is carried based on the predefined parameters but not suitable to dynamic networks as it has restricted adaptability. Although the routing protocol of these types is advantageous in many specific situations, it has several limitations when introduced to the dynamic networking scenario [7-8].

Recently, machine learning (ML) has been widely employed to solve network problems. Incorporating the potential of machine learning technology in routing mechanisms helps to optimize network resources. In general, there are three particular types of ML techniques viz. supervised, unsupervised, and reinforcement learning. In supervised learning (SL), both input and output variables are required to train the models [9]. In un-supervised learning (UL), the model learns explicit features and generalizes the data category with only input variables. Reinforcement learning (RL) is the agent and environment interaction mechanism that enables a system to automatically explore, learn, through a trial-and-error process. However, RL is more suitable and dominant in literature when focusing on routing problems because it does not require any dataset like other ML models such as SL and UL [10].

B. Reinforcement Learning

The Reinforcement Learning (RL) technique is a specific type of ML method that comprises agent function and its interaction with the environment. RL has illustrated great

potential in various decision-making processes, autonomous systems, telecommunication systems, robotics, and recommender systems. Fig. 1 represents a typical process of agent and environment interaction.

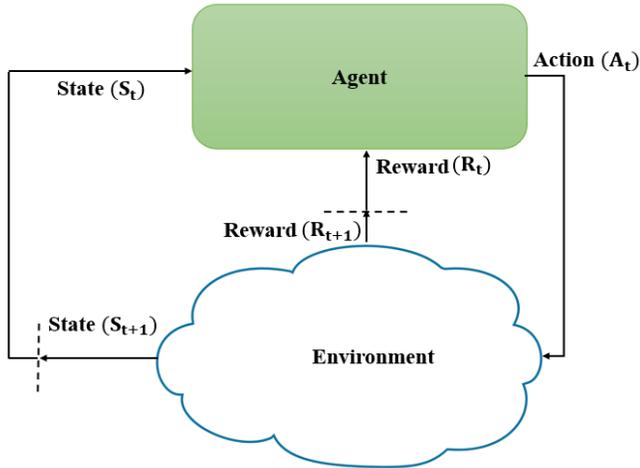


Fig. 1. Typical Function of Agent and Environment.

In typical RL, the principal of the agent interaction with the environment adopts a mathematical framework of the discrete-time stochastic control process, which is represented as a tuple such that: $\{S_t, A_t, F, \rho, \gamma\}$, where S_t refers to a state, A_t denotes action, F refers to feedback, i.e., reward (R_t) or penalty provided by the environment, ρ refers to the state transition such that: $(S_t \times A_t \times S_t) \in [0,1]$ and γ discount factor concerned with rewards. The modeling of RL is concerned with episodes, i.e., set of timesteps during which the agent performs the A_t and interacts with an environment by learning a policy (π_θ) determined based on the current state. Then the agent gets an immediate R_t from the environment based on its A_t taken and transfer to the next state S_{t+1} . In this regard, the A_t can be represented as follows: $A_t = \pi_\theta(S_t)$. The ultimate purpose of the agent is to determine a most suitable π° to maximize the discounted and sum of rewards received so far from any given state such that: $\pi^\circ = \max_{\pi_\theta} V^{\pi_\theta}(S_t)$, where $V^{\pi_\theta}(S_t)$ refers to the value function of π_θ with an input argument S_t numerically expressed as $V^{\pi_\theta}(S_t) = E_{\pi_\theta}[\sum_{j=0}^{\infty} \gamma^j R_{t+k} | S_t \in S]$ indicating the discounted progressive R_t achieved from S_t based on π_θ . However, the value of π° is determined using Q-function such that: $\pi^\circ = \max_{\pi_\theta} Q(S_t, A_t)$ after performing A in any given S numerically expressed as follows:

$$Q(S_t, A_t) = E_{\pi_\theta}[\sum_{j=0}^{\infty} \gamma^j R_{t+k} | S_t \in S, A_t \in A] \quad (1)$$

Where, A denotes action space and S denotes state space.

C. Motivation

Many researchers have explored the effectiveness of the RL in network problems. The literature has shown that that the RL-driven schemes perform well in a specific context. However, it suffers from huge overhead and performance issues in the context of dynamic networking scenarios where topology changes uncertainly and dynamically due to the mobility of sensor nodes. Although, the Q-learning and its

customized variant have been widely employed for designing routing schemes to improve the data packet transmission performance and resource efficiency. However, the issue with Q-learning is that it is not able to determine the optimal solution for the path selection in an appropriate time in the complex and dynamic large-scale networking scenario. Basically, in the large network, the state and action spaces are large, and since the Q-learning utilizes table-lookup mechanisms, it is usually subjected to the issue of dimensional disaster. In the real-time scenario, the network topology changes dynamically, and accordingly, the size of the network also changes. Therefore, an infinite process in the actual sense means that the mobile sensor nodes often leave and join the network dynamically. In this context, when there are more sensor nodes in the network, there will be a large state and action space, and the Q-table occupies a lot of memory. In this regard, the dimension of the state space increases exponentially with state variables, resulting in a proportional upsurge in the dimension of Q-table required to store the value of taking action in a state based on the current policy. Also, the agent requires a large time to explore the environment to learn the policy. Therefore, in a dynamic networking scenario like MANET, computing all possible states is challenging and impractical. However, few researchers suggested integrating deep learning with strong adaptability and generalization ability to solve many practical problems. However, some challenges still remain, which motivates us to introduce an effective solution regarding memory optimization without much affecting the routing performance and network resources.

Therefore, this paper introduces a unique modelling of the reinforcement learning driven routing technique that utilizes Knerva coding mechanisms in the agent modelling, which enables abstraction in the action policy learning towards exploration of optimal routing in the dynamic network. Another significant aspect of the proposed work is the usage of customized environment designed using Open AI Gym function Employing sparse distributed scheme in the routing design cloud efficiently optimizes the memory requirement and offers a better routing policy according to the varying network environment to meet the transmission requirements of different services.

The remaining section of this paper is organized as follows: Section II presents the related work and highlights the problem statement for the proposed work. Section III discusses the proposed system followed by its design and methodology. Section IV presents the environment modelling for the agent interaction to explore optimal route; Section V presents agent modelling for routing using Kanerva coding; Section VI presents the experimental evaluation and performance analysis of the proposed algorithm. Finally, Section VII concludes overall contribution of this paper.

II. RELATED WORK

In the literature, the application of the RL techniques has been widely employed to address the limitations of traditional approaches to the networking domain. However, the existing routing protocols based on RL can be classified into three different categories, viz. i) context-specific criteria, ii) design-

specific criteria, and iii) performance-specific criteria. In the context-specific criteria, the RL addresses networking problems such as related issues, such as routing, channel selection QoS, and resource optimization. The work carried out by Saleem et al. [11] implemented RL to address the problem associated with channel selection and routing in the cognitive radio network (CRN). In this study, the authors have designed a model-based intelligent system to optimize routing and QoS in the context of the cluster-based and packet delivery ratio (PDR), respectively. In Debowski et al. [12], Q-learning-based path selection mechanisms are developed to optimize the node resources. The work of Jung et al. [13] presented a data packet-driven efficient routing scheme in the un-manned robotic network, a kind of mobile ad-hoc network (MANET). In this study, a modified Q-learning is adopted to formula tea location-based routing technique considering the mobility factor of the sensor nodes. The work of Zeng et al. [14] presented a hybrid scheme formulated based on Q-learning and fuzzy logic system to minimize and achieve an efficient balancing scheme in the MCA collision in the flying Ad-hoc network. Here, fuzzy logic is employed to choose leader nodes considering the mobility pattern, and Q-learning is used to stimulate member node-rewarding to learn and evaluate multi-hop routes. The research work by Varshini et al. [15-16] presented a significant contribution in the networking, where the authors in [15] suggested a customized environment, namely NetAI-Gym, to evaluate RL agent for routing. In [16], the authors have presented a routing protocol based on Q-learning to select optimal routes. Also, the performance of presented routing schemes is evaluated with a rule-based agent algorithm. Hence, there are many RL-based approaches, but the existing studies lack modeling of a suitable environment to evaluate agent performance. However, there are few significant research works towards agent design and modeling. In the design-specific criteria, the researchers attempt to customize and enhance the design of agent mechanisms such as model-free approaches and model-based to achieve efficiency and accuracy in the model performance. The work carried out by Shen et al. [17] modeled a load balancing protocol based on the model-free approaches to

minimize the congesting in peer-to-peer networking systems. The concept of the RL is mechanized to observe the environment state, such as processing capacity, queries, and resources associated with each peer. Further, the algorithm determines the suitable peers to relay queries based on the state observation. The study of Hendriks et al. [18], designed a Q-routing mechanism to perform optimal path selection and overhead reduction in the Ad-hoc wireless network. This study utilizes the AODV protocol for the route discovery process, and Q-learning is used to optimize the path discovery concerning QoS requirements. Johnston et al. [19] have introduced an intelligent routing scheme for battel networks to meet the real-time requirements. In this scheme, an approach of Q-learning is utilized to generalize and learn the next-hops to perform successful transmission of unicast- packets to the end nodes. The study considers duplication of the packets during unstable paths, and the packets are forwarded securely through multi-hop routes. The study uses cost-metric for the case of duplication, where if the cost factor is closer to zero, then more possibly that path is broken; if closer to 1, the path is stable. The researchers presented techniques emphasizing state overhead, action overhead, control packet overhead, and performance optimization in the performance-specific criteria. In the study of Wang et al. [20], the RL is utilized in the software-defined networking (SDN) enabled Internet of Things to improve routing performance. The SDN controller has a global view of the nodes and adapts routing based on mobility and traffic conditions. Further, an optimal route is determined based on the Q-learning approach. In Lin et al. [21], an adaptive routing scheme is suggested based on Q-learning concerning QoS optimization, including delay, loss, and bandwidth factor. The study of Tang et al. [22] adopted RL to develop opportunistic routing to support video streaming in the application of multi-hop wireless networks. The researchers also adopted the deep RL concept to achieve efficiency in the routing protocol [23]. The deep RL technique is used in Lan et al. [24] to perform efficient routing in the SDN. Table I summarizes the above-discussed literature to provide a quick insight for the readers.

TABLE I. SUMMARY OF ABOVE-DISCUSSED LITERATURE

Citation	Network Type	RoutingContext	Design	QoS metrics
[11]	CRN	Cluster-based	Model Based	PDR
[12]	WSN	Data-driven	Model Free	Delay Energy
[13]	MANET	Data-driven	Model Free	Delay, Overhead
[14]	FANET	Data-driven	Model Free	Delay, Throughput
[15]	MANET	-	Model Free	-
[16]	MANET	Data-driven	Model Free	PDR, Delay
[17]	P2P	Cluster-based	Model Free	Search time
[18]	WANET	Data-driven	Model Free	Delay, PDR
[19]	Battel networks	Data-driven	Model Free	Throughput
[20]	SDN	Standard Protocol driven	Model Free	PDR
[21]	SDN	Route Request driven	Model Free	Bandwidth, Delay and loss
[22]	Multi-hop network	Data-driven	Model Free	Delay, Throughput
[23]	Wireless network	Survey	Survey	-
[24]	SDN	Data-driven	Model Free	PDR, Delay and loss

Following are the significant open issues explored based on the above-discussed literature.

- It has been found that the majority of the study lacks modeling of a suitable environment that supports the function of Open AI Gym to assess RL agent algorithm.
- Open-AI Gym is a toolkit for benchmarking the agent algorithm. However, it is not considered in the existing approaches in the context of network problem.
- Due to the ever-increasing requirements for accuracy and efficiency in decision-making process for network routing, various approaches have been suggested over the years that can only approximate the complexity of the routing problem.
- The applicability of the existing methods is limited to the specific context and is not much effective in dealing with dynamic scenario, where the network topology and size changes dynamically.
- Very few research studies concerning Q-routing are found to emphasize the overhead memory problem.

The problem statement for the proposed study can be stated as "it is a very challenging task to integrate reinforcement learning function in the memory-efficient routing mechanism in an uncertain and dynamically-changing network environment."

III. PROPOSED SYSTEM

The proposed study suggests a memory-efficient RL-driven routing mechanism. The proposed routing is based on the RL agent which is developed using function approximator that uses the Kanerva (K) coding scheme to store learnable parameters (weight and bias) to represent the learned policy for the action being performed by the agent towards exploration of better route establishment. The proposed algorithm searches for a near-optimal prototype set that provides a significant level of abstraction in memory consumption. The proposed algorithm is introduced in a dynamic network environment to perform path establishment for reliable data transmission.

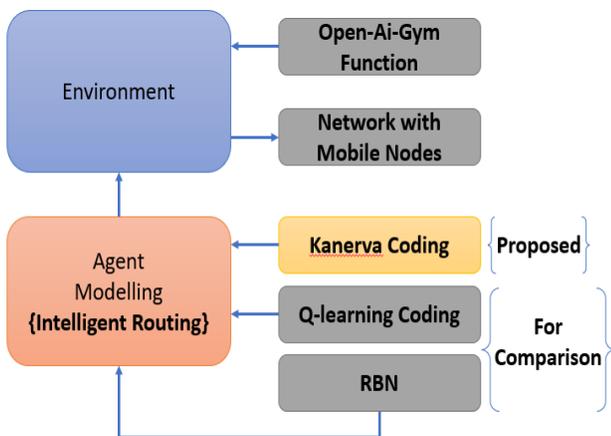


Fig. 2. Schematic Architecture of the Proposed System.

The schematic architecture of the proposed system is shown in Fig. 2, where environment modelling is carried out considering Ad-network with mobile nodes using Open-AI gym function. On the other hand, agent modelling is carried out to perform routing operation based on Kanerva coding technique and also the proposed study implements two other algorithm such as Q-learning and radial basis function (RBF) for the comparative analysis.

IV. ENVIRONMENT MODELLING

The proposed study performs environment modeling that imitates the scenario of the mobile wireless networking system. The design and development of the environment are inspired by the work carried out by [15], in which a customized environment is developed, namely Net-AI-Gym. The network is composed of mobile sensor nodes with Ad-hoc features. The network as the environment is modeled as $G(V,E)$, where V indicates vertices, i.e., sensor nodes, and E is the link for connecting the sensor nodes in the network. In this regard, the environment is represented as a collection of n vectors as in set: $\eta = \{\vec{N}_1, \vec{N}_2, \vec{N}_3, \dots, \vec{N}_n\}$, where, $\forall \vec{N}_k \in \eta$ denotes a sensor node with $\{X_k, R_k\} \in \vec{N}_k$, where X_k is the Node id and R_k denotes set of link and $k \in [1, n]$ and $n \in \mathbb{N}$, where $n \geq 2$. The study considers a mobile sensor node \vec{N}_k can be linked with many of the other sensor nodes within its proximity such that $\eta - \{\vec{N}_k\}$, therefore, $\forall n, R_k$ is represented as follows: $R_k = \{\vec{L}_1, \vec{L}_2, \vec{L}_3, \dots, \vec{L}_m\}$ s.t $\forall L_k \in R_k$ including X_k , and W_k , where the W_k denotes the weight of the R_k . Fig. 3 shows a flow diagram of the environment with the Open-Ai-Gym function.

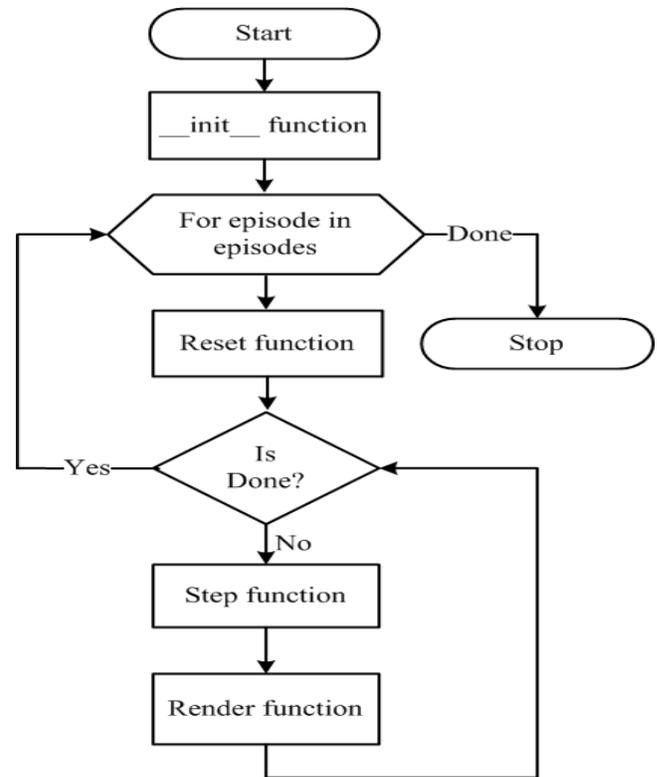


Fig. 3. Flow of Environment for Net-AI Gym [15].

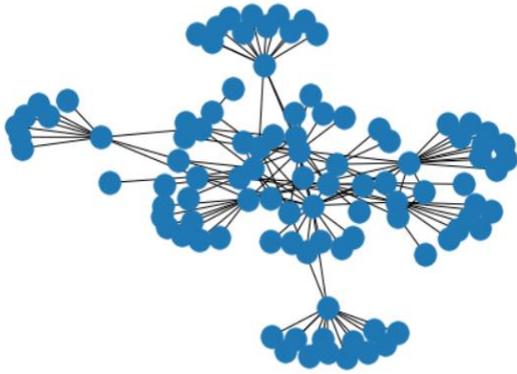


Fig. 4. An Environment with 100- Nodes Network.

Fig. 4 demonstrates the environment scenario with 100 mobile sensor nodes connected to each other. The design and development of the environment are carried out using the Open-AI gym function as mentioned in the flowchart depicted in Fig. 3 [15]. Open-AI gym enables the environment to satisfy the Markov process. The environment implemented in this study is scalable and flexible to N number of sensor nodes comprising Ad-hoc and mobility features. Thus, the proposed RL environment is the dynamic and uncertain imitating scenario of a mobile ad-hoc network. However, ensuring efficient routing is quite challenging due to the mobile and ad-hoc nature of the network. Therefore, the proposed study presents an efficient and sparse distributed memory-based agent model to perform routing operations in dynamic networks, discussed in the next section.

V. AGENT MODELLING

The prime objective of the study is to build an agent for solving the routing problem and optimizing the memory with the Kanerva coding. In the present study, the proposed agent mechanism uses function approximator as the Q function. However, the weights and biases of this function approximator are stored using the Kanerva coding. Due to which the storage space remains constant all the time. However, before discussing the proposed routing algorithm, it is better to understand the routing problem, its formulation, and the role of the function approximator in RL agent modeling.

A. Routing Problem

To determine the finest path from the source node to the destination node, context-adaptive and efficient routing mechanisms increase the probability of reaching the destination's data packets. Since the environment considered in the proposed study has a completely random and dynamic networking scenario, selecting the optimal number of intermediate sensor nodes for transmitting data packets is challenging. Thus, the routing process in a dynamic networking environment can be formulated as a Markov decision problem. Let us considered the sensor node n_i characterized by MDP tuple $\{S_i, A_i, C_i, T_i\}$. The S_i element of this tuple refers to set of states S in n_i . Let us considered N_i as a set of sensor nodes within the proximity or range (R_i) of n_i . In this regard, the state S in n_i comprises \vec{d} and e , where the vector d is the distance value of all sensor nodes such that: $d_{i,j} \forall n_j \in N_i$ and represents the energy value of all nodes

in the range of n_i such that: $e_{i,j} \forall n_j \in N_i$. The \vec{d} is obtained by computing the Euclidean distance between n_i and $n_j \in N_i$ as follows:

$$\vec{d} = \sqrt{(x_i^t - x_j^t)^2 + (y_i^t - y_j^t)^2} \quad (2)$$

Where, x and y is the positioning coordinates of the sensor nodes n_i and n_j . Moreover, the transmission or proximity range R_i of n_i can be determined into different intervals (I) of length l expressed as follows:

$$I = \frac{R_i}{l} \quad (3)$$

According to the above numerical equation (3), the distance between n_i and n_j is a positive integer $\{1 \dots I\}$ computed based on l and real distance value $d_{i,j}^t$ resides at time t . Here, the time ' t ' is considered because of the random nature of the network where the sensor nodes leave or join the network dynamically. Also, it is to be noted that $\forall n_i, l$ represents a unit of d and state interval I is subjected to the R_e^i . Furthermore, the remaining energy of $e_{i,j}, j \in N_i$ at $t + 1$ can be computed as follows:

$$e_{i,j}^{t+1} = (e_{i,j}^t - \chi_j^t) \quad (4)$$

Where, χ_j^t indicates the amount of energy utilized by n_j at t time. The illustration of R_i is shown in Fig. 5. Considering all the above notions, the entire state S can be expressed as follows:

$$S = (d_{n_i,j}^t, e_{n_i,j}^t) \quad (5)$$

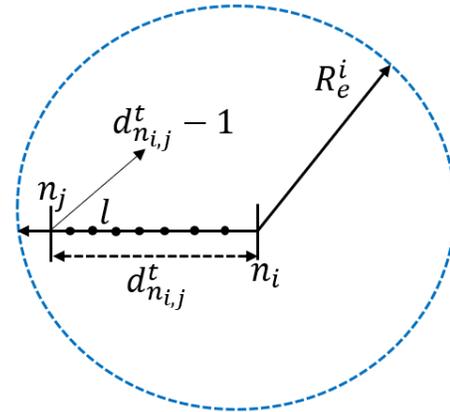


Fig. 5. Illustration of Transmission Range for n_i .

The second element A_i of the tuple represents a set of actions that n_i executes. The tuple element C_i refers to the return function of n_i such that: $C_i \leftarrow S_i \times A_i$ a Cartesian product of state-action space. The symbol T_i is the state transition probabilities for performing an action such that: $T_i \leftarrow S_i \times A_i \times S_i \in [0,1]$. This actually represents the transition from state S (eq. 5) at time t such that: S^t to next state at time $t + 1$ such that S^{t+1} . However, computing the precise value of T_i is usually impractical due to the absence of prior information about the network model, its random parameters, and its dynamic nature. In the proposed study, the development of agent is carried out based model-based

approach, and each mobile sensor node approximates its T_i using maximum likelihood approach and the possible $T_i \in \{\text{transfer, drop, reset, and delivered}\}$ and the path establishment process is completely in the control of the agent [15].

B. Agent Modeling based on Function Approximation

As discussed in previous section, the RL algorithm encounters communication and memory overhead problems when action space is very large in dynamic state spaces. In order to address this problem, the researchers have suggested the implementation of the function approximator, which is a basically an approach of neural network that the RL agents utilize to improvise its learning performance when introduced to dynamic and complex state spaces. Fig. 6 exhibits modeling of the agent using function approximator for dynamic network environment.

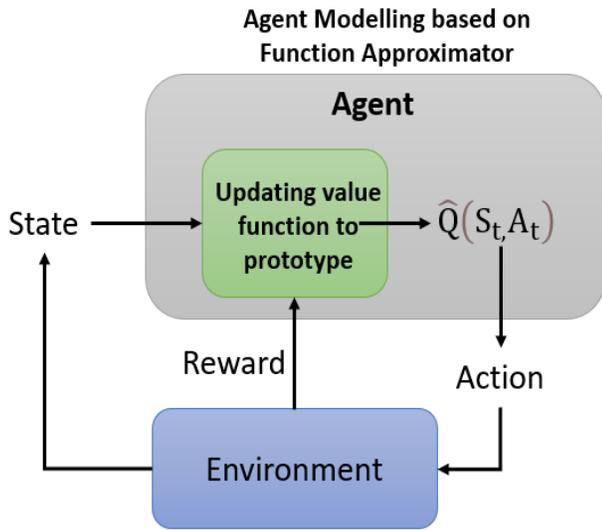


Fig. 6. Agent Modelling based Function Approximator.

In this work, the study utilizes simple artificial neural network (ANN) architecture that has parametrize function ' θ ' concerned with the learnable parameters, namely weight and biases, to represent approximated S_t and A_t value such that $\hat{Q}(S_t, A_t)$. The values for all S_t and A_t pairs extracted from the large space are mapped into abstract components in $\vec{\theta}$. The approximated $\hat{Q}(S_t, A_t)$ concerning $\vec{\theta}$ expressed as follows:

$$\hat{Q}(S_t, A_t; \vec{\theta}) = \vec{\theta}^T \vec{\varphi}_{S_t, A_t} \quad (6)$$

$$\vec{\theta} \vec{\varphi}_{S_t, A_t} = \sum_{i=1}^N \theta_{A_t}(i) \varphi_{S_t, A_t}(i) \quad (7)$$

Where, $\vec{\varphi}$ denotes vector that consists of prototypes with N components that are constructed by state representation. In the proposed study, Kanerva coding is used as a state representation technique. The ideology behind using Kanerva coding [25] in the proposed agent modeling is that the Kanerva coding considers a small state as a prototype to store the value functions. Kanerva coding maintains a set of prototypes p as parameterized elements for the approximation and a value $\theta(p, A_t)$ is stored and updated for each prototype p concerning A_t . The approximation of state-action (S_t, A_t) is

computed by a linear combination of $\vec{\theta}$ values of all adjacent prototypes of A_t , expressed as follows:

$$\hat{Q}(S_t, A_t) = \sum_{p \in D} \theta(p, A_t) \mu(S_t, p)$$

where D denotes adjacent p with respect to S_t . The mechanisms of Kanerva coding in the proposed agent is designed based on the following algorithm.

C. Kanerva Coding

Kanerva coding (K-coding) deals with an architecture of sparse distributed memory [25] that utilizes prototype states to characterize the input sample states. The implementation of K-coding in the proposed agent for performing routing operation has multiple advantages viz. i) with the increase in network dimension (state space) due to increase in the number of sensor nodes in the network does not exponentially increase the prototypes required to learn the policy. Thus, facilitating efficient storage utilization and better scalability, i.e., constant memory, even the network size is increasing. The prime objective of implementing K-coding is to optimize the prototype set required to characterize a state space in an uncertain, dynamic, and large network system with minimal memory cost. The Block diagram of a proposed agent with K-coding is shown in Fig. 7.

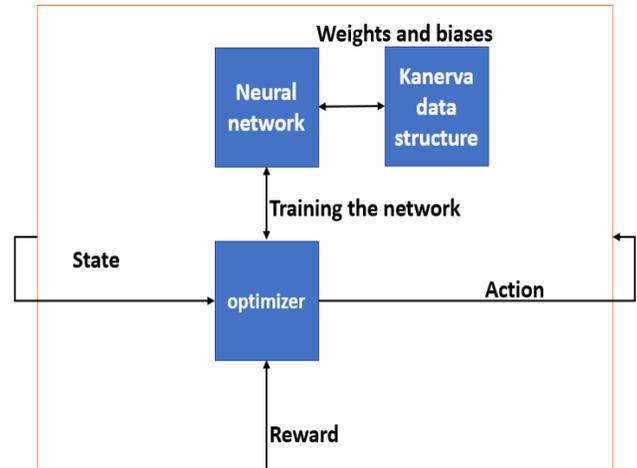


Fig. 7. Kanerva Coding in the Proposed Agent Function.

The proposed method uses K-coding as storage in order to store the values of weights and biases of the function approximator. The model works with the help of an ANN which employs regular weights and biases to find the best solution at the given state. In the case of networking, both state and action represent the current node in which the packet is present. The route is always decided with the help of ICMP packets. The agent will be present in all nodes, and the same will be updated everywhere as well. In the proposed method, Kanerva is used purely as a storage to the ANN, where it can store its weights and biases. Following is the complete algorithm for the efficient routing based on the K-coding function approximator agent mechanism.

Algorithm for routing with ANN and Kanerva Coding

Input: S, E, K, n, C₁, C₂, C₃, N

Output:

Start

1. **Init** S_t ∈ S(state)
2. Build ANN Model → M
3. M ← f₁(N, 253, N) // f₁ model building function
// where N is number of nodes
4. **Init**w(weights), b(biases)
// where, w & b initialized as random values
5. **For** E in 4000 **do** // E is number of episodes
6. A_t = model.predict(S) // A_t is action
7. S = Env(A_t) // State changes when action is performed
8. M.train(R_t) // R_t is reward
9. **For** i:wdo
10. **For** j:n **do** // j = 1 and n number of prototypes(P)
11. Compute D = f₂(P, S) // where D is the distance
// f₂ distance function (Euclidian)
12. **End for**
13. **End for**
14. I = f₃(D)
15. **For** m = 1:3
16. Ind_m = I(1 to c_m)
17. Store Ind_m
18. **End for**
19. **End for**

End

The algorithm takes parameters as input values K a set of S_t, n (ratio), closer prototype (C), where C = {c₁, c₂, c₃} utilized to determine the C to the current S_t based on the distance function. The proposed study considers the distance function as a Euclidean distance. In the first step of the algorithm randomly initializes p and takes input as a S_t. For each set of S_t i.e., K, the algorithm performs the computation of Euclidean distance between the prototype (p) and state S_t. The algorithm further stores the identity of computed distanced in vector format. In the next step of the algorithm, constructs a matrix Ind_m for the first 3 features and then performs the mechanism of offsetting by (m-1) x K. Basically, the K-coding mechanisms compute the length space between a state variable its actual distance. Further, the obtained data is then merged with a better-quality state similarity to achieve higher accuracy in its computations. K-coding diminishes the requirement for reallocation and resizing of prototypes, which significantly shortens the large dependencies of storing large action-space value in the Q-learning. Due to the strong learning ability and reduced computational complexity, the K-coding mechanism also improvises the entire learning experience.

VI. EXPERIMENTAL EVALUATION

The proposed work's design and implementation are carried out using Python programming language in the Anaconda development environment. The experiment analysis is carried out considering comparative analysis, where the performance of the proposed agent mechanism is compared

with other algorithms such as Q-learning and RBF. Both Q-learning and RBF are implemented in the study in RL agent design and evaluated on the same environment designed using the net-Ai gym environment proposed in a previous paper [15]. The following assumptions are considered in the simulation setting and the experimental analysis:

- The weights in the network represent the difficulty of packets being transferred.
- The weight is a composition of signal interruptions, battery, and distance.
- The weights keep varying to simulate dynamic or mobile networks.
- The number of nodes considered is 6 to 100 nodes.
- The various parameters shown here are recorded for networks with a various number of nodes.
- In this study, each network is trained for 4000 episodes.
- An episode is nothing but a simulation of a single packet from source to destination.
- The episode ends when the packet either drops or reaches the destination.

For the comparative study, the proposed study considered multiple performance metrics such as memory utilization, throughput analysis, average throughput, the processing time for route establishment, and analysis of the pathlength. Fig. 8 presents performance analysis regarding memory utilization.

The graph trend of Fig. 8 exhibits that the memory in Q learning increases exponentially, linearly in the case of RBN, and stays constant in the case of Kanerva coding.

The graph trend in Fig. 9 indicates that Q learning has low throughput, whereas RBN and K code has achieved higher throughput. Since K-code uses a function approximator in order to store the values, it underperforms a little bit compared to RBN; however, this difference is insignificant compared to Q learning. Even though K-coding underperforms slightly compared to RBN, it saves a lot of memory.

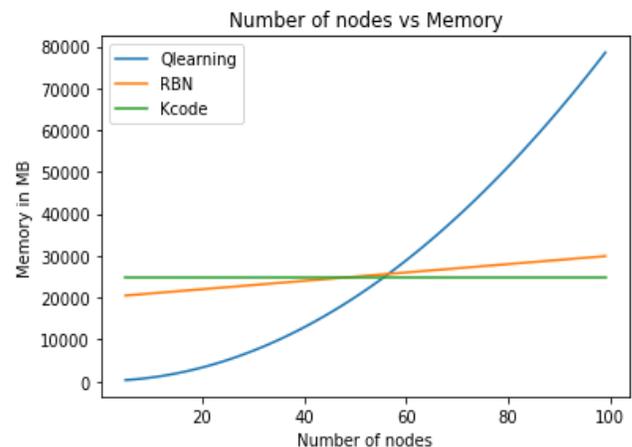


Fig. 8. Analysis of Memory.

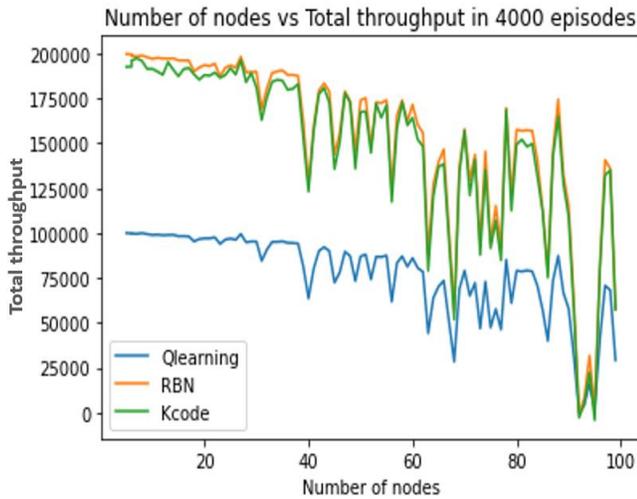


Fig. 9. Analysis of Total Throughput.

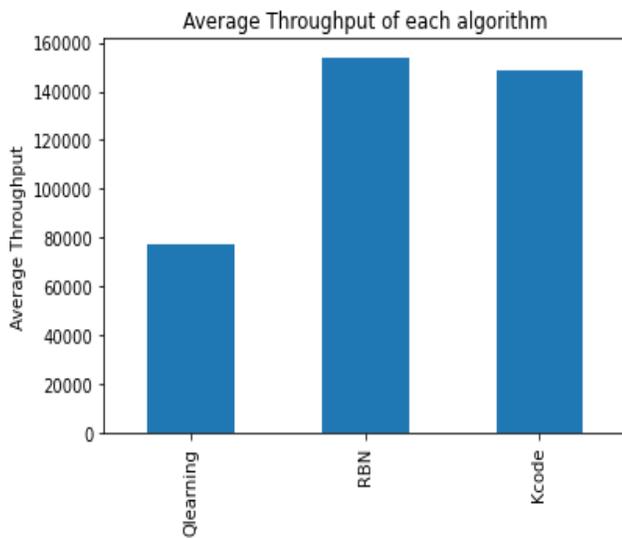


Fig. 10. Analysis of Average Throughput.

Fig. 10 shows the average throughput of each algorithm. The difference in the throughput of the RBN and K-coding is very insignificant.

Fig. 11 demonstrates the analysis of the average routing time of each algorithm. Routing time is defined as the time required by the algorithm to search for a suitable path in any network. Here Kanerva coding offers the least routing time, which is desirable. This is because the K-coding consumes lower memory and is faster to get trained.

Fig. 12 represents a change of path length along with nodes. It can be observed here that the K-coding always finds the shortest path. It is better than Q learning and RBN all the time.

A. Result Implication

- It is seen that the Q learning is not showing a good throughput. This is because the Q learning has less trainable parameters, and the table decides the reward. Even though the rewards are stored and stored aptly,

the mechanism to calculate the future reward isn't as robust as the other two methods.

- The Q learning fails to perform in the case of memory management as well since the number of actions and states increases with an increase in nodes. To be specific, the memory consumption increases exponentially since the rewards are stored in the form of a table.
- The purpose of the Kanerva coding is to maintain a constant memory throughout.
- As observed from the above results, Kanerva coding underperforms in only one aspect: throughput. However, it does not pose a significant disadvantage as compared to RBN.

The proposed routing is designed based on the RL agent that utilizes K-code to achieve abstraction in the state space. Therefore, the proposed agent mechanism dynamically establishes the best node path with a low computational burden under uncertain and dynamic network traffic conditions.

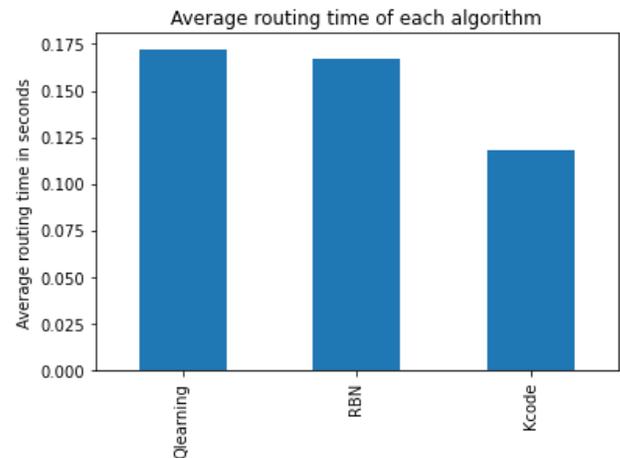


Fig. 11. Analysis of Average Routing Time.

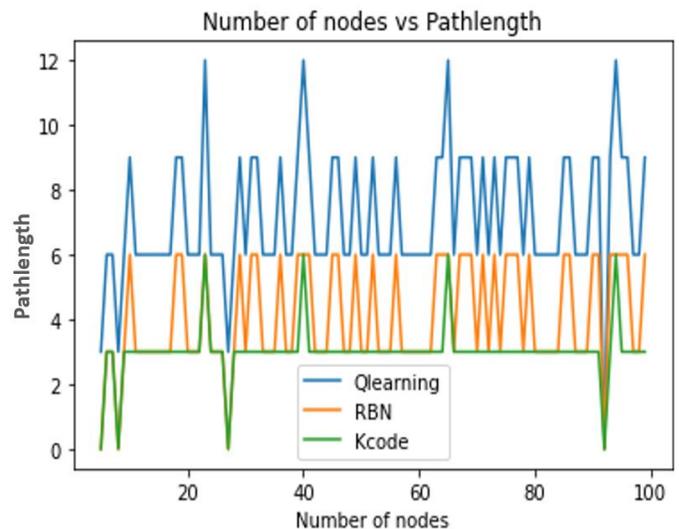


Fig. 12. Analysis of Pathlength.

VII. CONCLUSION

The proposed work is an extension of our previous research works, where in the first work, a suitable environment is designed to solve routing problems in network using the RL agent. On the other hand, the effectiveness of the proposed environment is evaluated in the second work by implementing a routing algorithm based on Q-learning and rule-based methods. In this paper, the proposed study improvises Q-routing performance to have better time and memory efficiency in the current work. The Q-learning consumes much memory and is not time efficient. RBN gives higher accuracy and time efficiency; however, the memory required for the algorithm will still increase with an increasing number of nodes. Hence, this work Kanerva coding is implemented to store the weights and biases of the function approximators used to build an agent for solving the routing problem and optimizing the memory. The benchmarking of the proposed system is carried out based on the comparative analysis concerning multiple network performance metrics. The study outcome proves the effectiveness of the proposed agent mechanism for routing operation under any given traffic condition in the network. In the future work, the proposed work can be extended in the context of multi-agent modeling of energy and security aware routing protocol in the dynamic networking environment.

REFERENCES

- [1] Ramasamy, Dr. Velmani. (2017). Mobile Wireless Sensor Networks: An Overview. 10.5772/intechopen.70592.
- [2] Lanzolla, A. and Spadavecchia, M., 2021. Wireless Sensor Networks for Environmental Monitoring.
- [3] Khalaf OI, Abdulsahib GM. Energy efficient routing and reliable data transmission protocol in WSN. Int. J. Advance Soft Compu. Appl. 2020 Nov 1;12(3):45-53.
- [4] Nakas C, Kandris D, Visvardis G. Energy efficient routing in wireless sensor networks: a comprehensive survey. Algorithms. 2020 Mar;13(3):72.
- [5] Prabha K. Performance assessment and comparison of efficient ad hoc reactive and proactive network routing protocols. SN Computer Science. 2020 Jan;1(1):1-7.
- [6] Thiagarajan R, Moorthi M. Efficient routing protocols for mobile ad hoc network. In2017 Third International Conference on Advances in Electrical, Electronics, Information, Communication and Bio-Informatics (AEEICB) 2017 Feb 27 (pp. 427-431). IEEE.
- [7] Fan X, Cai W, Lin J. A survey of routing protocols for highly dynamic mobile ad hoc networks. In2017 IEEE 17th International Conference on Communication Technology (ICCT) 2017 Oct 27 (pp. 1412-1417). IEEE.
- [8] Chandel A, Chouhan VS, Sharma S. A Survey on Routing Protocols for Wireless Sensor Networks. InAdvances in Information Communication Technology and Computing 2021 (pp. 143-164). Springer, Singapore.
- [9] Boutaba R, Salahuddin MA, Limam N, Ayoubi S, Shahriar N, Estrada-Solano F, Caicedo OM. A comprehensive survey on machine learning for networking: evolution, applications and research opportunities. Journal of Internet Services and Applications. 2018 Dec;9(1):1-99.
- [10] Usama M, Qadir J, Raza A, Arif H, Yau KL, Elkhatib Y, Hussain A, Al-Fuqaha A. Unsupervised machine learning for networking: Techniques, applications and research challenges. IEEE access. 2019 May 14;7:65579-615.
- [11] Y. Saleem, K. A. Yau, H. Mohamad, N. Ramli, M. H. Rehmani, "Joint channel selection and cluster-based routing scheme based on reinforcement learning for cognitive radio networks," in International Conference on Computer, Communications, and Control Technology, 2015.
- [12] B. Debowski, P. Spachos, S. Areibi, "Q-learning enhanced gradient based routing for balancing energy consumption in WSNs," in 21st IEEE International Workshop on Computer Aided Modelling and Design of Communication Links and Networks (CAMAD), 2016.
- [13] W.-S. Jung, J. Yim, Y.-B. Ko, "QGeo: Q-Learning-based geographic ad hoc routing protocol for unmanned robotic networks," IEEE Communications Letters, vol. 21, no. 10, pp. 2258-2261, 2017.
- [14] Z. Zheng, A. K. Sangaiah, T. Wang, "Adaptive communication protocols in flying ad hoc network," IEEE Communications Magazine, vol. 56, no. 1, pp. 136-142, 2018.
- [15] VarshiniVidyadhar, Nagaraj R and D V Ashoka, "NetAI-Gym: Customized Environment for Network to Evaluate Agent Algorithm using Reinforcement Learning in Open-AI Gym Platform" International Journal of Advanced Computer Science and Applications(IJACSA), 12(4), 2021.
- [16] VarshiniVidyadhar and R. Nagaraja, "Evaluation of Agent-Network Environment Mapping on Open-AI Gym for Q-Routing Algorithm" International Journal of Advanced Computer Science and Applications(IJACSA), 12(6), 2021.
- [17] X.-J. Shen, Q. Chang, L. Liu, J. Panneerselvam, Z.-J. Zha, "CCLBR: Congestion control-based load balanced routing in unstructured P2P systems," IEEE Systems Journal, vol. 12, no. 1, pp. 802-813, 2018.
- [18] T. Hendriks, M. Camelo, S. Latre, "Q2-routing: a QoS-aware Qrouting algorithm for wireless ad hoc networks," in 5th International Workshop on Cooperative Wireless Networks, Cartagena, Spain, 2018.
- [19] M. Johnston, C. Danilov, K. Larson, "A reinforcement learning approach to adaptive redundancy for routing in tactical networks," in IEEE Military Communications Conference, Los Angeles, CA, 2018.
- [20] C. Wang, L. Zhang, Z. Li, C. Jiang, "SDCoR: Software defined cognitive routing for Internet of vehicles," in IEEE Internet of Things Journal, 2018.
- [21] S.-C. Lin, I. F. Akyildiz, P. Wang, M. Luo, "QoS-aware adaptive routing in multi-layer hierarchical software defined networks: A reinforcement learning approach," in IEEE International Conference on Services Computing, 2016.
- [22] K. Tang, C. Li, H. Xiong, J. Zou, P. Frossard, "Reinforcement learning-based opportunistic routing for live video streaming over multi-hop wireless networks," in IEEE 19th International Workshop on Multimedia Signal Processing, 2017.
- [23] K. Arulkumaran, M. P. Deisenroth, M. Brundage, A. A. Bharath, "Deep reinforcement learning, a brief survey," IEEE Signal Processing Magazine, vol. Nov., pp. 26-38, 2017.
- [24] C. Yu, J. Lan, Z. Guo, Y. Hu, "DROM: Optimizing the routing in Software-Defined Networks with deep reinforcement learning," IEEE Access, vol. 6, no. 18, pp. 64533-54539, 2018.
- [25] R. Sutton and A. Barto. Reinforcement Learning: An Introduction. Bradford Books, 1998.

A Systematic Review of Published Articles, Phases and Activities in an Online Social Networks Forensic Investigation Domain

Aliyu Musa Bade¹

Department of Computer Science, Yobe State University
Damaturu, Nigeria

Siti Hajar Othman²

School of Computing, Universiti Teknologi Malaysia
Johor Bahru, Malaysia

Abstract—The purpose of this paper is to retrieve, evaluate and analyse the available published articles in five (5) relevant online databases from 2011 to 2021 and also critically identify the phases and activities involved in an Online Social Networks Forensic Investigation based on bibliometric analysis and Degree of confidence respectively in order to know the evolution in the research domain. A systematic literature review (SLR) technique was adopted by the author to search using pre-defined keywords. Only scholarly articles published between 2011 and 2021 written in English were included in the search. The total of 316 subscribed documents were collected from the five (5) online databases based on the search criteria although twenty-nine (29) are duplicates. ScienceDirect has the highest number with 189 documents and the year 2020 with the highest published articles. Six (6) phases and forty-three (43) activities were identified. According to a review of the recovered publications, no previous research has been done to statistically retrieve, evaluate and analyse the level of work that has been done in the domain of OSNFI, as well as the phases and activities involved in the forensic investigation of an online social networks crime.

Keywords—Forensic; investigation; model; online social networks; bibliometric analysis; degree of confidence

I. INTRODUCTION

Digital forensics has been studied for a decade, but it still appears to be a very young science, with many issues remaining unclear and ambiguous [1]. It is the science of collecting, preserving, examining, analysing, and presenting relevant digital evidence for use in legal proceedings [2]. The entire field of digital forensics investigation is still lacking in fundamental agreements which may be as a result that the field is relatively young [3]. It is a procedure, and not just one process, but a set of tasks and procedures that occur during the course of an investigation [2]. There is a lack of consistent definitions and language when it comes to the core parts of digital evidence investigation [4].

Millions of people use online social networks on a daily basis [5], which has facilitated new ways of connecting and sharing knowledge [6]. It has also resulted in a rise in excessive criminal activities [7], with criminals becoming more advanced in attempts to exploit technology to avoid detection and conduct crimes [6]; such as malware distribution, fraud, harassment, cyberbullying and cyberstalking. They also use online information to commit traditional crimes such as theft,

kidnapping, and murder. Furthermore, they use the information as tools to assess and gain access to their victims [8].

Forensics is used on social media platforms like Facebook, MySpace, Twitter, and LinkedIn. It is well known as social media forensics, and it's a subset of digital forensics and network forensics [9]. Online social networks are Web-based services which enable individuals to create a public or semi-public profile within a confined system [6], articulate a list of other users with whom they share a link, and display and traverse their list of connections as well as those created by others within the system [10]. Different SNSs, like Facebook, Twitter, and LinkedIn, are used to connect people and enable them to communicate with one another [5]. People build personal profiles from various social networking sites to share their thoughts, photographs, images, emails, and instant messaging [11], as well as to find old friends or people with common interests or problems through various social networking sites [12].

Rapid technological development can cause issues for users of the technology. The more advanced people's lives become, the more advanced crime becomes [13]. Social media platforms are becoming increasingly popular, with Facebook managing above thirty-one (31) million users in United Kingdom, Twitter managing fifteen (15) million, and LinkedIn having 10 million. With the proliferation of mobile phones, the use of social network services (SNS) has skyrocketed, this SNS stores a variety of data, including user conversations, user location information, personal networks, and user psychology which can be valuable evidence in a digital forensics investigation of an incident [14]. Other uses of social networking sites include, general chatting, broadcasting breaking news, setting up a date, tracking election results, planning disaster response, humour, and serious analysis [11].

There are five (5) sections in this thesis. The following is a synopsis of the contents of each section: Section 1 – Introduction: this section provides a summary of the research study as well as explanations for the findings that led to the contributions of this review. The review objective is briefly stated in Section 2, and the methodology of the systematic literature review (SLR) used throughout the review process is discussed in Section 3. Section 4 includes a discussion based on the data gleaned from the review process. Finally, Section 5 brings this review to a conclusion.

II. OBJECTIVE OF THE REVIEW

The review looks into information from significant published sources on the available publications in the domain of an online social network forensic investigation, as well as the phases and other activities involved in the investigation process. According to the literature review, there are no SLR type publications on the topic of online social network forensic investigation. As a result, the goal of this review is to find out the amount of work that has been carried out and published in the domain of an Online Social Network Forensic Investigation. In addition, to identify the numerous phases and activities that can be employed in the investigation of an online social network forensic crime. These objectives are important because variety of DFIMs exist, but majority of which take related methods [15]; [16]. They fail to address the fundamental differences and unique needs of online social networks [17]. However, because there is no universal way [10]; [18] in many cases, investigators conduct automated forensic investigations mostly using different methods [19].

III. METHODOLOGY

The SLR is a step-by-step process that enables researchers to create their own search procedure. This review was carried out in accordance with the technique for conducting SLRs as proposed by [20]. It is used in identifying the required information from the selected articles. This method was chosen because it makes it easier to capture, summarise, synthesise, and critically comment on any of the topics reviewed. The SLR process consists of the following steps:

- Step 1: Define the research questions.
- Step 2: Determine the data sources and search process.
- Step 3: Inclusion and exclusion criteria.
- Step 4: Results of searching and data extraction.
- Step 5: Discussion.

The total of three hundred and sixteen (316) articles linked to online social network forensic investigation were retrieved using the SLR approach from five (5) credible online journals. These online databases are: Scopus, Web of Science, IEEEExplore, ScienceDirect and Association for Computing Machinery (ACM) Digital Library.

A. Research Questions

RQ1. What are the available published articles in Scopus, Web of Science, IEEEExplore, ScienceDirect and Association for Computing Machinery (ACM) Digital Library in the domain of an Online Social Networks Forensic Investigation model from 2011 to 2021?

RQ2. What are the phases and activities involved in an Online Social Networks Forensic Investigation model Domain based on the Degree of Confidence?

B. Data Sources and Search Process

Five (5) online databases were accessed (Scopus, Web of Science, IEEEExplore, ScienceDirect, Association for Computing Machinery (ACM) Digital Library) and all available documents were retrieved based on the search key “[All:online] AND [All:social] AND [All:network] AND [All:f

orensic] AND [All:investigation] AND [All:model] AND [PublicationDate:(01/01/2011 TO 31/12/2021)]”. All articles which include any of the search term (online, social, network, forensic, investigation, model, publication date from 01/01/2011 to 31/12/2021) were retrieved. All articles from 2011 to 2021 were included in the search. This time frame was chosen because it would allow for the retrieval of a sufficient number of articles on the subject and the detection of a research trend. Despite that, the articles retrieved are relatively considered less considering the importance of the domain even though it’s young.

C. Inclusion and Exclusion Search Criteria

Only empirical research based on published literature in the field of online social network forensic investigation were evaluated. The search parameters were configured to retrieve only items authored in English and published between January 1, 2011 and December 31, 2021. Interviews, news, periodicals, correspondence, conversations, comments, letters to the editor, summaries of tutorials, meetings, workshops, panels, and poster presentations were all eliminated from the search.

We excluded the aforementioned categories of publications since we only sought to identify papers in the field of online social network forensic investigation, the majority of which could be found in full-text and peer-reviewed journal articles. Journal articles are discovered to go through review processes that ensure that only proven evidence is available.

Journals published more matured research when compared to other sources. Only full-text studies were chosen the availability of thorough assessment methods as opposed to articles that are only available in abstract form. Also, peer-reviewed articles were chosen since they determine the credibility and dependability of studies.

D. Search Results

A number of literature works dealing with the topic of an online social network forensic investigation are listed in Table I. The article list is divided into four (3) vertical categories and serves as a broad overview with the; (i) Name of online Database(s), (ii). Total document retrieved, and (iii) Categorization by Year of publication. Tables III and IV presents the selection of the OSNFIM development phases based on degree of confidence (DoC) and the OSNFI phases and their activities respectively. Fig. 1 shows the retrieved articles according to the year of publication, Fig. 2, Fig. 3 and Fig. 4 shows the Network, Overlay and Density visualizations of available OSNFIM documents on one of the online database (Scopus) based on bibliometric analysis. Fig. 5 shows the OSNFIM development phases based on DoC while Table III shows the list of Items, Links, Total link strength, Occurrence and Average publication year of every cluster.

IV. DATA EXTRACTION

Based on the search term used in the five (5) relevant online databases, the total of three hundred and sixteen (316) documents were retrieved. ScienceDirect has the highest number of retrieved documents of one hundred and eighty-nine (189) and the year 2020 with the highest number of published articles as presented in Table I.

TABLE I. ANALYSIS ON THE AVAILABLE JOURNALS IN THE DOMAIN OF OSNFIM

S.no	Name of online Database(s)	Total document retrieved	Categorization by Year of publication										
			2021	2020	2019	2018	2017	2016	2015	2014	2013	2012	2011
1	Scopus	30	2	3	6	2	6	3	2	3	1	0	2
2.	Web of Science	14	2	3	3	2	1	1	1	0	1	0	0
3.	IEEEExplore	12	0	1	2	2	1	3	1	0	0	0	2
4.	ScienceDirect	189	31	31	35	19	19	22	8	8	7	5	4
5.	Association for Computing Machinery (ACM) Digital Library	71	8	18	9	10	7	6	7	1	2	2	1
Summary		316	43	56	55	35	34	35	19	12	11	7	9

There are some duplicates among the 316 papers that have been retrieved. Scopus has retrieved a total of 31 documents, 12 of which are duplicates. ScienceDirect has three (3) articles, IEEEExplore has eight (8) articles, and Web of Science has one (1) article. The total number of documents retrieved from IEEEExplore is 21, although ten (10) of them are duplicates. In Scopus, there are eight (8) papers, while in Web of Science, there are two (2) papers. The total number of documents obtained by Web of Science is 14, although three (3) of them are duplicates. Two (2) in IEEEExplore and one (1) in Scopus. ScienceDirect has retrieved a total of 189 documents, three (3) of which are duplicates and all of which are in Scopus. There are 71 documents in the Association for Computing Machinery (ACM) Digital Library, but only one (1) is duplicated in Web of Science.

V. DISCUSSION

This section contains a detailed discussion in order to answer the research questions that have been posed:

RQ1. What are the available published articles in Scopus, Web of Science, IEEEExplore, ScienceDirect and Association for Computing Machinery (ACM) Digital Library in the domain of an Online Social Networks Forensic Investigation from 2011 to 2021?

The total of 316 subscribed documents were collected among which ScienceDirect has the total highest number with 189 documents and the year 2020 with the highest published journals as shown in Table I and Fig. 1 which both can relatively considered as less considering the importance of the domain even though it's young. Also, most of the documents retrieved are not related to the domain of interest while some are duplicates. But they were accessed due to the search term used will involves all documents having any of the word (online, social, network, forensic, investigation, model) appeared in it. After sorting the relevant/not relevant articles, it can be concluded that not up to 30% of the 316 documents retrieved were relevant to the domain of interest and twenty-nine (29) articles are duplicates as presented in Table II.

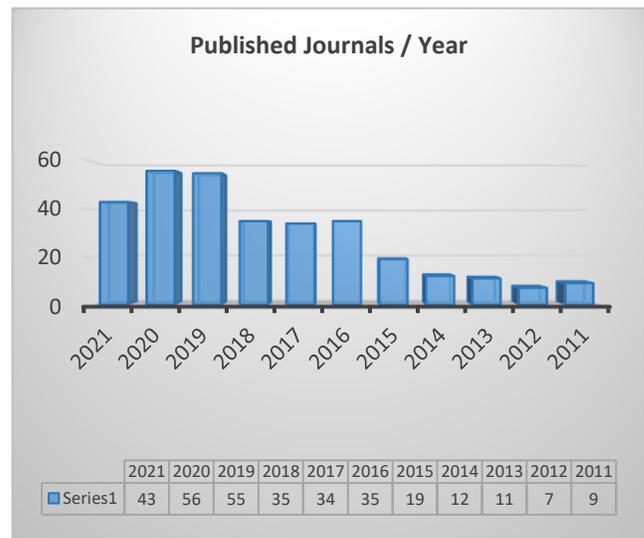


Fig. 1. Published Articles According to Year.

Therefore, more research has to be conducted and published in the domain of online social network forensic investigation (OSNFI) considering how technology is rapidly developing and crimes are increasing and becoming advanced day by day due to how people are becoming addicted to the use of social networking sites. This will help in creating awareness to the users and also help other researchers working in the domain.

TABLE II. EXTRACTION OF RELEVANT/NOT RELEVANT AND DUPLICATE DOCUMENTS

Name of Database	Total document retrieved	Relevant	Not Relevant	Total Duplicate
Scopus	30	7	23	12
IEEE	12	1	11	10
Web of Science	14	5	9	3
ScienceDirect	189	10	179	3
ACM	71	4	67	1
Summary	316	27	289	29

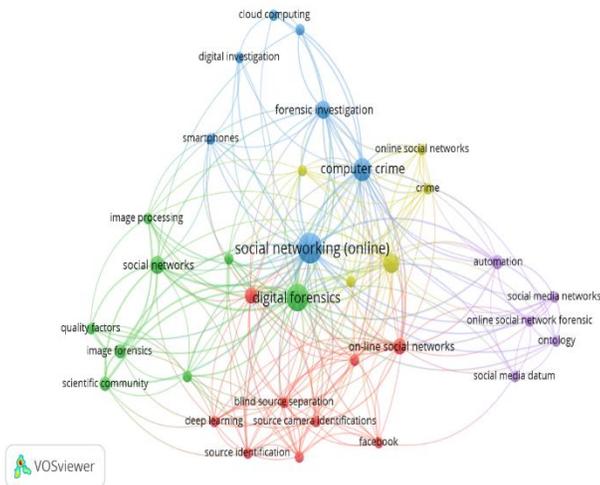


Fig. 2. Network Visualization of Available OSNFIM Documents on Scopus Database based on Bibliometric Analysis.

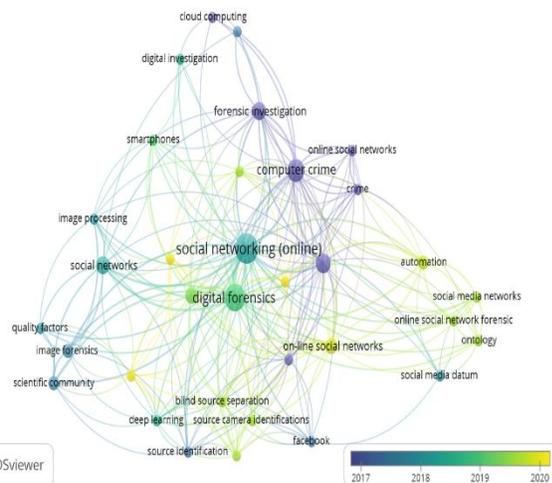


Fig. 3. Overlay Visualization of Available OSNFIM Documents on Scopus Database based on Bibliometric Analysis.

In 1926, Alfred Lotka introduced bibliometrics when he examined patterns of author output and presented the first criteria for bibliometrics [21]. Bibliometrics is a field of scientific inquiry that is gaining increasing interest from the scientific world and has swiftly grown and has been used to various academic domains. It is an excellent technique to retrieve, evaluate and statistically analyse quantifiable data in scholarly literature and also the merits of a certain topic area or a particular publication which can be used through its indicators to better reflect the evolution of a given research direction [22].

VOSviewer was used to conduct a co-occurrence analysis based on all keywords as the unit of analysis and Full counting method. The full counting technique indicates that each co-authorship, co-occurrence, bibliographical coupling, or co-citation link gets the same weight. The parameters were used in order to analyse the retrieved documents so as to have a clear perspective in the domain of OSNFIM as presented in Fig. 2,

Fig. 3 and Fig. 4. A total of thirty (30) documents were retrieved from the scopus online database after using the search term “[All: online] AND [All:social] AND [All:network] AND [All:forensic] AND [All:investigation] AND [All:model] AND [PublicationDate:(01/01/2011 TO 31/12/2021)]”. After conducting the analysis, thirty-four (34) item were generated based on five (5) clusters as in Table III.

The circles in Fig. 2 and Fig. 3 indicate the level of work which has been carried out and published in a specific area of research. It can clearly be seen that social networking (online) and digital forensics has the biggest circles based on the analysis. The domain of interest which is the online social network forensic investigation has one of the smallest circles even among its cluster. Therefore, this obviously indicates that not much work has been carried out in the domain even though it is considered young but very important.

RQ2. What are the phases and activities involved in an Online Social Networks Forensic Investigation Model Domain based on the Degree of Confidence?

Several models and frameworks have been proposed by [6]; [10]; [15]; [2]; [5]; [16]; [14]; [23]; [24]; [11]; [13]; [7]; [25]; and [17], but very few were designed with OSNFI in mind.

However [6]; and [10] proposed a digital forensic investigation model for online social networking and a digital forensic investigation model and its application design. Even though they tried in the automation of the entire process, there are some activities which requires manual handling which can decrease the dependability and credibility of evidence in criminal proceedings [10], added Iteration in all the investigation process and that can sometimes be very difficult tracing back at the source of the information collected [23]; [24]; [13]; [5] and [25], focused more on a particular platform or content rather than the entire OSN. Such platforms includes: WhatsApp, Cloud, Messenger, Imaging and Game.

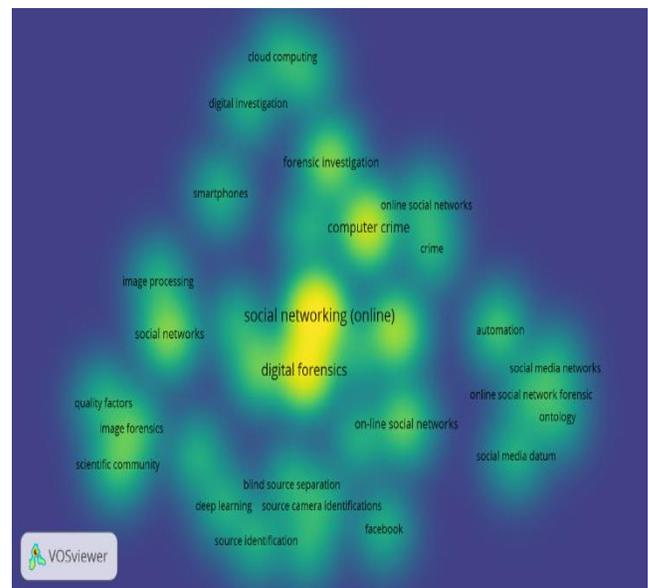


Fig. 4. Density Visualization of Available OSNFIM Documents on Scopus Database based on Bibliometric Analysis.

TABLE III. ITEMS, LINKS, TOTAL LINK STRENGTH, OCCURRENCE AND AVERAGE PUBLICATION YEAR

Item	Links	Total link strength	Occurrence	Avg. Pub. Year
Cluster 1				
Blind source separation	15	21	02	2019.50
Cameras	21	34	04	2019.25
Deep learning	17	19	02	2018.50
Facebook	13	14	02	2017.50
Information systems	15	18	02	2014.50
Online social networks	23	39	04	2019.75
Source camera identification	15	21	02	2019.50
Source camera identifications	15	21	02	2019.50
Source identification	15	17	02	2017.50
Cluster 2				
Digital forensic	21	81	11	2018.91
Image enhancement	14	16	02	2020.00
Image forensic	09	18	03	2017.67
Image processing	12	15	02	2018.00
Quality factor	08	13	02	2018.00
Scientific community	09	18	03	2017.67
Sensor pattern noise	15	18	02	2020.00
Social networks	17	32	05	2018.20
Cluster 3				
Cloud computing	05	06	02	2017.00
Computer crime	25	48	08	2016.62
Digital investigation	06	07	02	2018.50
Forensic investigation	18	33	05	2017.00
Smartphones	10	13	02	2019.00
Social networking (online)	33	92	14	2018.14
Social networking sites	06	08	02	2017.50
Cluster 4				
Crime	11	16	2	2015.50
Electronic crime countermeasures	25	46	6	2016.50
Iterative methods	15	19	2	2019.50
Online social networks	11	16	2	2015.50
Online social network (OSN)	16	19	2	2020.50
Cluster 5				
Automation	14	24	3	2019.67
Online social network forensic	9	14	2	2019.50
Ontology	9	14	2	2019.50
Social media datum	7	8	2	2018.00
Social media networks	9	14	2	2019.50
Summary: Items = 34, Cluster = 5, Links = 247 and Total Link Strength = 406				

One of the best OSN models were those presented by [18]; and [17]. They both proposed a semi-automated and automated

model for the domain of OSN. The author in [18] proposed a comprehensive digital forensic investigation process model that includes: acquisition and analysis of digital evidence. Iteration process is considered in their proposed model but the process is too common and non-specific. A digital forensic investigation process model for online social networks (FIMOSN) was presented by [17]. The model comprises of seven (7) phases and focused on automating the whole process activities. The model considered Iteration at a reasonable stage which is after analysis phase and before presentation but the evaluation process is entirely manual and this can slow the investigation process.

There are quite a number of models which recommend different phases and activities for the forensic investigation of online social networks. But for the purpose of coming up with a unified number and terms for this research, a total of five (5) models are randomly selected. According to [17], forensic investigation for online social networks consist of seven (7) phases; Pre-investigation, Incident specification, Extraction, Preservation, Analysis, Iteration and Presentation. [24] suggested six (6) phases; Identification, Preservation, Collection, Examination, Analysis and Presentation, [13] presented four (4) phases; Preparation, Incidence response, Laboratory process and Presentation, [6] recommended four (4) also; Preliminary, Investigation, Analysis and Evaluation. Therefore, the Degree of Confidence (DoC) is used to calculate the number of frequency of each term as demonstrated in Table IV and Fig. 5.

Degree of confidence is calculated by dividing the frequency of the number of times a phase appears in the models chosen by the total number of R1 models. The following is how DoC is calculated:

$$\text{Degree of Confidence} = \frac{\text{Frequency of Phase}}{\text{Total number of R1 models}} = n\% \quad (1)$$

Based on the Degree of Confidence (DoC), there are five (5) categories of phases well-defined and they are as follows:

- Very Strong (100 - 70%)
- Strong (69 - 50%)
- Moderate (49 - 30%)
- Mild (29 - 11%)
- Very Mild (10 - 0%)

After applying the DoC formula, it can be seen from Fig. 5 that, analysis and presentation phases has the Very Strong DoC of 100%.

$$\text{DoC (Analysis)} = \frac{5}{5} * 100 = 100\%$$

$$\text{DoC (Presentation)} = \frac{5}{5} * 100 = 100\%$$

Preservation phase has a Strong DoC of 60%

$$\text{DoC (Preservation)} = \frac{5}{5} * 100 = 60\%$$

TABLE IV. SELECTION OF OSNFIM DEVELOPMENT PHASES BASED ON DOC

S/No.	Phases	R1 Models					Frequency	DoC (%)
		[17]	[24]	[13]	[15]	[6]		
1.	Preliminary	✓	×	×	×	✓	2	40
2.	Preparation	×	×	✓	×	×	1	20
3.	Identification	×	✓	×	×	×	1	20
4.	Investigation	×	×	×	×	✓	2	20
5.	Incident Specification	✓	×	×	×	×	1	20
6.	Incidence Response	×	×	✓	×	×	1	20
7.	Acquisition	×	×	✓	✓	×	2	40
8.	Triage	×	×	×	✓	×	1	20
9.	Preservation	✓	✓	✓	×	×	3	60
10.	Collection	×	✓	×	×	×	1	20
11.	Examination	×	✓	×	×	×	1	20
12.	Analysis	✓	✓	✓	✓	✓	5	100
13.	Evaluation	×	×	×	×	✓	1	20
14.	Iteration	✓	×	×	×	×	1	10
15.	Presentation	✓	✓	✓	✓	✓	5	100

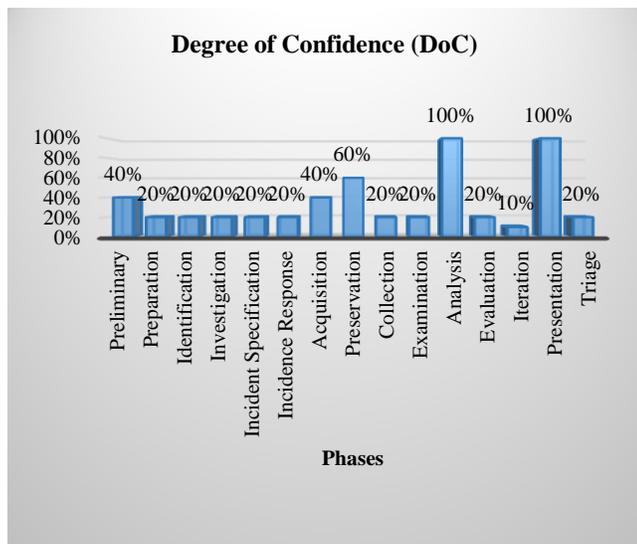


Fig. 5. OSNFIM Development Phases based on DoC.

Acquisition and Preliminary phases has moderate DoC of 40% each, Preparation, Identification, Investigation, Examination, Identification, Incident specification, Incident response and Collection phases has a Mild DoC of 20% while Iteration and Triage phases has a Very Mild DoC of 10%.

Any phase that is having the DoC as; Very Strong (100 - 70%), Strong (69 - 50%) or Moderate (49 - 30%) is selected while those with Mild (29 - 11%) or Very Mild (10 - 0%) were rejected. However, *iteration* phase was among the selected phases despite having the DoC of Very Mild (10%). It was selected because most of the previous models presented are adopting conventional practices; they are intended to offer guidance and a list of activities for human investigators. The method of automated investigation of OSNs is fundamentally iterative, investigators must continue to broaden the data collection process if the need arises [17]. Therefore, a total number of six (6) phases were selected and they are as follows:

- 1) *Preliminary*: This stage stresses two things: first, proper incident reporting, and second, formal authorization for investigation.
- 2) *Acquisition*: This is the procedure of obtaining information from any online social network.
- 3) *Preservation*: This is the secure keeping of property without altering or changing the content of data.
- 4) *Analysis*: This is the process of conducting an automated data sorting and filtering in order to obtain the most important data, which contains potential evidence.
- 5) *Iteration*: is a new round of data extraction with a wider scope.
- 6) *Presentation*: The investigators will choose relevant and appropriate evidence to present in court.

TABLE V. OSNFI PHASES AND THEIR ACTIVITIES

OSNFI Phases	Activities
Preliminary	<ul style="list-style-type: none"> ▪ Infrastructure readiness ▪ Incident notification ▪ Authorization ▪ Acknowledgment ▪ Construction ▪ Notification ▪ Survey
Acquisition	<ul style="list-style-type: none"> ▪ Identify Incident Parameters ▪ Identify Social Network sources ▪ Formulate PIEZ ▪ Initialize Parser ▪ Initiate Automated Extraction by using Parser ▪ Identification ▪ Searching ▪ Filtering ▪ Capturing ▪ Survey ▪ Transport ▪ Storage
Preservation	<ul style="list-style-type: none"> ▪ Preserve a forensic copy of Data Set
Analysis	<ul style="list-style-type: none"> ▪ Perform automated Analysis ▪ Sort and filter the data relevant to the inquiry ▪ Formulate hypotheses ▪ Examine the Data ▪ Test the Hypothesis ▪ Conclusion ▪ Reporting
Iteration	<ul style="list-style-type: none"> ▪ Formulate new hypotheses ▪ Identify the Involvement of new Entities ▪ Outline the Secondary Information Extraction Zone ▪ Repeat Steps
Presentation	<ul style="list-style-type: none"> ▪ Select Relevant Evidence ▪ Attach Suitable Metadata ▪ Add Visualizations ▪ Record Sequence of Steps ▪ Present the Evidence ▪ Conclusion ▪ Review ▪ Decision ▪ Interpretation ▪ Documentation ▪ Investigator ▪ CourtOfLaw

Therefore, because there is no any uniform method for conducting the investigation of an online social network crimes, these six (6) phases can be adopted in order to create a uniformity in the process of conducting the investigation.

Table V clearly defined the actions in each phase. A total of forty-three (43) activities were identified across the six (6) phases. These actions are regarded as the steps that must be completed in each phase in order to fulfill the investigation's goal.

VI. CONCLUSION

Due to the quick technology advancement, online social network forensic investigation is an essential young domain that requires considerable attention. Based on the findings of this study, it appears that, despite its importance and high demand, little work has been published in the field. Based on the search keyword, only 316 papers were obtained from five

(5) online databases (Scopus, Web of Science, IEEEExplore, ScienceDirect, and Association for Computing Machinery (ACM) Digital Library). After categorizing the articles into relevant and non-related categories, it was discovered that only about 30% of the 316 documents obtained were relevant to the topic of interest, with twenty-nine (29) being duplicates. This is an indication that more work has to be conducted in the domain of OSNFI. In addition, five (5) R1 models were utilised to identify the various phases and activities that can be used in the investigation of an online social network forensic crimes and based on the level of confidence, a total of six (6) phases and forty-three (43) activities were extracted (DoC).

REFERENCES

- [1] Pilli ES, Joshi RC, Niyogi R. Network forensic frameworks: Survey and research challenges. Digit. Investig. [Internet] 2010;7:14–27. Available from: <http://dx.doi.org/10.1016/j.diin.2010.02.003>.
- [2] Baca M, Cosic J, Cosic Z. Forensic analysis of social networks (case study). Proc. Int. Conf. Inf. Technol. Interfaces, ITI 2013;219–23.
- [3] Cohen F. Journal of Digital Forensics , Security and Law Column : Putting the Science in Digital Forensics. 2011;6.
- [4] Kohn MD, Eloff MM, Eloff JHP. Integrated digital forensic process model. Comput. Secur. [Internet] 2013;38:103–15. Available from: <http://dx.doi.org/10.1016/j.cose.2013.05.001>.
- [5] Kale S, Sahu PA. Forensic Imaging for Online Social Networks. 2014;3:166–70.
- [6] Zainudin, M N, Merabti, Madjid, Llewellyn-jones, David. A Digital Forensic Investigation Model for Online Social Networking. 2010;1–6.
- [7] Lu R, Li L. Research on forensic model of online social network. 2019 IEEE 4th Int. Conf. Cloud Comput. Big Data Anal. ICCCBDA 2019 2019;116–9.
- [8] Arshad H, Jantan A, Hoon GK, Butt AS. A multilayered semantic framework for integrated forensic acquisition on social media. Digit. Investig. [Internet] 2019;29:147–58. Available from: <https://doi.org/10.1016/j.diin.2019.04.002>.
- [9] Chang C-P. Knowledge Production from Social Network Sites - Using Social Media Evidence in the Criminal Procedure (Title of the Thesis) Knowledge Production from Social Network Sites - Using Social Media Evidence in the Criminal Procedure. 2014.
- [10] Mohd Zainudin N, Merabti M, Llewellyn-Jones D. Online social networks as supporting evidence: A digital forensic investigation model and its application design. 2011 Int. Conf. Res. Innov. Inf. Syst. ICRIIS'11 2011.
- [11] Montasari R. Digital Forensic Investigation of Social Media , Acquisition and Analysis of Digital Evidence. 2019;2:52–60.
- [12] Kleinberg JM. Challenges in mining social network data. 2007;13:4–5.
- [13] Rahman D, Rahadhian, Riadi I. Framework Analysis of IDFIF V2 in WhatsApp InvestigationProcess on Android Smartphones. Int. J. Cyber-Security Digit. Forensics 2019;8:213–22.
- [14] Jang YJ, Kwak J. Digital forensics investigation methodology applicable for social network services. Multimed. Tools Appl. 2015;74:5029–40.
- [15] Haggerty J, Casson MC, Haggerty S, Taylor MJ. A framework for the forensic analysis of user interaction with social media. Int. J. Digit. Crime Forensics 2012;4:15–30.
- [16] Abdalla A, Yayilgan SY. A Review of Using Online Social Networks. 2014;8531:3–12.
- [17] Arshad H, Omlara E, Oludare I, Aminu A. Computers & Security A semi-automated forensic investigation model for online social networks. Comput. Secur. [Internet] 2020;97:101946. Available from: <https://doi.org/10.1016/j.cose.2020.101946>.
- [18] Montasari R. A comprehensive digital forensic investigation process model Reza Montasari. 2016;8:285–302.
- [19] Valjarevic A, Venter HS. A Comprehensive and Harmonized Digital Forensic Investigation Process Model. J. Forensic Sci. 2015;60:1467–83.
- [20] Kitchenham B, Pearl Brereton O, Budgen D, Turner M, Bailey J,

- Linkman S. Systematic literature reviews in software engineering - A systematic literature review. *Inf. Softw. Technol.* [Internet] 2009;51:7–15. Available from: <http://dx.doi.org/10.1016/j.infsof.2008.09.009>.
- [21] Ahmad P, Asif JA, Alam MK, Slots J. A bibliometric analysis of Periodontology 2000. *Periodontol.* 2000 2020;82:286–97.
- [22] Wang X, Xu Z, Škare M. A bibliometric analysis of Economic Research-Ekonomiska Istraživanja (2007–2019). *Econ. Res. Istraz.* [Internet] 2020;33:865–86. Available from: <https://doi.org/10.1080/1331677X.2020.1737558>.
- [23] Chen L, Xu L, Yuan X, Shashidhar N. Digital Forensics in social networks and the cloud. 2015;1132–6. Available from: <https://doi.org/10.1109/ICCNC.2015.7069509>.
- [24] Anwar N, ImamRiadi. Forensic Investigation Analysis of WhatsAppMessenger Smartphone Against WhatsApp Messenger Smartphone Forensic Investigation Analysis Against Web-Based WhatsApp. 2017;3:1–10.
- [25] Taylor DCPJ, Mwiki H, Dehghantanha A, Akibini A, Kwang K, Choo R, et al. Science & Justice Forensic investigation of cross platform massively multiplayer online games : Minecraft as a case study. *Sci. Justice* [Internet] 2019;59:337–48. Available from: <https://doi.org/10.1016/j.scijus.2019.01.005>.

Deep Learning based Neck Models for Object Detection: A Review and a Benchmarking Study

Sara Bouraya, Abdessamad Belangour
Laboratory of Information Technology and Modeling
Hassan II University, Faculty of Sciences Ben M'sik
Casablanca, Morocco

Abstract—Artificial intelligence is the science of enabling computers to act without being further programmed. Particularly, computer vision is one of its innovative fields that manages how computers acquire comprehension from videos and images. In the previous decades, computer vision has been involved in many fields such as self-driving cars, efficient information retrieval, effective surveillance, and a better understanding of human behaviour. Based on deep neural networks, object detection is actively growing for pushing the limits of detection accuracy and speed. Object Detection aims to locate each object instance and assign a class to it in an image or a video sequence. Object detectors are usually provided with a backbone network designed for feature extractors, a neck model for feature aggregation, and finally a head for prediction. Neck models, which are the purpose of study in this paper, are neural networks used to make a fusion between high-level features and low-level features and are known by their efficiency in object detection. The aim of this study to present a review of neck models together before making a benchmarking that would help researchers and scientists use it as a guideline for their works.

Keywords—Object detection; deep learning; computer vision; neck models; feature aggregation; feature fusion

I. INTRODUCTION

Object detection is often called image detection, object identification, and object recognition; and all these concepts are synonymous. It is a computer vision method for locating instances of objects in an image or video sequence. Object detection algorithms, therefore, typically benefit from machine learning techniques or deep learning techniques to gain meaningful results. When humans look at images or videos, they could locate and recognize objects of interest easily. The goal of object detection is to mimic this intelligence using a computer. With recent advancements in Deep Learning-based computer vision models, Object Detection use cases are spreading more than ever before. A wide range of applications is implemented, for instance, self-driving cars, object tracking, anomaly detection, and video surveillance.

Object Detection could be divided into two main categories Deep Learning-based techniques and Machine Learning based techniques. Deep Learning based techniques could be separated into two approaches one stage detectors and two-stage detectors. Object Detection based Deep

Learning approaches are a set of models of Deep Learning, starting from input, then a backbone for feature extraction model, then neck model for feature fusion, and finally a head model class/box network.

The neck of the object detector refers to the additional layers existing between the backbone [1] and the head. Their role is to collect feature maps from different stages. The neck models are composed of several top-down paths and several bottom-up paths. The idea behind this feature aggregation existing in this model is to allow low-level features to interact more directly with high-level features, by mixing information from this high-level feature with the low-level feature. They reach aggregation and feature interaction across many layers, since the distance between the two feature maps is large. Several methods can reach be implemented in this part, for example, PAN [2] or FPN [3] (see Fig. 1).

Head is the last model of object detection, predicts bounding boxes and classes of objects and could be a sparse prediction that belongs to One-stage detectors such as YOLO [4], SDD [5], CenterNet [6], or a Dense prediction that belongs to Two-stage detectors, such as Fast R-CNN [7], Faster R-CNN [8], Mask R-CNN [9] (see Fig. 1). On the one hand, One Stage detectors have high inference speeds, these models predict bounding boxes in a one or single step without using region proposals. On the other hand, two stage detectors have high localization and recognition accuracy. Firstly, they use a Region Proposal Network to generate regions of interests; secondly, they send the region proposals for object classification and bounding-box regression.

We aim that our benchmarking study can provide a timely comparison of neck models of object detection for practitioners and researchers to further master research on object detection models. The rest of our study is organized as follows: In Section 2, we are going to discuss the different existing related works about feature aggregation. In Section 3, we list the neck neural networks about object detection used for feature fusion, their architecture is discussed also in their categories. In Section 4, our comparative study is presented. In Section 5, we highlight the different recognizable results and Section 6 covers the discussion. Finally, in Section 7, we conclude and discuss future directions.

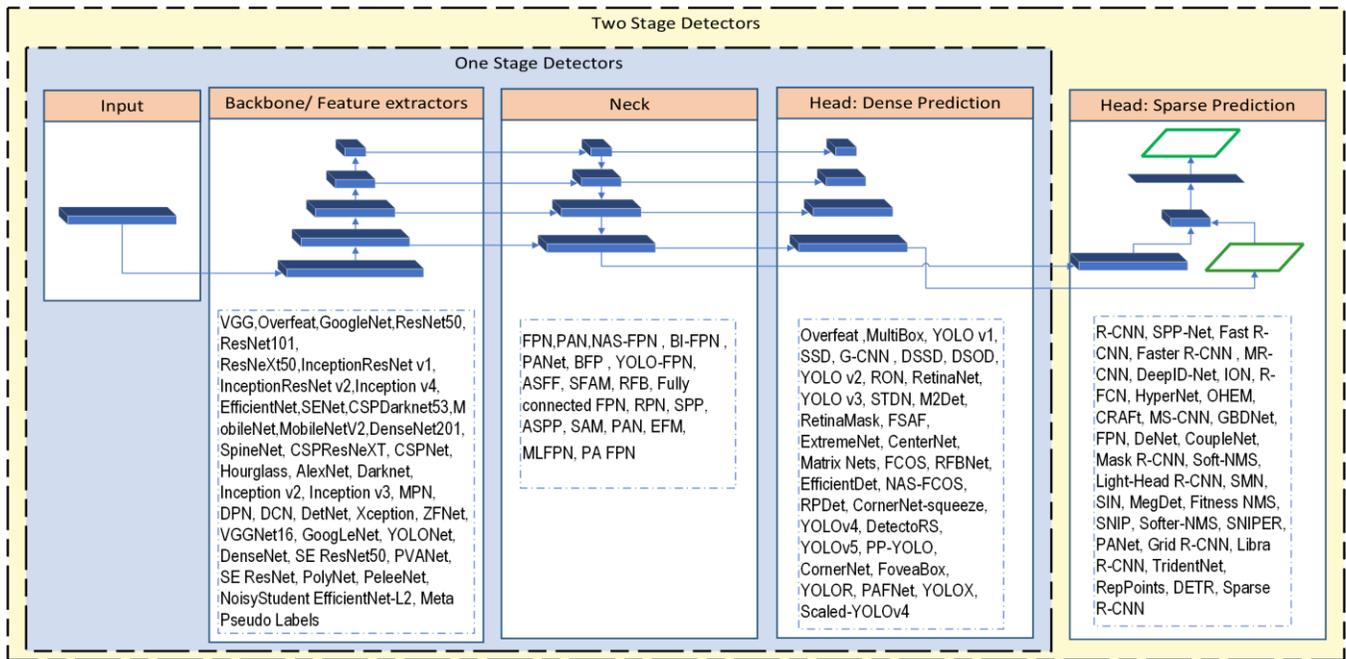


Fig. 1. Models' Taxonomy of Object Detectors in each Part Backbone, Head, and Neck.

II. RELATED WORK

Several scientific works and researches have been implemented to develop and evolve Object Detection applications and systems and depend on enormous methodologies of the deep learning era, machine learning era and other eras. Several researchers and scientists are expanding their implementation and research to develop and apply enormous methodologies. Such as the case of feature aggregation methods that are used to make a connection between low and high feature for better object recognition in video sequence and images. Feature aggregation is used widely in action recognition [10], [11], [12], [13], [14] and video description [15],[16]. Most of these methods use recurrent neural network (RNNs) in order to aggregate features from consecutive frames on the one hand. Exhaustive temporal-spatial convolution is used to extract temporal-spatial features, on the other hand. U-Net [17] was proposed to concatenate features from low level to high-level for medical image segmentation, and it achieved great success in that field. In order to gain an outstanding feature for object detection, the FPN stands for Feature Pyramid Networks aggregated both the transformed feature from the bottom-up weighted pyramid and the top-down lateral convolutions through a simple sum operation. Relied on Feature Pyramid Networks, several extensive works [18], [19], [20], [2] define new options on connectivity between scales. Attention based models also prove their efficiency in several applications of deep learning era [21], [22], [23], [24], [25], [26]. Self-attention models by measuring and applying a context-relied encoding summarized from a dimension of feature. All these works cited propose to aggregate and fuse features via element-wise concatenation or summation.

III. BACKGROUND

Since Feature Pyramid Networks appearance, the focus of this work is the object detector neck, the existing part between the backbone and the head. These techniques are useful for many reasons.

1) *Aggregation network models (FPN)*: FPN [3] is a top-down architecture with lateral connections, it is implemented in building high-level semantic feature maps at all scales (see Fig. 2).

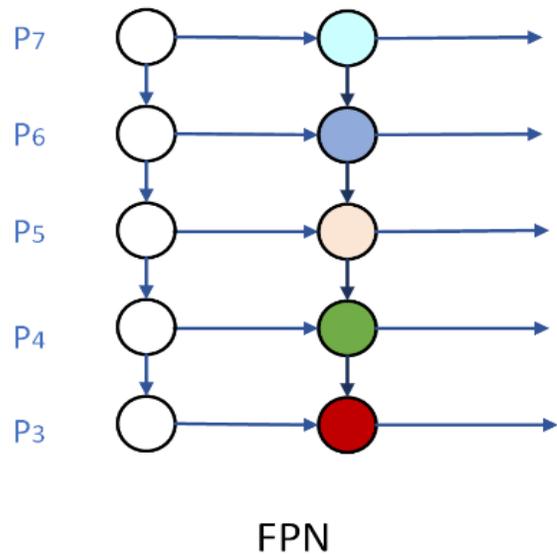


Fig. 2. FPN Architecture.

2) *Neural architecture search FPN (NAS-FPN)*: NAS-FPN [19] consists of a combination of top-down and bottom-up connections to fuse features across scales (see Fig. 3).

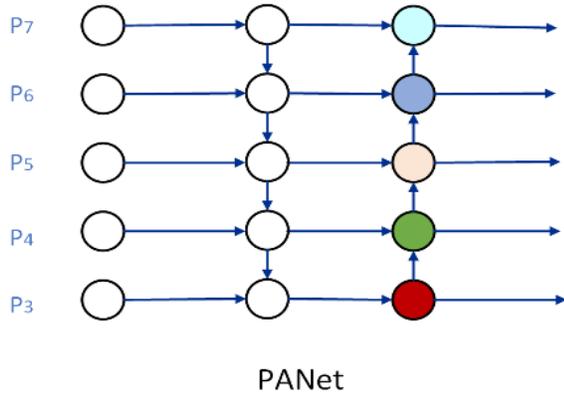


Fig. 3. PANet Architecture.

3) *Neural architecture search FPN (NAS-FPN)*: NAS-FPN [19] consists of a combination of top-down and bottom-up connections to fuse features across scales (see Fig. 4).

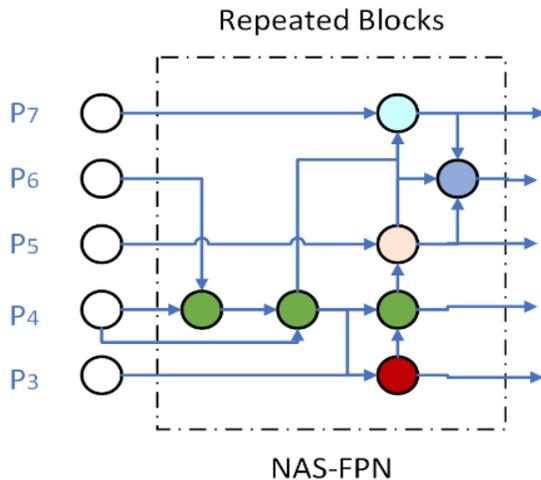


Fig. 4. NAS-FPN Architecture.

4) *Bi-directional feature pyramid network (BiFPN)*: BiFPN [27] is a type of feature pyramid network that allows fast and easy multi-scale feature fusion. BiFPN incorporates the other feature fusion models. It enables information to flow in the top-down and bottom-up directions, while using efficient and regular connections. This network improves the connections by removing some nodes and treats each bidirectional path as a feature network layer (Fig. 5).

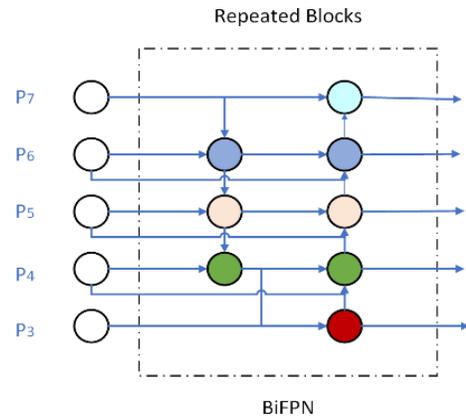


Fig. 5. BiFPN Architecture.

Based on the architecture above PANET is more performant then FPN et NAS-FPN, but the computation cost is higher.

5) *Fully-connected FPN*: Fully-connected, the calculation is the most complex all scales use the most complete connection (see Fig. 6).

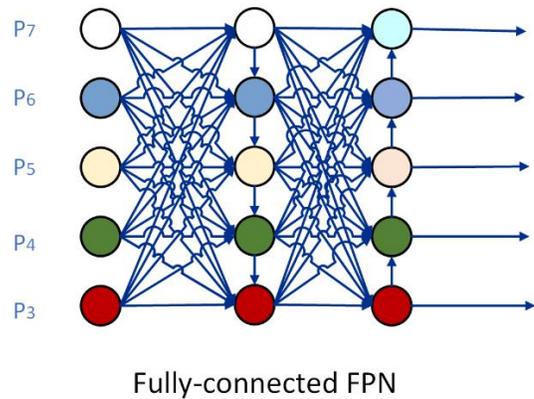


Fig. 6. Fully-Connected FPN Architecture.

6) *Simplified PANet*: Simplified PANet, this method simplifies and removes only one input node (see Fig. 7).

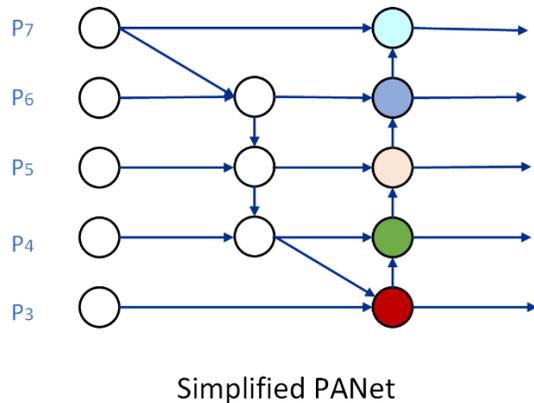


Fig. 7. Simplified FPN Architecture.

IV. COMPARISON

Table I below illustrates the models that we are going to compare based on different comparison metrics. The measures are gathered carefully to cover several methods.

This table illustrates the deep learning models used for the object detection task of the COCO dataset. It defines the used models for the prediction for classification and bounding

boxes. The Backbone determines the backbone used for feature extraction the number associated refers to the number of layers, and finally, the neck illustrates the feature aggregation network used.

Table I contains the model's name, Reference, Journal year, Year, Backbone, Neck, AP, AP₅₀, AP₇₅, AP_S, AP_M, AP_L (see Table I).

TABLE I. DETAILED COMPARISONS ON MULTIPLE POPULAR BASELINE OBJECT DETECTORS ON THE COCO DATASET

Model Ref	Journal	Model	Backbone	Neck	AP	AP ₅₀	AP ₇₅	AP _S	AP _M	AP _L
[18]	CVPR 2019	Libra R-CNN	ResNet-50	FPN	38.7	59.9	42.0	22.5	41.1	48.7
		Libra R-CNN	ResNet-101	FPN	40.3	61.3	43.9	22.9	43.1	51.0
		Libra R-CNN	ResNeXt-101	FPN	43.0	64	47	25.3	45.6	54.6
[8]		Faster R-CNN	ResNet-50	FPN	37.8	58.7	40.6	21.3	41.0	49.5
		Faster R-CNN	ResNet-50	AdaFPN	39.0	58.8	41.8	22.6	42.3	50.0
		Faster R-CNN	ResNet-50	AugFPN	38.8	61.5	42.0	23.3	42.1	47.7
		Faster R-CNN	ResNet-101	AugFPN	41.5	63.9	45.1	23.8	44.7	52.8
		Faster R-CNN	ResNext-101- 32x4d	AugFPN	41.9	64.4	45.6	25.2	45.4	52.6
		Faster R-CNN	ResNext-101-64x4d	AugFPN	43.0	65.6	46.9	26.2	46.5	53.9
		Faster R-CNN	MobileNet-v2	AugFPN	34.2	56.6	36.2	19.6	36.4	43.1
[28]	ICCV 2019	FCOS	ResNet-50	AugFPN	37.9	58.0	40.4	21.2	40.5	47.9
		FCOS	ResNet-50	FPN	39.1	57.9	42.1	23.3	43.0	50.2
		FCOS	ResNet-50	AdaFPN	40.1	58.6	43.2	24.1	43.6	50.6
		FCOS	ResNeXt-101	FPN	42.7	62.2	46.1	26.0	45.6	52.6
[9]	ICCV 2017	Mask R-CNN	ResNet-101	FPN	38.2	60.3	41.7	20.1	41.1	50.2
		Mask R-CNN	ResNeXt-101	FPN	39.8	62.3	43.4	22.1	43.2	51.2
		Mask R-CNN	ResNet-50	AugFPN	39.5	61.8	42.9	23.4	42.7	49.1
		Mask R-CNN	ResNet-101	AugFPN	42.4	64.4	46.3	24.6	45.7	54.0
		Mask R-CNN	ResNet-50	A ² -FPN	36.6	59.3	39.1	19.8	39.3	48.0
		Mask R-CNN	ResNet-101	A ² -FPN	37.9	60.8	40.5	20.6	41.8	50.1
[29]	CVPR 2018	CascadeR-CNN	ResNet-50	FPN	36.5	59	39.2	20.3	38.8	46.4
		CascadeR-CNN	ResNet-101	FPN	38.8	61.1	41.9	21.3	41.8	49.8
		CascadeR-CNN	ResNet-101	AC-FPN	45.0	64.4	49.0	26.9	47.7	56.6
[30]	ICCV 2017	RetinaNet	ResNet-101	FPN	39.1	59.1	42.3	21.8	42.7	50.2
		RetinaNet	ResNeXt-101	FPN	40.8	61.1	44.1	24.1	44.2	51.2
		RetinaNet	ResNet-50	AugFPN	37.5	58.4	40.1	21.3	40.5	47.3
		RetinaNet	MobileNet-v2	AugFPN	34.0	54.0	36.0	18.6	36.0	44.0
[31]	arXiv 2019	RetinaMask	ResNet-50	FPN	39.4	58.6	42.3	21.9	42.0	51.0
[32]	CVPR 2019	Grid R-CNN	ResNeXt-101	FPN	43.2	63.0	46.6	25.1	46.5	55.2
[33]	CVPR 2019	HTC	ResNeXt-101	FPN	47.1	63.9	44.7	22.8	43.9	54.6
		HTC	ResNet-50	FPN	38.4	60.0	41.5	20.4	40.7	51.2
		HTC	ResNet-101	FPN	39.7	61.8	43.1	21.0	42.2	53.5
		HTC	ResNet-50	A ² -FPN	39.8	62.3	43.0	21.6	42.4	52.8
		HTC	ResNet-101	A ² -FPN	40.8	63.6	44.1	22.3	43.5	54.4
		HTC	ResNeXt -101	A ² -FPN	42.1	65.3	45.7	23.6	44.8	56.0
[34]	CVPR 2020	DetectRS	ResNeXt-101-DCN	RFP	53.3	71.6	58.5	33.9	56.5	66.9
[35]	arXiv 2021	CenterNet2	Res2Net-101-DCN	BiFPN	56.4	74.0	61.6	38.7	59.7	68.6

Average Precision (AP)

AP % AP at IoU=.50:.05:.95

AP_{IoU=.50} % AP at IoU=.50

AP_{IoU=.75} % AP at IoU=.75

AP Across Scales:

AP_{small} % AP for small objects: area < 322

AP_{medium} AP for medium objects: 322 < area < 962

AP_{large} AP for large objects: area >962

V. RESULT

In this part, we are going to discuss the performance of different methods cited in Table I Libra R-CNN, Faster R-CNN, FCOS, Mask R-CNN, Cascade R-CNN, RetinaNet, RetinaMask, Grid R-CNN, HTC, DetectRS, CenterNet2 methods based on different feature aggregation networks and different backbone networks. In each model, we tried to fix either a backbone or a neck and see how the performance behave. These results show us the importance of both feature aggregation networks and feature extraction networks and how they impact the object detection models accuracy.

1) *Libra R-CNN*: We have compared Libra R-CNN [18] with different backbones. This comparison reveals that the act of changing backbones with a solid feature aggregation model changes the performance. Regarding, Libra R-CNN with ResNeXt-101 as a backbone on top of the quality range. The two last models based on ResNet-50 and ResNet-101 as backbones, Libra R-CNN based ResNet-101 gain the highest performance (see Fig. 8).

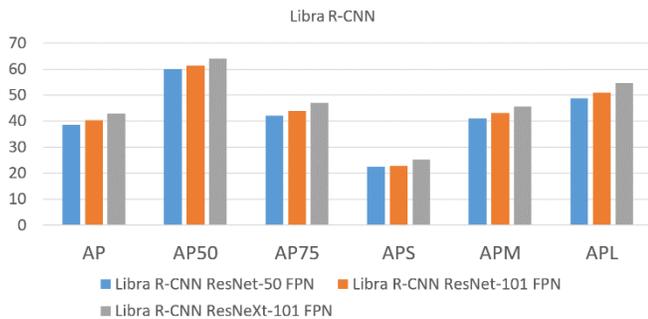


Fig. 8. Libra R-CNN Comparison based Different Feature Aggregation Models.

2) *Faster R-CNN*: Faster R-CNN [8] relying on ResNext-101-64x4d as a backbone and AugFPN as a feature aggregation model are leading the performance in this category. By fixing ResNet-50 as a backbone with changing different feature aggregation, the model based on AdaFPN gains the highest performance. Moreover, by fixing AugFPN and changing ResNext-101 the best performance was gained by ResNext-101-64x4d (see Fig. 9).

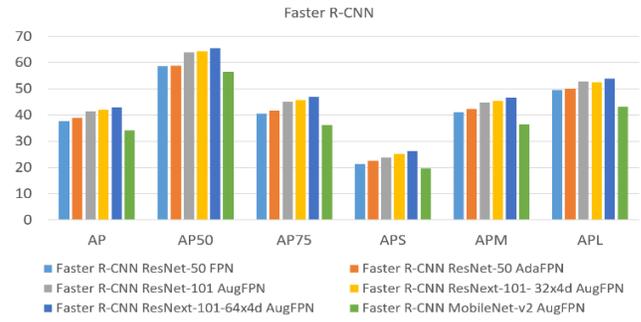


Fig. 9. Faster R-CNN Comparison based Different Feature Aggregation Models.

3) *FCOS*: The highest performance was obtained by FCOS [28] on the head, ResNext-101 as a backbone, and FPN as a feature aggregator model. By changing feature aggregation models FPN, AdaFPN, and AugFPN, moreover fixing ResNet-50 the AdaFPN gains the best performance in this category, after that FPN and finally AugFPN (see Fig. 10).

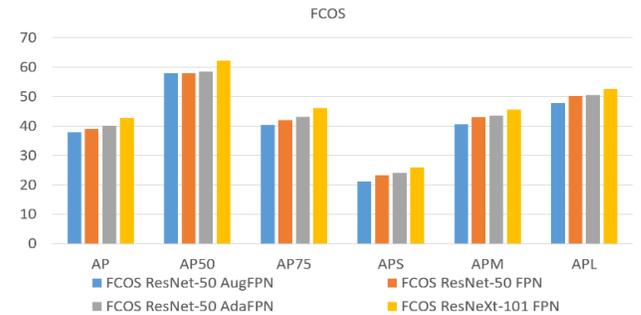


Fig. 10. FCOS Comparison based Different Feature Aggregation Models.

4) *Mask R-CNN*: Regarding Mask R-CNN [9] models based on a diversity of backbones and necks relied on our category, ResNet-101 and FPN combination leads the performance then, ResNeXt-101 and FPN. By fixing ResNet-101, mutating feature aggregation models the highest performance was gained by AugFPN, then FPN, and finally A2FPN. Concerning ResNet-50 as a backbone and A2 FPN or AugFPN as feature aggregation models, AugFPN attain the greatest performance (see Fig. 11).

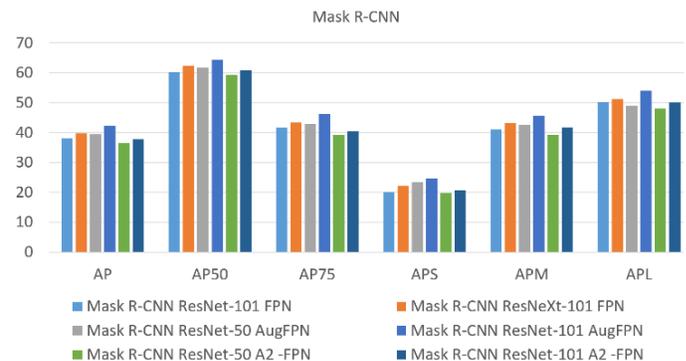


Fig. 11. Mask R-CNN Comparison based Different Feature Aggregation Models.

5) *HTC*: Related to HTC [33] model, ResNeXt-101 and A2FPN are leading in performance, the second performant fusion is ResNeXt-101 and FPN. Regarding the models based on ResNet as a backbone, ResNet-50 with A2FPN works better than ResNet-50 with FPN in terms of performance (see Fig. 12).

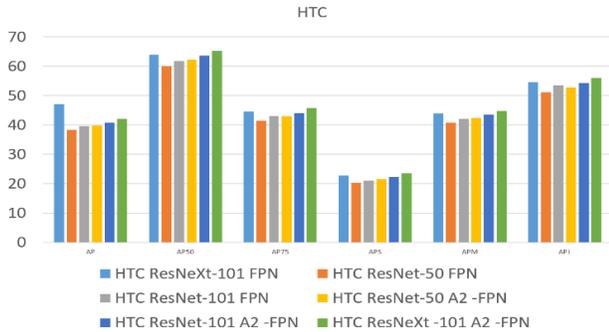


Fig. 12. HTC Comparison based Different Feature Aggregation Models.

6) *Cascade R-CNN*: Cascade R-CNN [29] performance was led by merging ResNet-101 and AC-FPN. The combination of ResNet-101 as a backbone and FPN neck has gained less performance (see Fig. 13).

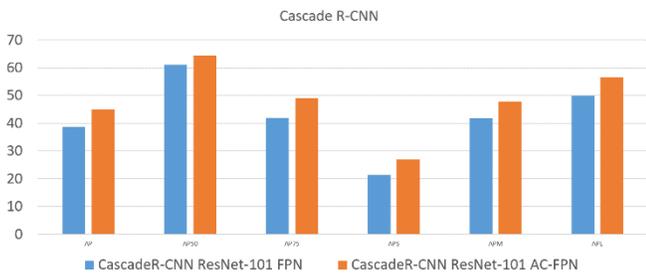


Fig. 13. Cascade R-CNN Comparison based Different Feature Aggregation Models.

7) *RetinaNet*: Regarding RetinaNet,[30] firstly, ResNeXt-101 as a backbone and FPN as a feature aggregation model compared to the other fusions, it has gained the highest performance; secondly, by merging ResNet-101 and FPN; and thirdly, ResNet-50 with AugFPN gains the performance, and finally, MobileNet-V2 with AugFPN (see Fig. 14).

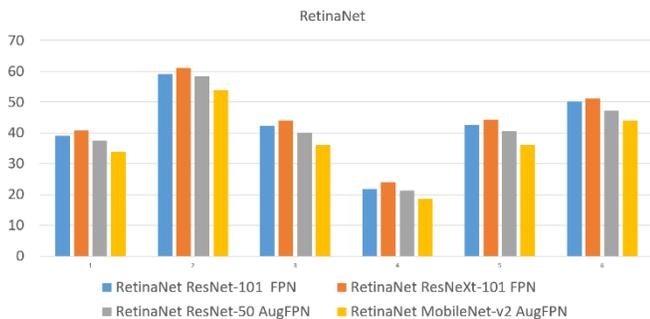


Fig. 14. RetinaNet Comparison based Different Feature Aggregation Models.

8) *Six Top average precision*: On the one hand, after extracting the 6 best models in terms of average precision, we

have preferred to compare the methods that gain the top average precision. On the other hand, in terms of performance and based on our spider, centerNet2 achieves the best performance. The best method is based on Res2Net101-DCN as a backbone and BiFPN as a feature aggregation model. The second rank is for DetectRS based on ResNeXt-101-DCN as a backbone and RFP as feature extraction (see Fig. 15).

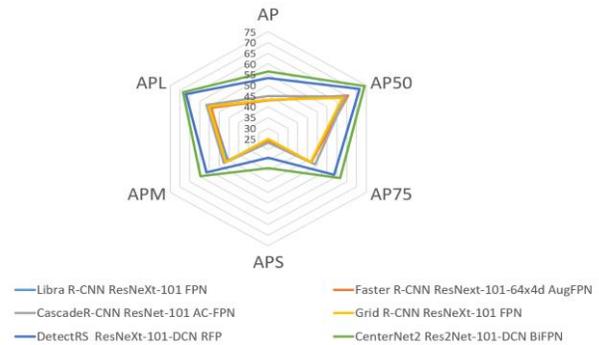


Fig. 15. Multicriteria Comparison based Different Feature Aggregation Models.

VI. DISCUSSION

In this paper, we have systematically depicted the importance of object detection components, covering the deep learning methodologies used in object detection, including, Two Stage detectors and one stage detectors.

Firstly, we have started by presenting object detection methodologies that have been categorized on traditional methods and based deep learning methodologies. Secondly, we have talked about the main arrangement of object detection based on deep learning that includes a backbone usually pretrained used to extract feature then feature aggregation model for merging high and low features called neck and finally, the head used for prediction.

Relied on our comparative study, we notice that the CenterNet2 with Res2Net-101-DCN as a backbone and BiFPN as a feature fusion model leads the performance and gains widespread dominance because of its supremacy regarding all criteria.

DetectRS with ResNeXt-101-DCN as a backbone and RFP as a feature fusion model is reaching the second score. HTC is gaining the third position with its high performance based on ResNeXt-101 as a backbone and FPN. We notice also that there is no intersection between all the compared algorithms, each algorithm gains its performance regarding all criteria that the underlying algorithm.

This comparison has also been made based on a set of criteria. The scores for each method evaluated were calculated using the Weight Score Model. Various scores or results have not only helped us determine an overall ranking, but they have also shown their internal strengths and weaknesses concerning each criterion.

This comparison has also revealed the importance of making a benchmark in order to have a global straightforward view of building efficient models with high performance.

One the one hand, we hold in mind that from this review and comparison study that object detection based deep learning models, backbone, neck and head, impacting highly the performance. On the other hand, generally, more used layers give high performance.

VII. CONCLUSION

From the study handed, it has been noticed that several scientists and researchers from a diversity of ethnicities are working day after day on the object detection field, due to its utmost importance. Several models are appearing every month with the growth of deep learning.

This comparison could be used as a support, by handing researchers a scientific comparison of different object detection methodologies and their main models, in order to build performant models.

A comparison of neck used for feature aggregation between high and low features has been presented. We have been interested in giving you different necks and analyse the performance of their global models.

Future work will be focusing on the implementation of some of the different models of object detection-based deep learning. We aim to implement, test, and analyze the results.

REFERENCES

- [1] S. Bouraya and A. Belangour, "Object Detectors" Convolutional Neural Networks backbones : a review and a comparative study," vol. 9, no. 11, pp. 1379–1386, 2021.
- [2] S. Liu, L. Qi, H. Qin, J. Shi, and J. Jia, "Path Aggregation Network for Instance Segmentation," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., pp. 8759–8768, 2018, doi: 10.1109/CVPR.2018.00913.
- [3] T. Y. Lin, P. Dollár, R. Girshick, K. He, B. Hariharan, and S. Belongie, "Feature pyramid networks for object detection," Proc. - 30th IEEE Conf. Comput. Vis. Pattern Recognition, CVPR 2017, vol. 2017-Janua, pp. 936–944, 2017, doi: 10.1109/CVPR.2017.106.
- [4] 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, doi: 10.1109/CVPR.2016.91.
- [5] W. Liu et al., "SSD: Single shot multibox detector," Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 9905 LNCS, pp. 21–37, 2016, doi: 10.1007/978-3-319-46448-0_2.
- [6] K. Duan, S. Bai, L. Xie, H. Qi, Q. Huang, and Q. Tian, "CenterNet: Keypoint triplets for object detection," Proc. IEEE Int. Conf. Comput. Vis., vol. 2019-October, pp. 6568–6577, 2019, doi: 10.1109/ICCV.2019.00667.
- [7] R. Girshick, "Fast R-CNN," Proc. IEEE Int. Conf. Comput. Vis., vol. 2015 Inter, pp. 1440–1448, 2015, doi: 10.1109/ICCV.2015.169.
- [8] S. Ren, K. He, and R. Girshick, "Faster R-CNN: Towards Real-Time Object Detection with Region Proposal Networks," pp. 1–9.
- [9] K. He, G. Gkioxari, P. Dollár, and R. Girshick, "Mask R-CNN," IEEE Trans. Pattern Anal. Mach. Intell., vol. 42, no. 2, pp. 386–397, 2020, doi: 10.1109/TPAMI.2018.2844175.
- [10] S. Sharma, R. Kiros, and R. Salakhutdinov, "Action Recognition using Visual Attention," pp. 1–11, 2015, [Online]. Available: <http://arxiv.org/abs/1511.04119>.
- [11] A. Kar, N. Rai, K. Sikka, and G. Sharma, "AdaScan: Adaptive scan pooling in deep convolutional neural networks for human action recognition in videos," Proc. - 30th IEEE Conf. Comput. Vis. Pattern Recognition, CVPR 2017, vol. 2017-January, pp. 5699–5708, 2017, doi: 10.1109/CVPR.2017.604.
- [12] Z. Li, K. Gavriluyk, E. Gavves, M. Jain, and C. G. M. Snoek, "VideoLSTM convolves, attends and flows for action recognition," Comput. Vis. Image Underst., vol. 166, pp. 41–50, 2018, doi: 10.1016/j.cviu.2017.10.011.
- [13] N. Ballas, L. Yao, C. Pal, A. Courville, and R. Convolution, "D ELVING D EEPER INTO C ONVOLUTIONAL N ETWORKS," pp. 1–11, 2016.
- [14] A. Karpathy and T. Leung, "Large-scale Video Classification with Convolutional Neural Networks."
- [15] J. Donahue, "Long-term Recurrent Convolutional Networks for Visual Recognition and Description," 2014.
- [16] N. Ballas, H. Larochelle, and A. Courville, "Describing Videos by Exploiting Temporal Structure," pp. 4507–4515, 2015.
- [17] O. Ronneberger, P. Fischer, and T. Brox, "U-Net: Convolutional Networks for Biomedical Image Segmentation," pp. 1–8.
- [18] J. Pang, K. Chen, J. Shi, H. Feng, W. Ouyang, and D. Lin, "Libra R-CNN: Towards balanced learning for object detection," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2019-June, no. 2, pp. 821–830, 2019, doi: 10.1109/CVPR.2019.00091.
- [19] G. Ghiasi, T. Y. Lin, and Q. V. Le, "NAS-FPN: Learning scalable feature pyramid architecture for object detection," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2019-June, pp. 7029–7038, 2019, doi: 10.1109/CVPR.2019.00720.
- [20] N. Wang et al., "NAS-FCOS: Fast Neural Architecture Search for Object Detection," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., pp. 11940–11948, 2020, doi: 10.1109/CVPR42600.2020.01196.
- [21] F. Chollet, "Xception: Deep Learning with Depthwise Separable Convolutions," CVPR, vol. 7, no. 3, pp. 1251–1258, 2014, doi: 10.4271/2014-01-0975.
- [22] A. Vaswani et al., "Attention is all you need," Adv. Neural Inf. Process. Syst., vol. 2017-Decem, no. Nips, pp. 5999–6009, 2017.
- [23] X. Wang and R. Girshick, "Non-local Neural Networks."
- [24] Y. Chen, "A 2 -Nets : Double Attention Networks," no. NeurIPS, 2018.
- [25] H. L. Fu Jun, Jing Liu, Haijie Tian, Yong Li, Yongjun Bao, Zhiwei Fang, "Dual Attention Network for Scene Segmentation."
- [26] Y. Chen, M. Rohrbach, Z. Yan, S. Yan, J. Feng, and Y. Kalantidis, "Graph-Based Global Reasoning Networks," vol. 1.
- [27] M. Tan, R. Pang, and Q. V Le, "EfficientDet: Scalable and Efficient Object Detection," pp. 10781–10790.
- [28] Z. Tian, C. Shen, H. Chen, and T. He, "FCOS: Fully convolutional one-stage object detection," Proc. IEEE Int. Conf. Comput. Vis., vol. 2019-October, pp. 9626–9635, 2019, doi: 10.1109/ICCV.2019.00972.
- [29] Z. Cai and N. Vasconcelos, "Cascade R-CNN: Delving into High Quality Object Detection," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., pp. 6154–6162, 2018, doi: 10.1109/CVPR.2018.00644.
- [30] T. Y. Lin, P. Goyal, R. Girshick, K. He, and P. Dollar, "Focal Loss for Dense Object Detection," IEEE Trans. Pattern Anal. Mach. Intell., vol. 42, no. 2, pp. 318–327, 2020, doi: 10.1109/TPAMI.2018.2858826.
- [31] C. F. Mykhailo and S. Alexander, "RetinaMask: Learning to predict masks improves state-of-the-art single-shot detection for free."
- [32] X. Lu, B. Li, Y. Yue, Q. Li, and J. Yan, "Grid R-CNN," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2019-June, pp. 7355–7364, 2019, doi: 10.1109/CVPR.2019.00754.
- [33] K. Chen et al., "Hybrid task cascade for instance segmentation," Proc. IEEE Comput. Soc. Conf. Comput. Vis. Pattern Recognit., vol. 2019-June, pp. 4969–4978, 2019, doi: 10.1109/CVPR.2019.00511.
- [34] S. Qiao, L.-C. Chen, and A. Yuille, "DetectorRS: Detecting Objects with Recursive Feature Pyramid and Switchable Atrous Convolution," 2020, [Online]. Available: <http://arxiv.org/abs/2006.02334>.
- [35] X. Zhou, V. Koltun, and P. Krähenbühl, "Probabilistic two-stage detection," 2021, [Online]. Available: <http://arxiv.org/abs/2103.07461>.

Naïve Bayes Classification of High-Resolution Aerial Imagery

Asmala Ahmad¹

Optimization Modelling Analytic and Simulation
(OptiMAS)

Faculty of Information and Communication Technology
Universiti Teknikal Malaysia Melaka, Melaka, Malaysia

Hamzah Sakidin²

Fundamental and Applied Sciences Department
Universiti Teknologi PETRONAS
Perak, Malaysia

Mohd Yazid Abu Sari³

Anjung Technology Sdn. Bhd
Ayer Keroh, Melaka, Malaysia

Abd Rahman Mat Amin⁴

Faculty of Applied Sciences
Universiti Teknologi MARA
Terengganu, Malaysia

Suliadi Firdaus Sufahani⁵

Faculty of Applied Sciences and Technology
Universiti Tun Hussein Onn Malaysia
Johor, Malaysia

Abd Wahid Rasib⁶

Faculty of Built Environment and Surveying
Universiti Teknologi Malaysia
Johor, Malaysia

Abstract—In this study, the performance of Naïve Bayes classification on a high-resolution aerial image captured from a UAV-based remote sensing platform is investigated. K-means clustering of the study area is initially performed to assist in selecting the training pixels for the Naïve Bayes classification. The Naïve Bayes classification is performed using linear and quadratic discriminant analyses and by making use of training set sizes that are varied from 10 through 100 pixels. The results show that the 20 training set size gives the highest overall classification accuracy and Kappa coefficient for both discriminant analysis types. The linear discriminant analysis with 94.44% overall classification accuracy and 0.9395 Kappa coefficient is found higher than the quadratic discriminant analysis with 88.89% overall classification accuracy and 0.875 Kappa coefficient. Further investigations carried out on the producer accuracy and area size of individual classes show that the linear discriminant analysis produces a more realistic classification compared to the quadratic discriminant analysis particularly due to limited homogenous training pixels of certain objects.

Keywords—Naïve Bayes; k-means; classification accuracy; training set size; discriminant analysis

I. INTRODUCTION

In remote sensing, classification is the process of assigning a pixel to a particular type of land cover. Classification uses typically a measurement vector or feature vector ω of data acquired from a spaceborne or airborne acquisition system. It aims to assign a pixel associated with the measurement ω at position x to particular class i , where $1 \leq i \leq M$ and M is the total number of classes. The classes are defined from supporting data, such as maps and ground data for test sites. Two types of classification are commonly used, supervised and unsupervised. Supervised classification starts from a

known set of classes, learns the statistical properties of each class and then assigns the pixels based on these properties. Unsupervised classification is a two-step operation of grouping pixels into clusters based on the statistical properties of the measurements, and then labelling the clusters with the appropriate classes. Supervised classification classifies pixels based on known properties of each cover type, it requires representative land cover information, in the form of training pixels [1],[2],[3]. Signatures generated from the training data will be in a different form, depending on the classifier type used. Examples of supervised classification classifiers include Naïve Bayes, Maximum Likelihood, Mahalanobis Distance, Parallelepiped and support vector machines. On the other hand, in terms of unsupervised classification, the clustering process produces clusters that are statistically separable, giving a natural grouping of the pixels [4]. Landcover information is then used in the following labelling process where clusters are assigned to classes based on the available landcover information. This has the disadvantages that (1) a cluster may represent a mixture of different landcover types and (2) a single landcover may be split into several clusters. Furthermore, the assignment of clusters to classes, also known as the labelling process, requires manual input using available knowledge and needs to be carefully performed after the clustering, to correctly label the clusters. Examples of unsupervised classification are K-means and ISODATA. These unsupervised and supervised methods have been used extensively on satellite images however, there is limited effort to investigate the performance of these methods on high-resolution aerial images [1],[2],[3],[4]. In this study, the performance of Naïve Bayes classification on a high-resolution aerial image is to be investigated where K-means clustering is initially performed in determining the training pixels.

II. UNSUPERVISED AND SUPERVISED CLASSIFICATION

A. K-means Clustering

K-Means algorithm is an iterative method to partition a given dataset into a user-specified number of clusters, K. Its objective is to minimize the average squared Euclidean distance of distance from their cluster centres [5]. Let μ_c denotes the mean for cluster centre c , and the K-Means objective function can be written as:

$$J(c, \mu) = \sum_{i=1}^k \sum_{j=1}^n \|x^j - \mu_c^i\|^2 \quad (1)$$

Where, J measures the sum of squared distances between each training example x^j and the cluster centroid μ_c^i to which it has been assigned. The inner-loop of K-Means repeatedly minimizes J with respect to c while holding μ fixed, and then minimizes J with respect to μ while holding c fixed. With this function well defined, the process can be split into several steps, to achieve the intended result. The starting point is a large set of data entries and defining the number of centres, k .

B. Naïve Bayes Classification

Generally, from the conditional probability theorem, the probability of an event A occurs given event B has already occurred is equal to the intersection of event A and B divided by event B [6],[7]. This can be expressed as:

$$P(A|B) = \frac{P(A \cap B)}{P(B)} \quad (2)$$

In the same way, the probability of an event B occurs given event A has already occurred can be expressed as:

$$P(B|A) = \frac{P(B \cap A)}{P(A)} \quad (3)$$

From the Commutative law, it can be easily proven:

$$B \cap A = A \cap B \quad (4)$$

Therefore (3) can also be written as,

$$P(B|A) = \frac{P(A \cap B)}{P(A)} \quad (5)$$

and,

$$P(A \cap B) = P(B|A)P(A) \quad (6)$$

Hence, (2) can be expressed as:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \quad (7)$$

This is popularly known as the Bayes' Theorem. $P(A|B)$ is also known as a posteriori probability of B. Event B is the evidence or feature. $P(A)$ is the priori of A or the prior probability. In real-world problems, multiple features B are typically considered. For n features, B can be expressed as a feature vector:

$$B = B_1, B_2, B_3, \dots, B_n \quad (8)$$

When these features are independent, the Bayes Rule can be extended to Naive Bayes:

$$P(A|B) = P(A|B_1, B_2, \dots, B_n) = \frac{P(B_1, B_2, B_3, \dots, B_n|A)P(A)}{P(B_1, B_2, B_3, \dots, B_n)} \quad (9)$$

Since $P(B_1, B_2, B_3, \dots, B_n|A)P(A)$ can be expanded into:

$$P(B_1, B_2, B_3, \dots, B_n|A)P(A) = P(B_1|A)P(B_2|A)P(B_3|A) \dots P(B_n|A) \quad (10)$$

and

$$P(B_1|A)P(B_2|A)P(B_3|A) \dots P(B_n|A) = \prod_{j=1}^n P(B_j|A) \quad (11)$$

Hence,

$$P(A|B_1, B_2, \dots, B_n) = \frac{\prod_{j=1}^n P(B_j|A)P(A)}{P(B_1, B_2, \dots, B_n)} \quad (12)$$

In remote sensing, the probability distributions of the data may take a variety of forms, but very frequently they are assumed to be Gaussian, more specifically having normal distribution [8],[9]. When each class obeys a multivariate normal distribution for N spectral dimensions, specifically the number of bands used, the probability that feature vector ω occurs in a specified class i can be defined as:

$$P(\omega|i) = (2\pi)^{-\frac{N}{2}} (|C_i|)^{-\frac{1}{2}} \exp\left(-\frac{1}{2}(\omega - \mu_i)^t C_i^{-1} (\omega - \mu_i)\right) \quad (13)$$

where,

$$C_i = \left\langle (\omega_j - \mu_i)(\omega_j - \mu_i)^t \right\rangle \approx \frac{1}{Q_i} \sum_{j=1}^{Q_i} \{(\omega_j - \mu_i)(\omega_j - \mu_i)^t\}$$

where μ_i is the class mean vector, C_i is the class covariance matrix for class i , Q_i is the number of pixels in class i , ω_j is the feature vector of the j th pixel and $|\cdot|$ is determinant. This assumption is likely to be suitable for data that comes directly from spectral band measurements, but should not be used if the feature vector contains more general types of data, e.g. band ratios, without first testing its validity.

The Naive Bayes classifier is based on Bayes' theorem of probability. In classification, the concern is to predict the classes given the measurement from different spectral bands [9],[10]. Therefore, the probability of class i occurs given the spectral measurement ω , $P(i|\omega)$, needs to be determined. From the Bayes' theorem, the a posteriori distribution $P(i|\omega)$ which is the probability that a pixel with feature vector ω belongs to class i , is given by:

$$P(i|\omega) = \frac{P(\omega|i)P(i)}{P(\omega)} \quad (14)$$

where $P(\omega)$ is the priori of ω , the prior probability, that is the probability of class i occurs before ω is known. $P(\omega|i)$ is the likelihood function, $P(i)$ is the a priori information, that's is the probability that class i occurs in the study area and $P(\omega)$ is the probability that ω is observed. $P(\omega)$ or the priori of ω can be expressed as:

$$P(\omega) = \sum_{i=1}^M P(\omega|i) P(i) \quad (15)$$

where M is the number of classes.

For Naïve Bayes, $\omega = \omega_1, \omega_2, \dots, \omega_n$

$$P(i|\omega) = P(i|\omega_1, \omega_2, \dots, \omega_n) = \frac{P(\omega_1, \omega_2, \dots, \omega_n|i)P(i)}{P(\omega_1, \omega_2, \dots, \omega_n)} \quad (16)$$

Expanding $P(\omega_1, \omega_2, \dots, \omega_n|i)$ gives:

$$P(\omega_1, \omega_2, \dots, \omega_n|i) = P(\omega_1|i)P(\omega_2|i)P(\omega_3|i) \dots P(\omega_n|i) \quad (17)$$

and

$$P(\omega_1|i)P(\omega_2|i)P(\omega_3|i) \dots P(\omega_n|i) = \prod_{j=1}^n P(\omega_j|i) \quad (18)$$

Hence,

$$P(i|\omega_1, \omega_2, \dots, \omega_n) = \frac{\prod_{j=1}^n P(\omega_j|i)P(i)}{P(\omega_1, \omega_2, \dots, \omega_n)} \quad (19)$$

Since $P(\omega_1, \omega_2, \dots, \omega_n)$ is constant given the input, the following classification rule can be used:

$$P(i|\omega_1, \omega_2, \dots, \omega_n) \propto \prod_{j=1}^n P(\omega_j|i) P(i) \quad (20)$$

$$\hat{i} = \operatorname{argmax}_i P(i) = \prod_{j=1}^n P(\omega_j|i) P(i) \quad (21)$$

Naïve Bayes classification is possible if the prior information $P(i)$ is available. This is the most powerful use of the Bayes Theorem.

Pixel x is assigned to class i by the rule:

$$x \in i \text{ if } P(i|\omega) > P(k|\omega) \text{ for all } k \neq i \quad (22)$$

III. METHODOLOGY

A. Personal Remote Sensing System (PRSS) Workflow

Image acquisition is carried out using an aerial imaging known as Personal Remote Sensing System or PRSS [11],[12]. The PRSS has been developed in the previous research for overcoming limitations in term of resolution besides cloud and haze effects of the space-borne remote sensing satellites [1],[13],[14],[15],[27]. This system consists of 1) aerial segment, 2) ground segment and 3) user segment. The aerial segment consists of a quad rotor UAV that is equipped with GPS and telemetry facilities and mounted with a high-resolution RGB camera [16],[17],[18]. Images are captured automatically at certain time interval and stored in the camera's storage card. Upon completing an image acquisition mission, the images in the card are transferred to the ground segment for subsequent image processing tasks. The ground segment consists of a laptop installed with softwares for controlling and tracking the UAV besides processing the captured images [19]. The processed images are finally uploaded to the cloud-based geospatial databases that can finally be accessed and personalised using a smart phone at the user segment. A user can make other request to the ground segment for images of other areas or objects. Upon receiving the request, the ground segment will prepare a new mission plan and it to the aerial segment for a new image acquisition mission to take place. The image used in this study was acquired on 28 March 2016 at 0956 local time. The UAV is flown at an altitude of 180 m at 0900 to 1100 MST (Malaysian Standard Time) and the sky was having clear conditions. The size of the image is 3000 rows by 4000 columns and the image format is JPG. Fig. 1 illustrates the PRSS workflow.

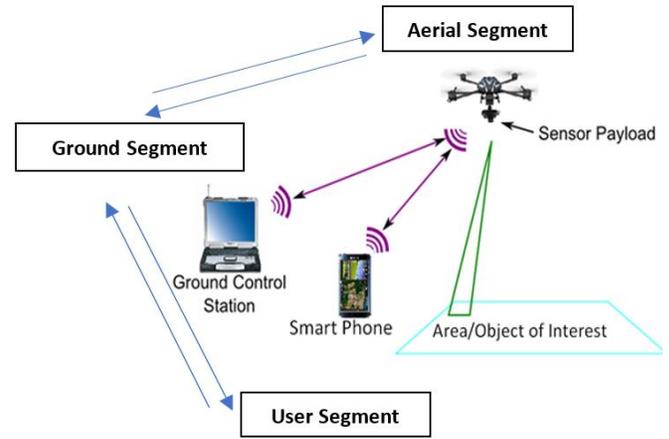


Fig. 1. PRSS Workflow.

B. Image Classification

The acquired image was initially processed using K-Means clustering algorithm [8]. The K-Means clustered image is later to be used together with the existing information of the study area in selecting the training pixels for Naïve Bayes classification later. The K-Means clustering algorithm is as follows.

- 1) An initial mean vector (point) is randomly specified for each of the K clusters. These points are to be the centre for each of the K clusters.
- 2) Next, the distances between every point of the image pixels and those centres are computed.
- 3) Each pixel is assigned to the cluster whose mean vector is the closest to the pixel vector. This leads to the formation of the first set of decision boundaries.
- 4) Based on the pixel vectors within each boundary, a new set of clusters mean vectors is then calculated and the pixels are reassigned accordingly to these new mean vectors.
- 5) The iterations are continued until there is no significant change in pixel assignments from one iteration to the next. Specifically, the magnitude of change from iteration $(i - 1)$ to iteration i summed over all K clusters can be expressed as:

$$\Delta\mu(i) = \sum_{k=1}^K |\mu_k^i - \mu_k^{i-1}| \quad (23)$$

The clustered image produced from the K-Means clustering is used to assist in collecting the training pixels for Naïve Bayes classification. The general procedures in Naïve Bayes classification are as follows:

- 1) The number of land cover types within the study area is determined.
- 2) The training pixels for each of the desired classes are chosen using land cover information for the study area together with the cluster map produced from the K-Means clustering.
- 3) The training pixels are then used to estimate the mean vector and covariance matrix of each class.

4) Finally, every pixel in the image is classified into one of the desired land cover types based on the predefined discriminant functions.

In Naïve Bayes classification, each class is enclosed in a region in spectral space where its discriminant function is larger than that of all other classes. These class regions are separated by decision boundaries, where the decision boundary between class i and j occurs when:

$$g_i(\omega) = g_j(\omega) \quad (24)$$

In this study, the linear discriminant function and quadratic discriminant function are utilised.

For linear discriminant function, $C_i = C_j = C$, thus:

$$-\frac{1}{2}(\omega - \mu_i)^t C^{-1}(\omega - \mu_i) - \frac{N}{2} \ln(2\pi) - \frac{1}{2} \ln(|C|) - \left(-\frac{1}{2}(\omega - \mu_j)^t C^{-1}(\omega - \mu_j) - \frac{N}{2} \ln(2\pi) - \frac{1}{2} \ln(|C|)\right) = 0 \quad (25)$$

which can be rewritten as:

$$-(\omega - \mu_i)^t C^{-1}(\omega - \mu_i) - \ln(|C|) + (\omega - \mu_j)^t C^{-1}(\omega - \mu_j) + \ln(|C|) = 0 \quad (26)$$

$$-(\omega - \mu_i)^t C^{-1}(\omega - \mu_i) + (\omega - \mu_j)^t C^{-1}(\omega - \mu_j) = 0 \quad (27)$$

This is a linear function in N dimensions that forms the decision boundary between class i and j .

For quadratic discriminant function, $C_i \neq C_j$, thus:

$$-\frac{1}{2}(\omega - \mu_i)^t C_i^{-1}(\omega - \mu_i) - \frac{N}{2} \ln(2\pi) - \frac{1}{2} \ln(|C_i|) - \left(-\frac{1}{2}(\omega - \mu_j)^t C_j^{-1}(\omega - \mu_j) - \frac{N}{2} \ln(2\pi) - \frac{1}{2} \ln(|C_j|)\right) = 0 \quad (28)$$

which can be rewritten as:

$$-(\omega - \mu_i)^t C_i^{-1}(\omega - \mu_i) - \ln(|C_i|) + (\omega - \mu_j)^t C_j^{-1}(\omega - \mu_j) + \ln(|C_j|) = 0 \quad (29)$$

This is a quadratic function in N dimensions that forms the decision boundary between class i and j .

C. Classification Accuracy

Classification accuracy is one of the key parameters required to judge the quality of land cover classification and can be defined as the degree to which the derived image classification conforms to the ‘truth’ [20]. One of the most important components in accuracy assessment is reference pixels [21]. In this study, make use of Google Maps and the available ground truth knowledge of the study area in collecting the reference pixels [22]. To do so, a systematic sampling is performed where the chosen reference pixels are distributed in a predefined pattern. Studies have shown that the most widely used technique to analyse reference data is to use a confusion or error matrix [23]. A confusion matrix works by comparing classification result with reference information, while accuracy is conveyed in terms of percentage of overall classification accuracy and producer accuracy [24],[25]. The acceptable of overall accuracy is 85%, with no class less than 70% accurate [26]. Kappa statistics

have been used as early as the 1980s as an additional classification accuracy measure to compensate for chance agreement [23].

Producer accuracy is a measure of the accuracy of a particular classification scheme and shows the percentage of a particular ground class that has been correctly classified. The minimum acceptable accuracy for a class is 70% [26]. This is calculated by dividing each of the diagonal elements in the table by the total of the column in which it occurs:

$$\text{Producer accuracy} = \frac{c_{aa}}{c_{\bullet a}} \quad (30)$$

where,

c_{aa} = element at position a^{th} row and a^{th} column

$c_{\bullet a}$ = column sum

A measure of behaviour of a classification can be determined by the overall accuracy, which is the total percentage of pixels correctly classified:

$$\text{Overall accuracy} = \frac{\sum_{a=1}^U c_{aa}}{Q} \quad (31)$$

where Q and U represent the total number of pixels and classes respectively. The minimum acceptable overall accuracy is 85% [28]. The Kappa coefficient κ is a second measure of classification accuracy which incorporates the off-diagonal elements as well as the diagonal terms to give a more robust assessment of accuracy than overall accuracy. This is computed as:

$$\kappa = \frac{\sum_{a=1}^U \frac{c_{aa}}{Q} - \sum_{a=1}^U \frac{c_{a\bullet} c_{\bullet a}}{Q^2}}{1 - \sum_{a=1}^U \frac{c_{a\bullet} c_{\bullet a}}{Q^2}} \quad (32)$$

Where $c_{a\bullet}$ is row sum and $c_{\bullet a}$ is column sum.

IV. RESULT AND DISCUSSION

Fig. 2 shows the study area displayed in (a) RGB, (b) red, (c) green and (d) blue channel with the corresponding histograms. It is obvious that the study area has two main groups of which are natural and artificial land covers or objects. This scenario is indicated by the bimodal nature of the red, green and blue channel histogram. For all histogram, it can be seen that the separation of the natural and artificial objects occur at the valley that is about at DN of 120 in which natural object pixels correspond to the lower DN values while artificial object pixels correspond to the higher DN values.

Fig. 3 shows the result of K-Means clustering for 5 clusters. By comparing with the RGB image in Fig. 2(a), most of the objects have been sensibly clustered. Due the nature of the K-Means clustering in which clustering process is merely based on statistical properties of the image, as expected there are clusters with more than one object and there are objects having more than one cluster. Shrub clusters (green) can be seen at the top right and bottom right of the image. There seems to be two road clusters with low-level road cluster (violet) stretches from the lower left to the upper right of the image while high-level road cluster (dark green) can be seen stretches from near the bottom middle to the top right of the image. Grassy ground cluster (maroon) can be seen mostly

between the shrub and low-level road cluster. Finally, vehicle cluster (turquoise) can be seen on both roads.

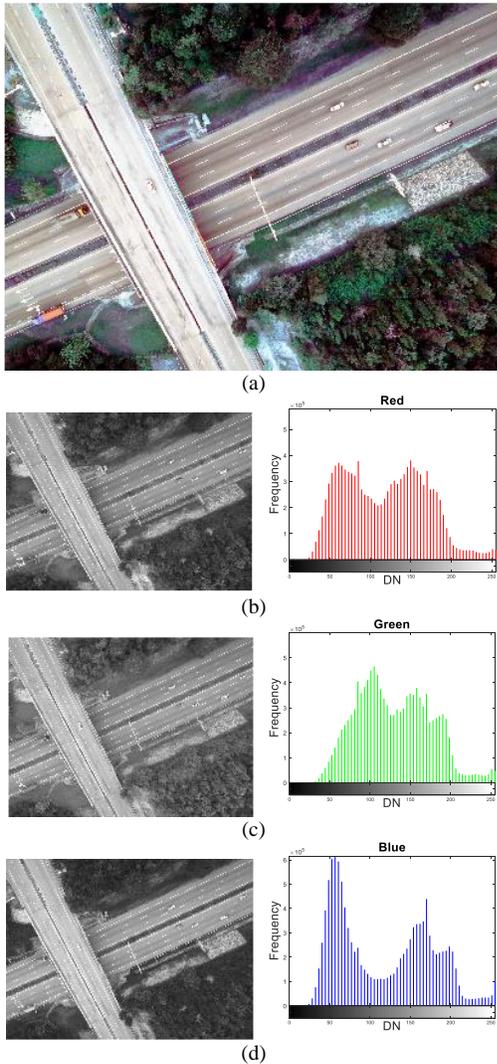


Fig. 2. The Scene Under Study in (a) RGB, (b) Red, (c) Green and (d) Blue Channel with the Corresponding Histograms.

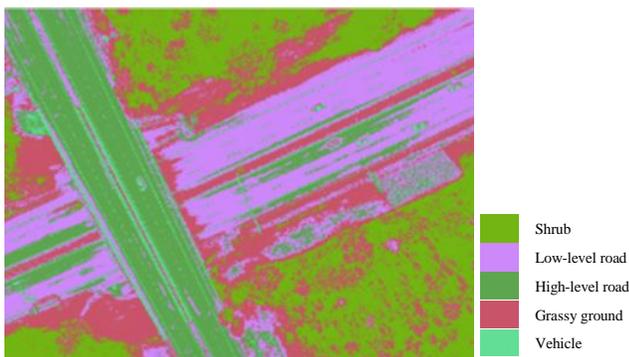


Fig. 3. 5-Cluster K-Means Clustering of the Study Area.

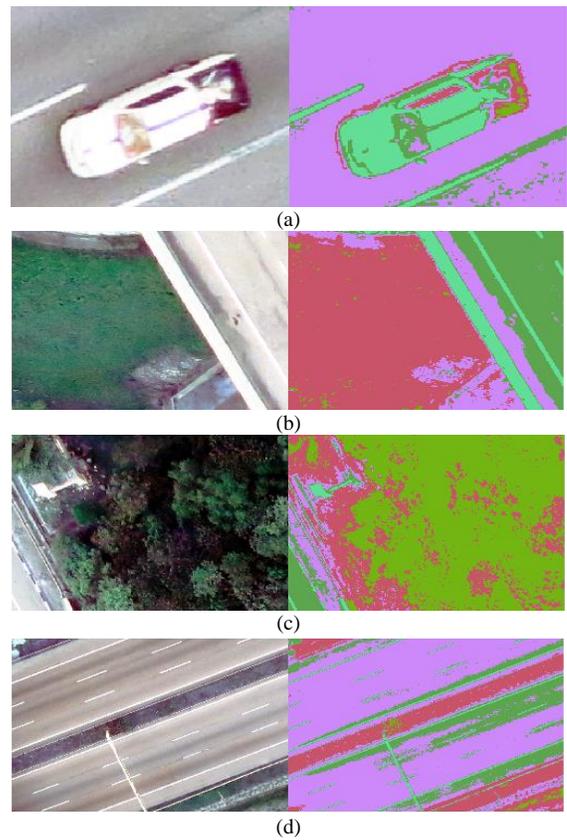


Fig. 4. RGB Image (Left) and Clustered Image (Right) for (a) Bright Vehicle, (b) Grassy Ground, (c) Shrub and (d) Road (Normal).

The outcome from the K-Means clustering is used to assist in selecting the training pixels for Naïve Bayes classification. In doing so, both the RGB and K-Means clustering image are displayed side by side and zoomed at the targeted objects. The zoom-in images for vehicle, grassy ground, shrub and road are shown in Fig. 4(a), (b), (c) and (d), respectively. This has provided a practically way for the spatial and spectral homogeneity criteria to be met in selecting the training pixels [8].

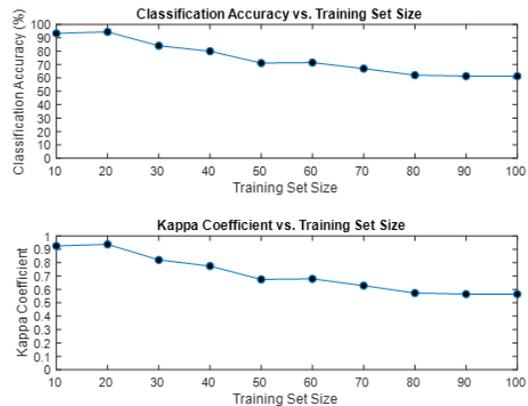


Fig. 5. Overall Classification Accuracy and Kappa Coefficient Versus Training Set Size using Linear Discriminant Analysis.

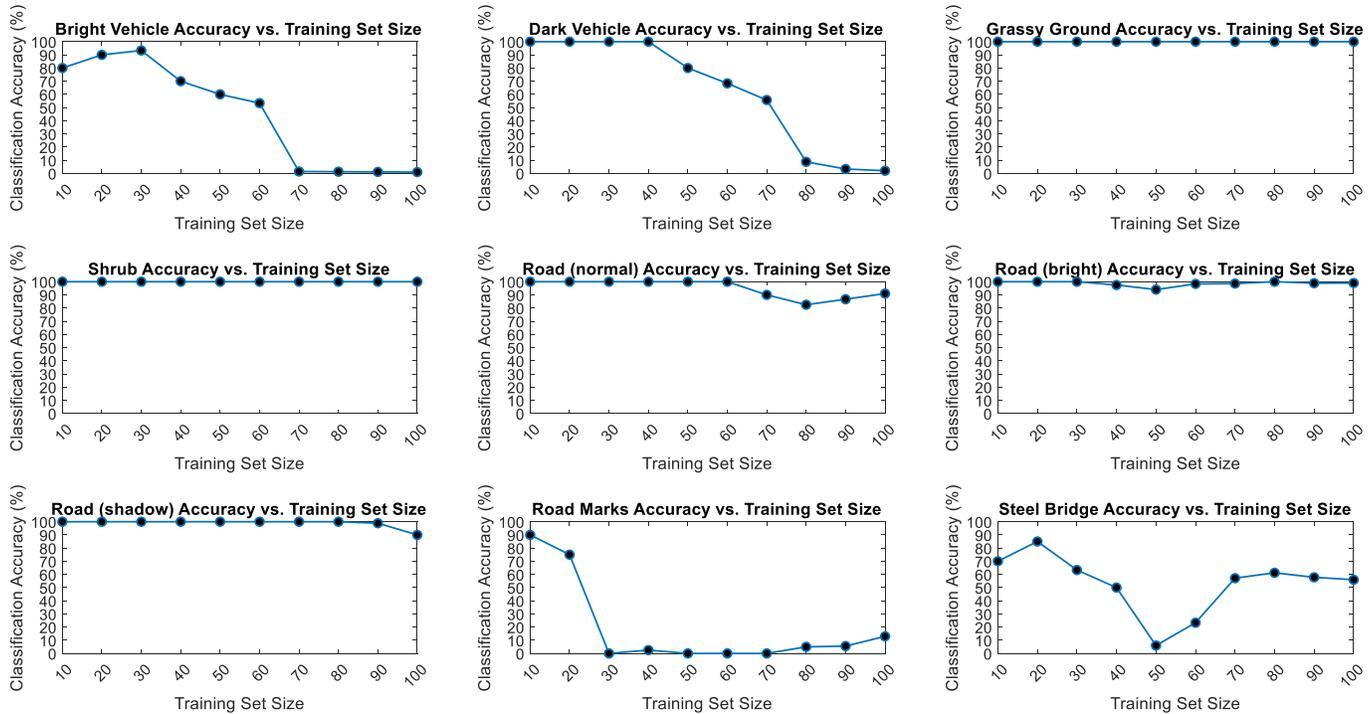


Fig. 6. Individual Class Classification Accuracy (Producer Accuracy) Versus Training Set Size for Classified Images using Linear Discriminant Analysis.

A. Naïve Bayes Classification using Linear Discriminant Analysis

For Naïve Bayes classification, the 9 classes identified are 1) Bright Vehicle, 2) Dark Vehicle, 3) Grassy Ground, 4) Shrub, 5) Road (Normal), 6) Road (Bright), 7) Road (Shadow), 8) Road Mark and 9) Steel Bridge. Due to the high image resolution, for Road class, three labels have been used to represent three different illumination conditions of the road. Fig. 5 shows plots of overall classification accuracy (top) and Kappa coefficient (bottom) versus training set size for the Naïve Bayes classification that is based on linear discriminant analysis. The 20 training set size gives highest overall classification accuracy (94.44%) and Kappa coefficient (0.9395) compared to the other sets. Plots of classification accuracy (producer accuracy) versus training set for all classes are shown in Fig. 6. It can be seen that Grassy Ground, Shrub and Road (Shadow) have the most stable accuracies for all training pixel sets while the least stable classes are Road Mark, Steel Bridge and Bright Vehicle. This is due to the facts that stable classes have more abundant homogeneous pixels compared to least stable classes in which can be visually seen from the K-means clustering image in Fig. 3. For the rest of the classes, generally high classification accuracies are gained at smaller compared to bigger training set sizes.

Fig. 7 shows the Naïve Bayes classified image using linear discriminant analysis. From visual comparison with the RGB image in Fig. 2(a), it is obvious that the most objects are correctly classified except for Road Mark, Steel Bridge and

Bright Vehicle. It can be seen that there are Bright Vehicle and Steel Bridge pixels that have been incorrectly assigned to the Road Mark class in which is also indicated by the confusion matrix in Table I. There also Road Mark pixels that have been incorrectly assigned to the Steel Bridge class and Bright Vehicle class. Table II shows the object, pixel count, pixel percentage and the corresponding area for classified image using linear discriminant analysis. The largest classes are Road (Normal), Grassy Ground and Road (Bright) with the corresponding area percentage of 26.9%, 22.9% and 18.8%. The smallest classes are Dark Vehicle, Bright Vehicle and Road Mark with the corresponding area percentage of 0.1%, 0.4% and 1.2%.

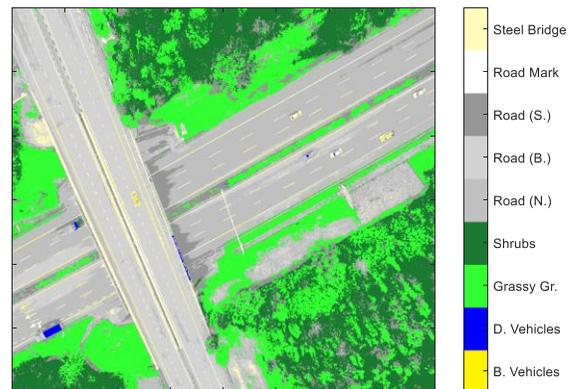


Fig. 7. Naïve Bayes Classified Image using Linear Discriminant Analysis.

TABLE I. THE CONFUSION MATRIX FOR THE NAÏVE BAYES CLASSIFICATION THAT USES LINEAR DISCRIMINANT ANALYSIS

Reference Pixels											
Classified Pixels		Bright Vehicle	Dark Vehicle	Grassy Ground	Shrub	Road (Normal)	Road (Bright)	Road (Shadow)	Road Mark	Steel Bridge	Total Classified Pixels
	Bright Vehicle	18	0	0	0	0	0	0	2	0	20
	Dark Vehicle	0	20	0	0	0	0	0	0	0	20
	Grassy Ground	0	0	20	0	0	0	0	0	0	20
	Shrub	0	0	0	20	0	0	0	0	0	20
	Road (Normal)	0	0	0	0	20	0	0	0	0	20
	Road (Bright)	0	0	0	0	0	20	0	2	0	22
	Road (Shadow)	0	0	0	0	0	0	20	0	0	20
	Road Mark	2	0	0	0	0	0	0	15	3	20
	Steel Bridge	0	0	0	0	0	0	0	1	17	18
	Total Ref. Pixels	20	20	20	20	20	20	20	20	20	180

TABLE II. CLASS WITH PIXEL COUNT, PIXEL PERCENTAGE OF THE AREA FOR CLASSIFIED IMAGE USING LINEAR DISCRIMINANT ANALYSIS

Class	Pixel (count)	Pixel (%)	Area (m ²)
Bright Vehicle	52454	0.4	1573.6
Dark Vehicle	15163	0.1	454.9
Grassy Ground	2744206	22.9	82326.2
Shrub	2241943	18.7	67258.3
Road (Normal)	3222214	26.9	96666.4
Road (Bright)	2260668	18.8	67820
Road (Shadow)	1053969	8.8	31619.1
Road Mark	138904	1.2	4167.1
Steel Bridge	270479	2.3	8114.4
Total Classified Pixels	12000000	100.1	360000

B. Naïve Bayes Classification using Quadratic Discriminant Analysis

For the Naïve Bayes Classification using quadratic discriminant analysis (Fig. 8), a gradual decrease in the overall accuracy can be seen as the training set size increases compared to that of using the linear discriminant analysis. The highest overall classification accuracy of 88.89% and the highest Kappa coefficient of 0.875 are shared by the 10 and 20 training set size. In term of individual class classification accuracy (producer accuracy) in Fig. 9, the most stable classes are Shrub, Road (Shadow) and Grassy Ground while the least stable classes are Road Mark, Steel Bridge and Road (Bright). A strange increasing trend occurs for Road (Bright). By

comparing the linear and quadratic discriminant analysis plots, overall, quadratic trend looks smoother compared to linear discriminant trend in which likely due to the more flexible criteria of the quadratic discriminant decision space. The classes with somewhat common producer accuracy trends are Shrub, Grassy Ground, Road (Shadow) and Road (Normal) due to the abundant homogenous training pixels. The classes having the most distinct trends are Road (Bright), Dark Vehicle and Steel Bridge due to the least homogenous training pixels.

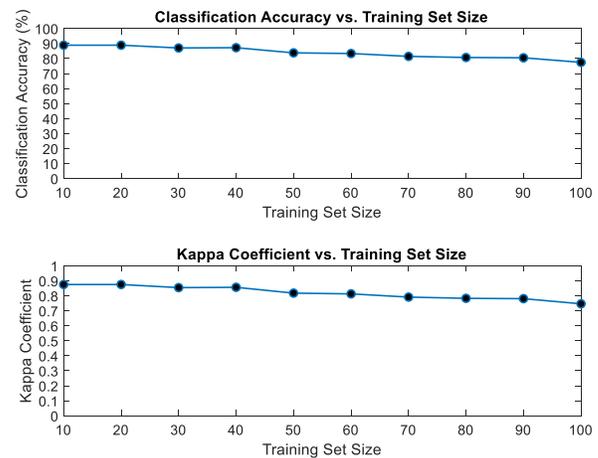


Fig. 8. Overall Classification Accuracy and Kappa Coefficient Versus Training Set Size using Quadratic Discriminant Analysis.

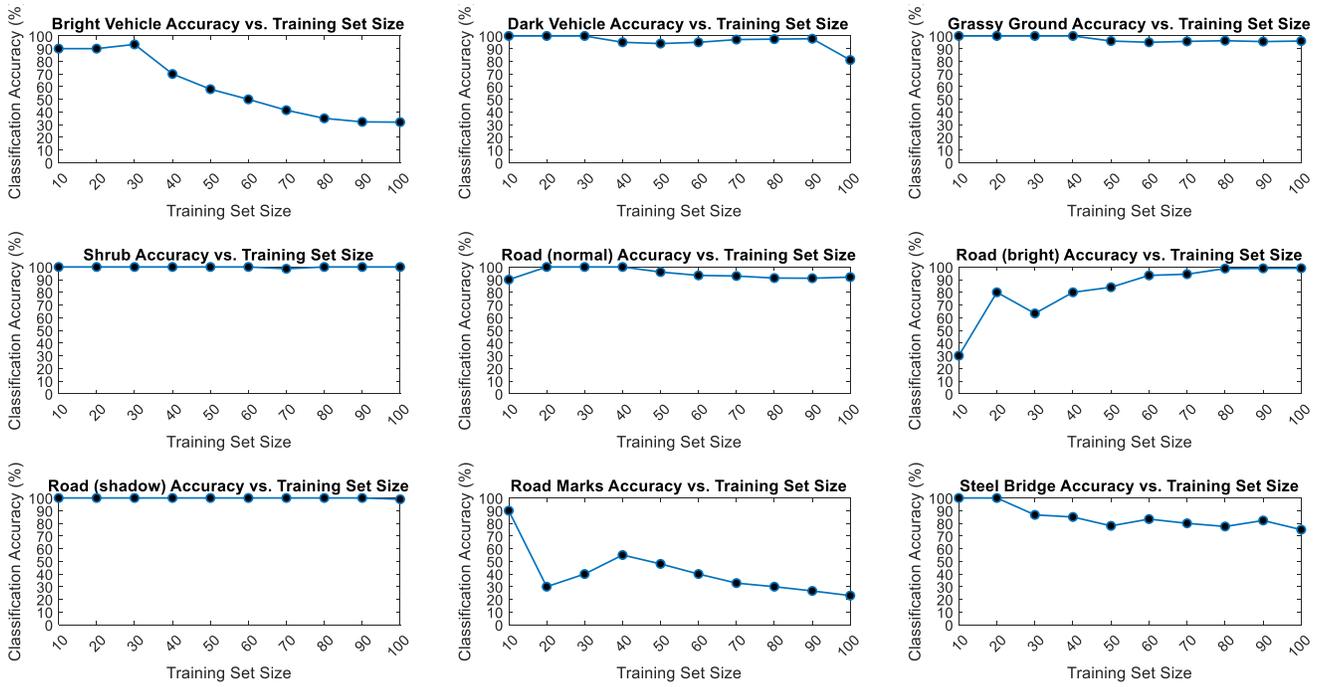


Fig. 9. Individual Class Classification Accuracy (Producer Accuracy) Versus Training Set Size for Classified Images using Quadratic Discriminant Analysis.

TABLE III. THE CONFUSION MATRIX FOR THE NAÏVE BAYES CLASSIFICATION THAT USES LINEAR DISCRIMINANT ANALYSIS

		Reference Pixels									
		Bright Vehicle	Dark Vehicle	Grassy Ground	Shrub	Road (Normal)	Road (Bright)	Road (Shadow)	Road Mark	Steel Bridge	Total Classified Pixels
Classified Pixels	Bright Vehicle	18	0	0	0	0	0	0	11	0	29
	Dark Vehicle	0	20	0	0	0	0	0	0	0	20
	Grassy Ground	0	0	20	0	0	0	0	0	0	20
	Shrub	0	0	0	20	0	0	0	0	0	20
	Road (Normal)	0	0	0	0	20	0	0	0	0	20
	Road (Bright)	0	0	0	0	0	16	0	0	0	16
	Road (Shadow)	0	0	0	0	0	0	20	0	0	20
	Road Mark	2	0	0	0	0	0	0	6	0	8
	Steel Bridge	0	0	0	0	0	4	0	3	20	27
	Total Ref. Pixels	20	20	20	20	20	20	20	20	20	180

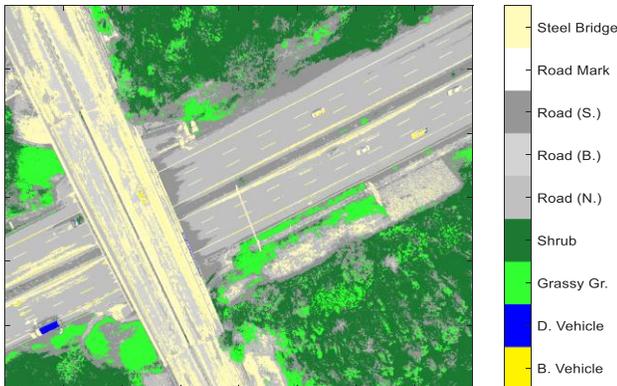


Fig. 10. Naïve Bayes Classified Image using Quadratic Discriminant Analysis.

Fig. 10 shows the Naïve Bayes classified image using quadratic discriminant analysis. It is obvious that there are more incorrectly assigned pixels compared to that of the linear discriminant analysis. It can be seen that there are Road (Bright) pixels that have been incorrectly assigned to Steel Bridge class in which is also indicated by the confusion matrix in Table III. Table IV shows the class with the pixel count, pixel percentage of the area for classified image using quadratic discriminant analysis. The largest classes are Road (Normal), Shrub and Road (Shadow) with the corresponding area percentage of 30%, 23.6% and 18%. The smallest classes are Dark Vehicle, Bright Vehicle and Road Mark with the corresponding area percentage of 0.1%, 0.5% and 0.9%.

TABLE IV. CLASS WITH PIXEL COUNT, PIXEL PERCENTAGE OF THE AREA FOR CLASSIFIED IMAGE USING QUADRATIC DISCRIMINANT ANALYSIS

Class	Pixel (count)	Pixel (%)	Area (m ²)
Bright Vehicle	54236	0.5	1627.1
Dark Vehicle	10415	0.1	312.5
Grassy Ground	1008987	8.4	30269.6
Shrub	2827918	23.6	84837.5
Road (Normal)	3602988	30	108089.6
Road (Bright)	641307	5.3	19239.2
Road (Shadow)	2160972	18	64829.2
Road Mark	108365	0.9	3251
Steel Bridge	1584812	13.2	47544.4
Total Classified Pixels	12000000	100	360000

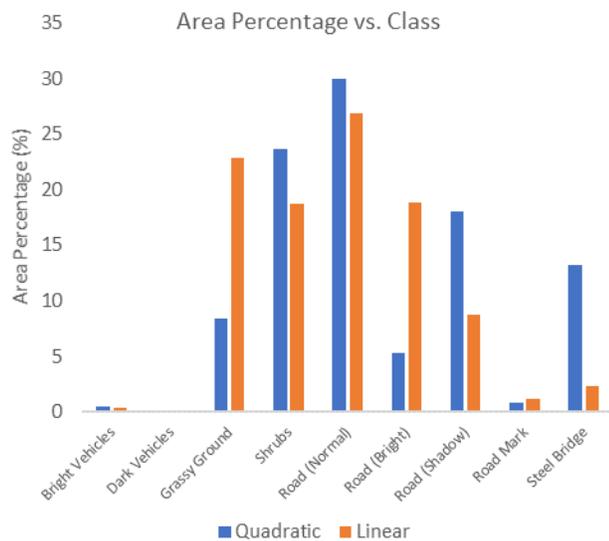


Fig. 11. Area Percentage Versus Class for Quadratic and Linear Discriminant Analysis.

Fig. 11 shows the area percentage versus class for the quadratic and linear discriminant analysis. From side-by-side area percentage comparison, Bright Vehicle, Dark Vehicle and Road Mark have about the same area sizes.

The classes having the most distinct area sizes are Grassy Ground, Steel Bridge and Road (Bright). The linear shows a more realistic area percentage compared to the quadratic discriminant analysis particularly due to its Steel Bridge having higher is larger than other abundant objects such as Grassy Ground and Road (Bright).

V. CONCLUSION

In this study, Naïve Bayes classifications on a high-resolution aerial image have been performed. K-means clustering of five clusters has been used as a guide in selecting the training pixels for the Naïve Bayes classification. The classification has been experimented for training set size 10 through 100 for linear and quadratic discriminant analysis. From, the classification outcomes, training set size 20 has been chosen due to having the highest overall classification accuracy and Kappa coefficient where the linear with 94.44%

overall classification accuracy and 0.9395 Kappa coefficient is higher than the quadratic discriminant analysis with 88.89% overall classification accuracy and 0.875 Kappa coefficient. The producer accuracy for individual classes of linear and quadratic discriminant analysis has yielded the classes having similar trends due to the availability of abundant homogenous training pixels compared with the classes with distinct trends due to the least homogenous training pixels. The linear discriminant analysis has been found to produce more realistic class area percentages of the study area compared to the quadratic discriminant analysis, particularly for Steel Bridge. Nevertheless, the performance of Naïve Bayes classification is greatly influenced by the way the sampling of the training pixels is made in which is not investigated in this study. Therefore, future work will take into consideration investigating the effects of different patterns of systematic sampling of training pixels on classification performance.

ACKNOWLEDGMENT

The authors would like to thank Universiti Teknikal Malaysia Melaka (UTeM) for funding this research through the Centre for Research and Innovation Management (CRIM) Publication Incentive Fund.

REFERENCES

- [1] A. Ahmad, U. K. M. Hashim, O. Mohd, M. M. Abdullah, H. Sakidin, A. W. Rasib and S. F. Sufahani, "Comparative analysis of support vector machine, maximum likelihood and neural network classification on multispectral remote sensing data" International Journal of Advanced Computer Science and Applications (IJACSA), vol. 9, no. 9, pp. 529–537, 2018.
- [2] Y. Lan, Z. Huang, X. Deng, Z. Zhu, H. Huang, Z. Zheng, B. Lian, G. Zeng and Z. Tong, "Comparison of machine learning methods for citrus greening detection on UAV multispectral images", Computers and Electronics in Agriculture, vol. 171, pp. 1 – 11, 2020.
- [3] M. Said, M. Hany, M. Magdy, O. Saleh, M. Sayed, Y. M. I. Hassan and A. Nabil, "Automated labeling of hyperspectral images for oil spills classification" International Journal of Advanced Computer Science and Applications (IJACSA), vol. 12, no. 8, 2021.
- [4] M. K. I. Rahmani, N. Pal and K. Arora, "Clustering of Image Data Using K-Means and Fuzzy K-Means", International Journal of Advanced Computer Science and Applications (IJACSA), vol. 5, no. 7, 2014.
- [5] M. Yang, H. Mei and D. Huang, "An effective detection of satellite images via K-means clustering on hadoop system", International Journal of Innovative Computing, Information and Control, vol. 13, no. 3, pp. 1037–1046, June 2017.
- [6] D. Park, "Image classification using Naïve Bayes classifier", International Journal of Computer Science and Electronics Engineering (IJCEE), vol. 4, no. 3, pp. 135–139, 2016.
- [7] Y. Ho, Y. Huang, H. Chu and L. Chen, "Adaptive sensing scheme using naïve Bayes classification for environment monitoring with drone", International Journal of Distributed Sensor Networks, vol. 14, pp. 1 – 12, 2018.
- [8] R. A. Schowengerdt, Remote sensing, models, and methods for image processing, 3rd ed., Academic Press: USA, 2007.
- [9] A. Ahmad and S. Quegan, "Analysis of maximum likelihood, classification on multispectral data", Applied Mathematical Sciences, vol. 6, no. 129, pp. 6425 – 6436, 2012.
- [10] Scikit-learn. Naive Bayes. Retrieved August, 2021, from https://scikit-learn.org/stable/modules/naive_bayes.html.
- [11] A. Yazid, R. A. Wahid, K. M. Nazrin, A. Ahmad, A. S. Nasruddin, D. Rozilawati, M. A. Hamzah and M. Razak, "Terrain mapping from unmanned aerial Vehicle", Journal of Advanced Manufacturing Technology, vol. 13, no. 1, pp. 1–16, 2019.

- [12] A. Ahmad, K. A. M. Fauzey, M. M. Abdullah, S. F. Sufahani, M. Y. A. Sari and A. R. M. Amin, "Noise and restoration of UAV remote sensing images " *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 11, no. 12, pp. 175–183, 2020.
- [13] A. Ahmad and S., Quegan, "The effects of haze on the spectral and statistical properties of land cover classification", *Applied Mathematical Sciences*, vol. 8, no. 180, pp. 9001–9013, 2014.
- [14] A. Ahmad, M. K. A. Ghani, S. Razali, H. Sakidin and N. M. Hashim, "Haze reduction from remotely sensed data", *Applied Mathematical Sciences*, vol. 8, no. 36, pp. 1755–1762, 2014.
- [15] A. Ahmad and S. Quegan, "The effects of haze on the accuracy of satellite land cover classification", *Applied Mathematical Sciences*, vol. 9, no. 49, pp. 2433–2443, 2015.
- [16] N. A. Sari, A. Ahmad, M. Y. A. Sari, S. Sahib and A. W. Rasib, "Development of rapid low-cost LARS platform for oil palm plantation", *Jurnal Teknologi*, vol. 77, no. 20, pp. 99–105, 2015.
- [17] F. Mahmood, K. Abbas, A. Raza, M. A. Khan and P. W. Khan, "Three dimensional agricultural land modeling using Unmanned Aerial System (UAS)" *International Journal of Advanced Computer Science and Applications (IJACSA)*, vo. 10, no. 1, 2019.
- [18] N. U. Din, B. Naz, S. Zai, B. and W. Ahmed, "Onion crop monitoring with multispectral imagery using deep neural network", *International Journal of Advanced Computer Science and Applications (IJACSA)*, vo. 12, no. 5, 2021.
- [19] M. Y. A. Sari, A. W. Rasib, H. M. Ali, A. R. M. Yusoff, M. I. Hassan, K. M. Idris, A. Ahmad and R. Dollah, "3D mapping based-on integration of uav platform and ground surveying", *International Journal of Advanced Computer Science and Applications (IJACSA)*, vol. 9, no. 12, 2018.
- [20] J. B. Campbell, "Introduction to remote sensing", London: Taylor & Francis, 2002.
- [21] S. V. Stehman, "Selecting and interpreting measures of thematic classification accuracy", *Remote Sensing of Environment*", vol. 62, pp. 77 – 89, 1997.
- [22] S. J. Miguel-Ayanz and G. S. Biging, "An iterative classification approach for mapping natural resources from satellite imagery" *International Journal of Remote Sensing*, vol. 17, pp. 957 – 982, 1996.
- [23] R. G. Congalton, "A review of assessing the accuracy of classification of remotely sensed data", *Remote Sensing of Environment*, vol. 37, pp.35 – 46, 1991.
- [24] T. M. Lillesand, R. W. Kiefer and J. W. Chipman, "Remote Sensing and Image Interpretation", 7th Ed. NJ, USA: John Wiley & Sons, 2015.
- [25] S. Koukoulas and G. A. Blackburn, "Introducing new indices for accuracy evaluation of classified images representing semi-nat ural woodland environments", *Photogrammetric Engineering and Remote Sensing*, vol. 67, no. 4, pp. 499 –510, 2001.
- [26] J. R. Thomlinson, P. V. Bolstad and W. B. Cohen, "Coordinating methodologies for scaling landcover classifications from site-specific to global: steps toward validating global map products", *Remote Sensing of Environment*, vol. 70, pp. 16 – 28, 1999.
- [27] A. Ahmad and S. Quegan, "Multitemporal cloud detection and masking using MODIS data", *Applied Mathematical Sciences*, vol. 8, no. 7, pp. 345–353, 2014.
- [28] M. A. Wulder, S. E. Franklin, J. C. White, J. Linke and S. Magnussen, "An accuracy assessment framework for large-area land cover classification products derived from medium-resolution satellite data", *International Journal of Remote Sensing*, vol. 27, pp. 663 – 683, 2006.

Secured and Provisioned Access Authentication using Subscribed User Identity in Federated Clouds

Sudan Jha¹, Sultan Ahmad^{2*}, Meshal Alharbi³, Bader Alouffi⁴ and Shoney Sebastian⁵

School of Sciences, Christ (Deemed to be University), NCR, New Delhi, India¹

Department of Computer Science, College of Computer Engineering and Sciences
Prince Sattam Bin Abdulaziz University, Alkharj, 11942, Saudi Arabia^{2,3}

Department of Computer Science, College of Computers and Information Technology
Taif University, P.O. Box 11099, Taif, 21944, Saudi Arabia⁴

Department of Computer Science, Christ (Deemed to be University), Bangalore-29, India⁵

Abstract—Cloud computing has become an essential source for modern trade or market environments by abled frameworks. The exponential growth of cloud computing services in the last few years has resulted in extensive use, especially in storing and sharing the data on various cloud servers. The current trend in the cloud shows that the cloud owners use relative functions and target areas in such a way that cloud customers access or store their data either in the same servers or related servers. Simultaneously, from the security point of view, the lack of confidence about the customer's data on the cloud server is still questionable. The hour's need is to provide the cloud service in a 'single port way' by forming the joint management policy to increase customer satisfaction and profitability. In addition to this, the authentication steps also need to be improvised. This paper discusses issues on the security authentication and access provisioning of the cloud service consumers in federated clouds using subscribed user identity. This work proposes the user identity verification module (UIdVM) in the cloud service consumer's authentication process to serve as a cloud broker to minimize the work overloads on the central cloud federation management system, thus enhancing the cloud security.

Keywords—Security authentication (SA); cloud federation (CF); cloud service provider (CSP); key distribution center (KDC); user identity verification module (UIdVM)

I. INTRODUCTION

Cloud computing is a rapidly growing technology to share/store data on the cloud server in a cost-effective manner (Timely and financial effectiveness). Cloud computing is a distributed-based service to the remote data consumer. Nowadays, cloud computing is used as a significant source and framework for modern trade or market environments. Consumers adapted to the online cloud service buy and sell products, and many of them spend their time accessing and share cloud resources daily. This has also led cloud computing technology to business society. Therefore, any number of people who are business owners prefer cloud services. Cloud computing technology helps enterprises and organizations make computing their resources addressable to the partner and consumer to achieve a more scalable, flexible, competent, and cost-effective circle for application development [1]. Presently, cloud-computing domains (public, private and hybrid clouds) furnish different services to minimize the repairing costs on various cloud services.

As described in [2], the initially formed cloud computing model has reached a high level of evolution, exposure to various extents to settle the primary characteristic of the prototype resource argument, interpose of services, lack of interoperability in data representation, quality of service degradation, and others.

A. Cloud Computing Service Providers (CCSP)

Cloud computing is the panoramic concept in the recent computing technology explained in several ways by many researchers. However, cloud computing is an unspecific term for the transaction of the distributed services in the networked hosts. It provides easy accessibility for the companies to use computing resources (e.g., an application, virtual machine) as a utility rather than developing by their own. In short, cloud computing is accessing/storing programs and data/resources over connected networks as an alternative using an individual hard drive/storage device.

The purpose of 'Cloud Computing Service Providers' (CCSP) is to solve cloud computing problems. These joint CCSPs are formally called cloud federations and are responsible for handling the most critical situations [3]. Cloud federation has been one of the murmuring terms since long when the issue of transacting from users' resources to the remote cloud server was raised. The issue was the transaction through an easy and pervasive way of accessing [4]. Different models have been discussed in this regard; however, cloud computing was built with the dual combinations of the cloud computing deployment model and cloud computing service model.

B. Cloud Computing Service Models

Cloud computing service model is a combination of three services/models. Software as a Service (SaaS) to help in using the cloud applications on consumer devices running on the cloud infrastructure as provided by the respective cloud providers. [5]. Platform as a service (PaaS: which provides platforms to allow the service consumers to develop, run, and control over all the cloud applications by removing the complicated building and maintaining of the cloud infrastructure [6] and thirdly, Infrastructure as a service (IaaS) which is the fundamental resources access provider on the cloud infrastructure. Physical and virtual machines, load balance, virtual storage, etc., are the essential resources availed

*Corresponding Author.

to the end-user through virtualization of the server. IaaS is used to deploy network platforms to provide the consumers with the process, storage, and other basic activities and computing resources. IaaS provides virtually limitless scalability, reduces infrastructure costs, and accelerates time to market [7,8].

C. Deployment Level of Cloud

This model means the mechanism or the ways of lay-outing the cloud structure that seems like on the actual environment. There are three basic types to deploy cloud computing. These are public cloud layout, private cloud layout, and hybrid cloud layout, but the NIST clarified into four as defined in [9]. There is a community cloud in addition to those three listed.

Private cloud: It provides strongly secured services used exclusively by the institution that owns the infrastructure and maintains full control over it. The private cloud infrastructure is planning for alone use by a standalone institution comprising multiple consumers (e.g., business units). It is governed and administrated by single private institutions/units.

Community cloud: is refers to an IT infrastructure owned and shared for collaboration between the group of institutions having common concerns. A community cloud is essential and more beneficial for the community cloud environment. This infrastructure is prepared for alone use by limited ownership of consumers from an institution with mutual concerns.

Fig. 1 and Fig. 2 demonstrate how the public cloud, hybrid cloud, and private cloud interact with the community with their respective service models. Fig. 1 is focused on SaaS, PaaS, and IaaS in terms of their application, platform, and infrastructure.

Public cloud: This cloud is open and accessible for all consumers. The type of clouds will provide the best economies of scale for the users, are inexpensive to set-up because It is open for the broad number of users on the internet. The public cloud is managed, operated, and governed by business, academic, governmental institutions, or by their joint.

Hybrid cloud: it is reasonable and more manageable for the cloud consumer and service provider, making the unity by collectively from two or more than two well-defined cloud infrastructures such as private cloud and community cloud [10].

The union of private and public clouds forms hybrid cloud. A cloud federation is a collective and collaborated cloud organization within agreed interests and common characters of consumers with (1) geographical dispersion, (2) a briefly and clearly defined commercialization system, and (3) federate agreement that governs a collection of independent and heterogeneous clouds. It should be confident enough to furnish impressive resource scalability, guarantee service performance, realize the dynamic distribution of participating resources, and respect end-to-end Service Level Agreement (SLA) established with its clients, as shown in Fig. 2 [11].

Objectives Motivations: The paper's main objective is to perform user authentication in the federated cloud providers using the subscribed user identity to access cloud service consumers' provisioning and maximize their satisfaction while using any cloud services.

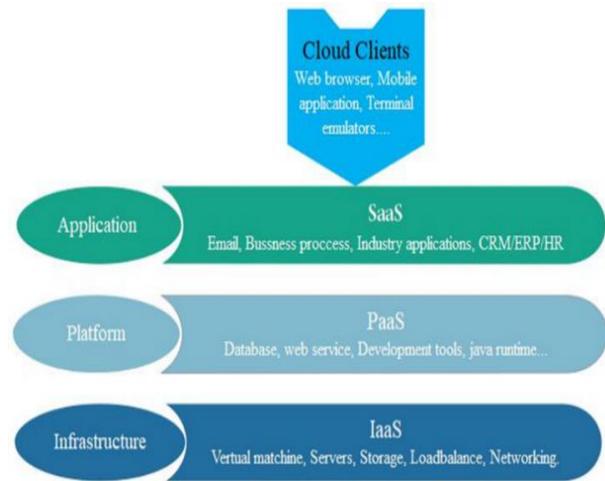


Fig. 1. Cloud Computing Service Models Arranged as Layers in a Stack.

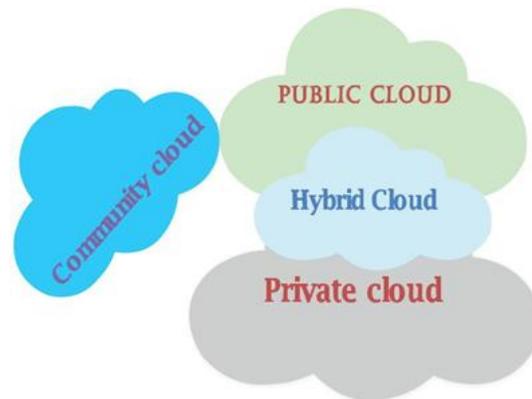


Fig. 2. Cloud Computing Deployment Model.

Many proposals regarding cloud federation are focus on architecture and benefits. There is a good number of works performed by many researchers regarding architecture and structural flows. Several kinds of research have been carried out on security authentication for cloud computing services.

However, in this paper, we aim to point out some sets of limitations. Sorting out these limitations will enhance the security authentication of cloud federation, since cloud federation is a collection of (a) volunteers and (b) 'agreed cloud servers/cloud service providers' who have some common goals to share the services in a central administrator or cloud management. i.e., there are many communications between the cloud federation members and the cloud consumer on the remote side. In this work, we aim to interact with the cloud service providers to resolve this kind of security vulnerabilities, including security authentication.

In this paper, we have calculated the convergence time with respect to a particular range of federation size and showed that the results obtained from our proposed model clearly indicate the effective reduction of the time consumption when the CSCs are using multiple identities to access the resources on multiple CSPs. Our proposed model also gives a dual combination of the cloud computing deployment model and the cloud computing service model.

Our contributions in this work are as follows:

- 1) Its calculated the convergence time wrt a particular range of federation size and show that the proposed model effectively reduces time consumption when using CSCs multiple identities to access various CSPs resources.
- 2) The proposed model gives a dual combination of cloud computing deployment and cloud computing service model.
- 3) Our results prove that time consumption is adequate while accessing the resources.
- 4) Our work proposes a CSP's consumers access provisioning model (algorithm) by which work-overload is reduced on the central management system. i.e. 25 logIn executions are executed in 3115 milliseconds (Fig. 10).

The rest of the paper is organized in the following order. Section 2 gives a background study about related work. Section 3 consists definitions of basic components that are involved in the cloud federation management system. In Section 4 the contribution of our proposed work is discussed. Section 5 has result and discussions. Finally, Section 6 concludes the paper and future scope.

II. BACKGROUND STUDY

Many works related to cloud computing security and cloud federation identity management and security authentication have been published. The related papers that are relevant to our paper are discussed as follows selectively. Several researchers examine and determine the characteristics of cloud federation to formalize it. The author of [3] describes the cloud federation as an intentional pooling of heterogeneous clouds running cooperatively to share idle resources contained in their domains and presents the cloud federation properties. These [1] allows the cloud server in the federation to automatically spread out resources to satisfy themselves, have high promotional opportunities of their resources to the remote cloud service consumers in the environment and to be highly competent in the modern market system, permit the clouds to offer idle resources and stakeholders to use the resources, and deliver services with defined requirements in service level agreement (SLAs).

A. Authentication and Authorization

A user centric approach, [12] provides a solution for the cryptographic process. In [13], paper discussed about the approval as well as responsibility of trust model. FermiCloud [14] followed the different protocol for the model but it took longer process of certification. In [15] given the idea, how to manage the cloud complexity with the help of software application. The different access control facilities are followed in the [16] model.

B. Unique Key Access

In [17] discussed about how to identify the unique cloud properties and manage those properties for the use of third parties. Stihler et al. [18] token methodology for the secure level of services. In the paper [19] given the two different authentication of encrypt the data and digital sign of the process. The paper [20], cloud storage system support for public users with the identity proof. The [21,22] proposed

different architecture for managing the cloud. In [23] followed the x and y access implementation virtual softwares.

C. Confidentiality, Integrity, and Availability

Santos et al. [24] extend the Terra [25] followed the different level of implementation in the virtual storage of infrastructure and different level of services. They discussed about the various methodology and procedure for accessing the stored information. Popa. et.al to access the group of data from the cloud. In [26], they also followed the fuzzy techniques for utilize the cloud resources. The author explained about the threats in cloud server, how to manage with open source application [27]. In [28], followed the supervisor techniques for remote controlling the procedures. The synchronize response of cloud and protocols are followed in the virtual cloud [29].

D. Security Policy Management

In [30] studies the cloud federation security issues about managing and controlling the access of an authorized party. It proposes a federated access control model (FACM) in which a third party, like a cloud service broker (CSB), is used. On the other hand, authors in [31] and [13] describe the federated cloud's benefits over the single cloud service briefly. They described from the user and cloud service provider's perspective and listed benefits for the cloud federation, which are highly scalable and flexible to enable the cloud providers to cost-effectively or cost-efficiently adjust their hosting capacity through cooperation with other single clouds. It shows the federated clouds relation and authentication. Still, it does not show how the remote cloud service cloud consumers can be authenticated to access the federated clouds on their proposed cross-cloud federation.

On the other hand, in cloud federation, the cloud consumers can retrieve services from different service providers without requiring multiple authentication processes using SSO techniques [32], [14].

Amazon cloud service provides a wonderful and robust secured service in the world [33][34]. Still, it does not make federated clouds in the market system with the other cloud service providers which are in working on related discipline (online shopping). According to [1], [9], [14], [17], cloud federation has various mutual benefits for the cloud service providers to use other service providers' infrastructures and/platforms based on their agreement. It is beneficial for both service providers and service users to efficiently and cost-effectively provide and consume cloud resources [35][36]. The federated clouds should authenticate themselves in the cross-cloud federation because cloud security is the responsibility of cloud service consumers and cloud service providers [4]. In the federated clouds, the cloud service consumers (CSC) should access the federated clouds using subscribed user Identity.

Conclusion of the background study/related works: The studies done in this section conclude that though most of the work published explores the possibility of the new features, they only discussed the benefits/advantages of cloud service providers in the federated clouds. The works that are analysed in the literature clearly mention that cloud service customers and cloud consumers are categorized into two segments, and cloud customers can get access provision in the federated

clouds. However, the cloud consumers possess denied access using the single cloud accounts in the federated clouds.

III. PREREQUISITES / DEFINITIONS

Components: The following are the basic components that are involved in the cloud federation management system. Here Cloud Federation Central Management System/Key Distribution Center (CFCMS/KDC) depicts the central management of the federated cloud and governs all over the transaction between cloud service providers (CSPs). It has all information about the federated clouds that agree to implement their communications in the cloud federation. We have used KDC instead of CFCMS as the alternative name, but not an abbreviation form. We have also used KDC instead of CFCMS in the designed algorithm.

UidVM: is the User identity Verification Module installed between cloud service consumers and cloud service providers because it acts as a mediator between the CSP and CSC. It registers the (cloud service consumers passcode) CSCpc MainDataCen-terId to make the connection between CSCs and CSPs. It creates healthy, safe, and fast communication between the CSCs and CSPs.

CSP: It is the cloud service provider federated in the cloud and governed under the cloud federation rule and provides the service to cloud service consumers.

CSC: is the cloud service consumer that accesses the provided data from the service providers.

CSCpc: The cloud service consumer's passcode is generated from the central system and verified by UidVM to get cross access permission.

The activities of cloud providers can be divided into various categories: Implementation support, utilize the resource, maintain the support, and protection.

The protection feature necessary for cloud providers' activities are described in Table I [11].

TABLE I. SECURITY AND PRIVACY FACTORS OF THE CLOUD PROVIDERS

Security Context	Description
Approval and Verification	These process of cloud identification schemes are followed.
Management of Authenticity and Availability	Heterogeneous techniques are followed in the service.
Secrecy, authenticity, and accessibility	Trying to assure the secrecy of data objects, enabling factors accounted, and making sure that assets are available if needed.
Observing and Issue Resolution	The cloud infrastructure is constantly monitored to ensure adherence with consumption data protection and auditor's report.
Strategy Administration	Creating and making regulations for concrete behaviors such as monitoring or conformity evidence.
Privacy	To protect the identification information for the cloud.

Prerequisites: Currently, cloud computing has been leading almost all business, education, and social communications. Many public and private organizations and institutions are connected through the internet, sharing and storing their data in the cloud. The cloud users may use one of these public, private, hybrid, and community clouds or others that they may create depending on their organization's infrastructure. In short, various sectors (e.g., educational, health, communications, military, etc.) are now become cloud service dependent.

The fundamental issue of cloud computing is that its security management system and ownership issues are complained about by the cloud service consumer. For solving these issues, the cloud is classified into the public cloud, private cloud, and hybrid cloud. On the other hand, community clouds have a long history with the emerging of cloud computing.

Recently inter-cloud, cloud federation, and other cloud infrastructure models have emerged. Whatever it is, our focus is cloud federation, which is one of the recent cloud models. Cloud federation is the best solution to reduce the infrastructure building cost, the increase business relationship between the cloud providers, the availability and accessibility of the cloud providers, etc.

Current Troubles of cloud federation: Even-though, cloud federation has several benefits and advantages for a cloud service provider, there are challenges and troubles raised by the cloud service consumers and cloud providers. As our survey and observation, we have listed below.

Security issue: Accessing and sharing of the data is still a questionable issue.

Load balancing: The cloud federation architecture can be designed in such a way that the central cloud federation server does more workload on the central cloud federation management system. More workload also leads to high traffic, and the server becomes slow to send or respond to the cloud service provider. Therefore, minimizing the central system workload is one of the critical issues for fast service.

LogIn steps: Today, users prefer fast-track accessing methods. Users of Cloud service consumers want the short and secure step to access online services (Cloud services). But, currently, the provisional service procedure has very boring and continuous steps to permit the service consumer to access the cloud resources. Therefore, this paper aims to shorten and remove such continuous steps of Cloud service provision (LogIn) for the cloud service consumer to access the cloud services.

Inclusion of the third intermediary: There is a need to include the cloud service consumer for authenticated access to share the services' benefits by minimizing multiple processes of login and accessing the data using the subscribed login accounts in the federated clouds.

IV. PROPOSED MODEL

Our proposed model has used the data to depict the cloud federation's various characteristics on both sides (cloud service provider and cloud service consumer). The simulations are carried out in CloudSim. Referring to recently published works [12], [14], we see that it is very difficult to perform actual/real-time experiments and implement new algorithms and technologies in actual cloud infrastructure. Therefore, we measured performance implementation first.

A. Proposed Model Motivation

Currently, many organizations and institutions are organized in a single group to form the cloud federation. From the perspective of cloud consumers, the need to use cloud resources is increasing. Still, some business cloud service providers (e.g., online shopping) don't have an agreed federated cloud system to access their customer's permission to use the subscribed account in the federated cloud. The online shopping companies' common goals are available and accessible to the online purchasers, and online purchasers also want to access and buy the product using their subscribed user account in the federated clouds. Therefore, our motivation is to reconcile that the CSP's need and CSC's need by proposing how the CSPs and CSC are authenticating each other using subscribed Identity in the federated clouds to assure the security between CSPs and CSCs.

B. Proposed Security Authentication

The cloud federation requires two sets of (improved) proposed rules, Service Level Agreement (SLA) [23], and Regional Service Condition Agreement (RSCA) [21]. SLA sets on the cloud federation central management system and agreed by the cloud service providers to govern all the interactions and resource sharing conditions between the CSPs. On the other hand, there may be a high load of CSC's service requests, which leads to work overload on the central system. RSCA handles this issue, and it is installed in the cloud federation central management system (CFCMS).

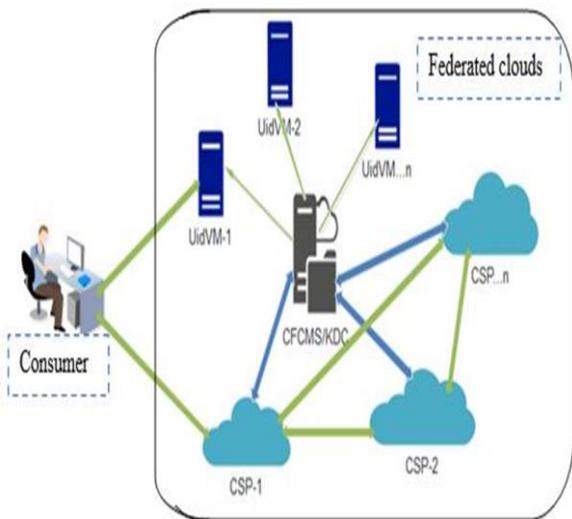


Fig. 3. Proposed Cloud Federations Architecture.

Security Authentication: It is performed between the cloud service consumers and cloud service providers. The cloud service consumers with cloud service providers through KDC and User Identity Verification Module (UIdVM), if it is cross-cloud service in the federated clouds, and cloud service providers each other through CFCMS using the Cloud Federation Security Authentication Key Distribution Center. All cloud service consumers and cloud service providers' information related to security authentication is registered on UidVM. All the agreement documents between the service providers and the regional code are placed on the cloud federation central management system (CFCMS) called the Key Distribution Center (KDC) that directs the user verification to different modules connected to the KDC. Fig. 3 shows the proposed cloud federations authentication architecture, and Fig. 4, the general diagram for CF authentication. Both Fig. 3 and Fig. 4 show the general flows that how users and providers' security authentication is performed).

C. Cloud Service Provider Authentication

Cloud service provider authentication is performed on cloud service providers to use the shared resources in the cloud federation infrastructure according to their agreement and authentication. They perform through a cloud federation central management system using a key distribution center to verify that the cloud server is registered or not in the federation. As shown in Fig. 4, when the authentication is performed, the following steps apply sequentially.

The cloud service provider sends the request to the cloud federation central management system or KDC. Cloud federation central management system verifies the cloud service provider's membership and other conditions based on the federation agreement.

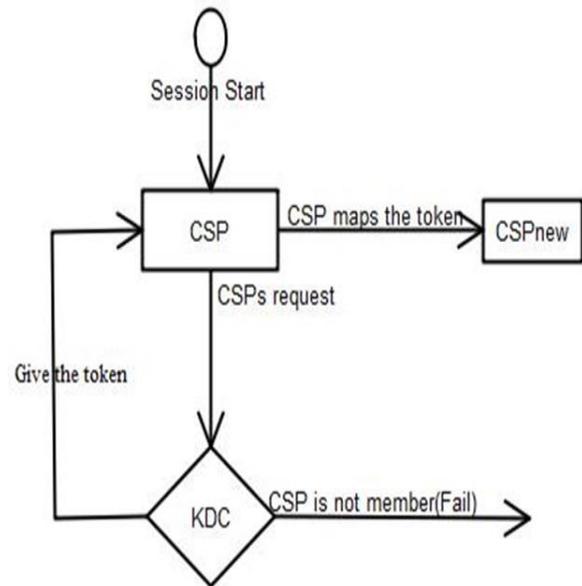


Fig. 4. State Diagram for Cloud Service Providers Authentication.

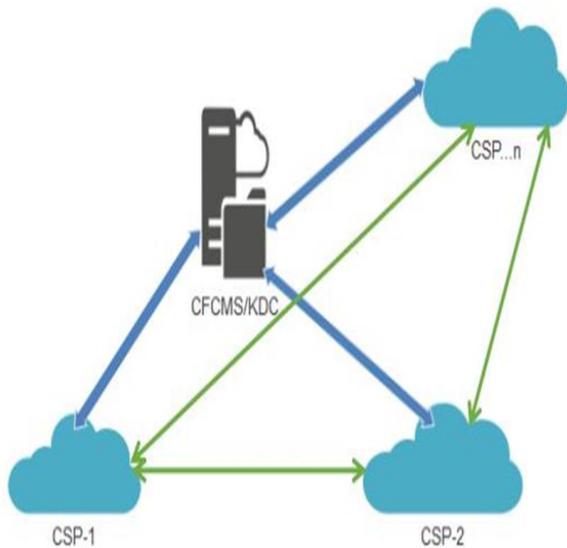


Fig. 5. The Process of Cloud Service Providers Authentication.

A cloud service provider gets permission and starts to access all resources regarding to the federation members' security agreement. As depicted in Fig. 5, cloud service consumer/user authentication is performed through a cloud federation central management system using a key distribution center. It helps the cloud service consumers access the federated clouds with a subscribed identity in any one of the federated clouds. Fig. 6 gives more insight details/highlights. When the authentication is performed, the following steps are applied sequentially.

(Note: Cloud service provider is a single cloud server owner that provides the service to the remote cloud service consumers).

Step 1: Cloud service consumer is a remote cloud service user/consumer that provides by the cloud service provider.

Step 2: Consumer/user sends the service request to the cloud service provider (to one of the federated clouds that the consumer has a registered account).

Step 3: Cloud service provider server verifies the user is registered or has an account.

Step 4: Cloud service provider gives access permission to the user on its own server. But, if the user wants to access other service providers (cross-service), then.

Step 5: User request to KDC to get the cross permission for another service provider's server through the current CSP, which is the user already registered.

Step 6: KDC sent the user's request to the UidVM after verifying the incoming request region.

Step 7: UidVM verifies the user and gives the token to the user to access other service providers in the federation.

Step 8: User maps the token to another cloud service provider server.

Step 9: User gets access to all federated clouds with the Subscribed login account.

D. Algorithm 1: Access Provision for Cloud Service Consumer

The following algorithm initializes every cloud service consumer and checks if these consumers are previously registered in the cloud or not. For registered consumers, access provisioning is checked by analyzing the CSC request. Based on this analysis, the grant of local permission or global permission is availed. Else, the access provisioning is denied. This enhances the convergence time and reduces the time consumption in the particular federation size.

```
1 Initialize: (CSC=Cloud Service Consumer, CSP=Cloud Service Provider)
2 do
3   if (CSC CSP) Check that if csc has registered account in csp or not exist.
4   if CSC have registered account in CSP then local controller analyses the CSC request, that if it is local access permission request or global(to another csps)
5   (CSC CSP) // if request is local, then CSP gives access permission to CSC
6   while
7   CSC CSP // here CSC does not exist in CSPs database that is why CSC is now denied the access permission
8   end
```

E. Algorithm 2: Cross Access Provisions for CSCs

Algorithm 2 maintains the central repository for each member and checks their validity. If membership is valid, then the access is provisioned to the member, thus allowing the member to enter into the cloud (cloud federation). These members are now mapped with the new resources and compare the clouds' utilization, whether they are overloaded or not or crossing the allocated time frame. If any of these occur, the member is allowed to access the cloud federation to reduce the overload.

```
1 Initialize: (CSC=Cloud service consumer, CSP=cloud service provider, UidVM=User identity Verification module, KDC=key distribution center, CSPn=new cloud service provider,
2 do
3   for (CSP 2 KDC) // Central management system check CSPs membership.
4   UidVM KDC//after checking the csp membership and sign, KDC give the access permission to CSP)
5   for (CSCpc 9 UidVM) // check the CSCPS in UidVM or not exist
6. UidVM// if CSCPC is exist in UidVM then UidVM give the token to CSC
7. CSC // CSC maps to the new CSP for resources.
8   while
9   CSP 2= KDC // Cross access provision is continued until CSP is
leave from the federation membership.
10  CSCPC @ UidVM// Cross access provision is continued through the federated clouds until CSCPC is EXIST in UidVM.
11  end
```

F. Algorithm 3: Load Balancing

Algorithm 3 calculates the execution time to handle the idle UidVM. A central management system can identify the idle or less loaded UidVM when calculating the on-progress tasks corresponding to the number of UidVM.

1 Initialize: (Initialize: How CFCMS calculate and identify the less loaded UidVM.

Let, number of on progress user request (nopur) =g, number of UidVM=h, UidVM= f, and number of waiting user request (nwur) =e. (g=nopur, h=nUidVM, e=nwur, f=UidVM.

(Please refer the short note above)

```

2 do
3 for (f < g/h)
4 f e // Assign the next waiting task to UidVM.
5 while
6 f > g/h
8 end
    
```

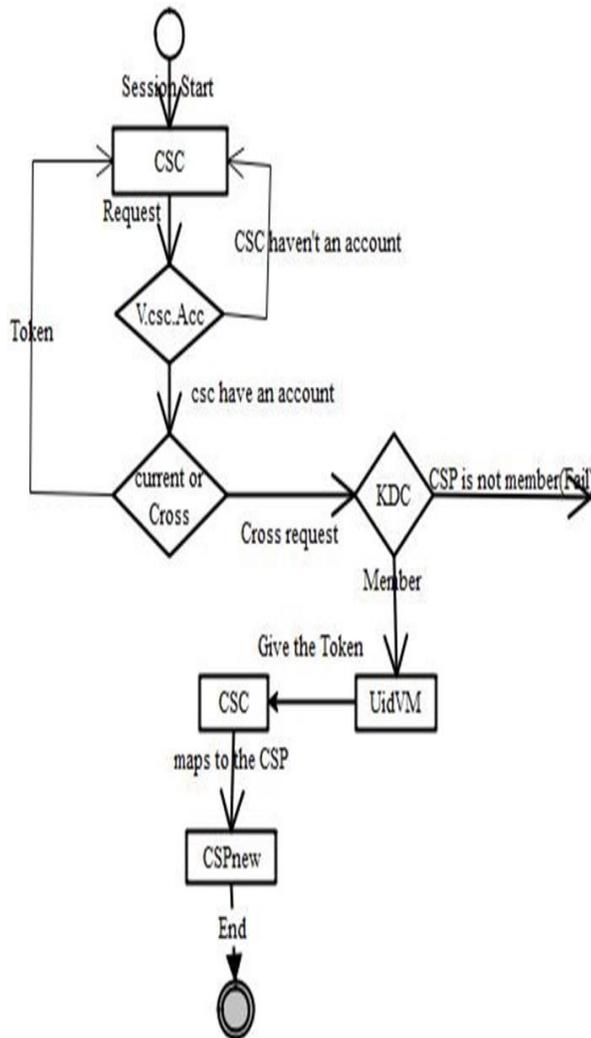


Fig. 6. State Diagram for Cloud Service Consumer/User Authentication.

Table II compares the proposed model with previously proposed models with respect to the three parameters Overload, Insurance, and access provisioning. Table II shows that previously published work is basically focused on ensuring the federated cloud security, assuring CSCs benefits, whereas, in our proposed model, we have illustrated by implementing subscribed identities to access the cloud resources from multiple cloud service providers. And from the results (Fig. 7, Fig. 8, Fig. 9, and Fig. 10), we can observe the effective reduction of the time consumption when the CSCs are using multiple identities to access the resources on multiple CSPs; i.e., our paper not only ensures or assures but validates them.

TABLE II. COMPARISON OF OUR PROPOSED MODEL WITH PREVIOUSLY PROPOSED MODELS

Factors/parameters	Proposed model	Existing scenarios
Overload	<ul style="list-style-type: none"> - identifies an idle module - calculates the time duration of each task, and then it reduces the idle UidVM. - Therefore, reduction of work overload on the central management system is effective and better ever 	<ul style="list-style-type: none"> - In [32], idp (identity provider) is responsible for identifying all the incoming requests - gives privileges according to their legal information. - As a result, it leads to high work overload on Idp.
Insurance	<ul style="list-style-type: none"> - Ensuring the security of the federated cloud through KDC and UidVM, including removal of duplicate data 	<ul style="list-style-type: none"> - Ensure security by removing the duplicating data (only) on the cloud server database [12]
Access provisioning	<ul style="list-style-type: none"> - Tries to assure the CSCs benefits in the federated clouds and threats them equally with the CSPs. 	<ul style="list-style-type: none"> - More focus on the benefits of cloud service providers rather than the CSC regarding access provisioning. - It doesn't work with other Cloud service providers [4], (example, online shopping)

V. RESULT AND DISCUSSION

We now compare our work with the most recent works that has been published recently as Table III.

Based on all the algorithms and the results obtained, we observe that.

1) Cloud service consumers can access the cloud resources using their subscribed id without any other requirements for each of CSPs in the federated clouds. This reduces the execution time when multiple users are using in the cloud federation considerably.

2) Work-overload is reduced on the central management system. Fig. 10 shows that 25 login executions are executed in 3115 milliseconds. That means the CFCMS can make communication and verification without any overload in around 3 seconds.

TABLE III. COMPARISON WITH RECENT WORKS

Year	Outcomes	Outcome of our proposed work
2017 [20] S.Ye, H. Liu, Y.-W. Leung, and X. Chu et. al.	<ul style="list-style-type: none"> - Used ADL to access the Cloud service - No subscribed id used - Reduction in the execution time is very low as they have used a software-defined technique (ADL) and the code complexity is high. - No discussion on multiple users where it is evident that in today's scenario, a cloud is hit by multiple users in practical it goes up to trillion hits in a minute 	<ul style="list-style-type: none"> - No requirements for each of CSPs in the federated clouds. - Reduced execution time
2017 [21], Katakam Srinivasa Rao et.al.	<ul style="list-style-type: none"> - Collective motion is a fundamental operation of robot swarms - A group of Reinsurance emulated Collaboration Mechanism in Cloud Federation is defined - Doesn't yield out the execution time - No reduction in the cloud performance evaluated - Cloud federation is discussed in detail, but no subscribed ID has been used to evaluate cloud computing time. 	<ul style="list-style-type: none"> - No requirements for each of CSPs in the federated clouds. - Reduced execution time

We, therefore, conclude that

- 1) CSP consumers have a high access provision.
- 2) The execution time is reduced, when multiple users are using cloud federation.
- 3) Efficient reduction in the work overload with 25 logins that too in 3115 milliseconds, as in Fig. 10.
- 4) Also, CFCMS communication and verification (without any overload) is in around 3 seconds.

The comparative results are depicted in Fig. 7, Fig. 8, and Fig. 9.

Fig. 7 shows an Efficient Reduction in the work overload with 25 logins that too in 3115 milliseconds. There is an efficient reduction in the execution time when multiple users are using in the cloud federation.

In Fig. 8, the federation size is evaluated from 2. We see that the convergence time is very high at each and every federation size for various work overloads. In this case, also, reduction is efficient and the work overload is attempted at minimal logins with minimal time.

Fig. 9 shows that each cloud service consumer's convergence time has maximal access to the cloud resources at every federation size. For this, we have performed extensive use of the data in cloud storage to save bandwidth and minimize the storage space. Again, there is a reduction in the execution time when multiple users are using in the cloud federation without any need for data deduplication authorization.

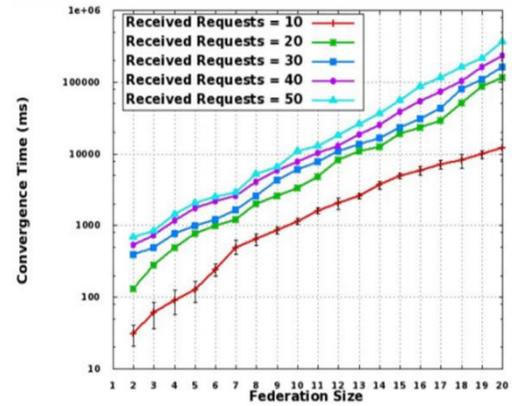


Fig. 7. Comparative Analysis with Katakam Srinivasa Rao vs. the Proposed Work.

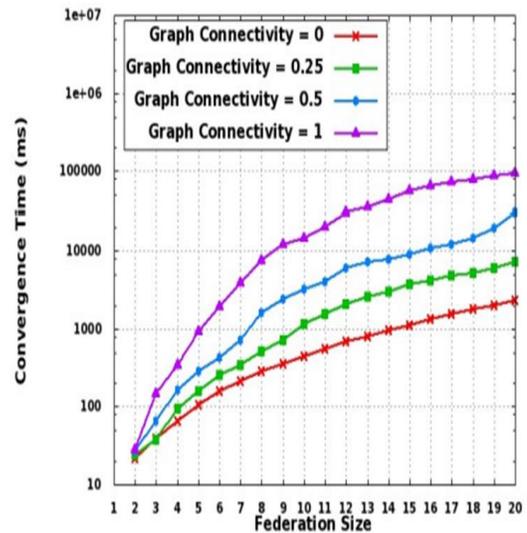


Fig. 8. Comparative Analysis with S.Ye, H. Liu, Y.-W. Leung, and X. Chu VS. our Proposed Work.

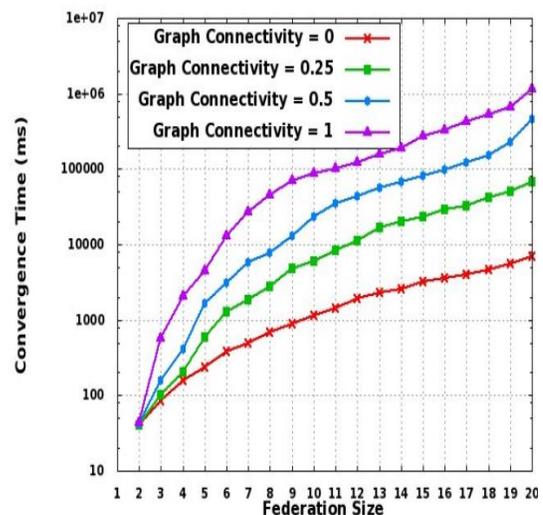


Fig. 9. Comparative Analysis with Vo, Tri Hoang, Woldemar Fuhrmann, Klaus-Peter Fischer-Hellmann, and Steven Furnell vs. the Proposed Work.

ACKNOWLEDGMENT

We thank the Deanship of Scientific Research, Prince Sattam Bin Abdulaziz University, Alkharj, Saudi Arabia for help and support.

TABLE IV. LIST OF ACRONYMS AND ABBREVIATIONS

SLA	Service Level Agreement
CSC	Cloud service Consumer
CSP	Cloud Service provider
CSCpc	Cloud Service Consumers pass-code
RSCA	Regional Service Condition Agreement
CFCMS	Cloud Federation Central Management System
UidVM	User identity Verification Module
KDC	Key Distribution Center
CF	Cloud Federation
nopur	number of on progress user request
nwur	number of waiting user request
UidVM	number of user identity Verification module

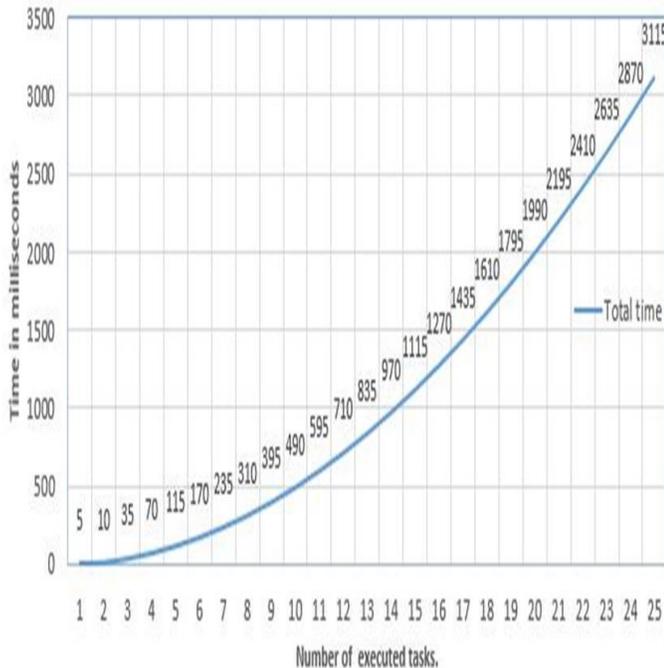


Fig. 10. Execution Time of user Login in the Cloud Federation.

Fig. 10 calculates the execution time to handle the idle UidVM. We have used the number of the on-progress user request (nopur), number of UidVM, and the number of waiting for user request (nwur). The central management system can identify the idle or less loaded UidVM when calculating the on-progress tasks corresponding to the number of UidVM, as described in Algorithm 3.

VI. CONCLUSION

Global communication has been dealing with one of the major issues – cloud services in terms of security and easy use. To resolve these types of cloud services consumers' complements, the researcher promotes the cloud federation. Cloud federation proposed in this work has resolved the issues mentioned earlier by reducing an execution time and a number of waiting users, and enhancing user request progress. The proposed system has proven that the central management system can identify the idle or less loaded UidVM when calculating 'on progress' tasks corresponding to the number of UidVM, as described in Algorithm 3. This is illustrated by implementing subscribed identities to access cloud resources from multiple cloud service providers. Results clearly indicate the effective reduction of the time consumption when the CSCs use multiple identities to access the resources on multiple CSPs.

Based on all the algorithms and the results obtained are (a) subscribed id is sufficient to access the service without the federated clouds thus reducing the execution time; (b) The work-overload is reduced on the central management system. Fig. 10 shows that 25 LogIn executions are executed in 3115 milliseconds.

REFERENCES

- [1] E. U. Directive, "95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of such Data," Official Journal of the EC, vol. 23, 1995.
- [2] U. States., "Health insurance portability and accountability act of 1996 [micro form] : conference report (to accompany h.r. 3103)." <http://nla.gov.au/nla.catvnl4117366>, 1996.
- [3] S. Pearson, "Privacy, security and trust in cloud computing," in Privacy and Security for Cloud Computing (S. Pearson and G. Yee, eds.), Computer Communications and Networks, pp. 3–42, Springer London, 2013. Computer Science & Information Technology (CS & IT) 147\.
- [4] R. Pike, D. Presotto, K. Thompson, H. Trickey, and P. Winterbottom, "The use of name spaces in plan 9," SIGOPS Oper. Syst. Rev., vol. 27, pp. 72–76, Apr. 1993.
- [5] Zamani AS, Akhtar MM, Ahmad S. Emerging cloud computing paradigm. International Journal of Computer Science Issues (IJCSI). 2011 Jul 1;8(4):304.
- [6] D. Bigo, G. Boulet, C. Bowden, S. Carrera, J. Jeandesboz, and A. Scherrer, "Fighting cyber crime and protecting privacy in the cloud." European Parliament, Policy Department C: Citizens' Rights and Constitutional Affairs, October 2012.
- [7] M. Y. uddin and S. Ahmad, "A Review on Edge to Cloud: Paradigm Shift from Large Data Centers to Small Centers of Data Everywhere," 2020 International Conference on Inventive Computation Technologies (ICICT), 2020, pp. 318-322, doi: 10.1109/ICICT48043.2020.9112457.
- [8] Jha, Sudan, Prashar, Deepak, and Elngar, Ahmed A. 'A Novel Approach Using Modified Filtering Algorithm (MFA) for Effective Completion of Cloud Tasks'. 1 Jan. 2020 : 8409 – 8417.
- [9] P. Mell and T. Grance, "The NIST Definition of Cloud Computing," tech. rep., July 2009.
- [10] D. Bernstein, "Containers and Cloud: From LXC to Docker to Kubernetes," IEEE Cloud Computing, vol. 1, no. 3, pp. 81-84, 2014.
- [11] NIST Special Publication 500–291 version 2, NIST Cloud Computing Standards Roadmap, July 2013, Available at <http://www.nist.gov/itl/cloud/publications.cfm>.
- [12] L. Zhou, V. Varadharajan, and M. Hitchens, "Integrating trust with cryptographic role-based access control for secure cloud data storage," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 560–569, July 2013.

- [13] R. Banyal, P. Jain, and V. Jain, "Multi-factor authentication framework for cloud computing," in Computational Intelligence, Modelling and Simulation (CIMSIM), 2013 Fifth International Conference on, pp. 105–110, Sept 2013.
- [14] H. Kim and S. Timm, "X.509 authentication and authorization in fermi cloud," in Utility and Cloud Computing (UCC), 2014 IEEE/ACM 7th International Conference on, pp. 732–737, Dec 2014.
- [15] N. Mimura Gonzalez, M. Torrez Rojas, M. Maciel da Silva, F. Redigolo, T. Melo de Brito Carvalho, C. Miers, M. Naslund, and A. Ahmed, "A framework for authentication and authorization credentials in cloud computing," in Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on, pp. 509–516, July 2013.
- [16] B. Tang, R. Sandhu, and Q. Li, "Multi-tenancy authorization models for collaborative cloud services," in Collaboration Technologies and Systems (CTS), 2013 International Conference on, pp. 132–138, May 2013.
- [17] M. A. Leandro, T. J. Nascimento, D. R. dos Santos, C. M. Westphall, and C. B. Westphall, "Multitenancy authorization system with federated identity for cloud-based environments using shibboleth," in Proceedings of the 11th International Conference on Networks, ICN 2012, pp. 88–93, 2012.
- [18] M. Stihler, A. Santin, A. Marcon, and J. Fraga, "Integral federated identity management for cloud computing," in New Technologies, Mobility and Security (NTMS), 2012 5th International Conference on, pp. 1–5, May 2012.
- [19] H. Li, Y. Dai, L. Tian, and H. Yang, "Identity-based authentication for cloud computing," in Cloud Computing (M. Jaatun, G. Zhao, and C. Rong, eds.), vol. 5931 of Lecture Notes in Computer Science, pp. 157–166, Springer Berlin Heidelberg, 2009.
- [20] S. Ye, H. Liu, Y.-W. Leung, and X. Chu, Reinsurance-Emulated Collaboration Mechanism in Cloud Federation, 2017 IEEE.
- [21] Rao, K. S. (2016). A Survey on Authorized Deduplication Techniques in Cloud Computing. International Journal of Engineering Science, 2102.
- [22] Vo, Tri Hoang, Woldemar Fuhrmann, Klaus-Peter Fischer-Hellmann, and Steven Furnell. "Identity-as-a-Service: An adaptive security infrastructure and privacy-preserving user identity for the cloud environment." Future Internet 11, no. 5 (2019): 116.
- [23] E. Carlini, M. Coppola, P. Dazzi, L. Ricci, and G. Righetti, "Cloud federations in contrail," in Euro-Par 2011: Parallel Processing Workshops (M. Alexander, P. D'Ambra, A. Belloum, G. Bosilca, M. Cannataro, M. Danelutto, B. Di Mar tino, M. Gerndt, E. Jeannot, R. Namyst, J. Roman, S. Scott, J. Traff, G. Vallée, and J. Weidendorfer, eds.), vol. 7155 of Lecture Notes in Computer Science, pp. 159–168, Springer Berlin Heidelberg, 2012.
- [24] J. Gouveia, P. Crocker, S. Melo De Sousa, and R. Azevedo, "E-id authentication and uniform access to cloud storage service providers," in Cloud Computing Technology and Science (CloudCom), 2013 IEEE 5th International Conference on, vol. 1, pp. 487–492, Dec 2013.
- [25] G. Dreo, M. Golling, W. Hommel, and F. Tietze, "Iceman: An architecture for secure federated intercloud identity management," in Integrated Network Management (IM 2013), 2013 IFIP/IEEE International Symposium on, pp. 1207–1210, May 2013.
- [26] N. Santos, K. P. Gummadi, and R. Rodrigues, "Towards trusted cloud computing," in Proceedings of the 2009 Conference on Hot Topics in Cloud Computing, HotCloud'09, (Berkeley, CA, USA), USENIX Association, 2009.
- [27] T. Garfinkel, B. Pfaff, J. Chow, M. Rosenblum, and D. Boneh, "Terra: A virtual machine-based platform for trusted computing," in Proceedings of the Nineteenth ACM Symposium on Operating Systems Principles, SOSP '03, (New York, NY, USA), pp. 193–206, ACM, 2003.
- [28] R. A. Popa, J. R. Lorch, D. Molnar, H. J. Wang, and L. Zhuang, "Enabling security in cloud storage slas with cloudproof," in Proceedings of the 2011 USENIX Conference on USENIX Annual Technical Conference, USENIX ATC'11, (Berkeley, CA, USA), pp. 31–31, USENIX Association, 2011.
- [29] D. Perez-Botero, J. Szefer, and R. B. Lee, "Characterizing hypervisor vulnerabilities in cloud computing servers," in Proceedings of the 2013 International Workshop on Security in Cloud Computing, Cloud Computing '13, (New York, NY, USA), pp. 3–10, ACM, 2013.
- [30] J. Sendor, Y. Lehmann, G. Serme, and A. Santana de Oliveira, "Platform level support for authorization in cloud services with oauth 2," in Proceedings of the 2014 IEEE International Conference on Cloud Engineering, IC2E '14, (Washington, DC, USA), pp. 458–465, IEEE Computer Society, 2014.
- [31] U. S. F. Law, "Right to financial https://epic.org/privacy/rfpa/, 1978. privacy act of 1978."
- [32] F. Liu, J. Tong, J. Mao, R. Bohn, J. Messina, L. Badger, and D. Leaf, NIST Cloud Computing Reference Architecture: Recommendations of the National Institute of Standards and Technology (Special Publication 500-292). USA: CreateSpace Independent Publishing Platform, 2012.
- [33] "Hypervisors, virtualization, and the cloud: Learn about hypervisors, system virtualization, and how it works in a cloud environment." Retrieved June 2015.
- [34] Ahmad S, Afzal MM. A Study and Survey of Security and Privacy issues in Cloud Computing. International Journal of Engineering Research & Technology (IJERT), ISSN: 2278-0181, Vol. 6 Issue 01, January-2017. <http://dx.doi.org/10.17577/IJERTV6IS010311>.
- [35] Uddin MY, Ahmad S, Afzal MM. Disposable Virtual Machines and Challenges to Digital Forensics Investigation. International Journal of Advanced Computer Science and Applications (IJACSA), 12(2), 2021. <http://dx.doi.org/10.14569/IJACSA.2021.0120299>.
- [36] Ahmad S, Afzal MM. Deployment of Fog and Edge Computing in IoT for Cyber-Physical Infrastructures in the 5G Era. In International Conference on Sustainable Communication Networks and Application 2019 Jul 30 (pp. 351-359). Springer, Cham.

Local Frequency Descriptor and Hybrid Features for Classification of Brain Magnetic Resonance Images using Ensemble Classifier

Shruthi G¹, Krishna Raj P M²

Department of Information Science and Engineering
M S Ramaiah Institute of Technology, Bangalore-560054, Karnataka, India

Abstract—A brain tumor is an irregular development of cells in the human brain that causes problems with the brain's normal functionalities. Early detection of brain tumor is an essential process to help the patient to live longer than treatment. Hence in this paper, a hybrid ensemble model has been proposed to classify the input brain MRI images into two classes: brain MRI images having tumor and brain MRI images with no tumor. The hybrid features are extracted by analyzing the texture and statistical properties of brain MRI images. Further, the Local Frequency Descriptor (LFD) technique is employed to extract the prominent features from the brain tumor region. Finally, an ensemble classifier has been developed with the combination of Support Vector Machine (SVM), Decision Tree (DT) and K-Nearest Neighbour (KNN) technique to successfully classify the brain MRI images into brain tumor MRI images and non-tumor brain MRI images. The proposed model is tested on the Kaggle brain tumor dataset and the performance of the method is evaluated in terms of accuracy, sensitivity, specificity, precision, recall and f-measure (f1 score-harmonic mean of precision and recall). The results show that the proposed model is promising and encouraging.

Keywords—Brain tumor; hybrid features; local frequency descriptor (LFD); ensemble classifier

I. INTRODUCTION

The brain tumor is developed due to the abnormal cell growth in the brain. To identify the brain tumor, two imaging modalities are extensively used such as Computed Tomography (CT) and Magnetic Resonance Imaging (MRI). Where MRI is less harmful to the human tissues as compared to CT and also it gives detailed visualization of the internal structure of the brain.

The brain tumor classification models are categorized into Machine Learning (ML) and Deep Learning (DL) techniques. Feature selection and extraction processes are extensively used in ML approaches for classification and to achieve good accuracy even on a small dataset, which consumes less computational time. On the other hand, DL methods extract and learn the features from an image directly with a large dataset. Hence in this proposed work, the conventional hybrid features and ensemble classifiers are designed for the effective classification of tumor and non-tumor brain MRI images. Texture, statistical and descriptor features are combined as hybrid features for effective analysis of tumor region. SVM [1,2], KNN [1], and DT [3,15] and have been ensemble for

accurate classification of tumor and non-tumor brain MRI images. The KNN needs less computation time with limited storage space and DT considers all possible consequences of a decision with following each direction to its end. SVM is mainly used in the two-class problem, which takes the labelled information from both the classes to produce a model file that can be used to categorize the new unlabelled or labelled information. Overall in this research, a hybrid ensemble classifier is used to boost the precision of the findings. A comparison of SVM, KNN, DT and the proposed hybrid ensemble classifier is also presented.

The remaining sections of the paper are structured as follows. The literature review is explained in Section 2, the proposed model for classifying brain MRI images as tumor or non-tumor is illustrated in Section 3. The classification analysis is discussed in Section 4. Section 5 outlines the experimental analysis of the proposed model and finally, Section 6 concludes the proposed work with future contributions.

II. LITERATURE SURVEY

Detecting a brain tumor is a time-consuming and complex process due to an intensity inhomogeneity, tissue overlap, and a lack of clear boundary differentiation between tumor and non-tumor brain regions. Over the years, several research works have been carried out by various researchers in the field of brain tumor detection and classification.

In [1] the authors have proposed a model for classifying brain MRI images by applying the GLCM technique for texture features and classification is achieved using supervised SVM and KNN algorithms. In [2] the authors have applied morphological function, anisotropic diffusion filter, Discrete Wavelet Transform (DWT) and SVM for classifying the brain MRI images. In [3] the authors have implemented Convolution Neural Network (CNN), Radial Basis Function (RBF) and Decision Tree (DT) for classifying brain MRI images. In [4] authors have implemented a novel approach for edge detection in two steps F-test for identifying the pixel variations and T-test based on contrast function which observes the edges in all four direction. The proposed model in [5] presents an edge detection model based on Neuro fuzzy-approach. The authors have developed an edge detection model in [6] by incorporating active contour model driven from cellular neural network. In [7] authors have proposed a

fuzzy logic based edge detection model by incorporating Triangular norms on DICOM images. In [8] the authors have proposed a image segmentation model by incorporating Particle Swarm Optimization (PSO) and outlier rejection combined with level set method. The authors in [9] have applied level set approach to extract microarray spot intensity features for classifying foreground and background pixels.

In [10] authors have developed a brain tumor prediction model using statistical features, Naïve Bayes classifier and morphological operation. Gabor wavelets and statistical features are employed in [11] for brain tumor detection and segmentation of brain MRI images. In [12] the authors have implemented a hybrid approach using DSURF features, HoG features and SVM for brain tumor classification. Local Frequency Descriptor (LFD) is used for texture feature extraction in [13] for tumor classification using Support Vector Machine (SVM), Decision Tree (DT) and Random Forest (RF). Local Frequency Descriptor is applied by authors in [14] on brain MRI images for studying the various properties of the brain tumor using Gray Level Co-occurrence Matrix (GLCM), Local Binary Patterns (LBP) and Second Orientation Pyramid (SOP). In [15] authors used Grey Level Run Length Matrix (GLRLM), Fuzzy C-Means (FCM) and SVM techniques for brain tumor detection and classification in MRI images. In [16] authors have applied Gabor Wavelet Transform (GWT), HOG and LBP techniques for studying the tumor region. SVM, DT, KNN, Naive Bayes and Random Forest (RF) classification models are used to categorize the brain MRI images into tumor and non-tumor classes. Authors in [17] have extracted Discrete Wavelet Transform (DWT) and statistical features for the classification of brain images using Multi-Layer Perceptron (MLP) classifier. A novel approach is suggested in [18] by implementing Gray-Level Co-occurrence Matrix (GLCM), Probabilistic Neural Network (PNN) and K-means clustering algorithm for brain tumor detection and classification. In [19] Authors have developed a classification model based on a CNN using texture and statistical features to predict normal and abnormal tissue in the brain. Then comparative analysis has been done on KNN, Logistic Regression, multi-layer perceptron, Naive Bayes, Random Forest (RF), and SVM classifiers.

In [20] authors have designed a brain tumor grading model using texture features, morphological features and SVM for brain tumor classification. Authors in [21] have extracting the features using gray-level co-occurrence matrix (GLCM) followed by tumor segmentation based on Discrete Wavelet Transform (DWT) and morphological operation for brain tumor classification. The model categorizes the brain tumor using Support Vector machine (SVM) classifier with classification accuracy of 98.91%. Authors have developed a brain tumor detection and classification model in [22] by applying k-means clustering algorithm to identify cluster with

tumor and is separated by applying morphological operation and region properties. The neural network based classifier categorizes the resultant tumor by extracting features like contrast, energy, correlation, kurtosis, and homogeneity along with perimeter and area into different classes.

In [23] authors have extracted area, perimeter, and eccentricity features for the classification of brain tumor using k-medoid clustering method and morphological operations. In [24] authors have proposed a hybrid ensemble approach based on the majority voting method, which incorporates RF, KNN and DT for classification of brain tumors by extracting Stationary Wavelet Transform (SWT), Gray Level Co-occurrence Matrix (GLCM) and Principal Component Analysis (PCA) features. Authors have developed a brain tumor detection model in [25] using deep learning based convolution neural network to classify the brain MRI images into tumor and non-tumor class. In [26] authors proposed a classification model by applying the preprocessing using the Gaussian filter and segmented the tumor region by incorporating region growing technique. The classification of the tumor has been done by extracting texture features and Genetic Algorithm (GA) is utilized to select the optimal texture features followed by KNN classifier in order to classify whether the brain MRI image is normal or not.

Author in [27] has done extensive survey on various existing brain tumor segmentation and classification methods from 2014 to 2019 and the same is presented and discussed.

As per the literature survey the problem of brain tumor detection is solved by various image processing and machine learning algorithms, but the actual semantic gap between tumor and non-tumor region is optimally less in the existing models. Hence to address the semantic gap we proposed the combination of statistical, textural and descriptive models in our research.

III. PROPOSED METHODOLOGY

The proposed brain tumor classification model is presented in this section. The main goal of this research work is to use effective feature extraction methods to reduce the misclassification of brain MRI images. Initially, MRI images are preprocessed to increase the semantic gap between the tumor region and non-tumor regions, after that the morphological action is performed to eliminate the possible non-tumor regions. Local Frequency Descriptor (LFD), texture and statistical features are extracted as hybrid features to analyze the various properties of the tumor region. Finally, an ensemble classifier is developed using Support Vector Machine (SVM), Decision Tree (DT), and K-Nearest Neighbour (KNN) along with the majority voting concept. The schematic representation of the proposed model is shown in Fig. 1.

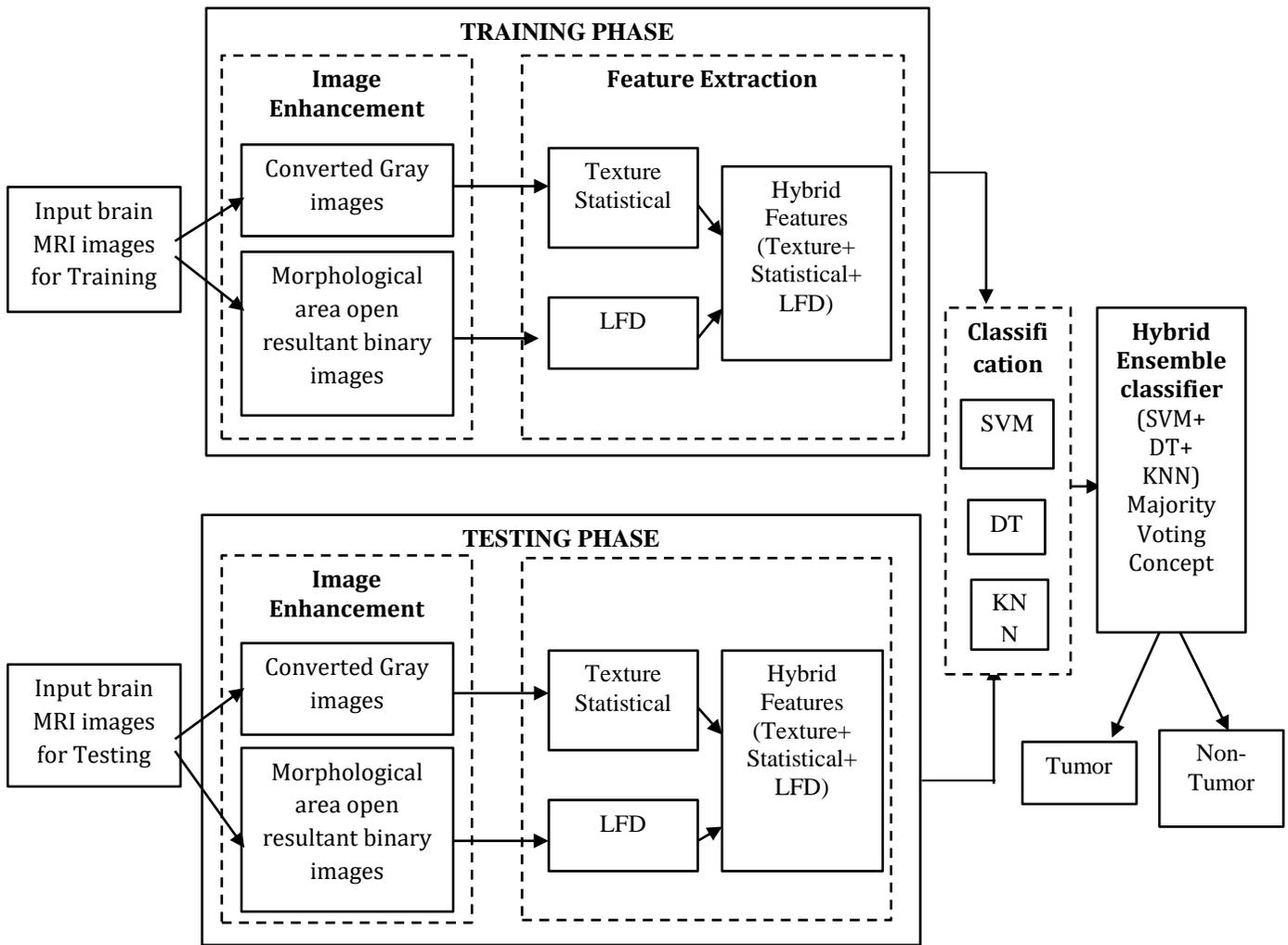


Fig. 1. Schematic Representation of the Proposed Hybrid Ensemble Model.

Algorithm: classification of brain MRI images

Required: Sequence of brain MRI images

1. For image = i to n (n is the total number of images)
2. G_i = Gray level of an image
3. Compute morphology function $bwareaopen$
 $E_n = bwareaopen(image) \sum_{i=1}^n G_i$
 1. $LFD_i = LFD_descriptor(E_n)$
 2. Extraction of texture and statistical features (TS):
 $TSO_i = TS(G_i)$
 3. Hybrid Features (HF): $HF = \sum_{i=1}^n (TSO_i + LFD_i)$
 4. SVM :
 $SVM(HF) = Weight^T * Datapoints + bias$
 where $SVM(HF) = 0/1/-1$
5. **KNN :**
 Choose K neighbour
 Calculate Euclidian distance between datapoints
 $KNN(HF) = \sqrt{(X_2 - X_1)^2 + (Y_2 - Y_1)^2}$

DT :

$$DT(HF) = \sum_{i=1}^n -P_i \log_2 P_i$$

Where P_i = proportion of samples belongs to class c for particular node.

Ensemble classifier(EC):

$$EC = \sum_{i=1}^n (SVM, DT, KNN)$$

6. Prediction based on Majority Voting concept.

A. Preprocessing

The preprocessing stage increases the distance between the tumor region and the non-tumor region by performing binarization and morphological operations. The outcome of binarization and morphological functions are shown in Fig. 2. The binarization process differentiates the tumor region pixels from background pixels. The morphological function is employed on an outcome of the binarization process to analyze the tumor region. The unwanted binary regions are eliminated by applying morphological area opening techniques to retain the tumor region.

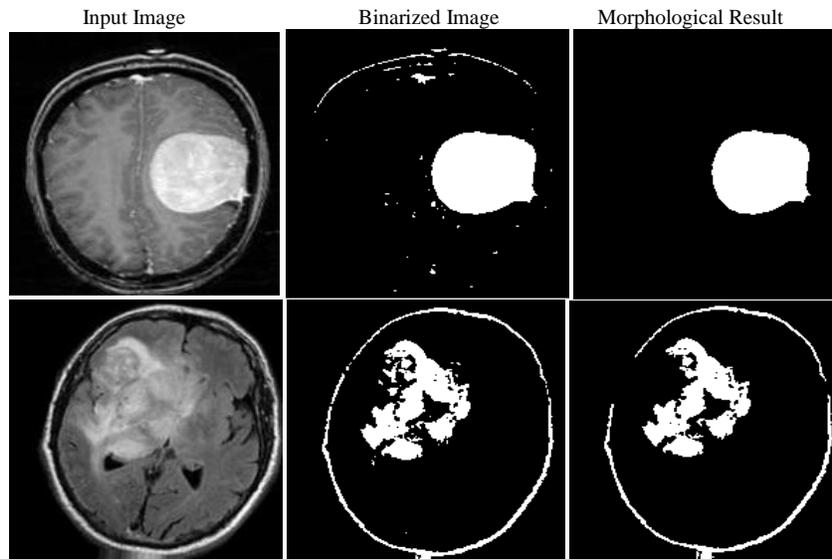


Fig. 2. Resultant Images of Binarization and Morphological Process.

B. Feature Extraction

In this proposed work texture, statistical and descriptor measurements are used to extract various features such as contrast, correlation, energy, homogeneity, mean, standard deviation, kurtosis, skewness, variance, smoothness, IDM, RMS and Local Frequency Descriptor (LFD).

1) *Texture and statistical features*: The texture of an image can be described easily with the help of statistical measurements. Texture analysis is an intimate property of the spatial domain that predicts the properties of an image that belongs to second-order statistics. In this paper, the GLCM method is applied on gray-level images to study the occurrence of pixels in the brain tumor region and statistical approaches are employed to analyze the characteristics of the brain tumor region.

a) *First-order statistical features*: The statistical analyzer is applied on brain MRI images to study the relationship among the pixels using standard deviation, mean, energy, kurtosis, entropy and skewness.

The characteristics derived from first-order statistics provide information about the gray-level distribution of the image. However, they provide no information about the relative placements of grey levels in the image. These characteristics are not able to determine whether all lower grey levels are grouped together or if they are swapped out for higher grey levels. A matrix of relative frequencies can be used to describe an occurrence of a gray-level arrangement. The second-order statistics are concerned with how often two pixels of grey level appear in the window separated by a distance.

b) *Second-order statistical features*: The Gray Level Co-occurrence Matrices (GLCM) gives the frequency of pairs of pixels that are separated by a specific distance. The GLCM technique uses the gray intensity value of an image i.e. G and the probability density function of the intensity level is i, i.e. P(i) to study the second-order statistical property.

$$P(i) = \frac{h(i)}{N} \quad (1)$$

Where h(i) is the histogram of intensity level i and N is the total number of intensities in the given image. The mathematical formulation and description of first-order and second-order statistical measurements are tabulated in Table I.

2) *Descriptor*: The proposed model is working on two-class problems to classify MRI images as a tumor or non-tumor. LFD is a binary descriptor that solves the problem of binary classification by adding Local Phase Quantizer (LPQ) and Local Binary Pattern (LBP) for identical feature extraction. Hence in this study, an effective Local Frequency Descriptor (LFD) is applied for analyzing the brain tumor region.

a) *Local Frequency Descriptor (LFD)*: The Local Frequency Descriptor (LFD) helps to extract local frequency information from the MRI images and due to its blur-invariant property, it is widely used in low-resolution images. LFD identifies Local Magnitude Descriptor (LMD) and Local Phase Descriptor (LPD) by performing Fast Fourier Transform (FFT) to analyze the local occurrences of pixels in the tumor region.

The LMD (Equation 2) uses position (i) and frequency (u) in the local pattern is indicated as M(u, i). where k is the centre position of the neighbouring pattern and is depicted as M(u, k).

$$f_{LMD}(u, i) = \sum_{k=1}^8 S(M(u, k), M(u, i)) 2^{k-1} \quad (2)$$

Quantize relationship is obtained by Equation 3.

$$S(M(u, k), M(u, i)) = \begin{cases} 1 & \text{if } M(u, k) \geq M(u, i) \\ 0 & \text{if } M(u, k) < M(u, i) \end{cases} \quad (3)$$

The qualitative textural features are extracted from the brain MRI images by employing local descriptors such as Local Phase Quantization (LPQ) and Local Binary Pattern

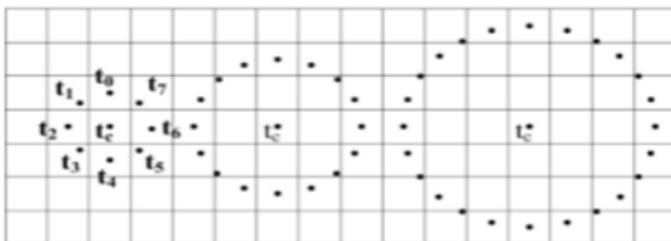
(LBP). These two techniques help to quantify the phase values in local neighbourhood pixels.

LPQ is applied to analyze the phase values in low resolution and blur MRI images using Fast Fourier Transform (FFT). LBP is employed to analyze the identical property of the brain MRI images which helps to assign the label for each pixel of an image by considering the threshold of neighbourhood pixels to result as a binary number. The different LBP variants are represented in Fig. 3 and the outcome of LBP is represented in Fig. 4. Finally, the LFD is achieved with the combination of LPQ and LBP to extract prominent textural properties from the MRI images.

3) *Hybrid features*: Generally, the semantic gap between tumor region and non-tumor region in gray level brain MRI images is considerably less. Due to this nature, the lowest numbers of features are insufficient to distinguish the tumor region from the non-tumor region. Even though the combination of common features also lead to insufficient representation of brain tumors. Hence a highly discriminative and sufficient combination of features is required to represent the brain tumor region in MRI brain images. In the proposed model the statistical and textural features are combined to obtain the highly discriminative features of the brain tumor. This hybrid feature helps to distinguish the brain tumor from the brain MRI images.

TABLE I. MATHEMATICAL FORMATION OF TEXTURE AND STATISTICAL FEATURES WHERE I,J,N,G=GRAY VALUES, P(I)=PROBABILITY VALUES, μ=MEAN,Σ=VARIENCE

Sl.No.	Features	Mathematical Formulation	Description
1.	Mean	$\sum_{i=0}^{G-1} iP(i)$	To study the brightness of the tumor region.
2.	Variance	$\sum_{i=0}^{G-1} (i - \mu)^2 P(i)$	The values of variance help to distinguish the brain tumor pixels and non-tumor pixels.
3.	Skewness	$\sigma^3 \sum_{i=0}^{G-1} (i - \mu)^3 P(i)$	Skewness is used to measure the symmetry or non-symmetry pixels in the brain MRI images
4.	Kurtosis	$\sigma^4 \sum_{i=0}^{G-1} (i - \mu)^4 P(i) - 3$	Kurtosis evaluates the microstructural environment of the brain.
5.	Energy	$\sum_{i=0}^{G-1} [P(i)]^2$	Energy studies the gray level distribution in the brain MRI images.
6.	Entropy	$\sum_{i=0}^{G-1} P(i) \log_2 [P(i)]$	Entropy analyses the randomness of textural regions in the brain MRI images.
7.	Smoothness	$1 - \frac{1}{1 + \sigma^2}$	The smoothness removes possible noise by performing spatial smoothing on brain MRI images.
8.	Contrast	$\sum_{i,j=0}^{N-1} P_{ij} (i - j)^2$	The contrast analyses the intensity variation in the brain MRI images.
9.	Correlation	$\sum_{i,j=0}^{N-1} P_{ij} \frac{(i-\mu)(j-\mu)}{\sigma^2}$	The correlation exhibits spatial relationships among intensity levels in the brain MRI images.
10.	Homogeneity	$\sum_{i,j=0}^{N-1} \frac{P_{ij}}{1+(i-j)^2}$	A homogeneous extracts the affinity or closeness of brain MRI pixels.
11.	IDM	$\sum_{i=0}^{N-1} \sum_{j=0}^{N-1} \frac{1}{1+(i-j)^2} P(i,j)$	IDM measures the local likelihood of the image and it gives a single or range of values to represent whether the brain MRI image is textured or non-textured.
12.	RMS	$\sqrt{\frac{1}{M} \sum_{i=1}^M y_i ^2}$	Root Mean Square calculates the number of changes across the pixel of brain MRI images.



R=1,N=8 R=2,N=16 R=3,N=24
Fig. 3. LBP Distance Variants.

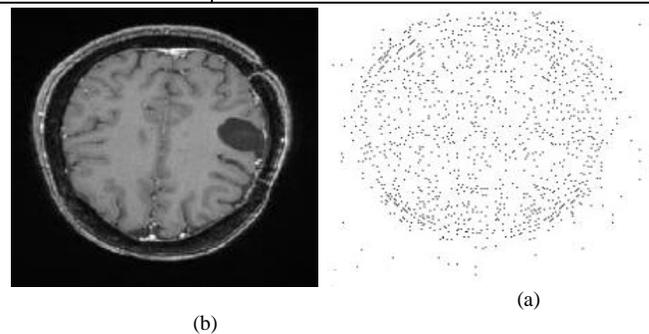


Fig. 4. (a) Input Image (b) Output of LBP for P=8, R=1. Where P is the Sampling Points, R is the Radius.

IV. CLASSIFICATION

Image classification is the task of extracting a collection of different attributes in an image and then mapping them to a specified class. As this research work is carried out on two-class problems, the supervised classification models named KNN, SVM and DT are considered to assign the given input brain MRI images into normal and abnormal classes. Further, the considered classifiers are ensemble to achieve an exact categorization of MRI images using the majority voting concept.

A. Support Vector Machine (SVM)

The linear SVM classifier is primarily used in the binary classification process. Since the proposed model classifies the given input MRI images into tumor and non-tumor classes, the linear-SVM classifier has been incorporated. The SVM classifier analyzes the hybrid features and trains the model to minimize the structural misclassification in MRI brain images. Later the trained SVM model is tested by providing untrained brain MRI images.

B. K-Nearest Neighbour (KNN)

The KNN classifier finds the optimal neighbours by studying the space among the hybrid features to observe the similarity and dissimilarity among the pixels. In the proposed model, the KNN classifier is incorporated to estimate the discrimination among the tumor region and non-tumor region within the K distance. In order to execute this, the KNN model is trained using hybrid features and then the trained KNN model is tested by providing untrained brain MRI images.

C. Decision Tree (DT)

The decision tree is a stage wise prediction algorithm to assign the given brain MRI image into a particular class. In the proposed model, the decision tree classifier repeatedly partitioning the hybrid features into smaller and more uniform features. These uniform features are used to train the DT classifier to distinguish the tumor and non-tumor regions and then the trained DT model is tested by providing untrained brain MRI images.

D. Ensemble Classifier (SVM+DT+KNN)

The ensemble classifier (SVM+DT+KNN) outperforms in achieving improved accuracy as compared to the individual classifier. The constituent classifier studies the hybrid features based on the principle of a respective classifier. From this, the prediction of the classifier differs from one to another. Hence, the majority voting concept is applied to consider the maximum prediction among the classifiers.

V. EXPERIMENTAL ANALYSIS

The performance of the proposed model is evaluated by conducting experimentation on the brain MRI Kaggle data set [28]. This data set contains 2065 tumor and non-tumor brain MRI images respectively. The proposed model is trained with 600 tumor and 600 non-tumor brain MRI images. The same model is tested with 485 tumor and 380 non-tumor brain MRI images.

The performance measures of the proposed model such as Accuracy (Equation 4): Accurately identified brain tumor samples to the whole pool of samples. Precision (Equation 5): Correctly identified samples over the correctly and incorrectly classified samples. Recall (Equation 6): Accurately classified samples over the correct classifier samples along with incorrectly rejected samples. Sensitivity (Equation 6): Sensitivity is a similar calculation of recall. Specificity (Equation 7): Number of accurately rejected samples over the accurately rejected samples along with incorrectly classified samples. F1 Score (Equation 8): Harmonic mean representation of the Recall and Precision. All these performance measures use certain parameters like True Positive (TP) represents the accurately classified samples, False Positive (FP) depicts the incorrectly classified samples, True Negative (TN) specifies accurately rejected samples and False Negative (FN) represents incorrectly rejected samples.

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{FP} + \text{FN} + \text{TN}) \quad (4)$$

$$\text{Precision} = \text{TP} / (\text{TP} + \text{FP}) \quad (5)$$

$$\text{Recall} = \text{Sensitivity} = \text{TP} / (\text{TP} + \text{FN}) \quad (6)$$

$$\text{Specificity} = \text{TN} / (\text{TN} + \text{FP}) \quad (7)$$

$$\text{F1 Score} = 2 * (\text{Recall} * \text{Precision}) / (\text{Recall} + \text{Precision}) \quad (8)$$

A. Discussion

Texture, statistical and descriptor features play an important role in the classification of brain MRI images into a tumor and non-tumor classes. The hybrid features help to identify the discriminative feature of the tumor region. Later, SVM, DT and KNN classifiers are combined as an ensemble classifier using the majority voting concept for best classification. Overall the proposed model outperforms all measuring terms such as accuracy, sensitivity, specificity, precision, recall and F1 score as compared to individual classifier outcomes and existing models. The performance analysis of an individual classifier and ensemble classifier is depicted in Table II. Fig. 5 represents the classification performance on the Kaggle dataset. Finally, the proposed model is compared with the state-of-the-art techniques of the existing methods and the comparative analysis is shown in Table III.

TABLE II. PERFORMANCE MEASURES ATTAINED WITH SVM, DT, KNN AND ENSEMBLE CLASSIFIERS

classifiers	TP	TN	FP	FN	Accuracy	Sensitivity	Specificity	Precision	Recall	F score
SVM	347	68	33	417	88.32%	88.14%	88.14%	88.65%	88.14%	88.25%
DT	367	38	13	447	94.10%	93.89%	93.89%	94.37%	93.89%	94.05%
KNN	367	50	13	435	92.72%	92.55%	92.55%	93.13%	92.55%	92.67%
Hybrid Ensemble classifier	380	1	0	484	99.88%	99.87%	99.87%	99.89%	99.88%	99.88%

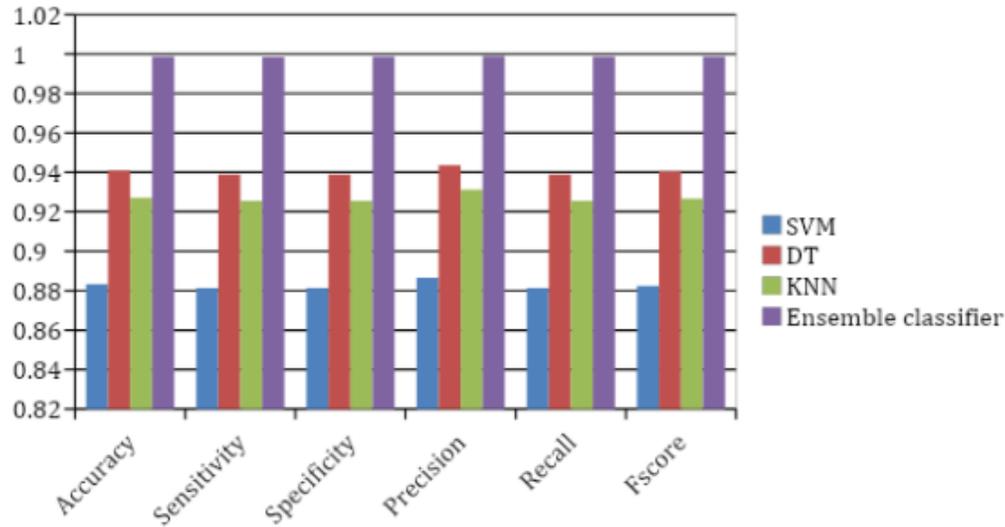


Fig. 5. Representation of Classification Performance Analysis.

TABLE III. COMPARATIVE ANALYSIS OF PROPOSED HYBRID ENSEMBLE MODEL WITH EXISTING MODELS

Authors /year	Methods	Accuracy
Devanathan et al.[29] /2020.	GLCM and SVM	97.56%.
Shahajad et al.[30] /2021	GLCM, heatmap features and SVM	92 %
Kiraz et al.[31] /2021	Mean, standard deviations, area, entropy and KNN	89.8%
Proposed hybrid ensemble method	(Texture +Statistical+LFD) Hybrid features and (SVM+DT+KNN) Ensemble classifiers	99.8%

VI. CONCLUSION

In this paper, we developed an effective and efficient hybrid ensemble model for extracting hybrid features and classifying brain MRI samples into tumor and non-tumor classes. Texture and statistical features are extracted to determine the presence of the tumor region in the brain MRI image. The local magnitude descriptor and local phase descriptor of brain MRI images are analyzed by employing the Local Frequency Descriptor (LFD). The effective property of the LFD supports the classifier to increase the efficiency of a classification process. The conventional classifiers such as SVM, DT and KNN are combined as an ensemble classifier using the majority voting concept for effective discrimination of brain MRI images. In the future, the probabilistic model needs to be incorporated to analyze the distribution of tumor pixels in brain MRI images.

REFERENCES

- [1] V. Wasule and P. Sonar, "Classification of brain MRI using SVM and KNN classifier," 2017 Third International Conference on Sensing, Signal Processing and Security (ICSSS), Chennai, India, pp. 218-223, 2017
- [2] A. R. Mathew and P. B. Anto, "Tumor detection and classification of MRI brain image using wavelet transform and SVM," 2017 International Conference on Signal Processing and Communication (ICSPC), Coimbatore, India, pp. 75-78, 2017.
- [3] M. Siar and M. Teshnehlab, "Brain Tumor Detection Using Deep Neural Network and Machine Learning Algorithm" 9th International Conference on Computer and Knowledge Engineering (ICCKE), Mashhad, Iran, pp. 363-368, 2019.
- [4] Khan, Asim Ur Rehman, Syed Muhammad Atif Saleem, and Haider Mehdi. "Detection of edges using two-way nested design." International Journal of Advanced Computer Science and Applications vol. 8, no. 3, pp.136-144, 2017.
- [5] Zribi, Fatma, and Noureddine Ellouze. "Edge Detection with Neuro-Fuzzy Approach in Digital Synthesis Images." INTERNATIONAL JOURNAL OF ADVANCED COMPUTER SCIENCE AND APPLICATIONS, vol.7, no.4, pp362-368, 2016.
- [6] Belean, Bogdan. "Active Contours Driven by Cellular Neural Networks for Image Segmentation in Biomedical Applications." STUDIES IN INFORMATICS AND CONTROL, vol.30, no. 3 , pp109-119, 2021.
- [7] Nagarajan, D., M. Lathamaheswari, R. Sujatha, and J. Kavikumar. "Edge detection on DICOM image using triangular norms in type-2 fuzzy." International Journal of Advanced Computer Science and Applications ,vol.9, no. 11, pp 462-475, 2018.

- [8] Belean, Bogdan, Robert Gutt, Carmen Costea, and Ovidiu Balacescu. "Microarray Image Analysis: From Image Processing Methods to Gene Expression Levels Estimation." *IEEE Access*, vol. 27, no. 8, pp 159196-159205, 2020.
- [9] Mekhmoukh, Abdenour, and Karim Mokrani. "Improved Fuzzy C-Means based Particle Swarm Optimization (PSO) initialization and outlier rejection with level set methods for MR brain image segmentation." *Computer methods and programs in biomedicine* vol.122, no. 2, pp 266-281, 2015.
- [10] Zaw, Hein Tun, Noppadol Maneerat, and Khin Yadanar Win. "Brain tumor detection based on Naïve Bayes Classification." In 2019 5th International Conference on Engineering, Applied Sciences and Technology (ICEAST), pp. 1-4. IEEE, 2019.
- [11] Nabizadeh, Nooshin, and Miroslav Kubat. "Brain tumors detection and segmentation in MR images: Gabor wavelet vs. statistical features." *Computers & Electrical Engineering* vol 45, pp.286-301, 2015.
- [12] Ayadi, Wadhah, Imen Charfi, Wajdi Elhamzi, and Mohamed Atri. "Brain tumor classification based on hybrid approach." *The Visual Computer* ,pp 1-11, 2020.
- [13] Tripathi, Prasun Chandra, and Soumen Bag. "Non-invasively grading of brain tumor through noise robust textural and intensity based features." In *Computational Intelligence in Pattern Recognition*, Springer, Singapore, pp. 531-539, 2020.
- [14] Maani, Rouzbeh, Sanjay Kalra, and Yee-Hong Yang. "Robust volumetric texture classification of magnetic resonance images of the brain using local frequency descriptor." *IEEE Transactions on Image Processing*, vol. 23, no. 10, pp 4625-4636, 2014.
- [15] Singh, Amritpal. "Detection of brain tumor in MRI images, using combination of fuzzy c-means and SVM." In 2015 2nd international conference on signal processing and integrated networks (SPIN), pp. 98-102. IEEE, 2015.
- [16] Amin , Javaria, Muhammad Sharif, Mudassar Raza, Tanzila Saba, and Muhammad Almas Anjum. "Brain tumor detection using statistical and machine learning methods." *Computer methods and programs in biomedicine* vol.177 , pp 69-79, 2019.
- [17] Latif, Ghazanfar, DNF Awang Iskandar, Jaafar M. Alghazo, and Nazeeruddin Mohammad. "Enhanced MR image classification using hybrid statistical and wavelets features." *Ieee Access* 7, pp 9634-9644, 2018.
- [18] Lavanyadevi, R., M. Machakowsalya, J. Nivethitha, and A. Niranjal Kumar. "Brain tumor classification and segmentation in MRI images using PNN." In 2017 IEEE International Conference on Electrical, Instrumentation and Communication Engineering (ICEICE), pp. 1-6. IEEE, 2017.
- [19] Abiwinanda, Nyoman, Muhammad Hanif, S. Tafwida Hesaputra, Astri Handayani, and Tati Rajab Mengko. "Brain tumor classification using convolutional neural network." In *World congress on medical physics and biomedical engineering*, pp. 183-189. Springer, Singapore, 2019.
- [20] Gupta, Manu, BVVSN Prabhakar Rao, and Venkateswaran Rajagopalan. "Brain tumor detection in conventional MR images based on statistical texture and morphological features." In 2016 International Conference on Information Technology (ICIT), pp. 129-133. IEEE, 2016.
- [21] Ansari, M. A., Rajat Mehrotra, and Rajeev Agrawal. "Detection and classification of brain tumor in MRI images using wavelet transform and support vector machine." *Journal of Interdisciplinary Mathematics*, vol 23, no. 5, pp 955-966, 2020.
- [22] Zulkoffli, Zuliani, and Talha Afzal Shariff. "Detection of Brain Tumor and Extraction of Features in MRI Images Using K-means Clustering and Morphological Operations." In 2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS), pp. 1-5. IEEE, 2019.
- [23] Gezimati, Mavis, Munyaradzi C. Rushambwa, and J. B. Jeeva. "Brain tumor detection and classification of MRI brain images using morphological operations." In *ICTMI 2017*, pp. 137-149. Springer, Singapore, 2019.
- [24] Garg, Ginni, and Ritu Garg. "Brain Tumor Detection and Classification based on Hybrid Ensemble Classifier." *arXiv preprint arXiv:2101.00216*, 2021.
- [25] Sultan, Hossam H., Nancy M. Salem, and Walid Al-Atabany. "Multi-classification of brain tumor images using deep neural network." *IEEE Access* vol. 7, pp 69215-69225, 2019.
- [26] Viji, KS Angel, and D. Hevin Rajesh. "An efficient technique to segment the tumor and abnormality detection in the brain MRI images using KNN classifier." *Materials Today: Proceedings* vol.24, pp 1944-1954, 2020.
- [27] Tiwari, Arti, Shilpa Srivastava, and Millie Pant. "Brain tumor segmentation and classification from magnetic resonance images: Review of selected methods from 2014 to 2019." *Pattern Recognition Letters* vol.131, pp244-260, 2020.
- [28] <https://www.kaggle.com/navoneel/brain-mri-images-for-brain-tumor-detection>
- [29] Devanathan, B., and K. Venkatachalapathy. "An Optimal Multilevel Thresholding based Segmentation and Classification Model for Brain Tumor Diagnosis." In 2020 4th International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 1133-1138. IEEE, 2020.
- [30] M. Shahajad, D. Gambhir and R. Gandhi, "Features extraction for classification of brain tumor MRI images using support vector machine," 2021 11th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 767-772, 2021.
- [31] Kiraz, Hüseyin. "Design and Implementation of Image Processing Method on Brain Tumor Detection with Machine Learning Approach." (2021).

Mutual Informative Brown Clustering based Multiattribute Cockroach Swarm Optimization for Reliable Data Dissemination in VANET

Mrs D.Radhika¹

Research Scholar

Cauvery College for Women (Autonomous)
Affiliated to Bharathidasan University
Tiruchirappalli, Tamilnadu
India

Dr. A.Bhuvaneshwari²

Associate Professor

Cauvery College for Women (Autonomous)
Affiliated to Bharathidasan University
Tiruchirappalli, Tamilnadu
India

Abstract—A vehicular ad hoc network (VANETs) intends to obtain communication for vehicular networks and enhances road safety and effectiveness with help of wireless technology. Data dissemination is an important process in communication. In VANETs system, Data dissemination plays a significant role. A novel Mutual informative brown clustering-based multi attribute cockroach swarm optimization (MIBCMCSO) technique is introduced for improving data dissemination. In reliable data dissemination, clustering and optimization are the two major process of proposed MIBCMCSO technique. Initially, clustering procedure is performed for separating entire network towards different groups of vehicle nodes namely distance, direction, density and velocity of node. For each group, cluster head was chosen among the members to efficient data with minimum delay. Secondly, multi attribute cockroach swarm optimization technique is applied for finding optimal cluster head through multi attribute functions such as residual energy, bandwidth availability, and distance. Then source node performs data dissemination destination via optimal cluster head. Simulation of MIBCMCSO as well as existing technique is performed by various performance parameters like packet delivery ratio, end to end delay and throughput. MIBCMCSO achieves higher consistency of data dissemination as well as lesser delay than conventional methods.

Keywords—VANET; data dissemination; mutual informed brown agglomerative clustering; multi attribute cockroach swarm optimization

I. INTRODUCTION

VANET is a wireless communication system used for disseminating multimedia information from one vehicle to other vehicles in the dynamic structure of the network. Reliable data dissemination is a significant process in a wireless network. To address this issue, a cluster-based optimization technique is introduced. Fig. 1 specifies the various types of routing protocols in VANET.

A new cluster-based reliable routing scheme called CEGRAOD was developed by Zahid Khan et al., (2019) [1] to find the most reliable path from the source to destination. A criterion for cluster members (CMs) and cluster heads (CHs) selection. The CVoEG model divides VANET nodes (vehicles) into an optimal number of clusters (ONC) used by

Eigen gap heuristic. The cluster includes vehicle was selected as a CH for maximum Eigen-centrality score. But, the method failed to use optimization technique for select the optimal cluster head. A multi valued DPSO is designed in [2] for identifying data dissemination from source to destination vehicle. In order to develop detection of optimal path in VANETs, Multi valued Discrete Particle Swarm Optimization (DPSO) was employed. While considering the more packets for dissemination, the performance of delay is not reduced.

Clustering and Probabilistic Broadcasting (CPB) method is developed in [3] for data dissemination. A clustering algorithm was to constrain the directions of vehicles exchange their data in a clustered way with adequate association period. In the created clustering structure was to broadcast the data between vehicles. Each cluster associate forwards the received packet to its cluster head was associated with the number of times the same packet was received through one interval. But, this approach minimizes delay, throughput is not improved. Novel data dissemination for VANETs was introduced in [4] for disseminating emergency messages with different traffic scenarios. In order to choose next forwarding vehicle (NFV), the segmentation of vehicle uses DDP4V. Though the efficient and reliable data dissemination protocol is designed for controlling data dissemination in highway and urban VANET scenarios, designed protocol failed to perform reliable data dissemination.

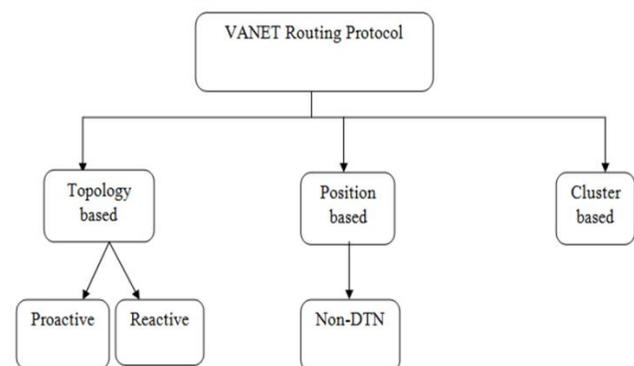


Fig. 1. Type of VANET Routing Protocol.

Data Dissemination protocol is introduced in [5] for data dissemination. Path-based clustering data dissemination protocol (PCDP) consists of two parts. The first part was a clustering formation clusters based on the expected path of the vehicle. The survivability of the cluster was enhanced by created cluster among nodes with the minimum difference by evaluated the designed paths of the vehicles. But, protocol reduces delay while using higher vehicle density, the reliability of data transmission remained unaddressed. An intelligent clustering-based optimization method was introduced in [6] to enhance the reliable data transmission for each vehicle. The moth flame optimization framework was optimizing the cluster and primary focus of the scheme was to improve the power in vehicular ad hoc networks. Flame optimization was proved by two variants of particle swarm optimization such as multiple-objective particle swarm optimization and comprehensive learning particle swarm optimization and a variant of ant colony optimization. But the designed optimization method failed to consider the multi-objective functions for solving the data dissemination.

Analytical network process (ANP) is introduced in [7] using the multi criteria tool for data dissemination through the optimal vehicle nodes. The various performance metrics such as reliability, delay remained unsolved. The stability of different candidate vehicles for NFV (Next Forwarder Vehicle) selection level was verified for sensitivity analysis of dissimilar development But, ANP method minimizes the latency but the reliable data dissemination was not performed. Passive data dissemination method is designed in [8] using cluster-based method. However, the energy-aware reliable data dissemination remained unsolved in VANET. The approach was consist on each vehicle for transmit periodical measures about the position, speed to other vehicles were the same signal range and same cluster. The previous division of the network into virtual sub-groups was easy management and data dissemination of messages. A replication-based distributed randomized approach was introduced in [9] to disseminate the information. Amount of data extend in network is restricted for decreasing transmission as well as increasing data dissemination delay. The approach failed to use cluster-based data dissemination in order to further minimize the delay. A hybrid method was developed in [10] for resolving utility-based maximization and choose data dissemination. The utility function was taken by the delivery delay, Quality of Service (QoS) and storage cost. With precise analysis was obtained the closed-form of the expected utility of a path and then attain the optimal solution of the problem with the curved optimization theory. But the method failed to achieve higher reliability in the data distribution. An Adaptive Data Dissemination Protocol (ADDP) was introduced in [11] for providing reliability to message transmission. In order to minimize communication and beacons in network, designed method employs various method for vigorously regulate beacon periodicity. Though the vehicles faces failures in message delivery, the vehicle movement direction was not considered.

Hybrid relay node selection method is presented in [12] to multi hop data dissemination with minimum delay as well as bandwidth utilization. The new hybrid scheme was obtain the

spatial allocation of the next-hop transmitted nodes with location to the present sending node. A hybrid scheme was that attempts to improve performance of VANETs over unstable node densities, traffic load conditions and mobility speed scenarios. While the chosen relay nodes is controlled for exploiting single selection criterion, the energy-based relay nodes selection is not carried out. Named Data Networking (NDN) approach is designed in [13] to deliver message contents with higher network throughput. A new protocol named Roadside Unit (RSU) assisted of Named Data Network (RA-NDN) was operating as a standalone node standalone RSU (SA-RSU)]. The approach was reduces the different vehicular densities, vehicular communication ranges and number of requesters with vehicular NDN via a real-world data set. But the performance of delay was not effectively reduced since it failed to use the clustering technique. Integrated message dissemination and traffic regulation were performed in [14] with higher network throughput. On-ramp traffic flow control method is used for controlling vehicles towards highway. But the packet delivery ratio was not improved. On-Demand Member-Centric Routing (OMR) protocol was developed in [15] for data dissemination. Routing protocols is employed for video streaming service at certain platoon member. However, the performance of the delay was not reduced.

A hybrid-fuzzy logic guided genetic algorithm (H-FLGA) approach was proposed in [16] for the software defined networking controller, to solve a multi-objective resource optimization problem for 5G driven VANETs. A Multi access Edge Computing (MEC) based delay-constrained k-hop-limited VANET data offloading method was developed in [17] to derive the potential V2V-V2I paths. TBD (Trajectory Based Dissemination) solution that transmits the information on the network according was proposed in [18] to the density of vehicles in the path from the source to the region of interest. A Multi-hop Cooperative Data Dissemination (MHCDD) based on buffer control was introduced in [19] which can be more efficient when applied with a Markov process. An ad-hoc-based solution was designed in [20] for V2V charging where both information dissemination and charging pairs allocation are performed over VANET. A hybrid data dissemination model with both vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) disseminations was proposed in [21] to reduce the traffic on the edge, in which the edge (infrastructure) selectively injects data to the vehicles and leverages the vehicle network to disseminate the data.

A. Major Contribution

The major contribution of the work MIBCMCSO technique is summarized as follows:

To improve the reliability of data dissemination in VANET, the MIBCMCSO technique is introduced. This contribution is achieved by performing the cluster based optimal cluster head identification. The mutual informed brown agglomerate clustering is applied to group the vehicle nodes based on the moving direction, velocity, and distance.

To improve the throughput, the multi attribute cockroach swarm optimization technique is applied for finding the optimal cluster head between source and destination based on

energy, distance, and bandwidth availability. The data dissemination is carried out via an optimal cluster head. This assists to minimize end to end delay of data dissemination.

B. Outline of Paper

The rest of paper is organized into five different sections. Section 2 describes the proposed methodology MIBCMCSO with a neat diagram. In Section 3, simulation settings are presented and various results of the different parameters are discussed in Section 4. Finally, the conclusion of the paper is presented in Section 5.

II. METHODOLOGY

An efficient algorithm called MIBCMCSO is introduced with the objective of improving data dissemination and minimizing the delay in VANET. The MIBCMCSO technique comprises the ‘n’ number of vehicle nodes to perform the data transmission within the communication range. The vehicle nodes are partitioned into ‘j’ number of clusters $c_1, c_2, c_3, \dots, c_j$ and the cluster head (N_H) is selected for disseminating the data packets from source vehicle (S_V) to destination vehicle (D_V). The flow process of the MIBCMCSO technique is shown in Fig. 1.

Fig. 2 illustrates the flow process of the proposed MIBCMCSO technique to obtain the better reliability of data dissemination with minimum delay. Initially, the clustering technique is applied for dividing the total network into different groups of vehicle nodes in the network based on the different characteristics such as vehicle density, direction, distance, and velocity. Then the data packet transmission is performed by selecting the cluster head using a multi attribute optimization technique. These two processes are clearly explained in the following sections.

A. Mutual informed brown agglomerative clustering. The first process of the proposed MIBCMCSO technique is to divide the total mobile nodes in the VANET into a number of groups. The mutual informed brown agglomerative clustering is the hierarchical clustering algorithm used to combine the two clusters into one move up the hierarchy. This clustering process is carried out based on their characteristics such as vehicle density, direction, distances, and velocities.

Initially, the vehicle moving directions from one location to another is computed. In the two dimensional space, the current coordinate of the vehicle is (P_1, P_2) and previous coordinate of the same vehicle is (Q_1, Q_2) .

$$\tan \theta = [(Q_2 - Q_1) / (P_2 - P_1)] \quad (1)$$

where, ‘tan θ ’ denotes a tangent function used to identify the moving direction of the node. Afterward, the distance between the two-vehicle nodes is measured using the given mathematical formula. The coordinates of one vehicle node are (u_1, v_1) and coordinates of another vehicle node (u_2, v_2) .

$$\alpha(\tau_i, \tau_j) = \sqrt{(u_2 - u_1)^2 + (v_2 - v_1)^2} \quad (2)$$

Where, $\alpha(\tau_i, \tau_j)$ represent the distance between two vehicle nodes in the two-dimensional space in the network. Then the velocity of the vehicle node is calculated based on their

movement in the given period of time. The mathematical for calculating the node velocity is given below:

$$\tau_{vel} = (\alpha_\tau / t) \quad (3)$$

Where, ‘ τ_{vel} ’ represents a velocity of the vehicle node, ‘ α_τ ’ denotes a distance moved by the node in a given time period (t). The node velocity is measured in meter per second (m/sec). Based on the above-said characteristics, Mutual informed brown agglomerative clustering is applied to group the vehicle nodes. The number of vehicle nodes ‘ $\tau_1, \tau_2, \tau_3, \dots, \tau_m$ ’ are distributed in a transmission range. Initially, the proposed clustering algorithm initializes the ‘k’ number of clusters in the given dimensional space. For each cluster, the mean (i.e. cluster centroid) is assigned to partitions the vehicle nodes.

The distance between the mean and the vehicle nodes is calculated. The Manhattan distance is calculated as given below. k n.

$$d_{ij} = \sum_{j=1}^k \sum_{i=1}^n |c_j - \tau_i| \quad (4)$$

Where, d_{ij} denotes a distance between the cluster mean c_j and τ_i represents the vehicle node. Then the node which is closer to the cluster mean is grouped into that particular cluster.

$$Y = \arg \min d_{ij} \quad (5)$$

where Y denotes a clustering output, arg min denotes an argument minimum function to find the minimum distance (d_{ij}) between the vehicle nodes and cluster mean. In this way, all the vehicle nodes are grouped into different clusters. After that, the mutual information between the clusters is computed for merging the clusters. The mutual information is used to compute the mutual dependence as given below.

$$D_m = p_r(c_1, c_2) * \log_2((p_r(c_1, c_2) / (p_r(c_1) p_r(c_2)))) \quad (6)$$

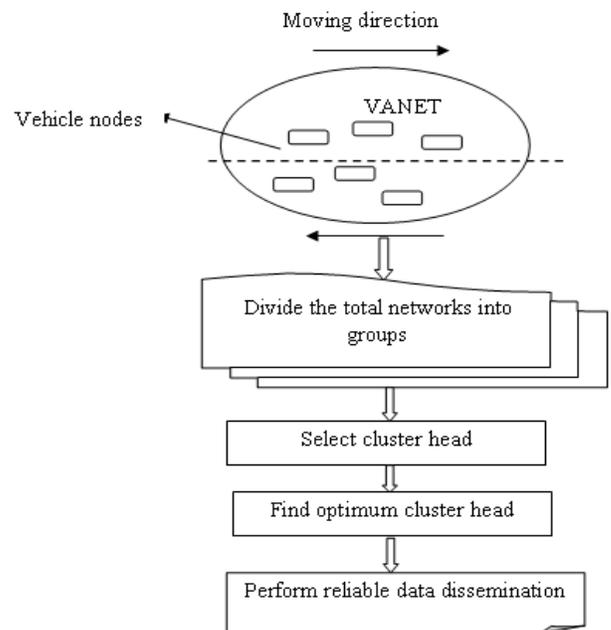


Fig. 2. Flow Process of Proposed MIBCMCSO Technique.

Where, D_m denotes a mutual dependence between the clusters (c_1, c_2) , $(p_r(c_1, c_2))$ denotes a joint probability distribution, and $p_r(c_1)$ and $p_r(c_2)$ represents a marginal probability of the clusters. The proposed clustering algorithm uses the gradient ascent function for finding the maximum mutual dependence between the clusters.

$$G(x) = \arg \max D_m \quad (7)$$

Where, $G(x)$ denotes a gradient ascent function, $\arg \max$ represents an argument of the maximum function used to find the maximum mutual dependence D_m between the clusters.

Finally, the merging process is carried out by combining the maximum dependence between the clusters. As a result, the number of clusters is obtained in output space. After that the cluster head is chosen through the minimum average distance among the other cluster members in the group. The cluster head acts as a data collector to route the information to their cluster members and to the roadside unit. The Mutual informed brown agglomerative clustering algorithm is described as follows:

Algorithm 1 Mutual informed brown agglomerative clustering

Input: Number of vehicle nodes ' $\tau_1, \tau_2, \tau_3, \dots, \tau_n$ '
 Output: Clustering of vehicle nodes
 Begin
 1. For each vehicle nodes ' τ_i '
 2. Measure $\tan \theta, \alpha(\tau_i, \tau_j), \tau_{vel}$
 3. Initialize the 'k' number of clusters
 4. Initialize cluster mean c_j
 5. Compute Manhattan distance d_{ij} between c_j and τ_i
 6. Find minimum distance between c_j and $\tau_i \arg \min d_{ij}$
 7. Group the vehicles to cluster c_j
 8. Calculate the mutual information between the clusters D_m
 9. Merge the clusters with maximum dependence $\arg \max D_m$
 10. End For
 11. Obtain the clustering results
 12. For each cluster
 13. Select the cluster head with minimum distance among the group members
 14. End for
 End

Algorithm 1 describes the step by step process of Mutual informed brown agglomerative clustering to group the vehicle nodes based on the node characteristics such as moving direction, distance, and velocity. The hierarchical clustering is applied for dividing the mobile nodes into different clusters. Then the cluster head is chosen for efficient data dissemination in VANET.

Multi-attribute cockroach swarm optimization was applied for detecting cluster head for data dissemination with minimum delay. The Multi-attribute cockroach swarm

optimization algorithm is inspired by the basic biological behaviors of the cockroach looking for their food based on multiple objective functions namely, energy, bandwidth availability, and distance. Initialize the populations of cockroach i.e. cluster heads in the search space.

$$C_s = \{Cr_1, Cr_2, Cr_3 \dots Cr_n\} \quad (8)$$

For each cluster head, the multiattribute function such as energy, bandwidth availability and distance is calculated to find the optimal one. The residual energy for each cluster head is mathematically estimated as given below:

$$E_R = (E_t - E_c) \quad (9)$$

Where, E_R represents the residual energy, E_t indicates total energy, E_c denotes consumed energy. Then bandwidth accessibility of the cluster head is estimated as follows,

$$B_A = (B_t - B_c) \quad (10)$$

Where, B_A denotes an available bandwidth between the cluster head, the total bandwidth is represented by B_t amount of bandwidth utilization is represented by B_c . The distance between the two clusters head $\alpha(\tau_i, \tau_j)$ is calculated.

$$\alpha(C_i, C_j) = \sqrt{(a_2 - a_1)^2 + (b_2 - b_1)^2} \quad (11)$$

Where (a_1, b_1) and (a_2, b_2) denotes a location coordinates of two cluster heads in the two-dimensional space. Based on the above-said parameters, the fitness of each individual Cr_i is computed.

$$FF = \{ (E_R > E_T) \ \&\& \ (B_A > B_T) \ \&\& \ \min \alpha(C_i, C_j) \} \quad (12)$$

Where FF indicates the fitness of the individual in the search space, E_R denotes residual energy, E_T is the threshold for residual energy, B_A indicates bandwidth availability, $\min \alpha(C_i, C_j)$ denotes a minimum distance among two cluster heads. In addition, each iterations of proposed algorithm involves three behaviors for solving various optimization problems namely chase-swarming, dispersing, and ruthless behavior based on the fitness of the individual in search space.

1) *Chase-swarming behaviors*: In the chase-swarming behavior, the strongest cockroach among the population is considered as a local best solution (x_l) form the small swarms and move towards the global optimum (x_g). Within this procedure, the local best solutions are taken randomly based on the best fitness. If the fitness of local best solutions (x_l) is greater than the (x_g) (x_g) i.e. $FF(x_l) > FF(x_g)$, then the position of the local best solutions is updated to a global best solution,

$$Cr_i = Cr_i + \delta * R * (x_g - Cr_i) \quad (13)$$

Where, Cr_i denotes a current local best solutions are updated as to global best, δ denotes a step which is a fixed value, R indicates a random number within $[0, 1]$, Cr_i is the local best individual position, and x_g is a global best position. Otherwise, the cockroach Cr_i goes to x_l (within its visibility) as given below,

$$Cr_i = Cr_i + \delta * R * (x_l - Cr_i) \quad (14)$$

Where, x_l denotes a local best solutions.

2) *Dispersion*: Another behavior is the dispersion of individuals which is carried out from time to time to maintain the diversity of cockroaches. Therefore, the behavior involves each cockroach performing a random step in the search space.

$$Cr_i = Cr_i + R(1, d) \quad (15)$$

Where, $R(1,d)$ denotes a d -dimensional random vector that the value is set within a certain range.

3) *Ruthless behaviour*: The final one is the Ruthless behavior which replaces the random individual into the current best individual (i.e. global best).

$$Cr_k = x_g \quad (16)$$

Where, Cr_k is a random integer within $[0, 1]$ and x_g is the global best position. This procedure was frequent once highest amount of repetition is attained. In this way, global optimum cluster head was selected for data dissemination for reducing end to end delay. Algorithmic process of optimization-based cluster head selection as given below,

Algorithm 2 Multi-attribute cockroach swarm optimization	
Input:	Number of cluster heads $CH_1, CH_2, CH_3, \dots, CH_m$ (i.e. cockroaches)
Output:	Select an optimal cluster head and perform data dissemination
Begin	
1.	Initialize the cockroaches populations $C_s = \{Cr_1, Cr_2, Cr_3 \dots Cr_n\}$ in search space
2.	For each Cr_i
3.	Measure the fitness FF
4.	While ($t < \text{Max_iteration}$) do
5.	If($(FF(Cr_i) > FF(x_g))$) then
6.	$Cr_i = x_g$
7.	Update the position $Cr_i = Cr_i + \delta * R * (x_g - Cr_i)$
8.	Else
9.	$Cr_i = x_l$
10.	Update the position $Cr_i = Cr_i + \delta * R * (x_l - Cr_i)$
11.	End if
12.	for $i = 1$ to N do
13.	$Cr_i = Cr_i + R(1, d)$
14.	$k = \text{random integer}([1, N])$
15.	$Cr_k = x_g$
16.	End for
17.	$t = t + 1$
18.	Obtain the global best solution
19.	Perform data dissemination via global best cluster head
End	

Algorithm 2 shows the processes of Multi-attribute cockroach swarm optimization to select the optimal cluster head for efficient data dissemination with minimum delay. The number of individuals is selected among the population. Then, the fitness is calculated to choose the cluster head in the network based on different behaviors of cockroach. This process is iterated until a maximum number of iteration gets reached. Finally, the technique performs the data dissemination via the selected cluster head.

III. SIMULATION SETUP AND PARAMETER SETTINGS

The simulation of proposed MIBCMCSO technique and existing CEGRAOD [1] and Multi valued DPSO [2] are implemented using NS2.34 network simulator where the 500 vehicle nodes are deployed in a square area of A2 (1100 m * 1100 m). The Random Waypoint model is used as node mobility in the simulation environment. The simulation time is set as 300 sec. The DSR protocol is used for cluster-based data dissemination in VANET. Table I describes the simulation parameters.

TABLE I. SIMULATION PARAMETERS AND VALUES

Simulation Parameters	Values
Network Simulator	NS2.34
Square Area	1100 m * 1100 m
Number of Vehicle Nodes	50,100,150,200,250,300,350,400,450,500
Number of Data Packets	25,50,75,100,125,150,175,200,225,250
Mobility Model	Random Waypoint Model
Speed of Sensor Nodes	0-20 m/s
Simulation Time	300 sec
Protocol	DSR
Number of Runs	10

Simulation of MIBCMCSO as well as existing technique were conducted by amount of vehicle nodes and data packets by different parameters are listed below.

IV. RESULT AND DISCUSSION

The simulation result analysis of the proposed MIBCMCSO technique and existing CEGRAOD [1] and Multi valued DPSO [2] are discussed in this section with parameters such as packet delivery ratio, end to end delay and throughput. The different performance metrics results are discussed using tables and graphical representation.

A. Impact of Packet Delivery Ratio

Packet delivery ratio is known as reliability. It is referred by amount of data packets correctly received to entire number of data packets transferred via source node. It is mathematically calculated by,

$$R = \left[\frac{\omega_{DR}}{n} \right] * 100 \quad (17)$$

Where number of data packet transferred is denoted as 'n' and amount of data packets successfully received is represented as ' ω_{DR} '. It is calculated by percentage (%).

TABLE II. PACKET DELIVERY RATIO

Vehicle Density	Packet Delivery Ratio (%)		
	MIBCMCSO	CEGRAOD	Multi Valued DPSO
50	94	84	80
100	95	86	82
150	96	88	84
200	95	89	85
250	96	88	84
300	97	90	85
350	96	91	86
400	95	90	85
450	97	91	86
500	96	89	85

Table II illustrates packet delivery ratio of data transmission versus vehicle density varies from 50 to 500. Reported results show packet delivery ratio is said to be improved using the MIBCMCSO technique as compared to other existing methods. Let us consider 50 vehicle densities for simulation, and 25 data packets are transferred via source node. Then destination node receives 24 data packets and the reliability of the MIBCMCSO technique is 96% whereas the reliability of the other two methods CEGRAOD [1] and Multi valued DPSO [2] are 84% and 80%, respectively. Fig. 3 illustrates various results of packet delivery ratio.

Simulation results of packet delivery ratio have different vehicle density of three methods MIBCMCSO and existing CEGRAOD [1] and Multi valued DPSO [2] are explained from Fig. 3. Graphical outcome clearly describes packet delivery ratio of data transmission in VANET is said to be improved using the MIBCMCSO technique with two existing methods. This improvement is achieved by applying the cluster based optimization process. In the clustering process, the different groups of vehicle nodes are obtained for efficient data transmission. Then the optimum cluster head selection effectively delivers the data packets from source to destination. The multi attribute cockroach swarm optimization considers the bandwidth availability to transmit the data packets. The maximum bandwidth availability minimizes the packet drop and increases data delivery. Table III specifies the simulation results of packet delivery ratio.

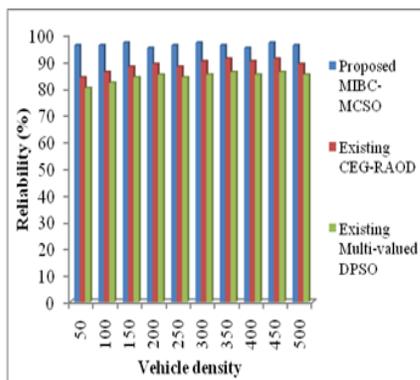


Fig. 3. Graphical Representation of Packet Delivery Ratio.

TABLE III. SIMULATION RESULTS OF PACKET DELIVERY RATIO

Parameters	CEGRAOD	Multi Valued DPSO
MIBCMCSO	14%	9%

B. Impact of End to End Delay

It refers to time difference among packet arrival time as well as data packet transmitting time. Therefore overall delay is expressed by,

$$D = \{t(D_a) - t(D_s)\} \tag{18}$$

As shown in Table IV, end to end delay of MIBCMCSO technique as well as existing CEGRAOD [1] and Multi valued DPSO [2] is described. The reported result evidently confirms that MIBCMCSO technique of end to end delay is reduced with other existing methods. A graphical result of end to end delay is illustrated from Fig. 4.

Fig. 4 depicts graphical illustration of end to end delay by vehicle density. From illustration, end to end delay of data transmission is comparatively lesser by MIBCMCSO with existing results. This is because of the clustering-based data transmission. In order to perform data transmission, the whole network is divided into the number of groups using a mutual information brown agglomerative clustering technique. The data transmission is carried out only through the cluster head instead of sending all the nodes in the network. Therefore, the end to end delay from source to destination is minimized. Let us consider 50 nodes for simulation and 25 data packets are considered for calculating the delay. MIBCMCSO receives the data packets with 9 ms of delay and CEGRAOD [1] and Multi valued DPSO [2] receives the packets with 14 ms and 17 ms. Similarly, the nine various results are carried out with respect to the number of nodes and different numbers of data packets. The simulation results of end to end delay are discussed in Table V.

C. Impact of Throughput

Throughput is referred by amount of data packets obtained on destination vehicle within specified time period. Therefore, throughput is expressed as follows,

$$T = \left(\frac{\omega_{DSR} (bits)}{time (sec)} \right) \tag{19}$$

TABLE IV. END TO END DELAY

Vehicle Density	End to End Delay		
	MIBCMCSO	CEGRAOD	Multi Valued DPSO
50	9	14	17
100	11	16	19
150	12	18	21
200	15	22	25
250	17	23	27
300	19	25	29
350	22	27	30
400	23	30	33
450	24	32	36
500	27	34	38

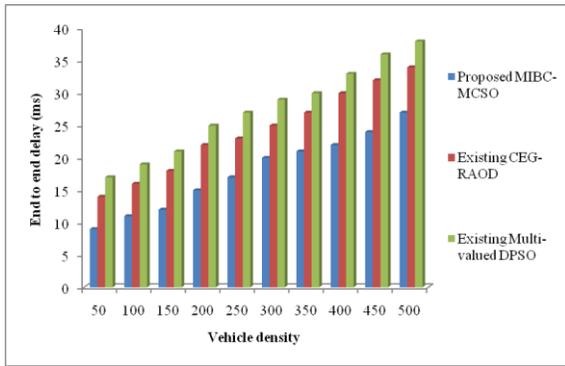


Fig. 4. Graphical Representation of End to End Delay.

TABLE V. SIMULATION RESULTS OF END TO END DELAY

Parameters	CEGRAOD	Multi Valued DPSO
MIBCMCSO	26%	37%

Where, T represents the throughput, $\omega_{DSR}(bits)\omega_{DSR}(bits)$ indicates amount of data packets obtained on destination in terms of bits. It is measured by bits per second (bps).

The simulation result of throughput versus data packets is transferred via source node is illustrated in Table VI. For experimental conduction, sizes of data packets are taken in the range from 10KB-100KB. While varying the input sizes, different throughput were achieved. Outcomes are plotted in two-dimensional graphical representation.

Fig. 5 depicts a graphical representation of the throughput versus sizes of data packets. The various sizes of data packets are given as input to horizontal pivot and throughput were acquired on vertical pivot. Throughput is comparatively increased than the existing methods. This significant development of the MIBCMCSO technique is obtained by the optimal cluster head selection using multiattribute swarm optimization. The minimum distance, higher residual energy, and maximum bandwidth availability are said to improve the data dissemination from source to destination through the optimum cluster head. The throughput results are given in Table VII.

TABLE VI. THROUGHPUT

Data Packet Size(KB)	Throughput		
	MIBCMCSO	CEGRAOD	Multi Valued DPSO
10	156	100	95
20	287	200	179
30	395	315	280
40	550	420	392
50	610	500	452
60	720	623	582
70	820	710	653
80	930	821	783
90	1050	910	872
100	1250	1052	986

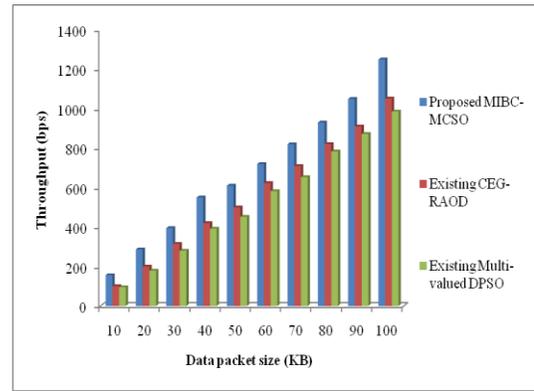


Fig. 5. Graphical Representation of Throughput.

TABLE VII. SIMULATION RESULTS OF THROUGHPUT

PARAMETERS	CEGRAOD	Multi Valued DPSO
MIBCMCSO	15%	36%

The above discussion of various results of metrics evidently proves that the MIBCMCSO technique improves the higher packet delivery rate data dissemination with minimum delay as well as higher network throughput.

V. CONCLUSION

An efficient clustering-based optimization technique called MIBCMCSO is proposed for reliable data dissemination. MIBCMCSO technique employs mutual informative brown clustering to collect mobile nodes towards various groups for data dissemination with minimum delay. Followed by, optimum cluster head selection was carried out through mobility metrics such as distance, energy, and bandwidth. Simulation is conducted by various parameters namely packet delivery ratio, delay as well as throughput. MIBCMCSO increases packet delivery ratio of data dissemination into vehicle network and minimizes delay compared with conventional methods. In future, multi-criteria optimization problem in the cluster head selection such as link stability, and link expiration time are used.

REFERENCES

- [1] Zahid Khan, Pingzhi Fan, Sangsha Fang and Fakhar Abbas, "An Unsupervised Cluster-Based VANET-Oriented Evolving Graph (CVoEG) Model and Associated Reliable Routing Scheme", IEEE Transactions on Intelligent Transportation Systems, pp. 1-16, 2019.
- [2] Manisha Chahal and Sandeep Harit, "Optimal path for data dissemination in Vehicular Ad Hoc Networks using meta-heuristic", Computers & Electrical Engineering, Elsevier, vol. 76, pp. 40-55, 2019.
- [3] Lei Liu, Chen Chen, Tie Qiu, Mengyuan Zhang, Siyu Li and Bin Zhou, "A data dissemination scheme based on clustering and probabilistic broadcasting in VANETs", Vehicular Communications, Elsevier, vol. 13, pp. 78-88, 2018.
- [4] Shahid Latif, Saeed Mahfooz, Naveed Ahmad, Bilal Jan, Haleem Farman, Murad Khan, and Kijun Han, "Industrial Internet of Things Based Efficient and Reliable Data Dissemination Solution for Vehicular Ad Hoc Networks", Wireless Communications and Mobile Computing, Hindawi, vol. 2018, pp. 1-16, 2018.
- [5] Joahannes B. D. da Costa, Allan M. de Souza, Denis Rosário, Eduardo Cerqueira and Leandro A. Villas, "Efficient data dissemination protocol based on complex networks' metrics for urban vehicular networks", Journal of Internet Services and Applications, Springer. vol 10, pp. 1-13, 2019.

- [6] Atif Ishtiaq, Sheeraz Ahmed, Muhammad Fahad Khan, Farhan Aadil, Muazzam Maqsood and Salabat Khan, "Intelligent clustering using moth flame optimizer for vehicular ad hoc networks", *International Journal of Distributed Sensor Networks*, vol. 15, issue. 1, pp. 1-13, 2019.
- [7] Shahid Latif, Saeed Mahfooz, Bilal Jan, Naveed Ahmad, Haleem Farman, Murad Khan, and Huma Javed, "Multicriteria Based Next Forwarder Selection for Data Dissemination in Vehicular Ad Hoc Networks Using Analytical Network Process", *Mathematical Problems in Engineering*, Hindawi, vol. 2017, pp. 1-18, 2017.
- [8] Abdelali Touil and Fattehallah Ghadi, "Efficient dissemination based on passive approach and dynamic clustering for VANET", *Procedia Computer Science*, Elsevier, vol. 127, pp. 369-378, 2018.
- [9] Xiyang Fan, Chuanhe Huang, Junyu Zhu and Bin Fu, "R-DRA: a replication-based distributed randomized algorithm for data dissemination in connected vehicular networks", *Wireless Networks*, Springer, vol. 25, issue. 7, pp. 3767-3782, 2019.
- [10] Min Xing, Jianping He, Lin Cai, "Utility Maximization for Multimedia Data Dissemination in Large-Scale VANETs", *IEEE Transactions on Mobile Computing*, vol. 16, issue. 4, pp. 1188-1198, 2017.
- [11] Rene Oliveira, Carlos Montez, Azzedine Boukerche and Michelle S. Wangham, "Reliable Data Dissemination Protocol for VANET Traffic Safety Applications", *Ad Hoc Networks*, Elsevier, vol. 63, pp. 30-44, 2017.
- [12] Osama Rehman and Mohamed Ould-Khaoua, "A hybrid relay node selection scheme for message dissemination in VANETs", *Future Generation Computer Systems*, Elsevier, vol. 93, pp. 1-17, 2019.
- [13] Sasirom Tiennoy and Chaiyachet Saivichit, "Using a Distributed Roadside Unit for the Data Dissemination Protocol in VANET With the Named Data Architecture", *IEEE Access*, Volume 6, 2018, Pages 32612- 32623.
- [14] Yu-Yu Lin and Izhak Rubin, "Integrated Message Dissemination and Traffic Regulation for Autonomous VANETs", *IEEE Transactions on Vehicular Technology*, Volume 66, Issue 10, 2017, Pages 8644 – 8658.
- [15] Chung-Ming Huang, Tzu-Hua Lin, Kuan-Cheng Tseng, "Data Dissemination of Application Service by Using Member-Centric Routing Protocol in a Platoon of Internet of Vehicle (IoV)", *IEEE Access*, Volume 7, 2019, Pages 127713 – 127727.
- [16] A. A. Khan, M. Abolhasan, W. Ni, J. Lipman and A. Jamalipour, "A Hybrid-Fuzzy Logic Guided Genetic Algorithm (H-FLGA) Approach for Resource Optimization in 5G VANETs," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 7, pp. 6964-6974, July 2019.
- [17] C. -M. Huang and C. -F. Lai, "The Delay-Constrained and Network-Situation-Aware V2V2I VANET Data Offloading Based on the Multi-Access Edge Computing (MEC) Architecture," in *IEEE Open Journal of Vehicular Technology*, vol. 1, pp. 331-347, 2020.
- [18] L. H. S. Lopes, R. A. F. Mini and F. Cunha, "A V2X Approach for Data Dissemination in Vehicular Ad Hoc Networks," 2019 IEEE Symposium on Computers and Communications (ISCC), 2019, pp. 1-6.
- [19] Banoth Ravi, Jaisingh Thangaraj, "Stochastic traffic flow modeling for multi-hop cooperative data dissemination in VANETs", *Physical Communication*, Volume 46, 2021.
- [20] Huda Abualola, Hadi Otrok, Rabeb Mizouni, Shakti Singh, "A V2V charging allocation protocol for electric vehicles in VANET", *Vehicular Communications*, 2021.
- [21] L. Yang, L. Zhang, Z. He, J. Cao and W. Wu, "Efficient Hybrid Data Dissemination for Edge-Assisted Automated Driving," in *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 148-159, Jan. 2020.

Face Age Estimation and the Other-race Effect

Oluwasegun Oladipo¹

Department of Computer and
Information Science, Covenant
University, Ota, Ogun State; CITM
Yaba College of Technology
Yaba, Lagos. Nigeria

Elijah Olusayo Omidiora²

Department of Computer Science
and Engineering, LAUTECH
Ogbomoso, Oyo State
Nigeria

Victor Chukwudi Osamor³

Department of Computer and
Information Sciences
Covenant University, Ota
Ogun State, Nigeria

Abstract—Age estimation is an automated method of predicting human age from 2-D facial feature representations. The majority of studies carried out in this research area use the FG-NET and MORPH 2 databases to train and test developed systems, which are lacking in black-face content. Most age frauds are perpetuated in the sub-Saharan African region due to the unavailability of an official database and unregistered births in the rural areas. The issues of unverified age in the region made it possible for under-age voters, under-age drivers, and the engagement of over-aged sportsmen. The other-race effect could reduce the performance of face recognition techniques, which could make techniques that work for white faces underperform when deployed for use in the predominately black face region. This study examines the other-race effect on face-based age estimation by analyzing the accuracy of an age estimation system trained with predominantly black faces against the same age estimation system trained with predominately white faces. The developed age estimation system uses a genetic algorithm-artificial neural network classifier and local binary pattern for texture and shape feature extraction. A total of 170 black faces were used for system testing. The result showed that the age estimation system trained with the predominantly black face database (GA-ANN-AES-855) outperformed the system trained with predominantly white faces (GA-ANN-AES-255) on testing with the aforementioned black face samples. The results obtained from the simulation were further subjected to inferential statistics, which established that the improvement in the correct classification rate was statistically significant. Hence, the other-race effect affects face-based age estimation systems.

Keywords—Component; face recognition; age estimation; other-race effect

I. INTRODUCTION

Computer-based age estimation is an automated way of predicting human age from 2-D features extracted from the face image. Most of the age fraud in recent days has been committed in Africa. The fraud goes unnoticed due to factors such as the unavailability of the national database of birth registration; some people give birth in unaccredited maternity centers and do not have the border to obtain birth certificates; and the acceptance of affidavit without questioning the authenticity [1].

Age validation and verification is one of the areas with least technological penetration in Africa. There is practically no popular IT-based system or tool to automatically verify an age claim. This made it possible for underage wards to beat systems and have access to documents like driver's license and

voter cards. Over-aged sportsmen still go unnoticed and people apply for jobs that are meant for people of lower ages. These are possible because of prevalent situation in Africa such as: Unclarified sworn to age affidavit that is not most-of -the-time confirmed, Birth certificate that was never collected at the point of giving birth to a child in the hospitals. Also, in sub-Saharan region of Africa, most people were not born in hospitals; as a result, most births were not documented by the National population commission [2].

In view of the above, most of the age claims made by the people in this region may not be true and are quite unreliable. Hence, there is a great need for an efficient and robust system for black-face age estimation and validation [2].

According to [3], most age estimation systems developed use MORPH II and FG-NET face databases, and these databases are scarcely populated with black face images, not considering the other-race effect. The other-race effect could make a face recognition technique that performs well with a specific race underperform when deployed for testing with faces of other races [4]. Hence, this study is aimed at examining the other-race effect on face-based age estimation. Memory depiction in humans and allied researches buttress the significance of other race in face recognition. The way human memory is depicted from literatures supports the consequence of the other race effect. This is evident in the phrasal saying; "they all look alike to me". Expanding this shows that some discriminating features makes identifying humans from the same race easily encoded and retrievable rather than the other race. The complications in the representation of human memory are what makes it seem like they all look alike despite being different individuals [5].

This property exhibited in humans can also be as a result of social prejudice, less frequent communication and little familiarity shared with people from different origin. During growth, a child's memory representation develops its ability to discriminate faces of his own race. In retrospect, this however mitigates the discernment capability of people within other race [6].

Theoretically, this can be explained from the principle of feature selection and associated processes. This selection begins during the child's development phase and procedure for facial identity discernment becomes memorably registered on a daily contact basis in a child. The aftermath is a deduction of excellent facial representation and encoding of faces which are seldom contacted and seen [7].

The other race effect could influence a computer-based recognition task such as age estimation, as it involves rigorous training procedure to aptly portray human faces. Also, there is a limited database on demographic category coverage for training different algorithms to identify the faces of individuals based on their respective racial backgrounds. Hence, an age estimation system that works well with white faces or other race might underperform when deployed for use with black faces [8][5].

The following are the objectives of the study:

- To develop a database of predominantly black faces.
- Training and testing of genetic algorithm-artificial neural network-based age estimation using the developed database.
- Performance evaluation of the age estimation system side by side with one trained with fewer black faces using correct classification.

The study is organized into five sections. Section I introduces the study with a brief discussion of the key words and also outlines the study objectives. Section II describes various related works in the area of face-based age estimation. Section III shows the methodology used in the study with their algorithms, while Section IV discusses the simulation result. The study is concluded in section V with recommendations for further studies.

II. RELATED WORK

Age prediction is often articulated in two categories. It's either categorized as a classification problem when a face is computed to be associated with one of $\{xa_1, xa_2, xa_3 \dots xa_N\}$ specified age group or as a regression problem which aims at evaluating age as a scalar $xa \in R$. [9][10], proffer a classification centered model which proceeds in two steps. The first step involved classifying faces to genders and race, while age is in turn estimated for the different and races. An ordinal classification model was deployed for age prediction in [11] [12]. Positioned decision boundaries are used in splitting the facial features into groups depending on their relational order. The ages are deduced by combining organized references from the positioned decision boundaries.

In the same vein, Han and Otto [13] [14] employed a hierarchical model for age prediction and also examined the effect of aging on features extracted from a 3-D face image. [15] Formulated a system for crowd density and age prediction despite sparse and unbalanced datasets, which are a common limitation to age estimation research. The developed system could harness the cumulative attribute approach to learning a regression model in the presence of face image dataset imbalances.

In [16], the author study offered a sparse regression approach, trained with the Face Recognition Grand Challenge database. The resulting model was tested using images in the FG- NET database. In [17], their study employed the use of deep learning architecture together with manifold learning for age estimation. The convolutional network was deployed for feature extraction and face aging features were obtained at

various layers of the system developed rather than just the top layer. The authors in [18] and [19] also pursue the use of a convolutional neural network (CNN) to increase the accuracy of the age estimation system.

The author in [20], developed an age estimation system using a back propagation artificial neural network trained with the FG-NET database. In this work, face images were classified into eight (8) age groups and principal component analysis was used for appearance and texture information representation.

The author in [21], examined the performance of age estimation systems developed using back propagation artificial neural network and self-organizing feature maps, which is an unsupervised learning paradigm neural network. The study employed principal component analysis for feature extraction and statistically examined which of the two aforementioned system performed better. The study deduction showed that the self-organizing feature map performed better than the back propagation trained artificial neural network.

The author in [22] showed that the performance of age estimation system can be improved by using large scale databases with deep learning algorithms. The study proposed a ranking CNN model that consists of basic CNN combined in series. The CNN content is trained with ordered age labels, and the final output is an aggregation formed from the binary output of constituent CNNs. It was concluded that ranking-CNN has the ability to outperform conventional CNN models.

The author in [23], deployed cumulative hidden layer approach to combat the issue of image dataset imbalances which are inherent in large databases. In the model learned age features using faces from neighboring ages uses a pair-wise relative signal in the supervision of the comparative ranking layer. The aging feature learning is fostered by the implemented ranking layer and also improves the age estimation of the overall model.

The author in [24] proposed a multi modal approach to age and gender estimation by using face images and speech recognition for age estimation. Two joint deep neural networks were trained with both appearance and depth information extracted from the face image. This is done alongside with the mel frequency cepstral coefficient extracted from speech samples. A novel cost function was developed to fine tune the joint deep neural network to ensure better accuracy and reduce the overhead of over fitting.

The author in [25], noted that fluctuation might result from deploying conventional convolutional neural network to face images in a video frame for age estimation. Furthermore, an attention mechanism was employed in addition to the convolutional network. This models an attention chunk which contains an aggregated feature space which is in turn presented as an encoded feature for age estimation. The stabilization of the frames is achieved using a novel loss function in order to achieve better age estimation of images in the frame.

The author in [26] used a variant of auto encoder for age, gender and race classification. In [27] their study, developed a hybrid system from the combination of CNN and Extreme Learning Machine (ELM). The CNN was adopted for age-

related feature extraction from the face images used while the ELM was deployed to classify into various age brackets. The study used the popular database MORPH II and the audience database for the training and testing of the developed system. The author in [28] leveraged the interrelationship of secondary demographic evidence such as race and gender in training a cascaded structured model. The secondary information assists in learning all the frameworks which are embedded in the parent network and sub-networks. This improved the accuracy of age prediction when compared to the previous age estimation system.

The author in [29] adopted the fusion of Local Discriminant Analysis (LDA), LBP, and Gabor filters for appearance, shape, and texture representation of the face image for age estimation. The study also used a combination of Support Vector Machine (SVM) and ANN to classify the age of the face into various age brackets. The ensemble was guided by the majority voting scheme and a computed age label was assigned from the combination of global and section-built matchers.

The author in [30] took cognizance of images taken in an uncontrolled environment and real-life situations using mobile phones. Such images have a degraded quality due to the phone camera's resolution. The images are fed into a conditional generative adversarial network (GAN) model to generate a reconstructed high-resolution version. The study used CNN for age estimation with PAL and MORPH face image databases for training and testing. Hasan & Mahdi [31] in their study used SVM as a classifier with LBP and FSM feature extraction techniques to represent face images. The two-way feature selection helped improve the performance of the age estimation system.

It is essential to keep track of the trends in research on automatic age prediction. Deep learning approaches seem promising but are known not to perform well with insufficient data [22]. Face image data collection is tedious in African contests. People over the age of 40 (fourth) find it difficult to enroll their faces. They are concerned that their true age will be revealed and will conflict with their official record at work, as some claim an age that is lower than their true age in order to secure available jobs for lower ages.

In order to ensure the limited black face dataset does not impair the performance of the developed system, the study uses a genetic algorithm modified back propagation trained artificial neural network-based classifier for age group estimation task. It also used selected data from the FG-NET database to complement the locally sourced data.

III. METHODOLOGY

Human faces are undoubtedly affected by physical development and the aging process. This facial alteration varies from person to person and is a consequence of a variety of factors like ancestry, health, lifestyle, gender, and race [28]. This study developed an age estimation system using a Genetic Algorithm (GA)-Artificial Neural Network (ANN). Local binary patterns were used for feature extraction in order to encode face images, which were trained using the GA-ANN

module. The architecture of the developed system is shown in Fig. 1.

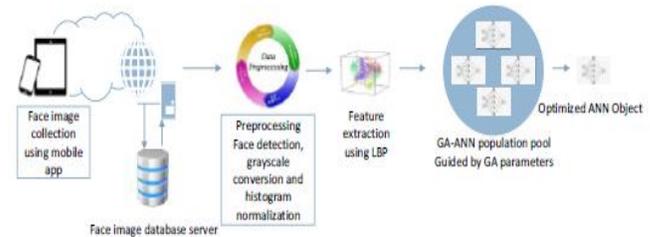


Fig. 1. The Developed Architecture.

It should be noted that the developed system used a shallow learning approach as opposed to the deep learning paradigm due to the limited number of face images in the database. The deep learning approach is known to have performance degradation issues with small datasets.

In order to examine the other-race effect in age estimation, the developed GA-ANN-based age estimation system was trained with the predominantly black face database developed for this study and also tested with 170 black face images. The result of this simulation was compared side by side with the result of a simulation done with the age estimation system trained with fewer black faces. The performance matrix used in this study is the Correct Classification Rate (CCR) of the age estimation system. The philosophy of the study is to examine if there is a significant difference in the performance of an age estimation system trained with more black faces when it is deployed for use with black faces. A One way ANOVA statistical tool was used for this purpose.

A. Face Image Collection

The face image collection was done using a custom built mobile application. The sequence diagram for the mobile app developed is shown in Fig. 2. The mobile application was developed to ease data collection from remote and distant locations. Fig. 3 displays the data collection module of the app. The mobile app is made available to voluntary candidates on Google Drive. The application was developed using HTML5, JavaScript, and CSS to ensure that it could be deployed for use across various mobile phone operating systems after compiling using CORDOVA. As a result, data sourcing was not restricted to specific locations and distances. The FG-NET facial database was used to complement the locally sourced data and create a data bank for training and testing the developed genetic-artificial neural network.

A total of 855 (eight hundred and fifty-five) images were collected using the mobile application developed. 500 (five hundred) images were selected for the FG-NET database to complement the acquired data in order to train and test the developed age estimation system. Fig. 4 shows sample images from the dataset. Table I shows the age distribution of faces in the database.

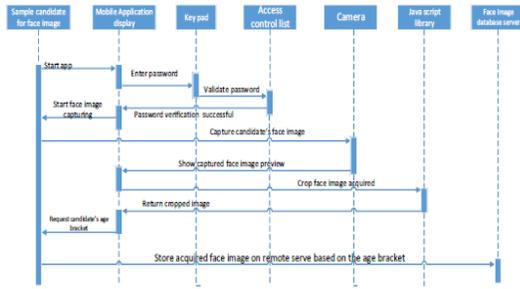


Fig. 2. UML Sequence Diagram for the Face Image Collection Module.

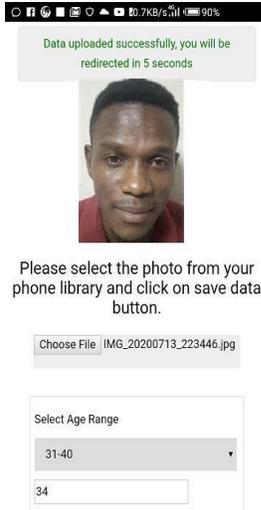


Fig. 3. Mobile App Interface.



Fig. 4. Sample Images from the Black Face Dataset.

TABLE I. DATASET AGE DISTRIBUTION

Age Groups	Black faces	FG-NET faces	Total
0 to 5	109	91	200
6 to 10	103	86	189
11 to 20	250	113	363
21 to 30	118	82	200
31 to 40	90	68	158
41 to 50	70	39	109
51 to 60	57	14	71
Above 60	58	7	65
Total	855	500	1355

B. Simulation Tool

The age estimation system shown in Fig. 1 was implemented using the MATLAB 2018 object-oriented programming tool. MATLAB was the tool of choice because of its rich computer vision library that makes implementing various techniques and algorithms easy.

C. Preprocessing

Images obtained from the mobile app are in-turn stored in age labeled directories on the online image server. During preprocessing the images are converted to grayscale after which the face area are detected using viola jones algorithm and automatically cropped out of the acquired face image. This was to ensure background information that could introduce noise into the system is eliminated. The resulting image is subjected to histogram normalization.

D. Features Extraction

The feature extraction technique used in this study is the Local Binary Pattern (LBP). The LBP is used to extract the age information in the face image. The motivation for the choice of the technique is its richness in encoding shape and texture information which are basic theoretical properties that forms the bases of face based age estimation.

Considering a 3x3 pixels with center pixel (xc,yc) intensity value be gc and local texture as $T = t(g_0, \dots, g_7)$ where $g_i (i = 0, \dots, 7)$ corresponds to the grey values of the 8 surrounding pixels. These surrounding pixels are thresholded with the center value gc as $t(s(g_0 - gc), \dots, s(g_7 - gc))$ and the function $s(x)$ is defined in (1). Then the LBP pattern at a given pixel can be obtained using (2) (Lakshmirabha, 2016).

$$S(x) = \begin{cases} 1, & x > 0 \\ 0, & x \leq 0 \end{cases} \quad (1)$$

$$LBP(Xc, Yc) = \sum_{i=0}^7 8(g_i - gc)2^i \quad (2)$$

The LBP feature extracted was further subjected to principal component analysis to reduce the feature set and ensure discriminating features are used as input to the GA-ANN classifier module. The feature vectors (I) from LBP serves as the training set for the PCA method. M be the total number of images in the training set. The deviation of each image from the mean image is calculated using the (3) and (4).

$$\psi = \frac{1}{M} \sum_{n=1}^M I_n \quad (3)$$

$$\phi_n = I_n - \psi \quad (4)$$

The variation among the eigenvectors of the covariance matrix is calculated using (5). The space where all this eigenvectors resides is called as eigenface space or eigenspace. All the training set images are projected into the eigenface space using (5). All training set images are projected to the eigenface space using (6).

$$C = \frac{1}{M} \sum_{n=1}^M \phi_n \phi_n^T = AA^T \quad (5)$$

$$\omega_k = U_k \cdot \phi = U_k \cdot (1 - \phi) \quad (6)$$

The Weighted Matrix $\Omega = [\omega_1, \omega_2, \dots, \omega_M]^T$ is the representation of a training image in the eigenface space. A

new test image is classified by extracting Gabor and LBP features. It is then mean subtracted using (4) followed by projection onto the eigenface space using (6). Weight matrix of the test image $\Omega T = [\omega_1, \omega_2, \dots, \omega_M]^T$ is calculated by projecting test image to eigenspace. This weighted matrix ΩT is used for classification purpose.

E. Classification using GA-ANN Module

The GA-ANN is a parallel combination of genetic algorithm and artificial neural network techniques. The GA is aimed at optimizing ANN parameters to generate an optimized ANN object that will in turn be used in predicting the age of a test image. The combination is motivated by the capacity of GA to traverse through a problem space in a timely manner in order to select the fittest candidate solution.

In order to achieve this hybrid system, ANN parameters are encoded as genes in genetic algorithm chromosome. The ANN parameters encoded as genes include the number of hidden layers, the Momentum update (MU), the Momentum update decreasing factor (MU_dec) and the learning rate. Fig. 5 describes a sample gene. The system uses one point crossover technique and Mutation probability (Mp) of 0.1. Other parameters include Number of GA generations (Ngen) and Population size (Ps). The Ngen and Ps used in this study is 100 and 15 respectively in order to ensure the system used for the simulation is not over labored. Candidates' fitness was computed using (7). Fig. 6 shows a sample reproduction mating of two parent in order to form offspring.

$$\text{Fitness} = \frac{1}{\text{MSE}} \tag{7}$$

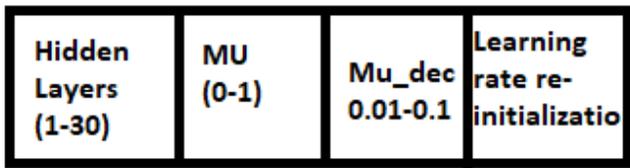


Fig. 5. Sample Chromosome Structure in the Modeled Genes

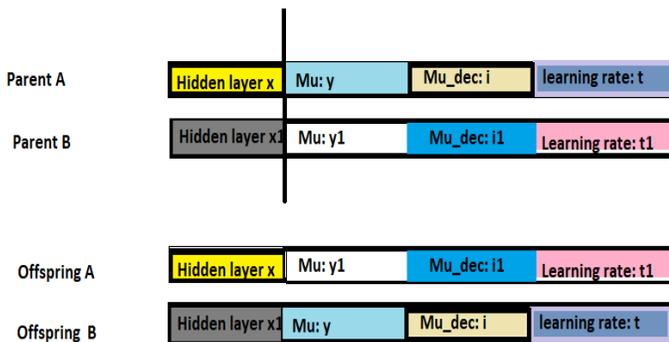


Fig. 6. Single Point Cross-over Implemented in the Developed Model.

The developed algorithm for the hybridized classifier is shown below.

1. Start
2. Set GA parameters (Cp, Mp, Ngen and Ps)
3. popCount = 0, Fitmax = 0, optimalAnnObject = NULL, genCount = 0
4. While PopCount <= Ps
5. Generate random values for the ANN parameters encoded into GA chromosome (Number of hidden layer, Mu, and Mu_dec)
6. Create parent (ANN object instances) in population
7. Increment the value of PopCount and create new parents by repeating steps 5-6
8. Compute the fitness of each parent (ANN object) using equation 3.
9. While gencount <= Ngen
10. Select parent with high fitness in descending order
11. If fitness (top 1 parent) > fitmax goto 12 else goto 13
12. Fitmax = fitness (top 1 parent) goto 14
13. Fitmax = Fitmax
14. OptimalAnnObject = Parent (with fitness, fitness)
15. Perform crossover on strongest parents to create new offspring and replace weakest parent with new child created
16. Mutate the population based on mutation probability
17. Compute the fitness of the new population (i.e. new ANN pool)
18. Increment genCount and repeat step (10) to (17) until genCount is equal to number of Ngen
19. optimalAnnObject is assigned GA-ANN with the global minimal solution
20. Return the GA-ANN object for classification
21. Stop

F. Age Estimation System Testing

Simulation I: A total of 170 (one hundred and seventy) black faces were used in testing the age estimation system. The age estimation system was trained using the predominantly black-faced database developed for the study. Testing implies that an unknown black face is fed into the optimized GA-ANN module in order to be classified into its appropriate age group. This simulated system is represented as GA-ANN AES-855.

Simulation II: The GA-ANN classifier module was trained with a database with reduced number of black faces. 600 black faces were replaced with faces from FG-NET. This resulted in a training dataset of 1100 FG-NET faces and 255 locally sourced black faces. 170 black faces were in-turn used to test the trained GA-ANN-based age estimation system. The simulation II is represented as GA-ANN-AES-255. The diagram of testing phase is shown in the Fig. 7 and the testing dataset used is shown in Table II.

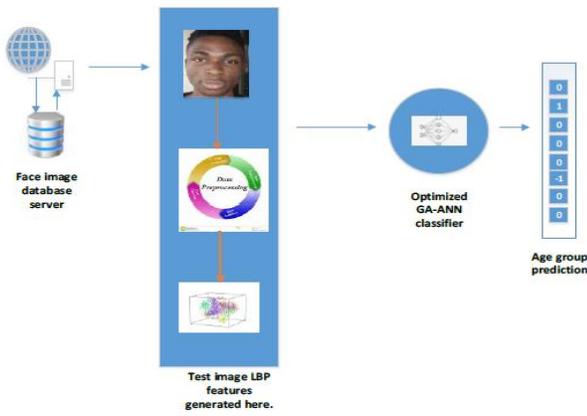


Fig. 7. Diagram of the Testing Phase Architecture.

TABLE II. AGE DISTRIBUTION OF TEST IMAGES

Age Groups	Number of test images
0-5	20
6-10	20
11-20	30
21-30	30
31-40	20
41-50	20
51-60	15
Above 61	15
TOTAL	170

G. Performance Evaluation

The performance of the age estimation system trained using the database containing 855 and 255 black faces, respectively were evaluated using the Correct Classification Rate (CCR). The CCR was computed using (8).

$$CCR = \frac{1}{n} \sum_{i=1}^n \delta(y, Y) \tag{8}$$

The ‘ δ ’ is an indicator variable, as such $\delta(y, Y)$ is computed as 1 if $y = Y$ and Zero when $y \neq Y$. The correct classification rate is used in order to take advantage of its ease of elucidation in discriminant analysis. It's also worth noting that calculating the correct classification rate doesn't need domain-specific data. As a result, this metric may be used to compare the classification accuracy of different models.

IV. RESULT AND DISCUSSION

This section discusses the results obtained from simulations I and II, respectively, presented in Tabular form. This study categories age into 8 age brackets namely 1-5, 6-10, 11-20, 21-30, 31-40, 41-50, 51-60 and above 60. Table III presents the CCR achieved for the age estimation system during simulation I and II, respectively.

The age estimation system simulated with the developed database (GA-ANN-AES-855) outperforms the system simulated using 255 black faces (GA-ANN-AES-255). The aggregate CCR for the GA-ANN-AES-855 is 91.18% and the CCR for the GA-ANN-AES-255 is 80%.

TABLE III. CORRECT CLASSIFICATION RATE FOR AGE ESTIMATION SYSTEM WITH 855 AND 255 BLACK FACES RESPECTIVELY

AGE	Test Images	GA-ANN-AES-855		GA-ANN-AES-255	
		Correct Classification	CCR (%)	Correct Classification	CCR (%)
0-5	20	18	90.00	14	70.00
6-10	20	18	90.00	16	80.00
11-20	30	30	100.00	27	90.00
21-30	30	26	86.67	24	80.00
31-40	20	19	95.00	17	85.00
41-50	20	18	90.00	16	80.00
51-60	15	13	86.67	11	73.33
Above 61	15	13	86.67	11	73.33
TOTAL/AG G	170	155	91.18	136	80.00

This result is in agreement with [8]. The reason for this is the other race effect. The more the population of a race in the training dataset, the better the recognition performance with a testing set of the same race. The result could also be seen to be in agreement with the discoveries in [5] that indicated that insight from racial information could affect the awareness of memory processes. In this case, age estimation, a computer-based recognition process, is being affected by the racial information in the training data.

Also, the trend in the results showed that the highest correct classification rates were achieved in the age brackets of 11–20. The age bracket has the highest number of images in the dataset — 363 images. This indicates that the discriminating ability of the encoded facial features in discerning age is improved with the quantity of images in the training dataset. This aligns with the discoveries of Oladele [20]. The AES performs less than expected when tested with faces that are not popular in the training dataset.

Fig. 8 shows the chart of the CCR of GA-ANN-AES-855 and GA- ANN-AES-255, respectively.

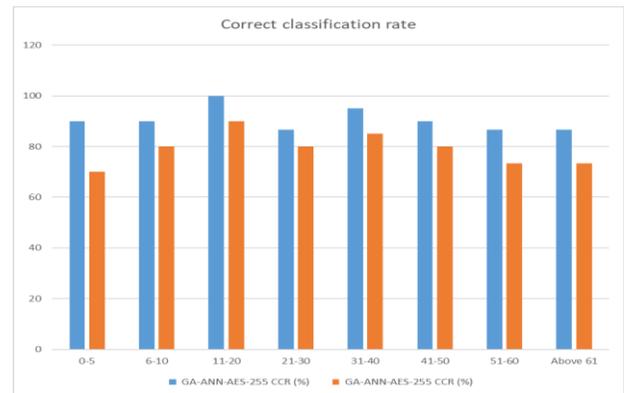


Fig. 8. Correct Classification rate: GA-ANN-AES-855 and GA-ANN-AES-255.

The result of the experimentation was further subjected to inferential statistics using one-way-ANOVA. The result is as shown.

The result, after subjecting Table II which showed the CCR of GA-ANN-AES-255 and GA-ANN-AES-855 to statistical analysis:

H_0 : No significant improvement in the CCR of GA-ANN-AES-855 over GA-ANN-AES-255

H_1 : There is significant improvement in the CCR of GA-ANN-AES-855 over GA-ANN-AES-255

Significance level = 0.05

Equal variances were assumed for the analysis.

Factor Information

Factor Levels Values

Factor 2 GA-ANN-AES-255, GA-ANN-AES-855

Analysis of Variance

Source	DF	Adj SS	Adj MS	F-Value	P-Value
Factor 1	544.6	544.64	16.56	0.001	
Error	14	460.4	32.89		
Total	15	1005.1			

The P-value (0.001) showed in the result of the analysis is less than 0.05. Hence, the alternative hypothesis is accepted and the null hypothesis is rejected. This implies that the improvement in correct classification rate of GA-ANN-AES-855 over GA-ANN-AES-255 is statistically significant.

V. CONCLUSION AND RECOMMENDATION

The study examines the effect of other-race effect on automatic age estimation. In order to achieve this, we developed a predominantly black face database that contains 855 black faces complemented with 500 FG-NET faces. The developed database was used in training a GA-ANN age estimation system. A second scenario is simulated, with the GA-ANN-based age estimation system trained with 255 black face images and 1100 FG-NET faces. Both systems were tested with 170 black faces to query if the heightened number of black faces in the developed image database ensures a better correct classification rate.

The study showed that the GA-ANN-AES-855 outperformed the GA-ANN-AES-255 with a CCR of 91.18% compared to the 80.00% shown by the GA-ANN-AES-255. Inferential statistics to show the improvement is statistically significant using one way ANOVA was conducted. The result of the statistical evaluation established that the improvement was significant and hence showed that the other-race effect could affect the performance of an age estimation system.

This study recommends the following:

1) The aggregation of various black face databases to form a huge face image database that can foster the use better techniques that perform when image data volume is much.

2) Deployment of the developed genetic algorithm-artificial neural network age estimation model on mobile phone platform to ensure age verification can be carried out using application built using such model.

3) The development of age estimation algorithms that will be robust enough to minimize other age effect in age estimation.

REFERENCES

- [1] R. Angulu, J. R. Tapamo, and A. O. Adewumi, "Age-group estimation using feature and decision level fusion," *The Computer Journal*, vol. 62, no. 3, pp. 346–358, 2018.
- [2] O. Oladipo, I. P. Osamor, V. C. Osamor, T. N. Abiodun, A. O. Omoremi, M. O. Odim, and R. H. Ekpo, "Face-age modeling: A pattern recognition analysis for age estimation," 2019 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), 2019.
- [3] D. Akinyemi and O. Onifade, "The impact of indigenous ethnicity on facial image analysis," *Academia Letters*, vol. 2, pp. 2–7, 2021.
- [4] J.L.Yaros, D.A. Salama, D. Delisle, M.S. Larson, B.A. Miranda and M.A.Yassa, "A memory computational basis for the other-race effect. Scientific reports, Vol 9, pp.1-11, December 2019.
- [5] J. Chen and X. Zhu, "The cross-race effect on face recognition and judgments of learning," *Proceedings of the 3rd International Conference on Culture, Education and Economic Development of Modern Society (ICCESE 2019)*, vol. 310, pp. 672–675, 2019.
- [6] M. Stelter and J. Degner, "Investigating the other-race effect in working memory," *British Journal of Psychology*, vol. 109, no. 4, pp. 777–798, 2018.
- [7] J. R. Collova, N. Kloth, K. Crookes, N. Burton, C. Y. Chan, J. H. Hsiao, and G. Rhodes, "A new other-race effect for gaze perception," *Journal of Experimental Psychology: Human Perception and Performance*, vol. 43, no. 11, pp. 1857–1863, 2017.
- [8] P. J. Phillips, F. Jiang, A. Narvekar, J. Ayyad, and A. J. O'Toole, "An other-race effect for face recognition algorithms," *ACM Transactions on Applied Perception*, vol. 8, pp. 1–11, January 2011.
- [9] J.D. Akinyemi and O.F.W Onifade. "A computational face alignment method for improved facial age estimation." In 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), pp. 1-6. IEEE, 2019.
- [10] G. Guo and G. Mu, "A framework for joint estimation of age, gender and ethnicity on a large database," *Image and Vision Computing*, vol. 32, pp. 761–770, 2014.
- [11] K.-Y. Chang, C.-S. Chen, and Y.-P. Hung, "Ordinal hyperplanes ranker with cost sensitivities for age estimation," *Conference on Computer Vision and Pattern Recognition*, August 2011.
- [12] K.k. Kamarajugadda and T.R Polipalli, "Extract features from periocular region to identify the age using machine learning algorithms. *Journal of medical systems*. Vol. 3, pp.1-5, July 2019.
- [13] H. Han, C. Otto, and A. Jain, "Age estimation from face images: Human vs. machine performance," in *Biometrics (ICB)*, 2013 International Conference, pp. 1–8, June 2013.
- [14] R. Angulu, J.R. Tapamo, and A.O. Adewumi, "Age estimation via face images: a survey. *EURASIP Journal on Image and Video Processing*, pp.1-35, June 2018.
- [15] K. Chen, K. Jia, H. Huttunen, J. Matas and J.K Kämäräinen, "Cumulative attribute space regression for head pose estimation and color constancy," *Pattern Recognition*, Vol. 87, pp.29-37. 2019.
- [16] A. Demontis, B. Biggio, G. Fumera, and F. Roli, "Super-sparse regression for fast age estimation from faces at test time," in *Image Analysis and Processing ICIAP 2015*, pp. 551–562, Springer, 2015.
- [17] X. Wang and C. Kambhamettu, "Age estimation via unsupervised neural networks," in *Automatic Face and Gesture Recognition (FG)*, 2015 11th IEEE International Conference and Workshops on, vol. 1, pp. 1–6, May 2015.
- [18] S. Hosseini, S.H. Lee, H.J. Kwon, H.I. Koo and N.I. Cho, "Age and gender classification using wide convolutional neural network and Gabor filter," In 2018 International Workshop on Advanced Image Technology (IWAIT), pp. 1-3., January 2018.
- [19] D. Yi, Z. Lei, and S. Z. Li, "Age estimation by multi-scale convolutional network," in *Computer Vision-ACCV*, pp. 144–158, 2015.

- [20] M. Oladele, E. Omidiora, and A. Afolabi, "A face-based age estimation system using back propagation neural network technique," *British Journal of Mathematics & Computer Science*, vol. 13, pp. 1–9, 2016.
- [21] E. Omidiora, M. Oladele, T. Adepoju, A. Sobowale, and O. Olatoke, "Comparative analysis of back Propagation neural network and self-Organizing feature map in Estimating age groups using facial features," *British Journal of Applied Science & Technology*, vol. 15, pp. 1–7, 2016.
- [22] S. Chen, C. Zhang, M. Dong, J. Le, and M. Rao, "Using ranking-cnn for age estimation," *2017 IEEE Conference on Computer Vision and Pattern Recognition (CVPR)*, 2017.
- [23] K. Li, J. Xing, W. Hu, and S. J. Maybank, "D2c: Deep cumulatively and comparatively learning for human age estimation," *Pattern Recognition*, vol. 66, pp. 95–105, 2017.
- [24] Z. Qawaqneh, A. A. Mallouh, and B. D. Barkana, "Age and gender classification from speech and face images by jointly fine-tuned deep neural networks," *Expert Systems with Applications*, vol. 85, pp. 76–86, 2017.
- [25] Z. Ji, C. Lang, K. Li, and J. Xing, "Deep age estimation model stabilization from images to videos," *2018 24th International Conference on Pattern Recognition (ICPR)*, 2018.
- [26] S. Zaghbani, N. Boujnef, and M. S. Bouhlel, "Age estimation using deep learning," *Computers & Electrical Engineering*, vol. 68, pp. 337–347, 2018.
- [27] M. Duan, K. Li, C. Yang, and K. Li, "A hybrid deep LEARNING Cnn-elm for age and gender classification," *Neurocomputing*, vol. 275, pp. 448–461, 2018.
- [28] J. Wan, Z. Tan, Z. Lei, G. Guo, and S. Z. Li, "Auxiliary demographic information assisted age estimation with cascaded structure," *IEEE Transactions on Cybernetics*, vol. 48, no. 9, pp. 2531–2541, 2018.
- [29] R. Angulu, J. R. Tapamo, and A. O. Adewumi, "Age estimation with local ternary directional patterns," *Image and Video Technology*, pp. 421–434, 2018.
- [30] S. H. Nam, Y. H. Kim, N. Q. Truong, J. Choi, and K. R. Park, "Age estimation by SUPER-RESOLUTION reconstruction based on adversarial networks," *IEEE Access*, vol. 8, pp. 17103–17120, 2020.
- [31] N.F Hasan and S. Q. Mahdi. "Facial Features Extraction Using LBP for Human Age Estimation Based on SVM Classifier." In *2020 International Conference on Computer Science and Software Engineering (CSASE)*, pp. 50-55. IEEE, 2020.

Polarity Detection of Dialectal Arabic using Deep Learning Models

Saleh M. Mohamed*, Ensaf Hussein Mohamed, Mohamed A. Belal

Department of Computer Science, Helwan University
Cairo, Egypt

Abstract—With the evolution of a new era of technology and social media networks, as well as an increase in Arabs sharing their point of view, it became necessary that this research be conducted. Sentiment analysis is concerned with identifying and extracting opinionated phrases from reviews or tweets. Specifically, to determine whether a given tweet is positive, negative, or neutral. Dialectal Arabic poses difficulties for sentiment analysis. In this paper, four deep learning models are presented, to be specific convolution neural networks (CNN), long short-term memory (LSTM), a hybrid of (CNN-LSTM), and Bidirectional LSTMs (BiLSTM), to determine the tweets polarities written in dialectal Arabic. The performance of the four models is validated on the used corpus with the use of word embedding and applying the (k-Fold Cross-Validation) method. The results show that CNN outperforms the others achieving an accuracy of 99.65%.

Keywords—Sentiment analysis; word embedding; sentiment classification; dialectal arabic; deep learning

I. INTRODUCTION

Sentiment analysis is a kind of natural language processing (NLP), where NLP, or computational linguistics, is the scientific research on human language from a computational perspective [1]. Natural language processing [2] is a large-scale field that includes applications and exploration such as translation, generation, understanding of human language, speech & named entity recognition, question answering, and information retrieval, and relationship extraction. Sentiment analysis (SA) uses natural language processing, statistical data, or machine learning techniques to extract the sentiment content of a text. SA, also called opinion analysis in the literature, is a process of automatically identifying opinions on certain topics in a text, whether they are “positive” or “negative” opinions.

Analysis of opinions or feelings continues to attract interest in industry and academics. Nowadays, sentiment analysis is extensively used in various languages. While considerable progress has been made in developing models to analyze sentiment, the field remains an active field of research for many languages throughout the world, especially for Arabic as the fifth most widely used and fourth most frequently used language on the Internet [3]. The analysis of Arabic language sentiments is still limited and considered difficult for a variety of reasons: First, there are very complex structures in the Arabic language. Second, the limited resources for Arabic SA make it difficult to find. Third, it contains a lot of morphological and highly ambiguous terms, many irregular structures, and a wide range of dialectal varieties without writing standards. The complexity of the Arabic language, as

discussed earlier, makes it fly in the face of most NLP applications [4].

Arabic is divided into three major categories [5]: 1) classical Arabic (CA), which is the language of the Quran; 2) modern standard Arabic (MSA), a standardized official language that can be written in the news and taught in schools; and 3) dialectal Arabic (DA), used in daily life and oral communication. It is usually an MSA mix of one or more Arab dialects used on social media [6].

Using different dialects on social media, allowing Arabic users to express their thoughts freely, complicates SA. In terms of phonology, morphology, lexical choice, and syntax, Arabic dialects are significantly different from MSA. The dialects of Arabic are divided into [7]:

- Egyptian Arabic (EA): Egyptian and Sudanian Arabic.
- Levantine (LA): Lebanese, Syrian, Palestinian, and Jordanian Arabic.
- Gulf Arabic (GA): Gulf Arabic for the Gulf region.
- Iraqi (IA): Iraqi Arabic.
- Maghrebi (MA): Maghrebi Arabic for Morocco, Algeria, Tunisia, Mauritania, and Libya.

The majority of previous Arabic sentiment analysis research was done on MSA. Where dialects are used, Egyptian (MSA/Egyptian) was the favorite one. Research has been conducted with dialects of (Lebanese, Syrian, Iraqi, Libyan, Algerian, Tunisian, and Sudanese). There are different approaches used in Arabic SA and its dialects. SA approaches are classified into four classes: supervised, unsupervised, semi-supervised, and hybrid [8].

Recently, the world has witnessed a great revolution in deep learning, which has become the cornerstone of many improvements in many fields. The English NLP work began early using deep learning models, and then Arabic NLP. The use of deep learning for Arabic SA has recently received greater attention, showing significant performance improvements [9].

Since efforts to apply deep learning are still limited, further experimental work in this field is needed. This paper focuses on the Arabic language, especially Colloquial Arabic with an Egyptian dialect, and introduces different deep learning models based on word embeddings to automatically detect the polarity of tweets as positive or negative.

*Corresponding Author.

The main contribution of this research is:

Four different deep learning models were proposed using convolution neural networks (CNN), long short-term memory (LSTM), a hybrid of (CNN-LSTM), and bidirectional LSTM (BiLSTM) on the corpus [10].

- The four models are presented with a comparative evaluation using a word embedding technique that represents words into vectors called "continuous bag of words" (CBOW)
- The proposed model outperforms previous related models. It outperforms the model presented by Mohammed and Kora [11], which uses the same models over the same corpus but differs by 24% in CNN, 10% in LSTM.
- The experiments were extended by applying the bidirectional LSTMs (BiLSTM).

The rest of the paper is organized as follows: In Section 2, related work in Arabic SA is presented. The method and materials are presented in Section 3. Section 4 presents the results of the experiments and discussion. Finally, Section 5 discusses the conclusion and our future work.

II. RELATED WORK

The literature presents several works of Arabic sentiment analysis. In this section, the published works of the last six years are covered in this area.

Many papers have been conducted between the years 2005 and 2020 that applied deep learning approaches. 77 papers work on Arabic with its dialects. 18 models of deep learning were applied by the researchers. CNN and RNN are considered the most commonly used models [12]. In the papers sampled in [13], modern standard Arabic (MSA) has been widely used among other types and Egyptian (MSA/Egyptian) is preferred when dialects are used.

There have been a few studies that work on DA or mix both MSA and DA, specifically (MSA/Egyptian). Table I summarises these studies by author, year, and the used methodology. Also, the results of these studies and the used datasets are shown in Table II.

Attia et al. [14] built a multilingual system with multi-class sentiment analysis using CNN. They applied their system to three datasets with three different languages, which are Arabic, English, and German, but here focusing on the Arabic language. For the Arabic language, they used the Arabic Sentiment Tweets Dataset (ASTD) dataset. The ASTD dataset consists of 10.6k tweets. The tweets were gathered from Egypt Trends and were not identified with a specific topic. Their system achieved an accuracy of 67.93% on the ASTD dataset.

Heikal et al. [15] applied two models, which are CNN and LSTM, to the same ASTD dataset. They also used multi-class sentiment analysis. The accuracy of their models is that CNN achieved 64.30% and LSTM achieved 64.75%. Also, similar work by Elnagar et al. [16] applied several models, which are CNN, LSTM, and CNN-LSTM. They tested their models on the Books Reviews in the Arabic Dataset (BRAD). The BRAD

dataset consists of 6.9k tweets in different Arabic dialects. CNN achieved an accuracy value of 89.61%, while LSTM and CNN-LSTM achieved 90.05% and 90.02%, respectively.

Another research by Abdellaoui et al. [17] proposed CNN and LSTM on two different datasets, which are ASTD and TEAD. The TEAD dataset consists of 6 million tweets that combine MSA and DA. They applied CNN and LSTM on both datasets. CNN and LSTM achieved precision values of 79% and 81%, respectively, on the ASTD data set, while they achieved 86% and 87.5% on the TEAD dataset.

TABLE I. STUDIES BY METHODOLOGY

Ref	Authors	Year	Methodology
[14]	Attia et al.	2016	CNN
[15]	Heikal et al.	2018	CNN LSTM
[16]	Elnagar et al.	2018	CNN LSTM CNN-LSTM
[17]	Abdellaoui et al.	2018	CNN LSTM
[18]	Abdullah et al.	2018	CNN-LSTM
[19]	Abu et al.	2019	LSTM BiLSTM
[20]	L. H. Baniata and S. Park.	2016	CNN-BiLSTM BiLSTM-CNN
[11]	Mohammed and Kora	2019	CNN LSTM CNN-LSTM

TABLE II. STUDIES BY EXPERIMENTAL RESULTS

Ref	DataSet	Results (Accuracy A, F1-Score F, Precision P, Spearman Correlation Scores S) %
[14]	ASTD	CNN (A=67.93, F=29.82)
[15]		CNN (A=64.30, F=64.09) LSTM (A=64.75, F=62.08)
[16]	BRAD	CNN (A=89.61) LSTM (A=90.05) CNN-LSTM (A=90.02)
[17]	ASTD	CNN (P=79) LSTM (P=81)
	TEAD	CNN (P=86) LSTM (P=87.5)
[18]	SemEval 2018 Task 1	CNN-LSTM (S=81.80)
[19]	ASTD	LSTM (A=42.00) BiLSTM (A=41.30)
	LABR	LSTM (A=42.00) BiLSTM (A=41.30)
	ShamiSenti corpora	LSTM (A=64.70) BiLSTM (A=61.80)
[20]	LABR	CNN-BiLSTM (A=86.43) BiLSTM-CNN (A=66.26)
[10]	Corpus on Arabic Egyptian tweets	CNN (A=75.72) LSTM (A=81.31) CNN-LSTM (A=88.05)

Abu et al. [19] developed the Shami-Senti corpus, which is regarded as the first Levantine corpus of DA. Then they apply DL models built for MSA on that corpus of DA. They applied LSTM and BiLSTM on ASTD and LABR datasets, but the result wasn't promising as it was around 50%. After that, they applied them again to the Shami-Senti corpus. The results were better than before, as they exceeded 60%.

L.H. Baniata and S. Park proposed a DL model for Arabic SA. They combined CNN and BiLSTM once, and BiLSTM and CNN another time, and compared the results. They tested both models on the LABR dataset. The results have shown that CNN-BiLSTM outperformed the other one by an accuracy value of 86.43%.

Another research by Abdullah et al. [18] developed the SEDAT system, which is used for detecting sentiments and emotions written in the Arabic language. They applied CNN-LSTM with the help of document embedding on the SemEval 2018 dataset. They showed the performance results with Spearman correlation scores with a value of 81.80%.

Mohammed and Kora [11] proposed a corpus of Egyptian tweets consisting of 40k tweets with their polarity. Then they applied three DL models, which are CNN, LSTM, and CNN-LSTM. CNN achieved accuracy with a value of 75.72%, LSTM achieved 81.31%, and CNN-LSTM 88.05%. Also, they applied a data augmentation technique, which affects DL performance.

Despite the fact that most models of deep learning have enhanced the accuracy of Arabic sentiment analysis, there is still potential for development. The findings of this review indicate that more efforts are needed to develop DL models. This motivated us to investigate various deep learning models to improve the accuracy of Arabic SA.

III. METHODS AND MATERIALS

This section shows the dataset that was used as well as the details of the proposed model.

A. Used Dataset

The dataset utilized is mainly drawn from the Corpus of Arabic Egyptian tweets [11], a corpus of 40,000 tweets written in the Egyptian dialect and modern standard Arabic (MSA). This corpus was built and labeled by Mohammed and Kora. It consists of positive and negative tweets of the same size as 20k tweets on several topics. Fig. 1 shows the tweet count along with their sentiment.

Mohammed and Kora constructed the corpus from clear, obvious tweets, which have a positive or negative sentiment. In addition, two independent experts were invited to check the annotation of the corpus to validate it.

B. Proposed Model

The proposed model is divided into four major phases: data pre-processing, tokenization, word embeddings, and different deep learning models, as shown in Fig. 2.

1) *Preprocessing*: Firstly, the preprocessing phase consists of two important main functions, which are data cleaning and preprocessing functions. The used corpus [10] is already filtered, cleaned, and tweets are labeled. Also,

repeated hashtags, tweets, emojis, and non-Arabic letters are removed from tweets. So, preprocessing functions were applied directly on tweets like removing stop words, stemming and tokenizing.

Table III shows tweet examples before and after applying preprocessing functions. Stop words are words that usually appear in all tweets but are not important. These words should be deleted because they will not be distinguished when used as features in classification tasks. Stemming is the way suffixes are removed and words are reduced in their word stem.

2) *Word embeddings*: Word embeddings are a type of word representation that lets words with the same meanings be represented in the same way. Different approaches are available for word embeddings, such as Glove [21], created by Stanford, FastText [22], created by Facebook, and Word2Vec [23], created by Google. In general, there are two Word2vec models: a Continuous Word Bag (CBOW) and Skip-Gram (SG). The CBOW model, which predicts the current target word using context, although the SG predicts the context using a given word.

In such a case, the CBOW model is used for word vector representation. A pre-trained word2vec model is first implemented to generate the feature vectors of words, which will be used later as pre-trained vectors to generate the semantic vectors of words.

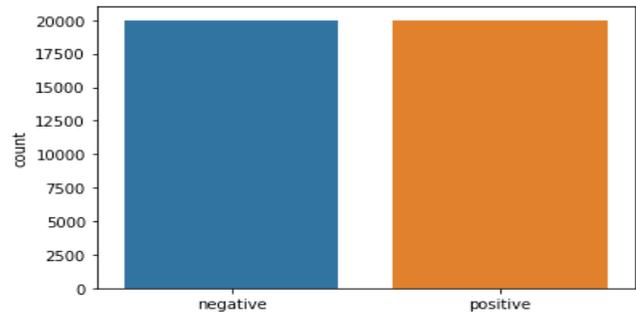


Fig. 1. Bar Chart of a Negative and Positive Count.

TABLE III. EXAMPLES FOR PRE-AND POST-PREPROCESSING TWEETS

pre-preprocessing Tweet	Post-processing tweet	Polarity
اكبر خطأ ترتكبه ان تعامل الناس باخلاقك انت مش باخلاقهم هما . Translated as : The biggest mistake you make is to treat people with your morals, not theirs.	كبر خطأ ركب عمل نفس خلق انت مش خلق	negative
دائما اكره اخر ليله في كل مكان . Translated as : I always hate the last night everywhere.	دما اكر اخر ليل كان	negative
احتاج صديق حقيقي يواسيني ويخفف عنى . Translated as : I need a true friend who comforts me and relieves me	حاج صديق حقيقي يواسننى يخفف عنى	positive
لازم اتعلم الثبات الانفعالى زيهم كذا . Translated as : I have to learn emotional stability like that.	لزم علم ثبت على زيهم	positive

3) *Model architecture:* In this section, four deep learning models are proposed to detect the polarity of Arabic text as shown in Fig. 2. In particular, the proposed models are convolution neural network (CNN), long short-term memory (LSTM), a hybrid of (CNN-LSTM), and bidirectional LSTMs (Bi-LSTM).

a) *CNN architecture model:* The convolution neural network (CNN) is a popular unsupervised learning algorithm. The CNN model architecture is shown in Fig. 3. Using the word2vec model, the word embedding is generated. The first layer of CNN is the convolution layer, which has 32 filters along with Relu activation. A filter size equal to 8 is added with a filter size equal to 8 to extract the characteristics of the phrases. These filters convert the input and create characteristic maps (varying lengths). The second layer is the global maximum pooling layer that captures the most essential information from previous characteristics. The third layer, the Gaussian noise layer, is added to moderate overfitting, which works as a regularisation layer. A fully connected layer takes the generated features and pools them together to create the final predictions, which constitutes the fourth layer. A dropout layer is then added to the network to regularise it and prevent it from overfitting. The last layer of the sigmoid function type is a dense (completely linked) layer. This layer produces the network output, which classifies the input tweet as positive or negative.

b) *LSTM architecture model:* The long short-term memory (LSTM) unit is commonly constructed from a cell for memory and three gates to control the information flow to and from the cell over time. The three gates are called an input gate, an output gate and a forget gate. The LSTM model layers are shown in Fig. 4. The word embeddings are delivered to the cells of LSTM after applying the embedding layer. On these word embeddings, LSTM cells are trained and their prediction

words are produced. A dropout layer is followed by a Gaussian noise layer to handle the overfitting by injecting noise during the time of training, and that reduces the computational effort during the time of testing. The words of the prediction are fully linked using a dense sigmoid layer.

c) *CNN-LSTM model:* This architecture was primarily named a Long-term Recurrent Convolutional Network or LRCN model, although the more generic name "CNN-LSTM" is used to refer to LSTMs that use CNN. The CNN extracts features from the sentences and represents them. however, LSTM works on extracted features where it takes the context and word ordering into consideration. Fig. 5 shows the CNN-LSTM architecture. It consists of an embedding layer that feeds into the convolution layer; after that, the output is considered as an input to the global max-pooling layer, followed by LSTM, followed by a dropout and Gaussian noise layer to regularise the output and prevent overfitting; and finally, a flattening layer with a sigmoid function that would give a negative or positive result.

d) *BiLSTM architecture model:* Generally, the BiLSTM is an expansion of regular LSTMs to increase model performance for sequence classification problems. This architecture is primarily known as the Bidirectional LSTM. Two LSTMs are trained in the input sequence instead of a single LSTM. The first is the input sequence, while the second is the input sequence is reversed. It can add to the network context and lead to faster and even more comprehensive learning of the problem. Fig. 6 shows the BiLSTM model layers. The embedded words are added after the use of the word embedding layer. Then apply BiLSTM to be trained on the embeddings of words and produce a set of word predictions that are linked with Gaussian dropout followed by a dense layer with a sigmoid function that would predict the sentiment of the result.

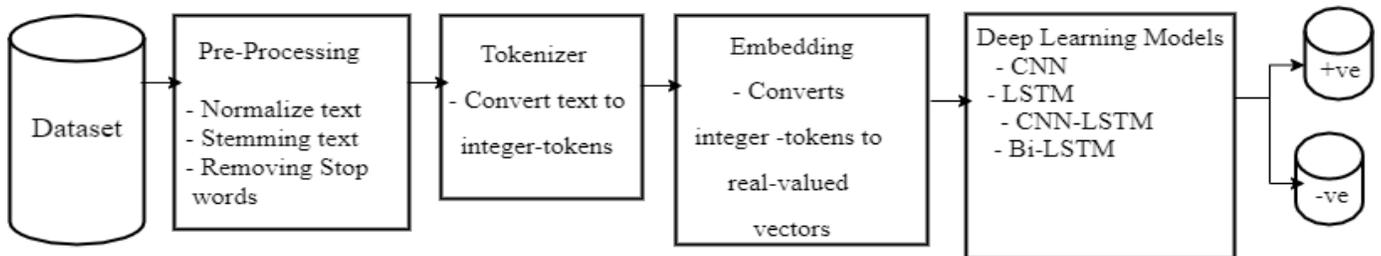


Fig. 2. Proposed Model Architecture.



Fig. 3. CNN Architecture Layers.

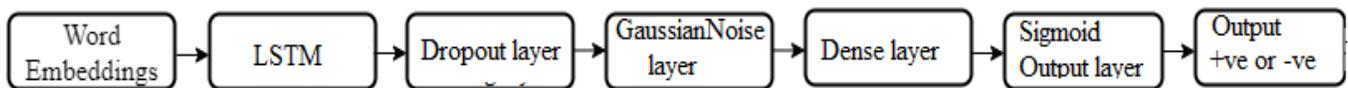


Fig. 4. LSTM Architecture Layers.

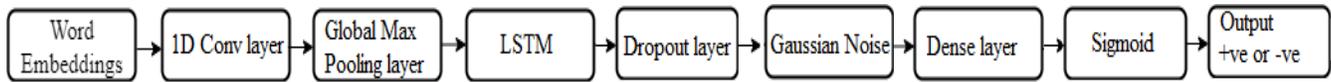


Fig. 5. CNN- LSTM Architecture Layers.

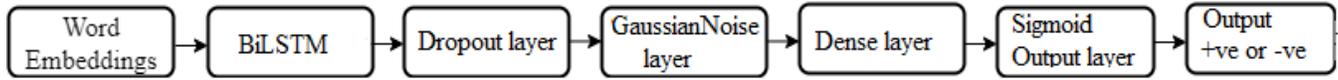


Fig. 6. BiLSTM Architecture Layers.

IV. RESULT AND DISCUSSION

The performance assessment of the proposed models is conducted using the most common evaluation metrics, which are accuracy, precision, recall, and F-measure. The (k-fold cross-validation) method is applied to the entire corpus [10] to evaluate the results. For the experimental setup, Google Colab Pro is used with a TPU hardware accelerator in Python 3.7.

A. Performance Evaluation Metrics

The confusion matrix is usually a type of matrix used to find the accuracy of classifiers. Each test data instance is assigned to an element, which belongs to a set of P, N comprising both positive, and negative class labels in the binary classification issue. There are four possible outputs given a model and an instance. (TP) the right number of tweets categorized as positive, (FP) the wrong number of tweets categorized as positive, (TN) is the correct number of tweets that are identified as negative, (FN) is the wrong number of tweets labeled as negative. A confusion matrix is created in the instances analysis of the given model and collection of test examples. Equation (1) displays the mathematical precision equation used to measure the true positive tweet, which indicates in Eq. (2) a part of positive tweets for a particular class. Equation (3) shows the mathematical equation for Accuracy. Equation (4) the F1score is determined by taking into account the recall and the precision of the test data.

$$\text{Precision} = \frac{TP}{(TP+FP)} \quad (1)$$

$$\text{Recall} = \frac{TP}{(TP+FN)} \quad (2)$$

$$\text{Accuracy} = \frac{(TP+TN)}{(TP+FP+TN+FN)} \quad (3)$$

$$\text{F1score} = \frac{(2 \times \text{Precision} \times \text{Recall})}{(\text{Precision} + \text{Recall})} \quad (4)$$

B. Experimental Result

The results of CNN, LSTM, CNN-LSTM, and BiLSTM are presented in this section. Each model was trained and tested using a data split (80%, 20%), bearing in mind that 10% is considered as a validation set for tuning the hyper-parameter. In addition, fivefold cross-validation is applied to improve performance, and each data division uses an average of five different runs. Given the equal distribution of the classes of positive and negative over the corpus, precision is a sufficient criterion for assessing the models. However, accuracy, recall, and f-score are also put into consideration as performance indicators for a proper interpretation of the findings.

Several experiments were conducted to enhance and achieve the best set of multiple hyper-parameters in each model. The optimal hyperparameter values utilized in the four models are shown in Table IV.

Table V displays the optimal CNN model combinations as well as the hyperparameters. The length of the sequence is 31, which is the biggest length of the tweet. In addition, 32 filters vary in 8 sizes of regions. Additionally, vocabulary size is determined by the number of words entered each time, and 10,000 words are selected.

In addition, the optimal settings in the LSTM model are shown in Table VI. In this setting, each layer of LSTM with 128 cells is used.

Table VII presents the best CNN-LSTM model configuration. This model is a hybrid of the previous two models in the same manner of settings except that the filter size is 16 instead of 8.

The BiLSTM settings are shown in Table VIII, which consists of one Bidirectional layer of LSTM using 128 cells.

TABLE IV. CNN, LSTM, CNN-LSTM AND BiLSTM HYPERPARAMETER VALUES

Learning rate	optimizer	Recurrent Dropout rate	Size of batch	# epochs
0.001	adam	0.5	32	100

TABLE V. CNN SETTING PARAMETERS

length of Sequence	#Filters	Filter size	Size of vocab
31	32	8	10,000

TABLE VI. LSTM SETTING PARAMETERS

LSTM size	LSTM layer	Recurrent dropout	Output dropout
128	1	20%	20%

TABLE VII. CNN-LSTM SETTING PARAMETERS

length of Sequence	31
# filters	32
Filter size	16
# LSTM layer	1
#LSTM cells	256
Recurrent dropout	20%
Output dropout	20%
Size of vocab	10,000

TABLE VIII. BiLSTM SETTING PARAMETERS

LSTM cells	BiLSTM layer
128	1

Table IX shows the results of the proposed model experiments using the 5-fold cross-validation method. The results indicate that CNN achieved values of 99.65%, 99.78%, 99.77%, and 99.78% for accuracy, precision, recall, and F-measure respectively. LSTM achieved 91.83% for accuracy value, 90.97% for precision value, 90.97% for recall value and 90.98% for F-measure. Although CNN-LSTM achieved accuracy with a value of 73.19%, precision with a value of 74.02%, recall with a value of 74.02%, and the value of F-measure is 74.02%. While BiLSTM achieved values of 91.73%, 91.74%, 91.74%, and 91.74 in accuracy, precision, recall, and F-measure, respectively.

TABLE IX. RESULTS OF PROPOSED MODELS

Model	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
CNN	99.650	99.775	99.774	99.775
LSTM	91.830	90.974	90.973	90.975
CNN-LSTM	73.19	74.025	74.024	74.023
BiLSTM	91.730	91.740	91.735	91.741

C. Baseline and Evaluation

In this part, the model's performance is compared with the latest work existing in the literature which was introduced by Mohammed and Kora [11]. They introduced a labeled corpus consisting of 40k tweets in colloquial Arabic. They also applied three deep learning techniques to their corpus. So their work is considered our benchmark. For evaluation, we used their corpus [10] to achieve a fair comparison.

The research [11] applied CNN, LSTM, and CNN-LSTM as models. After that, they used the train/test split validation method to validate and test their models. They used three different test sizes, 30%, 40%, and 20%, respectively. Then they average the accuracy values for each data split.

In this paper, we propose another strategy. We apply the same models with core modifications to their structure and different hyper-parameters. also, an additional model is proposed named BiLSTM.

In the proposed CNN, another pooling layer is added called the Global Max Pooling layer. In this case, we set the pool size to the same as the input size. So it reduces the dimensionality of the feature maps output by the convolutional layer. Also, Gaussian noise is added via a separate layer named the GaussianNoise layer after the Global Max Pooling layer which makes CNN noise regularization. This layer has a regularising effect and reduces overfitting.

Also in the proposed LSTM, a GaussianNoise layer is added between an LSTM recurrent layer and a dense fully connected layer. In the same way, the layer is added in the proposed BiLSTM between the bidirectional LSTM layer and the dense layer.

To avoid sampling bias, we can think of a slightly different validation method. So, k-fold cross-validation was introduced. The data is divided into K folds. The data is trained and tested on the single fold which has been left out. This is done for all combinations and the results are averaged in each case. The advantage is that both training and validation are used by all observations, and every observation is validated once. Typically, we use k=5, because it is good enough to balance computational complexity and accuracy of validation.

The results in Table X show that the proposed CNN model outperformed by 23%, 25%, 12%, and 24% in terms of accuracy, precision, recall, and F-measure, respectively. Fig. 7 provides a comparison between CNN and the proposed CNN.

Also, Table XI shows that the proposed LSTM model outperforms by 10%, 10%, 9%, 9% in terms of accuracy, precision, recall, and F-measure respectively. Fig. 8 provides a comparison between LSTM and the proposed LSTM.

Contrary to expectation, the result of the proposed CNN-LSTM was not as high as the case with CNN and LSTM. The practical results showed the extent of convergence between the proposed model and the original model, as shown in Table XII.

To complete the experiments, BiLSTM was applied as an extra model which achieved accuracy with a value of 91.73% as shown in Table XII.

TABLE X. COMPARISON BETWEEN THE PROPOSED CNN MODEL AND MOHAMMED AND KORA. [11]

Model	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
CNN	75.72	74.60	78.03	75.06
Proposed CNN	99.65	99.775	99.774	99.775

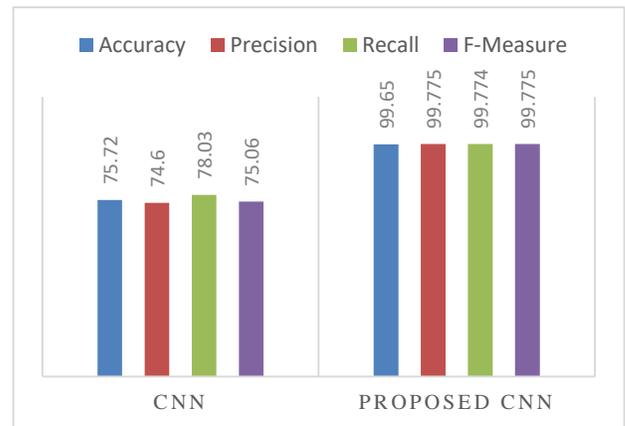


Fig. 7. CNN and Proposed CNN Comparison.

TABLE XI. COMPARISON BETWEEN THE PROPOSED LSTM MODEL AND MOHAMMED AND KORA [11]

Model	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
LSTM	81.31	80.92	81.99	81.25
Proposed LSTM	91.830	90.974	90.973	90.975

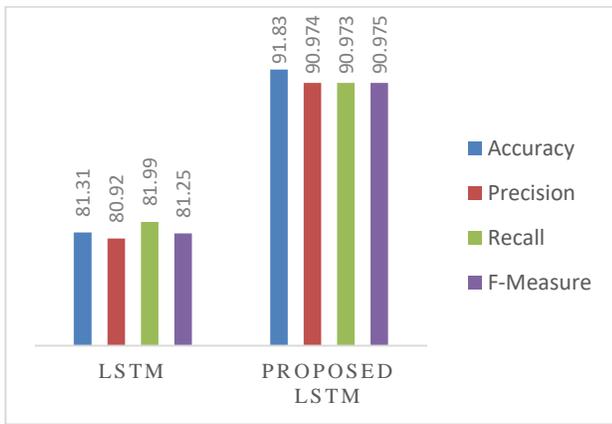


Fig. 8. LSTM and Proposed LSTM Comparison.

TABLE XII. COMPARISON BETWEEN THE PROPOSED MODEL AND MOHAMMED AND KORA [11]

Model	Accuracy (%)	Precision (%)	Recall (%)	F-Measure (%)
CNN -LSTM	78.46	80.27	77.38	77.86
Proposed CNN-LSTM	73.19	74.025	74.024	74.023
Proposed BiLSTM	91.730	91.740	91.735	91.741

V. CONCLUSION AND FUTURE WORK

This work focused on the problem of dialectal Arabic sentiment analysis using deep learning approaches. The proposed four deep learning techniques are tested on the used corpus. In particular, the proposed models are CNN, LSTM, and CNN-LSTM. Additionally, the experiments were extended by applying bidirectional LSTMs (BiLSTM). The obtained results show that the proposed CNN achieved an accuracy of 99.7%, the proposed LSTM achieved 91.83%, the proposed CNN-LSTM achieved 73.19%, and the proposed BiLSTM achieved 91.73%. The evaluation shows the higher performance of the proposed model in comparison with different models existing in the literature using the same corpus. Best results were achieved by using the combination of the Global Max Pooling layer and a GaussianNoise layer in the proposed CNN.

In future work, the CNN-LSTM model is planned to be improved so it will achieve better results. Also, we look forward to using other word representations such as Glove and FastText to see their effects on the results using different deep learning approaches. Additionally, we plan to use the data augmentation technique on the corpus to test its impact on corpus size and the performance of the deep learning approaches used.

REFERENCES

[1] K. Sarkar, "Sentiment polarity detection in Bengali tweets using deep convolutional neural networks," *J. Intell. Syst.*, vol. 28, no. 3, pp. 377–386, 2019.

[2] R. Baly, R. Hobeica, H. Hajj, W. El-Hajj, K. B. Shaban, and A. Al-Sallab, "A meta-framework for modeling the human reading process in sentiment analysis," *ACM Trans. Inf. Syst.*, vol. 35, no. 1, pp. 1–21, 2016.

[3] G. Badaro et al., "A survey of opinion mining in Arabic: A comprehensive system perspective covering challenges and advances in tools, resources, models, applications, and visualizations," *ACM Trans. Asian Low-Resource Lang. Inf. Process.*, vol. 18, no. 3, 2019, doi: 10.1145/3295662.

[4] A. Hamdi, K. Shaban, and A. Zainal, "A review on challenging issues in Arabic sentiment analysis," *J. Comput. Sci.*, vol. 12, no. 9, pp. 471–481, 2016, doi: 10.3844/jcsp.2016.471.481.

[5] A. Abdelwahab, F. Alqasemi, and H. Abdelkader, "Enhancing the Performance Of Sentiment Analysis Supervised Learning Using Sentiments Keywords Based Technique," in *CS & IT Conference Proceedings*, 2017, vol. 7, no. 1.

[6] E. Refaee and V. Rieser, "Benchmarking machine translated sentiment analysis for Arabic tweets," in *Proceedings of the 2015 Conference of the North American Chapter of the Association for Computational Linguistics: Student Research Workshop*, 2015, pp. 71–78.

[7] A. Hamdi, K. Shaban, and A. Zainal, "A review on challenging issues in arabic sentiment analysis," 2016.

[8] I. Guellil, H. Saadane, F. Azouaou, B. Gueni, and D. Nouvel, "Arabic natural language processing: An overview," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 33, no. 5, pp. 497–507, 2021, doi: 10.1016/j.jksuci.2019.02.006.

[9] A. Dahou, S. Xiong, J. Zhou, M. H. Haddoud, and P. Duan, "Word embeddings and convolutional neural network for arabic sentiment classification," in *Proceedings of coling 2016, the 26th international conference on computational linguistics: Technical papers*, 2016, pp. 2418–2427.

[10] R. Kora and A. Mohammed, "Corpus on Arabic Egyptian tweets." *Harvard Dataverse*, doi: doi:10.7910/DVN/LBXV90.

[11] A. Mohammed and R. Kora, "Deep learning approaches for Arabic sentiment analysis," *Soc. Netw. Anal. Min.*, vol. 9, no. 1, pp. 1–12, 2019.

[12] A. B. Nassif, A. Elnagar, I. Shahin, and S. Henno, "Jou," *Appl. Soft Comput. J.*, p. 106836, 2020, doi: 10.1016/j.asoc.2020.106836.

[13] A. al Owisheq, S. al Humoud, N. al Twaresh, and T. al Buhairi, "Arabic sentiment analysis resources: A survey," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 9742, no. 12, pp. 267–278, 2016, doi: 10.1007/978-3-319-39910-2_25.

[14] M. Attia, Y. Samih, A. Elkahky, and L. Kallmeyer, "Multilingual Multi-class Sentiment Classification Using Convolutional Neural Networks," pp. 635–640, 2016.

[15] M. Heikal, M. Torki, and N. El-Makky, "Sentiment analysis of Arabic Tweets using deep learning," *Procedia Comput. Sci.*, vol. 142, pp. 114–122, 2018.

[16] A. Elnagar, L. Lulu, and O. Einea, "ScienceDirect ScienceDirect An Annotated Huge Dataset for Standard and Colloquial Arabic Reviews for Subjective Sentiment Analysis," *Procedia Comput. Sci.*, vol. 142, pp. 182–189, 2018, doi: 10.1016/j.procs.2018.10.474.

[17] H. Abdellaoui and M. Zrigui, "Using Tweets and Emojis to Build TEAD : an Arabic Dataset for Sentiment Analysis," vol. 22, no. 3, pp. 777–786, 2018, doi: 10.13053/CyS-22-3-3031.

[18] M. Abdullah, M. Hadzikadic, S. Shaikh, and N. Carolina, "SEDAT : Sentiment and Emotion Detection in Arabic Text using CNN-LSTM Deep Learning," 2018, doi: 10.1109/ICMLA.2018.00134.

[19] K. Abu and C. Simon, "Can Modern Standard Arabic Approaches be used for Arabic Dialects ? Sentiment Analysis as a Case Study," 2018.

[20] L. H. Baniata and S. Park, "Sentence Representation Network for Arabic Sentiment Analysis," pp. 470–472, 2016.

[21] J. Pennington, R. Socher, and C. D. Manning, "Glove: Global vectors for word representation," in *Proceedings of the 2014 conference on empirical methods in natural language processing (EMNLP)*, 2014, pp. 1532–1543.

[22] A. Joulin, E. Grave, P. Bojanowski, and T. Mikolov, "Bag of Tricks for Efficient Text Classification," *arXiv Prepr. arXiv1607.01759*, 2016.

[23] T. Mikolov, I. Sutskever, K. Chen, G. Corrado, and J. Dean, "Distributed representations of words and phrases and their compositionality," *arXiv Prepr. arXiv1310.4546*, 2013.

Challenges in Developing Virtual Reality, Augmented Reality and Mixed-Reality Applications: Case Studies on A 3D-Based Tangible Cultural Heritage Conservation

Ahmad Zainul Fanani¹, Khafiizh Hastuti², Arry Maulana Syarif³, Prayanto Widyo Harsanto⁴

Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia^{1,2,3}

Faculty of Visual Communication Design, Institut Seni Rupa Indonesia Yogyakarta, Yogyakarta, Indonesia⁴

Abstract—A model that contributes in a simple, practical and effective way to develop 3D-based CH conservation applications involving the use of VR, AR and MR technologies was proposed based on the identification of challenges in developing applications. Identification was carried out by analyzing related and relevant articles selected randomly using Google and Google Scholar search engines. The model can prevent researchers from lack of planning in carrying out research in this field, and it is suitable for those just starting out with this type of research. In addition, this model can support researchers to more easily, practically and effectively implement 3D-based cultural heritage conservation by using virtual reality or augmented reality or mixed reality technology.

Keywords—Virtual reality; augmented reality; mixed reality; tangible cultural heritage; 3D-based cultural heritage conservation

I. INTRODUCTION

This article aims to study the use of virtual reality (VR), augmented reality (AR) and combination of VR and AR called mixed reality (MR) for the conservation of tangible cultural heritage in order to identify challenges in developing 3D-based tangible cultural heritage (CH) conservation. Tangible cultural heritage objects were focused on immovable objects such as building and historic places. Moving objects are also included in the discussion but in a small portion. Challenges were classified according to tasks in the development which were summarized based on cases found in related and relevant research articles. The identification results are then used to design a model for developing cultural heritage-VR (CH-VR), cultural heritage-AR (CH-AR) or cultural heritage-MR (CH-MR) applications. The model contributes in simply and practically way in determining a suitable method for developing 3D-based CH conservation applications using VR, AR or MR. Along with the development of this type of research which is increasingly rapid, the proposed model can prevent researchers who just starting out with this type of research from lack of planning in carrying out researches in this field. The method of selecting articles used as the source of the review is done by random searching using a search engine in the web of related and relevant journals, Google and Google Scholar, using the keywords virtual reality, augmented reality, mixed reality and cultural heritage. The articles listed in the search results were then selected based on the unique

content in the proposed development method. The number of articles was limited to 40 to 50 articles where the number is subjectively considered sufficient to represent the topic of discussion.

There are eight challenges identified in the collected articles: (1) time-based 3D reconstruction, (2) object characteristics or typology, (3) 3D reconstruction method, (4) application category, (5) research objective, (6) data management, (7) presentation method and (8) research evaluation. These eight challenges are not a procedure.

A brief explanation of CH, VR, AR and MR is described before entering into the main discussion. CH definition from The United Nations Educational, Scientific and Cultural Organization (UNESCO) is [1]:

“cultural heritage is, in its broadest sense, both a product and a process, which provides societies with a wealth of resources that are inherited from the past, created in the present and bestowed for the benefit of future generations. (<https://en.unesco.org>)”

The keywords of past, present and future in the CH definition are associated with conservation, and conservation requires educational efforts. The rapid development of information and communication technology is driving the implementation of computer and mobile technology as part of conservation and educational efforts for CH objects. These technologies can reach all humans, and can transform CH objects into digital form for human access without being limited by time and space.

During these decades, VR, AR and MR applications have developed rapidly and are widely used for the preservation of CH objects. In a limited definition: VR is a technology that can support users to interact with a 3D environment using electronic devices to feel the sensation of being in a virtual environment, and examples of electronic devices used in VR are the HTC Vive, Oculus Rift and PlayStation VR (PSVR), while AR simulates 3D models in a real environment that typically uses a mobile device, and MR is a combination of VR and AR which involves the interaction between humans, computers, virtual environments and real environments. All of these technologies use 3D models to create backgrounds for

virtual environments, or properties within real and virtual environments.

The structure of the rest of this paper is divided into sections as follows: Section II describes the time-based reconstruction in the 3D-based conservation development; Section III introduces object characteristics of cultural heritage and natural heritage; Section IV discusses the 3D reconstruction method; Section V describes the applications category; Section VI discusses the research objective; Section VII describes the data management; Section VIII discusses the presentation method; Section IX describes the research evaluation; Section X describes the analyzes that have been carried out and the development of the proposed model; and Section XI discusses the conclusion and future works.

II. TIME-BASED 3D RECONSTRUCTION

Basically, the 3D-based conservation development can be classified into two main time-based 3D reconstruction types, which are the current and past environments. The current environment-based 3D reconstruction refers to restored historical objects that were abandoned or damaged but have undergone restoration in accordance with, or at least close to, their conditions in the past, such as works of [2-7]. Meanwhile, the past environment-based 3D reconstruction is an effort to reconstruct the damaged or extinct historical objects based on their conditions in the past, such as works by [8-10].

The Old-Segeberg town house, a historic building located in German, was reconstructed into a 3D model for a CH-VR application [11]. Preserved artefacts in the city of Rethymno, Greece were reconstructed in 3D models by [2] in order to develop a 3D game-based learning by combining VR and AR and 360-degree video. These researches have a technical problem as one of the challenges, which is determining the best method in the use of VR or MR technology. This typical problem generally focuses on the technique of 3D reconstruction and connecting 3D model into VR, as well as in the works by [6-7]. A project called 3-D Digital Conservation of At-Risk Global Cultural Heritage (3DP-ARCH) to document transnational at-risk heritage objects and places was conducted by [5]. The 3D-ARCH project does not only focus on the documentation of cultural heritage objects, but it includes on the access to big data containing 3D models where big data management is the main problem in this project. An interactive multimedia-based model for the development of a VR application containing a collection of Bulgarian Cultural Heritage Sites was proposed by [3]. The proposed model contains texts, images and videos, 3D models and Audio records. This model is similar to the works by [5] but with a smaller area, which is within one nation. The real area where the cultural heritage objects are scattered, either transnational or within one nation, has the same problem in collecting data. Meanwhile, the number of the reconstructed objects determines the use of big data management. In this case, the model proposed by [3] lacks detail on data management issues, it tends to describe content and navigation of the application without addressing data management problems as [5] did.

In a work called Viking VR, [12] involved the museum curatorial and technical staff and archaeologist to reconstruct an environment of the Vikings era in Britain, as well as [10] who reconstructed the City of Nafplio in 19th century in 3D models by involving archaeologists and historians. Instead of involving archaeologists, [8-9] used a computational-based method in reconstructing damage and extinct objects. A computational-based method using a text-based documentation of classic archeology, sketches and images was proposed by [8] to reconstruct an extinct historical object, the Etruscan Tomb located in Italy, into 3D models. Meanwhile, a direct survey to collect architectural details, architectural analysis based on images, active sensors to control and compare results and deformations was conducted by [9] in order to reconstruct a damage historical object, the Castra Praetoria's walls located in Italy. Unfortunately, both [8] and [9] did not report an archaeologist expert evaluation to judge the suitability of the 3D models to the past environment. An evaluation of the reconstructed 3D model was conducted by comparing it to the historical pictures and literatures [9]. However, if archaeologists are not involved in reconstructing damage or extinct objects, the reconstructed 3D evaluation by archaeologists is a must.

The current environment-based 3D reconstruction focuses on the problem solving of 3D reconstruction method selection, application type selection (VR or AR or MR) and data management. Principally, the 3D reconstruction refers on the current state of the object as it is, so the involvement of archaeologists is optional. But when it involves more than just a visualization of cultural heritage objects. For example, capturing data which needs archaeological analysis and curation such in a work by [5], archaeologists must be part of a team. Meanwhile, the past environment-based 3D reconstruction also focuses on the problem solving in the current environment-based 3D reconstruction, but it needs the involvement of archaeologists in reconstructing the damaged or extinct historical objects based on the past environment or in evaluating the suitability of the reconstructed 3D model to the scientific description of the object as it was in the past time.

III. OBJECT CHARACTERISTICS (TYPOLOGY)

There is debate regarding the definitions of CH and natural heritage (NH). Some argue that CH is a man-made product, while NH is a gift from nature. Meanwhile, UNESCO defines CH by using the phrase 'works of man or the combined works of nature and man' but NH is defined without mentioning a single word of man [1]. So, we agree with the definition of CH as a man-made product. Furthermore, if there are two terms CH and NH, there should be a distinction between them, and man-made or not is a fundamental differentiator for defining the two terms. Based on our agreed definition of CH, an AR work of [13] containing the Pietraraja paleontological site visualization, which includes reconstructions of extinct living things, is not CH as stated in the article title, and NH is the appropriate term to use. Regardless of the inaccuracy in the use of the term, we continue to study this work by considering the content containing the AR development methods.

Next is to define objects that is used for 3D-based CH conservation. Old buildings do not always fit CH objects. An object must comply with traditional, chronological and geographical concepts, where the object is not only historical and artistic but must have cultural values or memory capacities within the object [14]. Thus, a list of CH objects released by local authorities or UNESCO can be used to confirm this.

The object characteristics include the size, number, location and structure. A sophisticated project, 3-D Digital Preservation of At-Risk Global Cultural Heritage (3DP-ARCH), conducted by [5] contains a large size and number of objects with varying structural complexity, as well as locations spread across nine countries. In contrast to 3DP-ARCH, [10] tried to reconstruct the historical city of Nafplio in Greece, as well as [15] who tried to reconstruct the various sizes and numbers of objects in an area called Little Manila in California, US, back in the 1940s. Meanwhile, [9] reconstructed objects with simpler complexity but have a broad size, which are ancient walls located in an area of nearly 17 hectares, as well as [16] who reconstructed a single complex object called the Roman Theater at Byblos located in Lebanese. The four conservation buildings where the Princeton University Campus is located were reconstructed by [17], and [18] reconstructed the Museum of King John III's Palace at Wilanów in Warsaw, Poland consisting of five rooms. The Dudsbury Hillfort visualization by [19] is a reconstruction of a typical large 3D landscape. Artifacts which are typical of small objects, are part of the 3D reconstruction. The Etruscan Tomb in Italy, including artifacts of funerary equipment, was reconstructed by [8], while [20] reconstructed relics collection of the Majapahit kingdom, Indonesia, and [21] reconstructed Haw Par Villa in Singapore, including two sumo statues.

A detailed analysis of the object characteristics determines the success of the 3D-based CH conservation development. There are cases of 3D reconstructions of objects that are large or extensive but have less structural complexity (ornamentation) than a single building, or even small artifacts. The challenge is to appropriately measure the object typology. This is essential for the initialization stage of 3D-based CH conservation development, and is related to the resources owned, including funding, so that there is no excessive target as in the conceptual model proposed by [3] which targets the 3D reconstruction of all historical sites in Bulgaria without being supported by a clear design of the model implementation and research timeline, considering that one research project must have a clear duration in its implementation.

IV. 3D RECONSTRUCTION METHOD

Some of the works relied on documentation of cultural heritage objects and software engineers including the use of artificial intelligence methods in 3D reconstruction. Considering the 3D model is a basic component of delivering information, the reconstruction must be carried out carefully so as not to mislead. Methodology in 3D reconstruction is divided into survey-based such as laser scanning and photogrammetry, and reconstruction-based which involves an

interdisciplinary team to work based on documentation of cultural heritage objects [22]. Reconstruction-based techniques uses traditional 3D modeling technique, where the modeling process is conducted based on notes, literatures, images, building blueprint, videos and other documentations. Meanwhile, the survey-based technique uses a collection of photos (sequence) for automatic 3D modeling based on artificial intelligence approach.

A 3D reconstruction of ancient walls located in an area of nearly 17 hectares were reconstructed using a number of total stations to do topographic survey where the results were then used to control the photogrammetric model, and also a direct observation was conducted to get some of the architectural details used for the 3D model texture [9]. Laser scanning and photogrammetry were also used by [18] for a 3D reconstruction of a historic building. Images or photos used for input in photogrammetry must be properly prepared. The different cameras and resolutions used to capture the data from a single object provide more complexity for automatic 3D reconstruction. The number of vertices (cloud subsampling) were reduced using random method [18].

A 3D reconstruction of the Etruscan hypogeum tomb complete with the funerary equipment was conducted by [8] a combination of survey-based and reconstruction-based techniques, in which small artefacts from funerary equipment were reconstructed using a laser scanner and the tomb was reconstructed using a traditional 3D modeling technique. They also conducted an addition 3D reconstruction for damaged artefacts. The damage artefacts, which firstly were reconstructed using a laser scanner, were continued to be restored using a traditional 3D modeling technique. The division of reconstruction tasks by reconstruction-based has a dominant portion of the survey-based was performed in a 3D reconstruction was performed by [13] and [23]. In a 3D reconstruction of an ancient Roman house by [23], photogrammetry was used only for walls, while the building was reconstructed using traditional 3D modelling. Meanwhile, [13] prefer to use traditional 3D modeling to reconstruct fossil forms based on documentation of living species that have become extinct at the paleontological site of Pietraraja, Italy.

One of the challenges in 3D reconstruction is that 3D modeling requires high computer specification. Photogrammetry is currently the most 3D reconstruction technique used in many researches; it provides low cost of both software and hardware [24]. However, survey-based techniques used for complex structures or large objects still require much higher computer specifications. Moreover, the precision of 3D models reconstructed using photogrammetry technique depends on the object's real environment and object size, where only isolated building and small artefacts are suitable for this technique [8, 25]. The use of survey-based reconstruction for automated 3D reconstruction as well as traditional 3D modeling techniques for reconstruction requires more time and human resources. Appropriate preparation based on time-based reconstruction analysis and environmental analysis of objects including budget should be made to select the 3D reconstruction method, whether survey-based or reconstruction-based or combine the two methods.

V. APPLICATION CATEGORY

The selection of the category of application is in accordance with the type of time-based reconstruction that underlies application development which in general can be categorized in documentation and restoration. The use of time-based representation is to limit the definition of documentation and restoration, and to avoid bias in the terminology of restoration which also can be defined as part of documentation work.

In the context of time-based reconstruction, the documentation category relates to current environment-based reconstruction, while the restoration category relates to past environment-based reconstruction. Documentation means visualization in which physical CH objects are transformed into virtual forms so that users can virtually see CH objects. When an element of restoration is added to the visualization, the category changes from documentation to restoration.

The category of documentation can be found in the example of work in The Visualization of Dudsbury Hillfort by [19], The Visualization of the Selimiye Mosque of Edirne by [4], 3DP-ARCH by [5], Tomb of Sultan by [26] and Capturing Aboriginal Heritage by [27]. Meanwhile, the category of restoration can be found in the example of work in Aurelian Wall at Castra Praetoria by [9], The Ancient City of Sarmizegetusa by [28], The Church of Santa Maria Paganica in L'Aquila by [29], Nafplio in the 19th Century by [10] and The Restoration Project of Alaca Imaret Câmî by [30]. In most of cases, combination of survey-based and reconstruction-based methods is performed for 3D reconstruction for either the documentation or reconstruction category.

VI. RESEARCH OBJECTIVE

In the field of computer science, specific objective is related to the application development methodology based on its categories, either documentation or restoration. In other words, specific objective is to find appropriate methods to document or restore a CH object in the form of a 3D model and present it using VR or AR or MR. Meanwhile, general objective is related to the needs of users, such as for education, economic and tourism.

In fact, some researchers tend to focus on immersive outcomes or the works of technology without clearly evaluating the achievement based on the general objective. Especially for educational objectives where many studies claim that its application was developed for education. Delivering education is not just showing things. There must be a set of parameters or at least a general description to measure the achievement of education delivery which is not found on the reports in the development of AR for the Monuments of Crete by [2], AR for the Paleontological Site of Pietraraja by [13], and AR-based Art Gallery for education by [31]. In contrast with [32] who performed a comparison test by control and treatment groups involving a number of students in evaluating their work called ScollAR, a digital learning platform containing VR section and AR section to deliver education. Meanwhile, [33] used Software Usability Measurement Inventory (SUMI) model, a survey instrument to

measure user perceptions of software usability, to evaluate their work containing VR for The Island of San Andres.

Referring to the definition of museum, virtual museum is a type of application for education. The definition of museum includes the educational element as [34] states that:

“the missions of museum do not only consist of conserving and exhibiting treasures and objects that provide us with information but include the provision of educational tasks” (p. 1257).

The International Council of Museums (ICOM) also emphasizes that the educational element is part of the definition of museum. The ICOM states that [35]:

“a museum is a non-profit, permanent institution in the service of society and its development, open to the public, which acquires, conserves, researches, communicates and exhibits the tangible and intangible heritage of humanity and its environment for the purposes of education, study and enjoyment”.

The example of virtual museum can be found in the development of Alt-Segeberger Bürgerhaus by [11], Viking VR by [12], Virtual Artifact by [20] and The Maritime Museum of Kotor by [36]. Regardless of the use of the term virtual plaza rather than museum, [3] proposed an excessive target in documenting all CH sites in Bulgaria without a clear methodology for data management. The same thing happened to several other researchers who used the term virtual museum without paying attention to the fulfillment of the rules and characteristics of the museum or without explaining the implementation of how the museum works in their application which basically they are trapped in visualization or developing application in the domain of documentation category, or might be in the education category but not delivered in museum form. VR development for museums often does not consider museum's concept and policies [37] and neglects visitor experience related to the real experience of visiting museums, and museum systems and organizations [38].

Another general objective in developing VR or AR or MR for CH objects is to support the economy as [39] proposed in extending VR and AR applications with 3D printing feature for an economy value, while examples for tourism can be found in the work of the Deoksugung palace in South Korea and the An Post Museum in Republic of Ireland virtual tours by [40], the Princeton University Campus virtual tours by [17] and The Jeju-mok Government Office and the Gwandeokjeong Pavilion virtual tours by [41].

VII. DATA MANAGEMENT

Object characteristics, 3D reconstruction methods, application categories, and research objectives influence the complexity of data management. Data management includes management of data source, collected data, 3D reconstruction data, 3D model data, application log data and others including metadata management. All data categories must be related to each other to support application maintenance, application performance enhancements, and application extends or updates. There is a lot of discussion material for data management that is not sufficient to cover in this article.

Several examples of case studies in data management are used to open up insights.

A clear example can be found in the development of a virtual museum. Learning in museums should support a constructivist approach that allows visitors to gain knowledge spontaneously through their personal experiences, and virtual museums can support such learning [42]. Thus, data management mechanisms in real museums must be implemented in virtual museums. In this case, data management is not only applied to historical objects, stakeholder engagement data also needs to be managed. In order to substitute the role of historians who accompany and answer visitor questions, [36] proposed a method of information retrieval in managing object information data, by allowing users to enter keywords in the application which are then sent to the database via the internet to obtain information on the object. Another example in historic building is [43] who focused on managing metadata containing historic building information to support context-aware risk management for people who follow the update of information on the CH object.

Data management in VR, AR or MR application development is rarely found in related articles, and the topic is still wide open for research. Many challenges are faced in it. The metaphorical principle that implements the design of a real object or system into an application needs to be considered.

VIII. PRESENTATION METHOD

The presentation method refers to the selection of VR or AR or MR technology for 3D-based conservation application, including the way to present the application to the users. The VR museum environment must be designed as immersive as possible in order to attract users to enjoy educational and entertainment experiences including influencing users to physically visit the museum [44]. Indeed, even all categories of applications, whether VR, AR or MR and their extensions, such as games or virtual museums and others should consider the immersive output in their presentation. On the other hand, 3D data management requires high costs, at least for the provision of computers with high specifications. This includes the users who must use a device with high specifications to be able to run 3D-based applications.

One of the challenges in presenting 3D-based applications is the ease of access through devices owned by the user directly, which can be a smart phone, tablet or computer. On the other hand, user-owned devices have very varied specifications. Therefore, the determination of visual quality must consider the computation load that must be carried by the device to run the application.

In general, the visual quality of a 3D model is highly dependent on the number of 3D points that are used to construct or deform objects, and on rendering techniques that involve textures and lighting. The number of 3D points affects the render speed. Therefore, low-poly 3D models are preferred for applications that run on mobile devices, especially smart phones. Real-time rendering for high quality 3D environment on mobile devices is a challenge in developing 3D-based

applications [45]. At this stage, the role of the 3D engineer is decisive. Researchers can coordinate with 3D engineers to make observations on several applications to run on several device specifications as a comparison. Observation results can be used to determine visual quality based on target device specifications. Immersive reality can be obtained using the following devices: head mounted display with video and optical see-through used for AR or MR and blocked headsets used for VR, spatial augmented reality, hand-held-devices, desktop screen and projection, and cave automatic virtual environment (CAVE) [46]. The 3D-ARCH project conducted by [5] does not only focus on the development of building a 3D environment and augmented reality interaction, but it includes on how to organize big cultural heritage data to be virtually learned using head mounted device, CAVE, mobile augmented reality devices platform, big screen television with high-speed access to the 3D processing, high quality render and high-capacity data storage, all of which are very expensive, including the use of a supercomputer. Of course, not all projects are sophisticated with high budgets.

With all the limitations in the hardware, AR provides a breakthrough in easy access to 3D-based applications by allowing users to interact with applications using their own mobile devices. Moreover, during and after the Covid-19 pandemic era, hygiene issues will affect user behavior regarding the use of VR support devices, such as head mounted devices. In a new normal era, it is not recommended to use one device for multiple users without implementing health protocols. This condition becomes a dilemma, adding devices means increasing budgets, while using a limited number of devices means increasing the frequency of cleaning, and this can have an adverse impact on the smooth functioning of the devices.

At present, VR and AR technologies for 3D-based CH conservation have been found in various studies, while the application of MR technology is still limited, because MR technology has enormous challenges [46]. Devices to support MR, such as Google ARCore, Apple ARKit and Microsoft MixedReality-Toolkit only conceived for indoor usage, and these devices are not support for outdoor experience [47]. Changes in environment and movement of objects are still a problem in MR, including its application to mobile applications [48]. An example of MR for CH is showed by [25] who displayed the 3D environment that the user sees through the HoloLens onto the monitor screen.

In addition to virtual museums, game applications are also applied in 3D-based CH conservation such as the historical city of Nafplio by [10], Viking VR by [12] and The Little Manila in the late 1940s in California by [15]. One of the challenges in using games for CH conservation is the screenplay that doesn't change history. Another challenge is the development of intelligent virtual agents that are able to socially interact with users [49]. The existence of intelligent virtual agents in the 3D-based CH conservation are interesting. It is like watching a Jurassic Park movie not through the screen, but being in it. It gives more challenge and worth studying, in which cinematography may also be used to characterize the intelligent virtual agents.

IX. RESEARCH EVALUATION

Four parameters, which are the presence, enjoyment, attitude change, and visit intention, were used by [41] to evaluate user acceptance for a VR application in which TV video clips were inserted. Meanwhile, [33] used SUMI method which consists of efficiency, affect (likeability), helpfulness, control, learnability and global measurement for evaluation based on user acceptance. A different evaluation method was proposed by [50] who added 360-degree video storytelling to a VR application, and used electroencephalography (EEG) to evaluate user acceptance based on brain signals data related to factors of the presence, engagement, and immersion that are obtained after playing the application. In addition to measuring the ease of operation of the application, [19] conducted a survey to evaluate the similarity of the 3D model to the original object, and the level of realistic.

Most of researchers use survey techniques to get feedback about the application, such as using the SUMI method. In measuring the level of immersion or the similarity between 3D models with the original objects or the application functions design and others, most researchers also use feedback from users without an appropriate respondent screening method.

There is a gap in these measurement cases. Users who never or rarely use VR, AR or MR applications have a tendency to give good feedback. On the other hand, users who have a lot of experience in using the application, or experts in VR, AR or MR, can provide more valuable feedback. Archaeologists, historians and other relevant experts have a capacity to evaluate a similarity measurement. Applications

are developed for use by users; therefore, users should give their opinion which can be used to measure the achievement of output, but the method of collecting opinions about the application must be designed more clearly and rigidly. Other challenges in designing evaluations are: measuring real work systems by applying them to applications as in the case of virtual museums, measuring data management on artifact collections, or computations as the specific objectives.

X. DISCUSSION

Eight challenges, which are time-based 3D reconstruction, object characteristics or typology, 3D reconstruction method, application category, research objective, data management, presentation method and research evaluation, including the problem-solving method identified and described above are interesting and very helpful in developing the model of 3D-based CH conservation (Fig. 1). Before designing the research implementation, the trivial thing that can make a big impact is to be sure the target object is part of the cultural heritage category.

The center of the model is the research objective which consists of specific objectives related to the designation of the application being developed, and general objectives that can be for education, economic and tourism. The research objective has typical problem-solving in data management, 3D reconstruction and presentation methods. In the diagram, the three problem-solutions are denoted by dashed lines and gray boxes. Even so, it does not rule out problem-solving in developing a model or method for typology analysis and research evaluation.

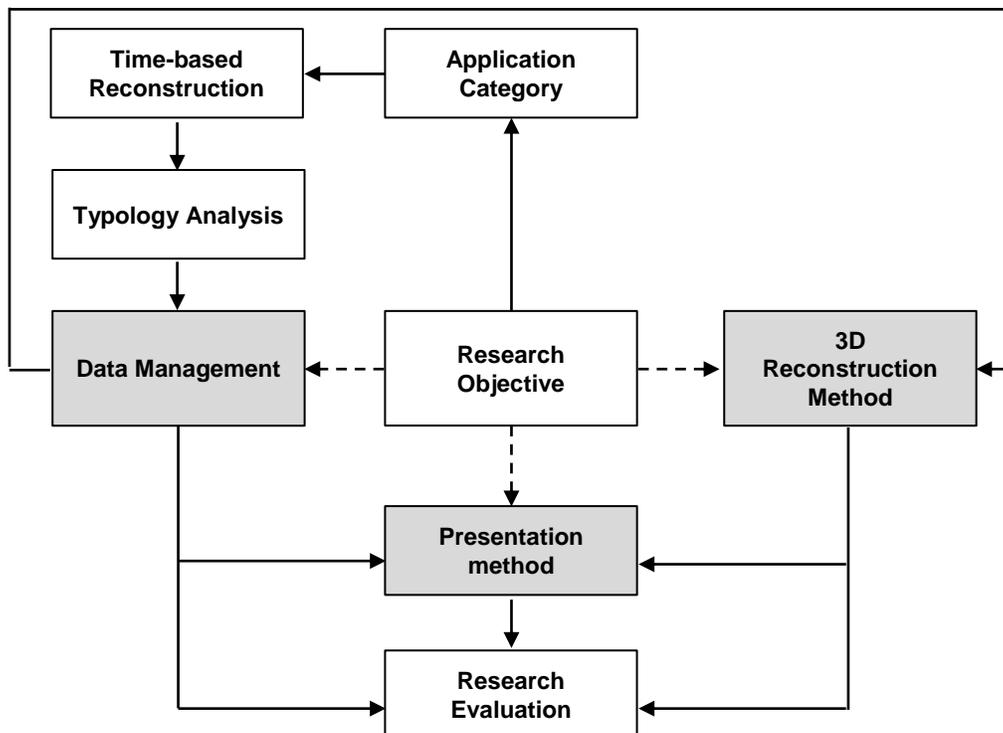


Fig. 1. 3D-based CH Conservation Development Model

Back to research objective as the center of the model. Once the objective is determined with a confirmed CH object, the application category, either documentation or restoration, can be identified. The restoration category relates to an effort to reconstruct the damaged or extinct historical objects based on their conditions in the past, while the documentation category relates to a 3D reconstruction based on the current state of the real environment. The application category defines the time-based reconstruction. The documentation category is derived to the current environment-based reconstruction, while the restoration category is derived to the past environment-based reconstruction. The involvement of archaeologists and historians can be an option in environment-based reconstruction today, but is obligation in environment-based reconstruction of the past. Furthermore, typology analysis is carried out to collect data based on object characteristics. Analysis can be conducted through direct observation or documentation-based. The results of the analysis are sent to the data management.

Data management controls data flow from research design, and before, during and after 3D reconstruction, including presentation methods, research evaluation, and during application use. The challenge in data management is finding the best method of organizing the various data categories to support easy data management and information access, both for developers, clients (such as museum managers) or application users. Data management has challenges that are still wide open for research in this topic, especially in developing applications that have characteristics such as virtual museums where human-computer interactions data must be processed while the application is used. In the data management, the typology data are used to determine data collection technique in order to select the 3D reconstruction method.

The 3D reconstruction method is divided into survey based and reconstruction based. Survey-based using photogrammetry, laser scanning and other supporting tools, such as a total station. Meanwhile, the one based on reconstruction is traditional 3D modeling. The challenge in this task is finding the best method to make a 3D model as closely as possible to the original object as in the work of Cai et al. (2016) and Canciani et al. (2016). The combination of survey-based and reconstruction-based methods for 3D reconstruction is the most widely used, in fact the combination of these two methods has become an integral part of the past environment-based reconstruction. Determination of the proportion of the combination can be done by considering the characteristics of the object. Furthermore, the reconstruction of the object into the 3D model begins, including the application of textures, also including other tasks that have been defined in the data management.

The results in the 3D reconstruction and data management are applied in the presentation methods in which VR, AR or MR applications are developed. Challenges in presentation methods include data management implementation, VR or AR or MR technology selection, visual quality (immersive application) control, human-computer interaction method selection and the graphical user interface design.

After the application is finished, evaluation is carried out to measure the achievement of defined general objectives and specific objectives. Research is evaluated by measuring the achievement of the proposed problem-solving which can be based on the efficiency and or effectiveness of the computational load in the 3D reconstruction process or in presentation method or in data management, or stakeholder perceptions.

The development of 3D-based CH conservation involves individuals from various backgrounds, such as archaeologist, historian, curatorial, 3D engineers, sound engineer, programmer and others, including stakeholders. Expert test by involving archaeologists, historians, curators and graphic designer can be carried out to measure various elements related to the object being modeled into 3D. User acceptance test by involving related experts and users can be performed to measure the acceptance of perceptions from stakeholders. SUMI evaluation model like the one used by Musa et al. (2018) can be applied in user acceptance test. Other testing methods may also be performed, such as data management testing or testing based on computational processes.

XI. CONCLUSION AND FUTURE WORK

The use of VR, AR and MR in 3D-based CH conservation is growing rapidly. On the other hand, there are still researches with poor planning as found in several articles in these case studies. This article aims to develop a 3D-based CH conservation model that implements VR, AR and MR technology using the case study method. The model provides a clear description as a practical guide for researchers just beginning research on this topic.

For future work, the model will be implemented and tested in 3D-based CH conservation for a historical building object called Lawang Sewu located in the city of Semarang, Indonesia.

ACKNOWLEDGMENT

Thank to Ministry of Research, Technology, and Higher Education of The Republic Indonesia for financial support through the 1st year Hibah Penelitian Terapan Tahun 2021.

REFERENCES

- [1] https://en.unesco.org/creativity/sites/creativity/files/cdis/heritage_dimension.pdf (accessed on May 5, 2021).
- [2] L. Argyriou, D. Economou, and V. Bouki, "360-degree Interactive Video Application for Cultural Heritage Education", in: 3rd Annual International Conference of the Immersive Learning Research Network. 26-29 June 2017, Coimbra, pp. 297-304. DOI: 10.3217/978-3-85125-530-0-44.
- [3] A. Bachvarov, D. Chotrov, Y. Yordanov, and Z. Uzunova, "Conceptual Model of the VR Module for Virtual Plaza for Interactive Presentation of Bulgarian Cultural Heritage", in: AIP Conference Proceedings 2172, 7-13 June 2019. Sozopol, Bulgaria, pp. 1-5. DOI: 10.1063/1.5133585.
- [4] T.P. Kersten, B. Büyüksalih, F. Tschirschwitz, T. Kan, S. Deggim, T. Kaya, and A.P. Baskaraca, "The Selimiye Mosque of Edirne, Turkey – An Immersive and Interactive Virtual Reality Experience using HTC Vive", in The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences, Volume XLII-5/W1, 22-24 May 2017, Florence, Italy, pp. 361-367. DOI: 10.5194/isprs-archives-XLII-5-W1-403-2017.
- [5] N. Lercari, J. Schulze, W. Wendrich, B. Porter, M. Burton, and T.E. Levy, "3-D Digital Conservation of at-risk Global Cultural Heritage",

- Catalano, C.E., De Luca, L. (Eds), Eurographics Workshop on Graphics and Cultural Heritage, 2016, pp. 193-197. DOI: 10.2312/gch.20161395.
- [6] B.J. Fernandez-Palacios, D. Morabito, and F. Remondino, "Access to Complex Reality-Based 3D Models using Virtual Reality Solutions", *Journal of Cultural Heritage*, 23(2017), pp. 40-48. DOI: 10.1016/j.culher.2016.09.003.
- [7] E.Y. Putra, A.K. Wahyudi, and C. Dumingan, "A Proposed Combination of Photogrammetry, Augmented Reality and Virtual Reality Headset for Heritage Visualization" in 2016 International Conference on Informatics and Computing (ICIC), 28-29 October 2016, Mataram, Indonesia, pp. 43-48.
- [8] S. Batino, M. Callieri, D. Duranti, M. Dellepiane, P. Pingi, E. Siotto, and R. Scopigno, "Virtual Reconstruction of an Etruscan Tomb", in 17th International Conference on Cultural Heritage and New Technologies, 5-7 November 2018, Vienna, Austria, 13 pages.
- [9] M. Canciani, E. Conigliaro, M. Del Grasso, P. Papalini, and M. Saccone, "3D Survey and Augmented Reality for Cultural Heritage. The Case Study of Aurelian Wall at Castra Praetoria in Rome", in *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Volume XLII-B5, 12-19 July 2016, Prague, Czech Republic, pp. 931-937. DOI:10.5194/isprsarchives-XLII-B5-931-2016.
- [10] A. Kargas, G. Loumos, and D. Varoutas, "Using Different Ways of 3D Reconstruction of Historical Cities for Gaming Purposes - The Case Study of Nafplio", *Heritage*, 2(3), 2019, pp. 1799-1811. DOI: 10.3390/heritage2030110.
- [11] T.P. Kersten, F. Tschirschwitz, "Development of a Virtual Museum Including a 4D Presentation of Building History in Virtual Reality", in *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Volume XLII-2/W3, 1-3 March 2017, Nafplio, Greece, pp. 403-409. DOI: 10.5194/isprs-archives-XLII-2-W3-361-2017.
- [12] G. Schofield, G. Beale, N. Beale, M. Fell, D. Hadley, J. Hook, D. Murphy, J. Richards, and L. Thresh, "Viking VR: Designing a Virtual Reality Experience for a Museum", in *Proceedings of the 2018 Designing Interactive Systems Conference*, June 2018, Hongkon, China, pp. 805-815. DOI: 10.1145/3196709.3196714.
- [13] R. Fistola, A. Rastelli, C. Pham, and F.O. Amore, "Augmented Reality for Cultural Heritage: A New Dimension for the Perceptual Knowledge", *Materials Science and Engineering*, 949, 012053, 2020, pp. 1-9. DOI: 10.1088/1757-899X/949/1/012053.
- [14] M. Vecco, A definition of cultural heritage: From the tangible to the intangible. *Journal of Cultural Heritage*, 11 (2), 2010, pp. 321-324. DOI: 10.1016/j.culher.2010.01.006.
- [15] S. Vu, D. Cliburn, J. Helgren, J. Salyers, K. Canniff, A. Johnson, M. Milliken, T. Reardon, K. Sabbatino, and A. Stephan, "Recreating Little Manila through a Virtual Reality Serious Game", in 3rd Digital Heritage International Congress held jointly with 24th International Conference on Virtual Systems & Multimedia, San Francisco, CA, USA, 2018, pp. 1-4, DOI: 10.1109/DigitalHeritage.2018.8810082.
- [16] G. Younes, R. Kahil, M. Jallad, D. Asmara, I. Elhadj, G. Turkiyyah, and H. Al-Harithy, "Virtual and Augmented Reality for Rich Interaction with Cultural Heritage Sites: A Case Study from the Roman Theater at Byblos". *Digital Applications in Archaeology and Cultural Heritage*, 5, 2017, pp. 1-9. DOI: 10.1016/j.daach.2017.03.002.
- [17] R.K. Napolitano, G. Scherer, and B. Glisic, "Virtual Tours and Informational Modeling for Conservation of Cultural Heritage Sites". *Journal of Cultural Heritage*, 29, 2017, pp. 123-129. DOI: 10.1016/j.culher.2017.08.007.
- [18] K. Choromański, J. Łobodecki, K. Puchała, and W. Ostrowski, "Development of Virtual Reality Application for Cultural Heritage Visualization from Multi-Source 3D Data", in *The International Archives of the Photogrammetry, Remote Sensing and Spatial Information Sciences*, Volume XLII-2/W9, 6-8 February 2019, Bergamo, Italy, pp. 261-267. DOI: 10.5194/isprs-archives-XLII-2-W9-261-2019.
- [19] D. John, D. Hurst, P. Cheetham, and H. Manley, "Visualising Dudsbury Hillfort: Using Immersive Virtual Reality to Engage the Public with Cultural Heritage. Robert, S., Michael, W. (Eds), Eurographics Workshop on Graphics and Cultural Heritage, 2018, pp. 193-197. DOI: 10.2312/gch.20181360.
- [20] A.G. Sooi, A. Nugroho, M.N. Al Azam, S. Sumpeno, and M.H. Purnomo, "Virtual Artifact: Enhancing Museum Exhibit using 3D Virtual Reality", in 2017 TRON Symposium (TRONSHOW), Tokyo, 13-14 December 2017, Tokyo, Japan, pp. 1-5. DOI: 10.23919/TRONSHOW.2017.8275078.
- [21] B. Tan, Y. Cai, Y. Zhang, X. Wu, Y. Chen, and B. Yang, "Virtual Reality Continuum for Heritage at Haw Par Villa in Singapore", in *VRCAI '16: Proceedings of the Symposium on VR Culture and Heritage*, 3 December 2016, Zhuhai, China, pp. 71-74. DOI: 10.1145/3014027.3014030.
- [22] R.P. Barratt, "Defining a Methodology for 3D Approximations in Archaeology: The Issue with Alternative Models", in 23rd International Conference on Cultural Heritage and New Technologies, 12-15 November 2018, Vienna, Austria, 12 pages.
- [23] R.G. Boboc, M. Duguleană, G-D. Voinea, C-C. Postelnicu, D-M. Popovici, and M. Carrozzino, "Mobile Augmented Reality for Cultural Heritage: Following the Footsteps of Ovid among Different Locations in Europe". *Sustainability* 11(4), 1167. 2019. DOI: 10.3390/su11041167.
- [24] J. Pakkanen, A. Brysbaert, D. Turner, and Y. Boswinkel, "Efficient Three-Dimensional Field Documentation Methods for Labour Cost Studies: Case Studies from Archaeological and Heritage Contexts", *Digital Applications in Archaeology and Cultural Heritage*, 17(2020) e00141, 2020, pp. 1-12. DOI: 10.1016/j.daach.2020.e00141.
- [25] H. Rahaman, E. Champion, and M. Bekele, "From Photo to 3D to Mixed Reality: A Complete Workflow for Cultural Heritage Visualisation and Experience", *Digital Applications in Archaeology and Cultural Heritage*, 13(2019) e00102, 2019, pp. 1-12. DOI: 10.1016/j.daach.2019.e00102.
- [26] Z.S. See, D. Santano, M. Sansom, C.H. Fong, and H. Thwaites, "Tomb of a Sultan: A VR Digital Heritage Approach", in 3rd Digital Heritage International Congress held jointly with 24th International Conference on Virtual Systems & Multimedia, San Francisco, CA, USA, 2018, pp. 1-4, DOI: 10.1109/DigitalHeritage.2018.8810083.
- [27] T. Trescak, A. Bogdanovych, M. Williams, and T. Sloan, "Capturing Aboriginal Heritage in Virtual Reality", in *Proceedings of VRST '17*, 8-10 November 2017, Gothenburg, Sweden. DOI: 10.1145/3139131.3141213.
- [28] E. Demetrescu, E. d'Annibale, D. Ferdani, and B. Fanini, "Digital Replica of Cultural Landscapes: An Experimental Reality-based Workflow to Create Realistic, Interactive Open World Experiences", *Journal of Cultural Heritage*, 41, 2020, pp. 125-141. DOI: 10.1016/j.culher.2019.07.018.
- [29] G. De Gasperis, A. Cordisco, and F. Cucchiara, "Immersive Virtual Reality as a Resource for Unaccessible Heritage Sites", *Materials Science and Engineering*, 364, 012035. 2018, DOI: 10.1088/1757-899X/364/1/012035.
- [30] K. Oudatzi, "Virtual Reality in Restoration of Historic Buildings: 3D Model Projection of the Restoration Project of Alaca Imaret Câmi with Intuitive And Interactive Application Through Hyper Realism Technology", in 16th International Conference on Virtual Systems and Multimedia, 20-23 October 2010, Seoul, Korea, pp. 361-364, DOI: 10.1109/VSM.2010.5665931.
- [31] C. Perra, E. Grigoriou, A. Liotta, W. Song, C. Usai, and D. Giusto, "Augmented Reality for Cultural Heritage Education", in: *IEEE 9th International Conference on Consumer Electronics*, 8-11 September, 2019, Berlin, Germany, pp. 333-336. DOI: 10.1109/ICCE-Berlin47944.2019.8966211.
- [32] M. Puggioni, E. Frontoni, M. Paolanti, and R. Pierdicca, "ScoolAR: An Educational Platform to Improve Students' Learning through Virtual Reality", in *IEEE Access*, 9, 2021, pp. 21059-21070. DOI: 10.1109/ACCESS.2021.3051275.
- [33] R. Zamora-Musa, J. Vélaz, and H. Paez-Logreira, "Evaluating Learnability in a 3D Heritage Tour", *Presence: Virtual and Augmented Reality*, 26(4), 2017, pp. 366-377. DOI: 10.1162/PRES_a_00305.
- [34] B. Gunay, "Museum Concept from Past to Present and Importance of Museum as Centers of Art Education", *Procedia-Social and Behavioral Sciences*, 55, 2012, pp. 1250-1258.

- [35] <https://icom.museum/en/resources/standards-guidelines/museum-definition/> (accessed on June 4, 2021).
- [36] A. Sochenkova, N. Podzharaya, P. Trofimov, G. Novikova, "Design and Implementation of Information Retrieval Mechanism for the Virtual Museum Creation", in 7th Mediterranean Conference on Embedded Computing, 10-14 June 2018, Budva, Montenegro, pp. 1-4. DOI: 10.1109/MECO.2018.8406084.
- [37] N.A. Haddad, "Heritage Multimedia and Children Edutainment: Assessment and Recommendations", *Advances in Multimedia*, 2014, 13 pages, DOI: 10.1155/2014/579182.
- [38] M. Shehade, and T. Stylianou-Lambert, "Virtual Reality in Museums: Exploring the Experiences of Museum Professionals". *Applied Science*, 10, 4031. 2020. DOI:10.3390/app10114031.
- [39] T.H. Jung, and M.C.T. Dieck, "Augmented Reality, Virtual Reality and 3D Printing for the Co-Creation of Value for the Visitor Experience at Cultural Heritage Places", *Journal of Place Management and Development*, 10(2), 2017, pp.140-151, DOI: 10.1108/JPMD-07-2016-0045.
- [40] T.H. Jung, H. Lee, N. Chung, and M.C.T. Dieck, "Cross-cultural Differences in Adopting Mobile Augmented Reality at Cultural Heritage Tourism Sites", *International Journal of Contemporary Hospitality Management*, 30(3), 2017, pp. 1621-1645. DOI: 10.1108/IJCHM-02-2017-0084.
- [41] H. Park, J. Kim, S. Bang, and W. Woo, "The Effect of Applying Film-Induced Tourism to Virtual Reality Tours of Cultural Heritage Sites", in 3rd Digital Heritage International Congress held jointly with 24th International Conference on Virtual Systems & Multimedia, San Francisco, CA, USA, 2018, pp. 1-4. DOI: 10.1109/DigitalHeritage.2018.8810089.
- [42] E. Ch'ng, Y. Li, S. Cai, and F-T. Leow, "The Effects of VR Environments on the Acceptance, Experience, and Expectations of Cultural Heritage Learning", *Journal on Computing and Cultural Heritage*, 13, 1, Article 7 (February 2020), 21 pages. DOI: 10.1145/3352933.
- [43] J. Lee, J. Kim, J. Ahn, and W. Woo, "Context-aware Risk Management for Architectural Heritage using Historic Building Information Modeling and Virtual Reality" *Journal of Cultural Heritage*, 38, 2019, pp. 242-252. DOI: 10.1016/j.culher.2018.12.010.
- [44] H. Lee, T.H. Jung, M.C.T. Dieck, and N. Chung, "Experiencing Immersive Virtual Reality in Museums", *Information and Management*, 57(5). 2019, DOI: 10.1016/j.im.2019.103229.
- [45] D.A. Plecher, M. Wandinger, and G. Klinker, "Mixed Reality for Cultural Heritage", in *IEEE Conference on Virtual Reality and 3D User Interfaces (VR)*, Osaka, Japan, pp. 1618-1622. DOI: 10.1109/VR.2019.8797846.
- [46] M.K. Bekele, and E. Champion, "A Comparison of Immersive Realities and Interaction Methods: Cultural Learning in Virtual Heritage", *Frontiers in Robotics and AI*, 6, 2019, pp. 1-12. DOI: 10.3389/frobt.2019.00091.
- [47] P. Fogliaroni, "Mixed Reality for Archeology and Cultural Heritage", in *Proceedings of the 2nd Workshop on Computing Techniques for Spatio-Temporal Data in Archaeology and Cultural Heritage co-located with 10th International Conference on Geographical Information Science (GIScience 2018)*, 28 August 2018, Melbourne, Australia, pp. 13-19.
- [48] S. Rokhsaritalemi, A. Sadeghi-Niaraki, and S-M. Choi, "A Review on Mixed Reality: Current Trends, Challenges and Prospects", *Applied Sciences*, 10(2), 2020, 26 pages. DOI: 10.3390/app10020636.
- [49] O.M. Machidon, M. Duguleana, and M. Carrozzino, "Virtual Humans in Cultural Heritage ICT Applications: A review", *Journal of Cultural Heritage*, 33, 2018, pp. 249-260. DOI: 10.1016/j.culher.2018.01.007.
- [50] F. Škola, S. Rizvić, M. Cozza, L. Barbieri, F. Bruno, D. Skarlatos, and F. Liarokapis, "Virtual Reality with 360-video Storytelling in Cultural Heritage: Study of Presence, Engagement, and Immersion". *Sensors* 2020, 20, 5851, 2020, 17 pages. DOI: 10.3390/s2020585.

Trust-based Key Management Conglomerate ElGamal Encryption for Data Aggregation Framework in WSN using Blockchain Technology

T.G.Babu¹

Research Scholar
Vels Institute of Science,
Technology and Advanced Studies, Chennai, India

Dr.V.Jayalakshmi²

School of Computing Sciences, Vels Institute of Science,
Technology and Advanced Studies
Chennai, India

Abstract—In wireless sensor networks (WSN), data aggregation is a widely used method. Security issues like data integrity and data confidentiality became a significant concern in data aggregation when the sensor network is deployed in a hostile environment. Many researches may carry out several works to tolerate these security issues. However, there were some limitations like delay, the arrival rate of packets, and so on. Hence, to overcome the existing problems, this approach offers a blockchain-dependent data aggregation scheme in WSN. The main intention of the proposed work is to generate a certificateless key generation so that the proposed system's secrecy rate is improved. The use of blockchain is employed for security purposes, and it enables the user to acquire the information stored internally in an effortless manner. Initially, deployment of sensor and base station (BS) is carried out, followed by node registration at which the public/private keys are generated. The computation of private hash values is carried by performing certificateless key generation. After that, the formation of blockchain is made using the PoW (Proof of Work) detection algorithm followed by the aggregation of data. In the data aggregation process, Elgammal based cryptographic approach is introduced to acquire member data, perform aggregation logic, and transfer the aggregated data. Finally, cluster-based routing is established with the use of Knapsack based cluster routing strategy. The performance investigation of the proposed system is estimated and the outcomes attained are compared with the existing techniques in terms of arrival rate, average delay, and the delay ratio of the packets. The investigation illustrates that the suggested approach is better than the traditional techniques.

Keywords—Wireless sensor networks; data aggregation; PoW detection scheme; blockchain technology; cluster formation; key generation; security; delay ratio

I. INTRODUCTION

Generally, WSN comprises disseminated micro-devices named sensors that might embed and have innumerable detection capabilities or sensing capabilities. The risks that face security of WSN arise from inside and outside a network frequently. The suitable network nodes are negotiated and enforced to act as malicious nodes. The security-related issues resolving has a thoughtful influence on the development and design trends of WSNs and consist of extensive consideration that attracts in the traditional works [1]. The WSN sensors are compact generally and thus utilize the constrained resource of

battery. This sensor, in turn, aggregates data and thus transmits it to the targeted location called base station (BS). The data received at BS are analyzed to create the decision for various prescribed applications like IOT based products. This node operates or functions as a repeated one to transmit data to the sink and other nodes. Moreover, the power source of WSN should be adequately utilized as this could not be exchanged or recharged. This WSN basis is exaggerated by numerous constraints like energy efficiency, scalability, fault tolerance, and so on. The WSN sensor, in turn, exhausts energy mostly in two ways that are sensing environmental parameters and the transmission of data to the base station over sensor nodes. The insufficient source of power is observed as the important problem in wireless sensor networks, and henceforth the node failure and network failure rise [2]. Additionally, the usage of optimal energy in the framework of WSN is required for attaining more performance and a high lifetime. Therefore, sensors grouping as corresponding clusters has been utilized for reducing the drainage of network energy and thus to enhance the reliability of the network. Several methods have been carried out with respect to sensor network construction with the solutions presented for resolving issues related to layer and the protocols that connect some things like scalability, optimum use of energy resources in sensors, environment, energy consumption, error tolerance, change in network regulations, low cost and so on. These problems are being addressed by various researchers [4]. One such advantage of employing data aggregation is that the data was to be transmitted in an efficient way with negligible latency of data. Various data aggregation algorithms have been presented so far to enhance the sensor network lifetime. The inadequate power source are regarded as the key issue in wireless sensor network and hence the network failure and node failure arises. Further the optimal energy usage in WSN is needed for obtaining high lifetime and more performance. So grouping of sensors into the corresponding clusters has been employed for decreasing the network energy drainage and thereby to increase the network reliability. Every Cluster possess Cluster Head and an effective framework like our proposed system is required to reduce the consumption of energy. Security enhancement is also a challenging issue of WSN at the time of aggregation. Here we study and propose a secure cryptosystem based on blocking of data. The blockchains invention overwhelms the

constraint issue of a centralized manner. Blockchain offers admirable functionalities similar to decentralized architecture, a transparent system, and security. Also, Blockchains are employed for efficient and secured data transmission [3, 4]. Though, blockchain frameworks for IoT strategies might cause lower latency, lower throughput, and delay-related issues. The present system on blockchain employs storage and high processing power. The huge amount of heterogeneous data in blockchain IoT, such as WSN outcomes in the consumption of huge energy at the time of data transmission from various sources [5-7]. Moreover, the major dispute in data aggregation is the data heterogeneity in the network. Therefore, there is a need to enhance the network security since WSN are prone to various attacks like injection attacks, replay attacks, and tampering attacks, and so on. Several works have been employed to address the existing issues over data privacy and security in blockchain-based IoT. The presented scheme aims at proposing an efficient framework for node registration and formation of blockchain using data aggregation and cluster-based routing. The blockchain formation is carried using a PoW detection algorithm along with data aggregation. Each cluster, in turn, possesses a cluster head for reducing energy consumption. The presented technique employs data aggregation using Elgammal based encryption which enables effective data aggregation model.

A. Contribution

The main intention of the proposed work is:

- To generate a certificateless key generation such that the secrecy rate of the proposed system is improved.
- To employ blockchain technique security purpose using PoW detection algorithm and is integrated with data aggregation scheme.
- To form a cluster based on the cluster-based routing protocol.

B. Organization

The residual portion of this manuscript is systematized as shown: Section II is the illustration of various existing techniques review. Section III is the depiction of a detailed explanation of the proposed mechanism. The analysis of the proposed system performance is shown in Section IV. Lastly, the conclusion and future enhancement are narrated in Section V.

II. RELATED WORK

In this section, various existing techniques employed are reviewed. In this [8], the author presented a scheme of blockchain-based multi-WSN authentication models. The IoT nodes were categorized as cluster head nodes, base stations, and ordinary nodes as per their variations inability that was formed as hierarchical networks. The blockchain network is thus constructed with two varied kinds of nodes that form a hybrid blockchain scheme that includes public and local chains. In this hybrid model, the mutual authentication identity of nodes at several scenarios of communication was realized, the operation of ordinary node identity authentication was accomplished by means of local blockchain, and the identity authentication of cluster head node was realized in the public

blockchain. The security and performance analysis illustrates that the performance and security of the scheme offer comprehensive security with an enhanced rate of performance. This [9] suggested a protocol of extremely secured CAKE (codeword Authenticated Key Exchange) that depends on one-way verification along with OTP (one-time-password) verification. This protocol was then related to other traditional schemes of mutual verification that portray substantial energy and time consumption reduction. The presented protocol in turn supports privacy, mutual authentication, and integrity and thus could counter various attacks such as replay attack, offline guess occurrence, impersonation attack, DoS attack, and so on and thus preserves forward secrecy perfect and creating the etiquette an appropriate one for several WSN applications.

In [10] developed a scheme of the blockchain-dependent framework with decentralization integrated with the privacy preservation and authentication in WSN aided IoTs. The registration, certification, and revocation process was utilized intended for the base station (BS) and sensor nodes communication in the cloud framework. In this approach, the CHs transmit information gathered at the base station. Meanwhile, BS saves entire key constraints on the disseminated blockchain, and a huge amount of data was then transferred to the cloud for storage purposes. The certificates that were revoked of all malicious nodes were then eliminated by BS from the blockchain. The proposed system performance was examined in terms of authorization delay, communicational and computational overhead, certification delay, and detection accuracy—the comparative outcome and the security authentication aid the advantage of the projected scheme over traditional ones.

In [11] utilized technology of blockchain for building the incentive scheme of nodes as per the storage of data for WSN. In this approach, data storing nodes were satisfied with digital money. If the information kept by the node were huge, then recompense would be more. However, two blockchains were constructed. One was employed for storing data of each node, and the other was to control the data access. Also, the proposed scheme adopts the data possession that was provable for replacing the proof of work (PoW) in the original bitcoins for carrying out the storage and mining of new data blocks that reduces the computing power greatly on comparing the PoW scheme. The conserving hash function was also necessary for comparing the new blocks and stored blocks of data. Thus, the new data could be stored in a node that was closest to previous data, and only varied subblocks were stored. Therefore, the node's storage space in the network was reduced greatly.

In [12] discussed the survey of an in-depth blockchain-based approach for the detection of malicious nodes, an examination of exhaustive blockchain technique integration with the WSN (BWSN), and insight for this novel approach. The contribution of blockchain for WSN was also explained in this survey, which includes aggregation, along with auditing, information analysis storage, auditing, event logs, and the offline query process. Thus, the presented schemes examine the centralized models of WSN for the security problems together with the blockchain discussion for the management of

security like preserving information integrity, ensuring node longevity, guaranteeing privacy, and so on.

In [13] suggested a blockchain-dependent scheme of data provenance (BCP) which was compression-free, at which provenance was kept on nodes together distributivity with the packet path, and the BS could retrieve on-demand provenance through the inquiry method. The edge computing-dependent network monitoring comprised of H-nodes (high-performance nodes) was organized near or above WSN that retains the WSN data provenance in the blockchain-dependent dataset. The authenticity, provenance, and security were then protected. Both experimental outcome and simulation analysis represents that the proposed BCP scheme was much effective in terms of energy and secured on comparing the distributed provenance of data.

In [14] suggested an energy-effective decentralized mechanism of trust with the use of the blockchain-dependent solution for multi-mobile code on behalf of sensing the interior attacks in the SN (sensor node) enabled IoT. The outcome validates improved concert of presented technique over traditional ones with 43.94% and 2.67% a reduced amount of overhead message in the Greyhole and blackhole attack circumstances correspondingly. Likewise, the detection time of malicious nodes was decreased by 20.35% and 11.35% at both Greyhole and blackhole attacks. These two factors show a dynamic part in enhancing the lifetime of the network.

In [15] presented a massive blockchain-enabled IoT data collection (MIDC) intellectual context for supporting the security, efficiency, and trust of the huge collection of data for the huge-scale varied WSNs. Specifically, a series of novel framework technology was presented. Initially, a huge scale heterogeneous WSN concerted individuality so as to guarantee a reliable source of data. Next, the scheme of Ranked massive aggregation of data so as to collect massive IoT data in a secured and efficient manner. Thirdly, the blockchain-dependent massive management of IoT data systems was depicted for constructing trust over various parties. The simulation analysis and the experimental prototype prove the framework's effectiveness.

In [16] presented a novel scheme of data aggregation depending on the clustering of node and extreme machine learning scheme (EML) for reducing the erroneous and redundant data. The analysis, along with the real-time databases, represents that the presented scheme outdoes the prevailing system consistently in relation to data clustering accuracy and efficiency of energy in WSN.

In [17] suggested a privacy preservation and energy efficiency algorithm CBDA (chain-dependent data aggregation). In this scheme, sensor nodes were systematized as a network topology of the tree. The leaf nodes of the tree were reconnected successively with one another to form several chain network topologies. The suggested approach CBDA attains less consumption of energy and higher accuracy of aggregation at the time of data aggregation. The simulation outcomes attained were compared with traditional ones, and attained outcome reveals that the presented scheme outperforms other traditional mechanisms.

In [18] presented a scheme of new ring-dependent in-network data aggregation to solve existing issues. The network was then portioned as rings, and the aggregated data was executed from outside to inside as a ring form. The analysis shows the effectiveness of the presented scheme.

[19] projected an energy-effective mechanism of data aggregation (EEDAM) that was protected by a technique of blockchain. The suggested technique employs a mechanism of aggregation of data at the level of the cluster for saving energy. The edge computation was employed for offering trusted on-demand services to the IoT deprived of the lowest delay. Since the blockchain was united inside the cloud server, the edge was authenticated by blockchain for offering secured services to IoT. At last, the performance simulation was estimated, and the proposed system performance was compared with traditional algorithms. The outcomes show that the projected operational strategy was reduced effectively and offers security to IoT, which extends WSN.

III. PROPOSED WORK

A detailed narration on the proposed system methodology is depicted in this part. The overall flow of the proposed mechanism is shown Fig. 1.

A. Deployment of Sensor and Base Station

1) *Network model:* Blockchain technology was utilized for designing DWSNs based on WSN for achieving trustworthiness. This technique comprises of huge stationary numbers or sensor nodes moving and the BS, which assigns partial certificateless public/private pair of keys to the nodes. There were two kinds of SN's: (1) the nodes having huge storing space, communication capabilities, and computing termed as H_{SS} -sensors, which comprises of consent network. (2) nodes having lower storage space, communication capability, and computing termed as normal node called L_{SS} -sensors.

Let us assume that there were N number of nodes in the WSN with N_H H_{SS} -sensors and N_L L_{SS} -sensors, here, $N_T = N_H + N_L$ and $N_H \gg N_L$. From WSN perspectives, the network is divided into a number of clusters as per the region at which the CHs are H_{SS} -sensors and the cluster member are the L_{SS} -sensors. From the blockchain viewpoint, H-sensors act like a node of consensus that forms a blockchain network termed stake blockchain. Owing to the analysis like storage, communication, and computation, L_{SS} -sensors remain just normal or ordinary nodes that will not participate in any consensus part. This is worth noticing that the BS, a unified device, might not link consensus, consequently H_{SS} -sensors might form a system that is decentralized, and the management of key does not depend on the base station BS. This BS role is to assign a unique individuality simply to each node. The node Id L_{SS}^i is employed for indicating the H_{SS} -sensor H_{no}^i . The key generation center (KPC) that is hosted by BS, in turn, generates the parameters of the community system and consequently issues the certificateless private/public pairs

of keys for each WSN's node. In the model of the network, a pairwise key recognized by certificateless public/private key is then spitted among the two nearby nodes, whereas the cluster

key is being distributed among the nodes in the cluster. Fig. 2(a) and 2(b) indicates the Sensor establishment of the network model.

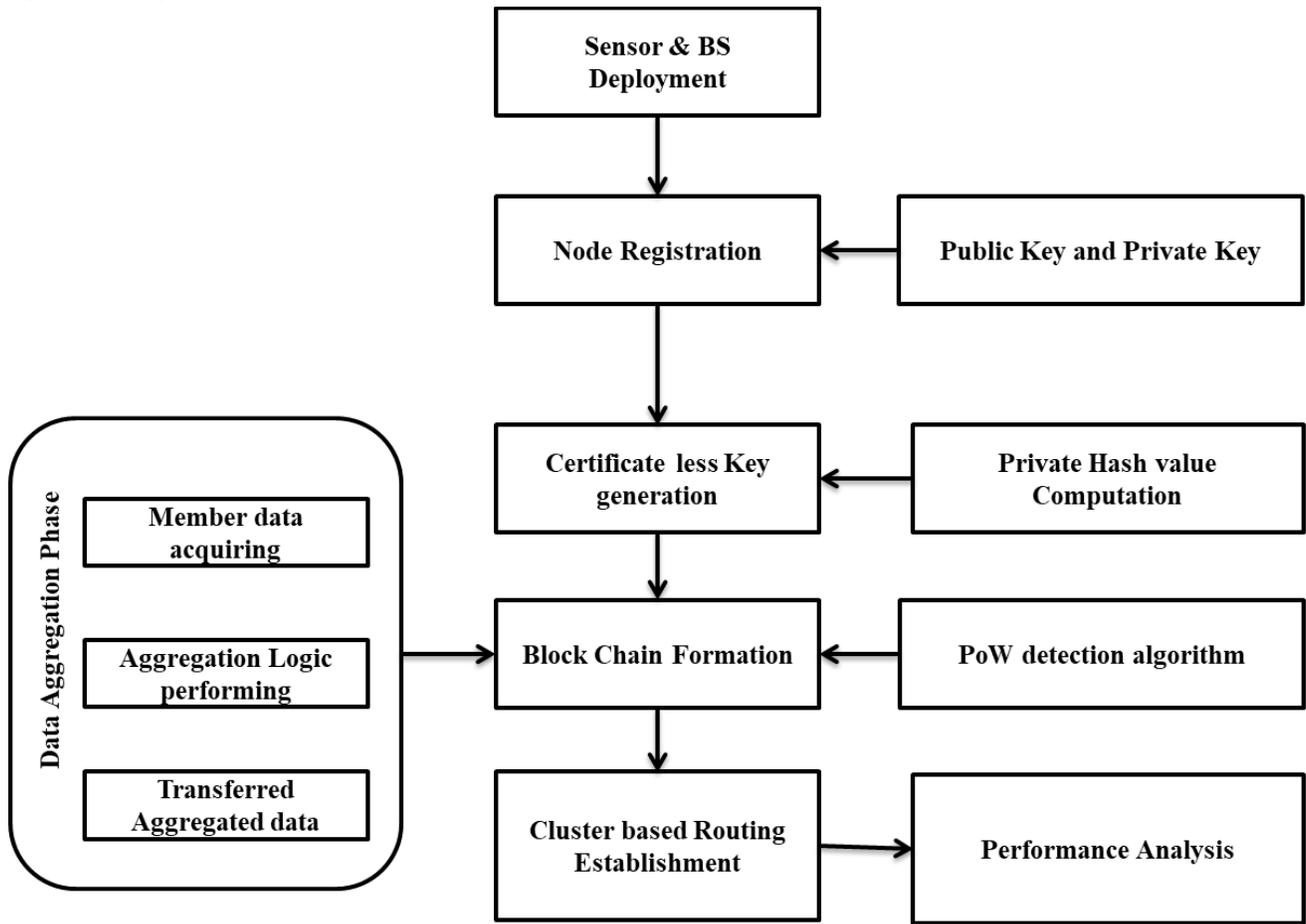


Fig. 1. Overall Workflow of the Proposed System.

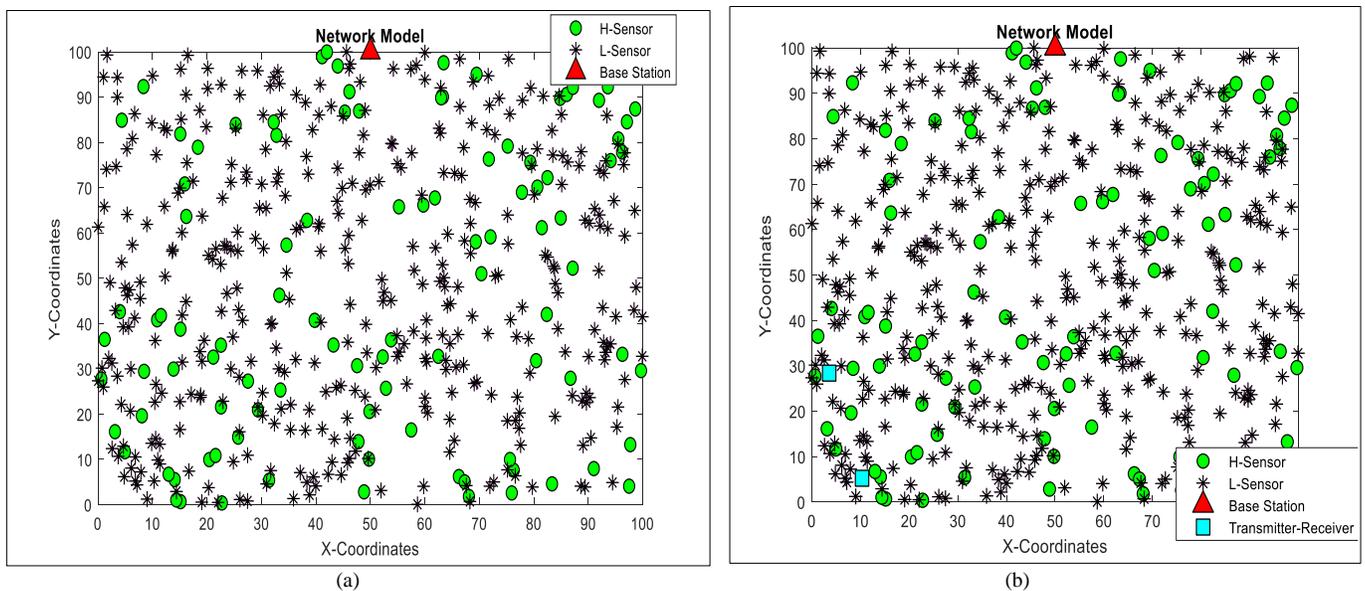


Fig. 2. (a) Network Model Deployment, (b) Deployment of the Network Model.

2) *An Attack model*: It was supposed that the opponent could not perform impersonation and cloning attacks however could perform several other attacks like pseudo-BS attack, interruption attack, etc., at the system setup. It is too assumed that BS might be impersonated or invaded. Moreover, once the nodes are captured, the adversary could augment a malicious node to the network for playing a legitimate node termed as an impersonation attack. Likewise, this technique presents the following requirements on security in the management of secured keys:

a) *Backward and Forward secrecy*: the node that has been logged out or else logged out by force might not lead to taking part in the communication of the cluster. However, this could not attain session information and could not be able to send a valid packet that is encrypted. Backward security refers to the new member that could not decrypt the information of the session before it joins.

b) *Resistance in contradiction of impersonation and cloning*: the technique should have the function of node substantiation or detect the malicious node for preventing in contradiction of node impersonation and cloning occurrences.

c) *Resistance in contradiction of pseudo BS attack*: once the adversary generates the pseudo-BS, this could not affect the registration of the node.

The presented scheme too prevents the BS and the compromised nodes from collaborating for reaching the stealing data and controlling the network's goal.

B. Registration of Node

After the deployment of the network, the BS, in turn, generates the system parameters and thus aids H-sensor nodes in registering the nodes. The legitimate nodes list is being maintained by blockchain technology.

1) *System parameters generation*: At BS, KPC selects the n -bit prime q_n thus recognizes the tuple $\{H_q, E/H_q, G_q, P\}$, here $n \in Z^+$. After that, the KPC, in turn, computes the public key of the system $K_{pub} = K_{pr}P$, here K_{pr} is a master private key and $K_{pr} \in Z_q$. Simultaneously, there consists of a cryptographic hash function as $\{H_a, H_b, H_c, H_d\}$. Consider that t is the symmetric key length and the base station, in turn, publishes $\delta = \{H_q, E/H_q, G_q, P, H_a, H_b, H_c, H_d\}$ too retains secret of K_{pr} .

2) *Generation of session less private/public key*: The base station employs L_{ss}^i for indicating the exclusive uniqueness of each L_{ss} -sensor L_{no}^i , then employs H_{ss}^i for denoting each H-sensor's H_{no}^i Unique identity. After that, the certificateless private/public key generation was described for H_{ss}^i which are the similar functions applied for L_{ss}^i . Next, the entire node H_{no}^i chooses a $H_{ss}^x \in Z_q$ secret value by computing $PH_{ss}^i = K_{pr}H_{ss}^iP$. The KPC is then utilized for generating public/private keys of the H_{no}^i over the H_{ss}^i input parameters and PH_{ss}^i . Besides, a KPC in turn selects $H_{ss}^r \in Z_q$, which is the BS's private key and too termed as skBS by returning the partial private/public key pair (H_{ss}^r, H_{ss}^d) on computation as shown:

$$H_{ss}^R = H_{ss}^r P \quad (1)$$

$$H_{ss}^d = H_{ss}^r + K_{pr} \quad (2)$$

$$H_{ss}^d = H_{ss}^r + K_{pr} \text{hash}_0(H_{ss}^i, H_{ss}^R, PH_{ss}^i) \text{mod } q \quad (3)$$

Here, H_{ss}^R termed as a BS's public key and called as pk_{BS} .

Once H_{ss}^i takes (H_{ss}^R, H_{ss}^d) , this will authenticate whether the subsequent calculation grasps.

$$H_{ss}^d P = H_{ss}^R + \text{hash}_0(H_{ss}^i, H_{ss}^R, PH_{ss}^i) K_{pub} \quad (4)$$

In case the above equations are true, then H_{ss}^i sets the full public key $pk_{H_{ss}^i} = (PH_{ss}^i, H_{ss}^R)$, full private key $sk_{H_{ss}^i} = (H_{ss}^d, H_{ss}^x)$, and thereby records RHj as the BS's public key termed pk_{BS} .

3) *Generation of Genesis Block*: Once the generation of keys for entire nodes is accomplished, the BS distributes information to the entire H_{ss}^i -sensor nodes through the message msg that consist of a list of registration comprised of identifiers and the public keys of those nodes over $msg = \langle setup, pk_{BS}, sk_{BS}(\text{hash}_0(\varphi), \varphi) \rangle$.

The H-sensor node utilizes pk_{BS} verified beforehand for verifying pk_{BS} And signature. In case the successful verification is being inscribed to the innovative block through the witness node (one H_{ss}^i -sensor node) underneath the PoW scheme. Formerly, the witness node broadcasts the block instantly, and once over 50% of the consent node authenticates over the block, it specifies that this was noted on the mechanism of blockchain. The block produced initially is too termed as the block of genesis.

In case the authentication fails, the H-sensor nodes broadcast the warning messages $Warn_{msg}$ regarding the hacked base station or else the pseudo-BS attack. Those warning messages are then collected in the message pool by the witness node. As soon as over 50% of the nodes broadcast a piece of comparable warning information, the message is written to a new block by the witness node by propagating them to the other nodes for the purpose of verification. Till the nodes more than 50% verify and pass new block, this is chained as their individual blockchain nearby. This means that BS is being negotiated and therefore requires some human interventions for checking and recovering the BS. This is worth notable that in case the genesis block is not being linked to the local blockchain, H-sensor is simply required to link a new block that stores the warning data to the local blockchain. Else, owing to the blockchain's tamper-proofing property, H_{ss}^i -sensor relates the new block afterward the block of genesis; this means the blockchain that comprises H-sensors is termed trust mechanism, and the entire blockchain information could not be modified.

C. Secure Key Management Scheme

The construction of secured key management is described in a detailed manner depending on the blockchain that comprises various phases. This is the system design's epitome that includes node registration. Table I represents the list of notations, grouping, and movement. Also, the solutions for presenting the deterministic detection of compromised nodes

are also offered. The common model is that a blockchain to be the trusted database that offers protected decision making. This is a reliable database, and reliably it stores the variations in the sensor state. The major notations for this scheme are illustrated:

TABLE I. NOTATIONS LIST

Notation	Definition
BS	Base Station
q_n	n bit prime number
K_{pub}	Public key of KGC $K_{pub} = K_{pr}P$
K_{pr}	Master private key
P	An additive cyclic group's point generator G_P
Z_q	Group of integers that are multiplicative
E	An elliptic curve
H_q	a, b, x, y are the elliptic curve parameters
pk_x	Any node's full public key n_x , $pk_x = (P_x, R_x)$
sk_y	Any node's full private key n_y , $sk_y = (d_x, pr_x)$
M_{xy}	Pairwise master key between n_x and n_y
m_{xy}	Pairwise encryption key between n_x and n_y
CK_i	Cluster key which is distributed between nodes of the i^{th} cluster
$H_{mac}(mes, key)$	Message authentication code using hash computation with message mes and key key
$E_{key}^{sym}(mes)$	Algorithm of symmetric key encryption for encrypting the messages mes with key key

D. Formation of Blockchain using PoW Detection Algorithm and Data Aggregation

Blockchain mechanism is a distributed, trusted record that is very appropriate for the P2P systems and thus functional for the protection of privacy and social networks. Moreover, due to the establishment of high-cost blockchain among the resource constraint H_{ss} --sensor nodes, a mechanism of consensus, is much critical for resolving the issue of excessive consumption of resources can resolve the issue of unnecessary consumption of a resource was very critical.

The system of consensus acts as a blockchain technology core; hence several great kinds of research on the mechanism of consensus have emerged. Though the consumption of resources is small in Paxos and Raft algorithm, the nodes can't be able to reach a consensus if there is a malicious attack like random process errors. Likewise, the PBFT scheme does not have good scalability. Therefore, an algorithm of proof of work (PoW) is employed in WSNs. This avoids the consumption of a huge amount of computational power and has the process of a faster-producing block in the blockchain. On the other hand, lower consumption of energy is highly suitable for WSN. Because of the quick speed of block production, H-sensor nodes could reach consensus quickly and thus makes a decision on the issue. Also, this proposed algorithm makes the blockchain system more scalable for

connecting sensor nodes. By means of this approach, it is contentious in relation to decentralization degree and having the features of trust from the cryptographic and mathematical systems that are highly helpful for constructing the dispersed management of key with trustworthiness. By considering the traditional WSN scenarios, the proposed one makes a compromise option for trust-based requirements.

The PoW detection scheme illustrates a system that needs a non-significant but feasible quantity of effort for determining the malicious nodes or malicious use of computing power like sending spam emails or injecting denial of service (DoD) attacks. This concept was adopted to secure digital money and was introduced by Hal Finney in 2004 from the idea of "reusable proof of work" using the SHA-256 hashing scheme. It is considered that the most trustworthy approach for achieving consensus in blockchain technology, and it helps in attaining decentralization, thereby ensuring transaction validation. Thus, the use of this detection algorithm helps in identifying malicious activities both in the base station and nodes.

E. Aggregation of Data using Elgammal Approach

This technique employs the Elgammal scheme for data aggregation, which employs encryption and decryption phases. For the cluster head selection, encryption has been processed. The cluster member developed was employed for the data acquisition and cluster weight determination. On performing the logic of aggregation, the members are subjected to the phase of data aggregation. The aggregated data transferred is being subjected to the analysis of performance for the estimation of the proposed scheme. Also, Knapsack based energy efficient protocol has been employed in the proposed method for the formation of the cluster. Thus, from this, the shortest path prediction was estimated by means of establishing route establishment with the energy-optimized path.

The process of Elgammal encryption is the system of a public-key cryptographic scheme that utilizes asymmetric key encryption for the purpose of communication among two parties and thus for encrypting the messages [20]. The data aggregation-based Elgammal encryption system is defined below. In this, the algorithmic steps for encryption, data aggregation, and decryption of the aggregated data has been described as shown:

The input of the data aggregation algorithm is sensor data S_N^D and the output will be aggregated data D_{aggr} , encrypted data S_i^C and decrypted data S_i^{Decry} . Initially, the key generation process takes place at which the large prime numbers p will be chosen, and the primitive root is estimated as follows:

$$p_r = \text{mod}(g, p) \tag{5}$$

Then, the m, n are chosen randomly among the limit of $(1 \leq m \leq p - 2)$ and $(1 \leq n \leq p - 2)$ correspondingly. The secret integer is computed as follows:

$$c = \text{mod}(g^m, p) \tag{6}$$

The combined public keys are represented by $\{p, g, c\}$, followed by private keys as $\{m, n\}$. The data sensed is then encrypted with the public keys, and the following process is carried out in the encryption process performance as shown:

$$s = g^n \pmod p \quad (7)$$

$$S_i^c = S_i^D \cdot c^n \pmod p \quad (8)$$

// S_i^c is the cryptography text.

After that, the process of data aggregation is performed for the entire sensed information by,

$$D_{aggr} = S_i^{c1} + S_i^{c2} + \dots + S_i^{ct} \quad (9)$$

Finally, the decryption is carried out for the aggregated data as:

$$s^m = c^n \pmod p \quad (10)$$

$$S_i^{Decry} = D_{aggr} \cdot \bar{c}^n \pmod p \quad (11)$$

F. Cluster Formation using Knapsack based Protocol

The proposed system employs an energy-efficient protocol based on Knapsack to enhance overall system performance and cluster formation. This approach provides a fast variation for memory overhead, low network utilization, low processing, and dynamic link conditions, which thus uncast the destinations routing in the Ad hoc networks. Fig. 3 indicates the cluster formation of our proposed system.

The Knapsack with the energy-based approach is employed for the process of cluster formation. In this, the input is the Sensor nodes S_N , Base station BS , sensors data S_N^D and the output will be selected Cluster head CH_i , selected cluster member CM_i . At first, the entire number of nodes N are being deployed in the dimensions of network $M * M$. The entire elements in the established network are in the stationary mode only, and the nodes deployed energy are not recharged back that are in the heterogeneous environment. The entire sensor nodes are employed as a power control for the varying transmit power amount. The entire nodes are termed as BS locations that are located at the sensor field. Each sensor node has the unique identity S_{id} . The energy usage for the transmission of the sensed packet S_N^D at distance d_i is represented as

$$E_{Tx}(m, d_i) = \begin{cases} mE_{elec} + m\delta_f d_i^2 & d_i \leq \rho \\ mE_{elec} + m\delta_m d_i^4 & d_i > \rho \end{cases} \quad (12)$$

Here

δ_f – the free space

δ_m – multipath fading channel model

E_{elec} – electronic energy that depends on some factors includes the modulation and digital coding

ρ – threshold distance

The energy consumption taken for receiving such packet is shown as:

$$E_{Ry}(m) = m * E_{elec} \quad (13)$$

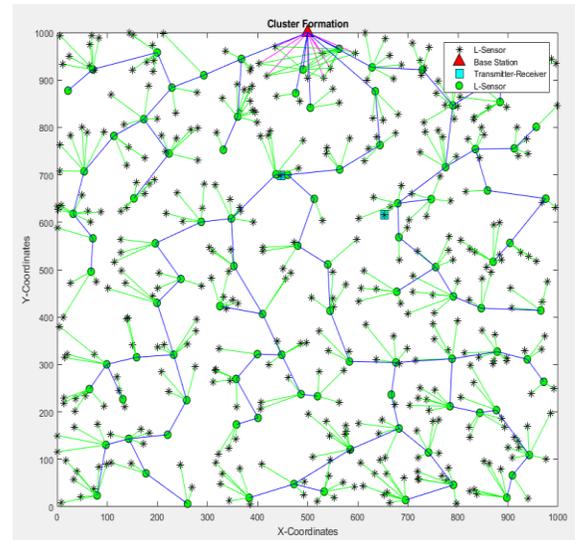


Fig. 3. Cluster Formation.

Based on the probability, the random nodes are selected by,

$$S_R = \frac{p_{sr}}{1 - p_{sr}(r \pmod{\frac{1}{p_{sr}}})} \quad (14)$$

Here,

p_{sr} is the percentage of neighbor nodes number

Then, the neighbor node selection based on the Euclidean distance is illustrated as shown:

$$d_i = \sqrt{(x_1 - x_2)^2 + (y_1 - y_2)^2} \quad (15)$$

$$dr = d_i - d_j \quad (16)$$

d_i – distance between random nodes and member nodes.

d_j – distance between random nodes and base station BS .

The number of nodes for each sensor is found, and the set is formed with respect to distance as.

for $i = 1:N$

for $j = 1:N$

$$d_i = \sqrt{(x_i - x_j)^2 + (y_i - y_j)^2} \quad (17)$$

if $d_i < \varphi$ // φ – sensing range

$CM\{i\} = \{j\}$ // CM – cluster member group

Finally, the CH selection is generated based on the multi-objective fitness function attained from the knapsack problem having two parameters like residual energy and the sensing range φ

$$fit_{val} = c_1 \left[\frac{E_{res}^m - E_{res}^i}{E_{res}^m} \right] + c_2 \left[\frac{\varphi^m - \varphi^i}{\varphi^m} \right] \quad (18)$$

Here, E_{res}^m – maximum residual energy.

E_{res}^i – residual energy for sensors.

φ^m – maximum sensing range.

φ^i sensing range of each sensor.

c_1 & c_2 are the constant value with a random number.

The list of those members and the information on formed CH will be stored in the routing table, and the routing table is utilized for selecting the second CH once certain rounds are completed. The presented approach employs a simple model for communication energy consumption. Based on the receiver and transmitter distance, the multipath fading channel or the free space method was employed.

The required energy to transmit packets over that distance was established in the above-mentioned steps. The energy consumption of receiving the packets is found in the next step. Afterward, the random deployment, random number of nodes were selected on the probability basis for the chosen node S_R . Depending on the provided equation, the random nodes are selected. On following this, the neighbor nodes are determined based on the Euclidean distance, which thus offers distance among the member and random nodes.

IV. PERFORMANCE ANALYSIS

The performance is estimated and the outcomes attained are related to the traditional mechanisms to verify the efficiency of the projected strategy.

Fig. 4 is the comparative analysis of the packet's arrival rate. The average delay of the packets in a slot-wise manner is estimated, and the outcomes of the proposed scheme. We compared with the existing techniques like TB-BP, QL-BP, RLBC, and Blockchain MDP [21]. The analysis shows that the proposed system delivers a good outcome by giving a reduced range of delay rates.

Fig. 5 illustrates a comparative estimation of the arrival rate of the packets vs. the average delay of packets (slots) with 50% malicious node presence. The proposed system delay is estimated and is correlated with the existing techniques like TB-BP, QL-BP, RLBC, and Blockchain MDP. The comparative analysis represents that the proposed mechanism offers a lower delay rate with a 50% malicious node. Thus, the system is effective than others.

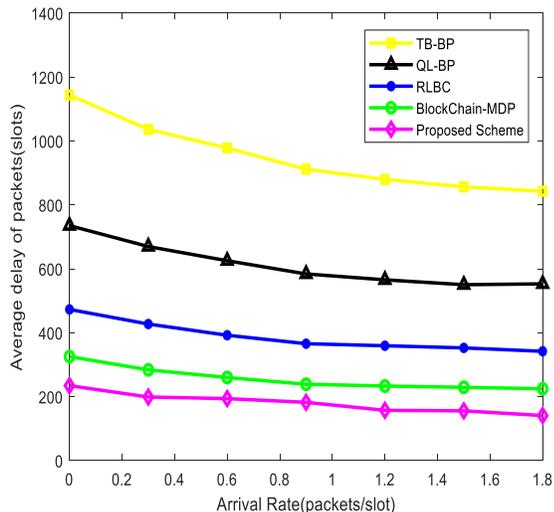


Fig. 4. Comparative Estimation of the Arrival Rate of the Packets.

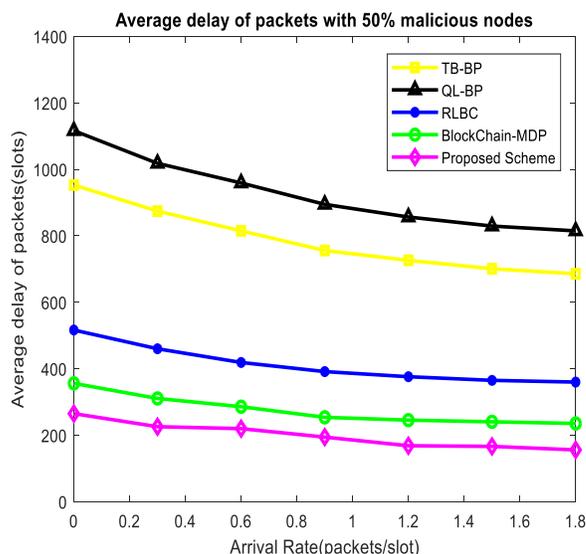


Fig. 5. Comparative Estimation of the Arrival Rate of the Packets with 50% Malicious Nodes.

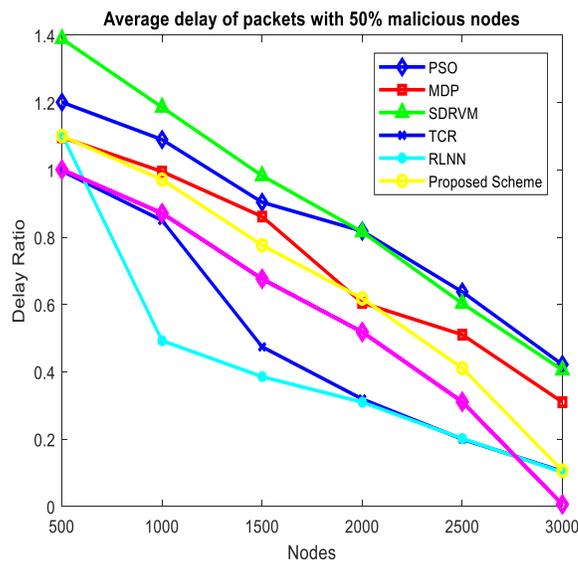


Fig. 6. Comparative Estimation of Delay Ratio of the Packets.

The overall delay ratio of the proposed detection system is estimated. The proposed scheme will indicate the outcomes attained and compared with the traditional mechanisms like PSO, MDP, SDRVM, TCR, and RLNN [22] in Fig. 6. The analysis shows that the existing system has a higher delay ratio, whereas the proposed scheme offers a better delay ratio than other existing methods. Therefore, the proposed approach is said to be an effective one in comparing the other traditional techniques.

V. CONCLUSION

A blockchain-based data aggregation scheme was presented along with the certificateless key generation. The significant contribution of the proposed work was to generate the certificateless key, which provides the expiring time of key, and to employ blockchain technique with the use of PoW detection scheme integrated with data aggregation procedure.

Then the formation of the cluster was carried out by the routing protocol. Thus, the use of blockchain and key generation aids in secured storage and transmission of packets. The performance analysis was carried out in terms of the packet's delay ratio, average delay, and arrival rate. The outcomes attained were compared with existing techniques, and the effectiveness of the proposed scheme over existing methods was projected. In future we aim to enhance the proposed approach with high level cryptosystems with cure the energy efficient.

REFERENCES

- [1] X. Wang, S. Garg, H. Lin, G. Kaddoum, J. Hu, and M. S. J. I. I. o. T. J. Hossain, "A secure data aggregation strategy in edge computing and blockchain empowered Internet of things," 2020.
- [2] I. Mosavvar and A. Ghaffari, "Data aggregation in wireless sensor networks using firefly algorithm," *Wireless Personal Communications*, vol. 104, no. 1, pp. 307-324, 2019.
- [3] L. Zhu, K. Gai, and M. Li, "Blockchain and Internet of Things," in *Blockchain Technology in Internet of Things*: Springer, 2019, pp. 9-28.
- [4] M. Kaur and A. J. A. H. N. Munjal, "Data aggregation algorithms for wireless sensor network: a review," vol. 100, p. 102083, 2020.
- [5] S. Ghai, V. Kumar, R. Kumar, and R. Vaid, "Optimized Multi-level Data Aggregation Scheme (OMDA) for Wireless Sensor Networks," in *Mobile Radio Communications and 5G Networks*: Springer, 2021, pp. 443-457.
- [6] B. VANASWI and S. Suresh, "Secure Data Aggregation Technique for Wireless Sensor Networks in the Presence of Various Attacks."
- [7] R. Aishwarya, S. S. J. A. i. N. Babu, and A. Sciences, "Privacy-preserving access control on data aggregation for wireless sensor networks," vol. 11, no. 6 SI, pp. 224-232, 2017.
- [8] Z. Cui et al., "A hybrid blockchain-based identity authentication scheme for multi-WSN," vol. 13, no. 2, pp. 241-251, 2020.
- [9] P. S. Mehra, M. N. Doja, and B. J. I. J. o. C. S. Alam, "Codeword Authenticated Key Exchange (CAKE) lightweight, a secure routing protocol for WSN," vol. 32, no. 3, p. e3879, 2019.
- [10] R. Goyat et al., "Blockchain-based data storage with privacy and authentication in Internet-of-things," 2020.
- [11] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. J. M. I. S. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," vol. 2018, 2018.
- [12] R. L. Kumar, F. Khan, A. L. Imoize, J. O. Ogbobor, S. Kadry, and S. J. I. A. Rho, "Blockchain-Based Wireless Sensor Networks for Malicious Node Detection: A Survey," 2021.
- [13] Y. Zeng, X. Zhang, R. Akhtar, and C. Wang, "A blockchain-based scheme for secure data provenance in wireless sensor networks," in *2018 14th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN)*, 2018, pp. 13-18: IEEE.
- [14] N. Tariq, M. Asim, F. A. Khan, T. Baker, U. Khalid, and A. J. S. Derhab, "A blockchain-based multi-mobile code-driven trust mechanism for detecting internal attacks in the internet of things," vol. 21, no. 1, p. 23, 2021.
- [15] L. Zhang, F. Li, P. Wang, R. Su, and Z. J. I. I. o. T. J. Chi, "A Blockchain-Assisted Massive IoT Data Collection Intelligent Framework," 2021.
- [16] I. Ullah and H. Y. J. J. o. S. Youn, "Efficient data aggregation with node clustering and extreme learning machine for WSN," vol. 76, no. 12, 2020.
- [17] S. Hu, L. Liu, L. Fang, F. Zhou, and R. J. I. A. Ye, "A novel energy-efficient and privacy-preserving data aggregation for WSNs," vol. 8, pp. 802-813, 2019.
- [18] J. Zhang, P. Hu, F. Xie, J. Long, and A. J. I. A. He, "An energy-efficient and reliable in-network data aggregation scheme for WSN," vol. 6, pp. 71857-71870, 2018.
- [19] A. Ahmed and S. Abdullah, "Cloud-based Energy Efficient and Secure Service Provisioning System for IoT using Blockchain," 2021.
- [20] M. K. Al-name and S. M. Ali, "Improved El Gamal public-key cryptosystem using 3D chaotic maps," *Bulletin of Electrical Engineering and Informatics*, vol. 10, no. 1, pp. 404-411, 2021.
- [21] J. Yang, S. He, Y. Xu, L. Chen, and J. J. S. Ren, "A trusted routing scheme using blockchain and reinforcement learning for wireless sensor networks," vol. 19, no. 4, p. 970, 2019.
- [22] M. Revanesh and V. J. T. o. E. T. T. Sridhar, "A trusted distributed routing scheme for wireless sensor networks using blockchain and meta - heuristics - based deep learning technique," p. e4259, 2021.

Statistical Analysis for Revealing Defects in Software Projects: Systematic Literature Review

Alia Nabil Mahmoud¹, Vítor Santos²

Information Management” Systems Management and Information Technologies”
NOVA IMS – Information Management School, Universidade Nova de Lisboa, Lisboa, Portugal

Abstract—Defect detection in software is the procedure to identify parts of software that may comprise defects. Software companies always seek to improve the performance of software projects in terms of quality and efficiency. They also seek to deliver the soft-ware projects without any defects to the communities and just in time. The early revelation of defects in software projects is also tried to avoid failure of those projects, save costs, team effort, and time. Therefore, these companies need to build an intelligent model capable of detecting software defects accurately and efficiently. The paper is organized as follows. Section 2 presents the materials and methods, PRISMA, search questions, and search strategy. Section 3 presents the results with an analysis, and discussion, visualizing analysis and analysis per topic. Section 4 presents the methodology. Finally, in Section 5, the conclusion is discussed. The search string was applied to all electronic repositories looking for papers published between 2015 and 2021, which resulted in 627 publications. The results focused on finding three important points by linking the results of manuscript analysis and linking them to the results of the bibliometric analysis. First, the results showed that the number of defects and the number of lines of code are among the most important factors used in revealing software defects. Second, neural networks and regression analysis are among the most important smart and statistical methods used for this purpose. Finally, the accuracy metric and the error rate are among the most important metrics used in comparisons between the efficiency of statistical and intelligent models.

Keywords—Defects; software projects; statistical model; linear regression; logistic regression

I. INTRODUCTION

Software companies aim to improve the quality of software projects in terms of their accuracy and efficiency. Software companies consume from 50% to 75% of the total budget of software projects in finding and fixing defects in those projects [1]. In the CHAOS report, many software projects vary in size (small, medium, and large projects) and, therefore, cost. These projects use many software development methods such as waterfall and agile. Several software projects failed due to the development and testing phase, as shown in Table I. A standard software development cycle has six phases, namely, planning, analysis, design, implementation, testing, and maintenance. In the development phase, developers modify source code that may lead to many defects in a software project. In modifications, developers should be careful not to produce any new defects in these projects. The testing phase is crucial to software projects. It is responsible for delivering the final project or product efficiently to customers without any defects and in time. Many

factors, such as McCabe and Halstead, help developers find and fix defects in those projects, as shown in Table II. Nevertheless, there is difficulty in using these factors in medium and large-scale projects. Thus, developers need a statistical or intelligent model capable of predicting defects in software projects accurately and efficiently.

Many reasons lead to the failure of software development projects. These are the lack of experience of the project team, lack of knowledge of the code language, insufficient experience in the field, etc. Software defects in the development phase are among the most critical problems facing software companies because the many defects lead to those projects' failure. The avoidance of software defects is to gain clients' trust by providing a quality product. According to the CHAOS report, many software projects still fail because of the many reasons that have been mentioned earlier [2]. However, the direct reason for these projects' failure is the emergence of many software defects, as shown in Table I [2].

It was performed a compressive study about the relevant related work using PRISMA methodology. The PRISMA explanation gives the minimum set of items for detailing a precise audit. It comprises the four-phase flow diagram, which permits us to utilize the Clarification and Elaboration document to go through cases and clarifications and find the meaning and method of reasoning for each item on the checklist. For a clear understanding of PRISMA, perusing the Clarification and Elaboration document is unequivocally recommended. The PRISMA Stream Graph delineates the stream of data through the diverse stages of a Precise Audit. It maps out the number of records recognized, included, and prohibited and the reasons for avoidances.

TABLE I. CHAOS REPORT BY AGILE VERSUS WATERFALL [2]

Size	Method	Successful	Challenged	Failed
All Size Projects	Agile (Scrum)	39%	52%	9%
	Waterfall	11%	60%	20%
Large Size Projects	Agile (Scrum)	18%	29%	53%
	Waterfall	3%	55%	42%
Medium Size Projects	Agile (Scrum)	27%	62%	11%
	Waterfall	7%	68%	25%
Small Size Projects	Agile (Scrum)	58%	38%	4%
	Waterfall	44%	45%	11%

TABLE II. SOFTWARE METRICS OF MCCABE AND HALSTEAD TO REVEAL SOFTWARE DEFECTS [7]

Factor ID	Factor	Description
1	Loc	McCabe's line count of code
2	v(g)	McCabe "cyclomatic complexity"
3	eV(g)	McCabe "essential complexity"
4	Iv(g)	McCabe "design complexity"
5	N	Halstead total operators + operands
6	V	Halstead "volume"
7	L	Halstead "program length"
8	D	Halstead "difficulty"
9	I	Halstead "intelligence"
10	E	Halstead "effort": effort to write program
11	B	Halstead "Number of Delivered Bugs"
12	T	Halstead's time estimator: time to write program
13	LOCode	Halstead's line count
14	LOComment	Halstead's count of lines of comments
15	LOBlank	Halstead's count of blank line
16	LOCodeAndComment	Halstead's count of lines which contain both code and comments
17	uniq_Op	Unique operators
18	uniq_Opnd	Unique operands
19	total_Op	Total operators
20	total_Opnd	Total operands
21	branchCount	Of the flow graph
22	defects	Module has/has not one or more reported defects

Many researchers, such as [3] and others [4]; [5] have suggested many factors to detect software defects. However, to date, there is no formal study to determine the critical factors to help software companies detect software defects with a reasonable degree of accuracy. Most researchers such as [6] and others also used scientific methods and models to detect software defects, but these models were weak in accuracy and results. Thus, software companies need a formal study to determine the critical factors to build a statistical model capable of detecting software defects with high results and accuracy.

The paper is organized as follows. Section 2 presents the materials and methods, PRISMA, search questions, and search strategy. Section 3 presents the results with an analysis, and discussion, visualizing analysis and analysis per topic. Section 4 presents the methodology. Finally, in Section 5, we discuss the conclusion.

II. MATERIALS AND METHODS

The methodology is composed of three steps. First, PRISMA was used to find appropriate manuscripts in our research based on the manuscript title and the experimental

results of the manuscripts. Second, bibliometric analysis was used to find the common terms that influence the revealing of software defects in terms of critical factors, performance metrics, and intelligent and statistical methods. Finally, the manuscripts were analyzed in detail to extract the most important factors and statistical methods used in detecting software defects and linking them to the results of the bibliometric analysis.

The systematic literature survey presents an evaluation of the scientific community's contributions to the topic of revealing software defects by using a rigorous and auditable methodology based on the PRISMA approach.

The PRISMA method is composed of five phases, as follows:

- Identification of relevant manuscripts of the domain or domains.
- Screening of titles, abstracts, papers without experiments, and position papers.
- Eligibility analysis.
- Full-text screening exclusion.
- Final papers to be analyzed in detail.

It was also adopted a bibliometric map; the bibliometric map is used to find the relationships between common software defects domain terms [8]. To this end, three phases were followed, evaluating the following quantities:

- Words frequency.
- Most common words.
- Frequency of these common words in the final manuscripts of the study.

By following PRISMA [9], this section is structured in the following way: (1) our research questions, (2) followed paper search strategy, (3) bibliometric map, (4) inclusion and exclusion criteria, and (5) final paper selection.

A. Research Questions

The study aims to provide a state-of-the-art review of current research efforts in revealing software projects. It was started by introducing the reader to specific topics concerning research objectives and employed methods. Particularly, the survey addresses the following research questions, aiming to identify the adoption techniques that have been applied in the overall domain of revealing software defects:

RQ1: What kinds of metrics have been adopted in software defects (SD)?

RQ2: Which statistical or intelligent techniques have been adopted for SD?

RQ3: What performance metrics have been adopted in the literature in the prediction of SD?

B. Search Strategy

A literature survey, generally, recommends searching several available journal and conference paper repositories to

determine if similar work has already been performed, aiding in locating potentially relevant studies. The papers counted were searched in two electronic repositories, Scopus, and Web of Science. This study's covered topics were multidisciplinary, including, Software, Computer Science, Engineering, Mathematics, Environmental Science, Telecommunications, and Multidisciplinary Sciences. However, both repositories were used. The analysis showed that most of the publications from Web of Science were in Scopus as well. A repeated search process was performed to identify publications that have in their titles, abstracts, or keywords the following expressions: "software-defects" (or software defects, or defect or projects defects), and "machine learning" in Fig. 1.

Phase 1, the search string was applied to all electronic repositories looking for papers published between 2015 to 2021, which resulted in 627 publications.

Phase 2 followed a 5-step approach. In step 1, we excluded manuscripts based on titles (e.g., software defects, regression, and machine learning), which narrowed the set to 211 publications. In step 2, we excluded manuscripts based on abstracts screening, which resulted in 117 publications. In the following step 3, we excluded manuscripts reporting research without experiments, resulting in 83 publications.

Subsequently, in step 4 of phase 2, we excluded position manuscripts which gave us the final figure of 29 publications, as shown in Fig. 2.

(software-defects OR defect OR projects) AND (OR "data mining" OR forecasting OR "machine learning" OR "neural network" OR "clustering" OR "artificial intelligence" OR "prediction" OR "predictive" OR "statistical" OR analysis")

Fig. 1. Search query for Scientific Manuscripts to Extract the Best Studies in Software Defects.

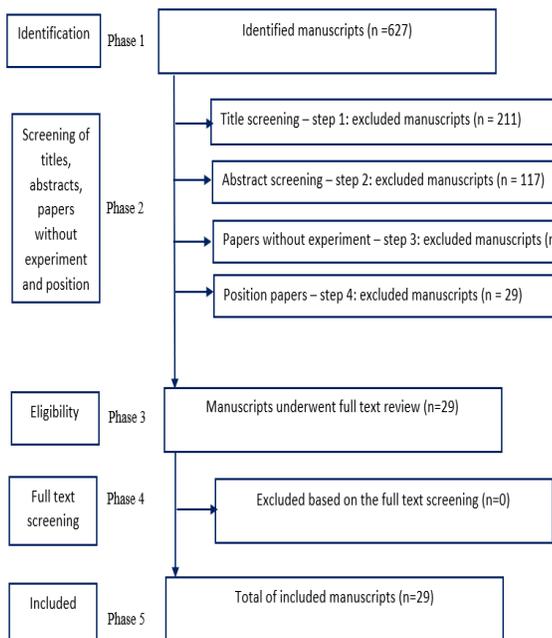


Fig. 2. Scientific Steps for Analyzing the Proposed Manuscripts “PRISMA Flow Chart”.

In phase 3, manuscripts underwent a full-text reading and review, which lead to no exclusions (the result of phase 4).

As a result of our paper selection approach, the final list included 29 manuscripts (phase 5), analyzed in detail in this paper. These were further divided into the following four categories, as shown in Tables III and IV.

- Regression analysis studies to reveal Software Defects.
- Studies of Software Defects Prediction.

TABLE III. REGRESSION ANALYSIS STUDIES TO REVEAL SOFTWARE DEFECTS

No	Ref	Application	Dimensions	Method of Solution and Performance Metrics
1	S.N. Umar[10]	Software testing defect prediction model-a practical approach	Total number of test cases executed, test team size, allocated development effort, test case execution effort, and the total number of components delivered	Multiple linear regression. R square and standard error
2	(Dhiauddin & Ibrahim, 2012)[11]	A Prediction Model for System Testing Defects using Regression Analysis	Software complexity, test process, errors, the severity of the defect, and validity of defect	Multiple linear regression. Adjusted R square
3	E. A. FELIX and et al [12]	Integrated Approach to Software Defect Prediction	Defect acceleration, namely, the defect density, defect velocity, and defect introduction time	Statistical analysis. Adjusted R square and correlation coefficient
4	D. VERMA and et al [13]	Prediction of defect density for open source software using repository metrics	software size, number of developers, commits, and the total number of defects	Multiple linear regression. R square
5	D. Sharma and et al [14]	Identification of latent variables using factor analysis and multiple linear regression for software fault prediction	Coupling between object classes, depth of inheritance tree, lack of cohesion of methods, and weighted methods per class	Multiple linear regression. R square and Adjusted R square
6	O. Sari and et al [15]	Use of Logistic Regression Analysis for Bug Prediction	Weighted method count, depth of inheritance tree, lack of cohesion in methods, number of attributes, and number of methods	Logistic regression. Standard error
7	G. MAUSA and et al [16]	Software Metrics as Identifiers of Defect Occurrence Severity	Software size, number of code lines, and the total number of defects.	Correlation coefficients and logistic regression. Error rate

8	Peng H. and et al [17]	presented a model for predicting defects in software projects	Software size, number of code lines, and the total number of defects.	Logistic regression. Standard error
9	M. Dhillon and et al [18]	An empirical model for fault prediction on the basis of regression analysis	Weighted method count, depth of inheritance tree, lack of cohesion in methods, number of attributes, and number of methods	Logistic regression. Precision, recall, and f1 measure
10	X. Chen and et al [19]	Multi-Objective Effort-Aware Just-in-Time Software Defect Prediction	diffusion [Number of modified subsystems], size [line of codes], history [The number of unique changes to the modified files], and finally, experience [Developer experience].	Logistic regression. Accuracy

			various kernel methods		Sigmoid kernel). Accuracy
6	F. Zhang and et al [24]	Towards building a universal defect prediction model		The weighted method programming language, issue tracking, total lines of code, total number of files, the total number of commits, and the total number of developers	K-mean clustering. AUC
7	A. Marandi and et al [25]	An approach of statistical methods for improving software quality		Post-delivery rework effort, actual effort, cost of the appraisal, cost of prevention, and cost of failure	Statistical analysis. Standard error
8	G. RajBahadur and et al [26]	The impact of using regression models to build defect classifiers		Object-oriented metrics	Linear regression, logistic regression, random forest, support vector machine, and neural network. AUC
9	S. Rathore and et al [27]	Predicting the number of faults in a software system using genetic programming		Total number of modules, number of lines of code, and number of faulty modules	Genetic programming. Recall and error rate
10	M. Sirshar and et al [28]	Comparative Analysis of Software Defect Prediction Techniques		Product and process metrics	Neural Network, Naive Bayes, Deep Forest technique. Error rate
11	M. Rawat and et al [29]	Software defect prediction models for quality improvement: a literature study		Object-oriented code, product, and process metrics	Regression models. Accuracy
12	S. Feng and et al [30]	Complexity-based Oversampling Technique to alleviate the class imbalance problem in software defect prediction		Line of code, number of children, and weighted method per class	Complexity-based Oversampling. Error rate
13	S. Patil and et al [31]	Predicting software defect type using concept-based classification		Interface, syntax, and standard [build-config-install]	Concept-based Classification. F1 score
14	J. Jiarpakdee and et al [32]	The impact of automated feature selection		inconsistent and correlated	Automated Spearman correlation. Error rate

TABLE IV. STUDIES OF SOFTWARE DEFECTS PREDICTION

No	Ref	Application	Dimensions	Method of Solution and Performance Metrics
1	A. H. Yousef [7]	Extracting software static defect models using data mining	McCabe and Halstead metrics	Data mining techniques. Accuracy, Precision, Recall, and F1 score
2	Karuna P and et al [20]	Statistical analysis of metrics for software quality improvement	Violation of programming standards, error in data representation, error in design logic, and assorted error type	Statistical analysis. Mean and standard deviation
3	Sukanya. V and et al [21]	An enhanced evolutionary model for software defect prediction	McCabe and Halstead metrics	Enhanced genetic algorithm, genetic algorithm, and neural network. Precision
4	Y. Koroglu and et al [22]	Defect prediction on a legacy industrial software: a case study on software with few defects	Product and process metrics	Data mining techniques. AUC
5	L. KUMAR and et al [23]	An effective fault prediction model developed using an extreme learning machine with	Complexity, coupling, cohesion, and inheritance in the code	Extreme learning machine with various kernel methods (e.g., Linear kernel, Polynomial kernel, and

		techniques on the interpretation of defect models		
15	A. Bangash and et al [33]	On the time-based conclusion stability of cross-project defect prediction models	Time, types of the projects, software development process	Mathews Correlation Coefficient. F-score
16	S. Morasca and et al [34]	On the assessment of software defect prediction models via ROC curves	Lines of code and complexity	Receiver Operating Characteristic. Error rate

III. RESULTS, ANALYSIS, AND DISCUSSION

This section introduces two main parts, which are bibliometric analysis and analyzing previous works in detail. The first part shows the relationships between common terms in intelligence, statistical techniques, and performance metrics used in the previous study. The second part seeks to find the scientific gap between proposed manuscripts in this study to build a novel model to overcome the issues for revealing defects in software projects.

A. Visualizing Analysis

It was used VOS viewer ("VOS viewer," n.d.), a Visualizing bibliometric network, to find common terminology in two areas: software defects and statistical techniques, across the 29 manuscripts under analysis. This tool supported the study with visual information enabling us to explore the relations between the domains of software defects and statistical techniques. Moreover, it helped to find the most common dimensions, clustering, and variety techniques able to answer the research questions.

Fig. 3 represents the visualization of a network map that displays the relations between the most popular terminology, how it is linked. The larger node represents the popular terminology in manuscripts, and the size of it represents the number of times these words appeared in manuscripts. VOS viewer splits the terminology into clusters according to the relevance concerning each other.

It was performed the analysis on the title and abstract using a binary counting method of 759 examined keywords with a minimum threshold of 2 occurrences, resulting in 57 terminologies, as shown in the figure. The largest nodes representing the important nodes of each cluster in the network map are determined as "Regression" (red), "cluster" (yellow), "software engineering" (green), "neural network" (blue), and finally "software defect prediction" (purple).

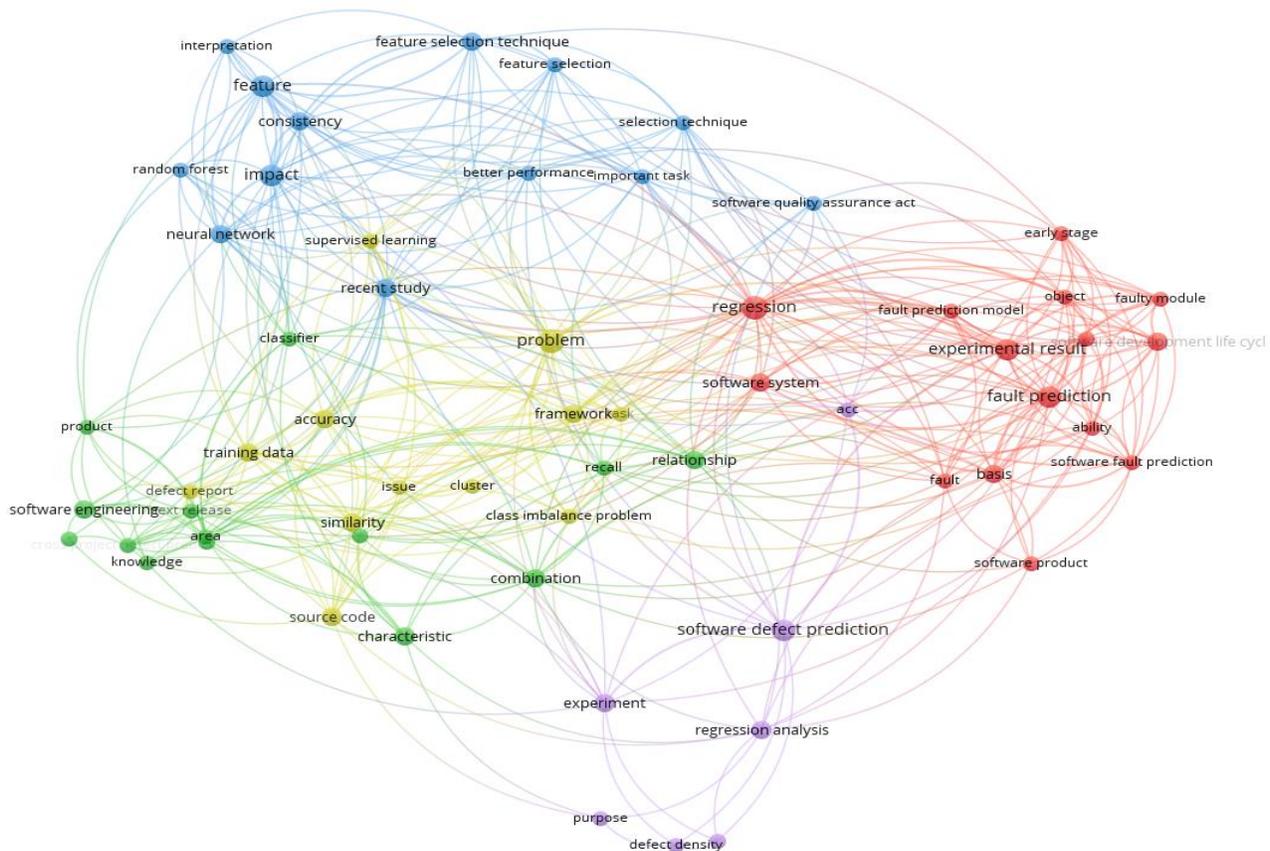


Fig. 3. The Relationships between the Common Terms using the Bibliometric Map.

Looking closer at the network map in Fig. 1, we can see that the 5 clusters are connected between them; for instance, the "regression" term is connected to "fault prediction model" in the same red cluster, it connected to "cluster" and "accuracy" in the yellow cluster, it is also connected to "software engineering" and "recall" in the green cluster. Finally, it is also connected to "neural network" and "feature selection" in the blue cluster; it is also connected to "software defect prediction" and "defect density." Besides, the term "software engineering" in the green cluster is connected to "cluster" in the yellow cluster, "regression" in the red cluster, and "neural network" in the blue cluster. Moreover, the terms "random forest" and "feature selection" are connected to "neural network" in the blue cluster, "recall" and "software engineering" in the green cluster, "cluster" in yellow cluster, "regression" and "fault prediction model" in the red cluster and "software defect prediction" and "defect density" in the purple cluster.

Finally, by analyzing the network map in Fig. 1 was possible to identify the important terms in each cluster, as follows:

- In the red cluster: "regression" and "software prediction model."
- In the yellow cluster: "cluster" and "accuracy."
- In the green cluster: "recall" and "software engineering."
- In the blue cluster: "random forest", "feature selection" and "neural network"
- In the purple cluster: "software defect prediction" and "defect density."

B. Analysis per Topic

RQ1 drove to look for metrics, data sources, and critical factors able to reveal software defects. Our review of papers S1 to S26 allowed us to extract such critical factors. Dimensions such as software status [No. of defects], OOP [Depth of Inheritance Tree and No. of Methods], McCabe Metrics [Line Count of Code], and Halstead Metrics [Effort to Write Program and Time to Write Program] seem to be highly considered when studying the revealing of software defects in software companies. Table V shows the variety of metrics used in predicting defects in software projects. The studies of S1, S4, and S16 relied on team dimension (team size and the number of developers) to predict software defects in software projects. The studies of S2, S3, S4, S7, S8, S12, S15, and S26 relied on software status dimensions (software complexity, number of defects, and software size) to detect defects in those projects. Moreover, the studies of S5, S6, S9, S15, S16, S18, and S21 relied on the OOP dimension (coupling between object classes, depth of inheritance tree, number of methods) also to reveal defects in those projects. Also, the studies of S7, S8, S10, S11, S13, S16, S19, S22, and S26 relied on McCabe metrics (line count of code, cyclomatic complexity, essential complexity, and design complexity) to find the optimal intelligent techniques to predict defects in software projects. Finally, the studies of S1, S3, S11, S13, S16, S17, S25 relied on Halstead Metrics (total operators + operands, effort to write the program, number of delivered bugs, count of lines of comments, and time to write a program) to forecast defects in various software projects. We observed that four factors are the most used in predicting defects in software projects. These are the number of defects, depth of inheritance tree, number of methods, and line count of code.

TABLE V. MAJOR FACTORS IN SOFTWARE DEFECT PROJECTS

Dimensions																			
		Team		Software status			OOP			McCabe Metrics				Halstead Metrics				Other Factors	
		Size	No. Developers	software complexity	No. of Defects	Software Size	Coupling between Object classes	Depth of Inheritance Tree	No. of Methods	Line Count of Code	Cyclomatic Complexity	Essential Complexity	Design Complexity	Total Operators + Operands	The effort to Write Program	Number of Delivered Bugs	Count of Lines of Comments	Time to Write Program	
S.N. Umar [10] S1	Software testing defect prediction model-a practical	✓	-	-	-	-	-	-	-	-	-	-	-	-	✓	✓	-	-	✓
M.D. Suffian and et al S2 [11]	A Prediction Model for System Testing Defects using Regression Analysis	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	✓

E. A. FELIX and et al. S3 [12]	Integrated Approach to Software Defect Prediction	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	✓	✓
D. VERMA and et al. S4 [13]	Prediction of defect density for open source software using repository metrics	-	✓	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-	-	-
D. Sharma and et al. S5 [14]	Identification of latent variables using factor analysis and multiple linear regression for software fault prediction	-	-	-	-	-	✓	✓	✓	-	-	-	-	-	-	-	-	-	✓
O. Sari and et al. S6 [15]	Use of Logistic Regression Analysis for Bug Prediction	-	-	-	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-
G. MAUSA and et al. S7 [16]	Software Metrics as Identifiers of Defect Occurrence Severity	-	-	-	✓	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-
Peng H. and et al. s8 [17]	presented a model for predicting defects in software projects	-	-	-	✓	✓	-	-	-	✓	-	-	-	-	-	-	-	-	-
M. Dhillon and et al s9 [18]	An empirical model for fault prediction on the basis of regression analysis	-	-	-	-	-	-	✓	✓	-	-	-	-	-	-	-	-	-	✓
X. Chen and et al. s10 [19]	An empirical model for fault prediction on the basis of regression analysis	-	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	✓
A. H. Yousef s11 [7]	Extracting software static defect models using data mining	-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Karuna P and et al. s12 [20]	Statistical analysis of metrics for software quality improvement	-	-	-	✓	-	-	-	-	-	-	-	-	-	-	-	-	-	✓

Sukanya.V and et al s13 [21]	An enhanced evolutionary model for software defect prediction	-	-	-	-	-	-	-	-	✓	✓	✓	✓	✓	✓	✓	✓	✓	-
Y. Koroglu and et al s14 [22]	Defect prediction on a legacy industrial software: a case study on software with few defects	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓
L. KUMAR and et al. s15 [23]	An effective fault prediction model developed using an extreme learning machine with various kernel methods	-	-	✓	-	-	✓	✓	-	-	-	-	-	-	-	-	-	-	-
F. Zhang and et al. s16 [24]	Towards building a universal defect prediction model	-	✓	-	-	-	-	-	✓	✓	-	-	-	-	-	-	✓	-	-
A. Marandi and et al s17 [25]	An approach of statistical methods for improving software quality	-	-	-	-	-	-	-	-	-	-	-	-	✓	-	-	-	-	✓
G. RajBahadur and et al s18 [26]	The impact of using regression models to build defect classifiers	-	-	-	-	-	✓	✓	✓	-	-	-	-	-	-	-	-	-	-
S. Rathore and et al. s19 [27]	Predicting the number of faults in a software system using genetic programming	-	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-
M. Sirshar and et al. s20 [28]	Comparative Analysis of Software Defect Prediction Techniques	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓
M. Rawat and et al. s21 [29]	Software defect prediction models for quality improvement: a literature study	-	-	-	-	-	✓	✓	✓	-	-	-	-	-	-	-	-	-	✓

S. Feng and et al. s22 [30]	Software defect prediction models for quality improvement: a literature study	-	-	-	-	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	✓
S. Patil and et al. s23 [31]	Software defect prediction models for quality improvement: a literature study	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓
J. Jiarpakdee and et al s24 [32]	Software defect prediction models for quality improvement: a literature study	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓
A. Bangash and et al. s25 [33]	Software defect prediction models for quality improvement: a literature study	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	-	✓	✓	
S. Morasca and et al s26 [34]	Software defect prediction models for quality improvement: a literature study	-	-	✓	-	-	-	-	-	✓	-	-	-	-	-	-	-	-	-	-

While addressing RQ2, we examined the techniques applicable in predicting defects in software projects. With this goal, we analyzed manuscripts S1 to S26 and noticed that techniques such as multiple linear regression, logistic regression, and machine learning are the most adopted, as shown in Table VI. Moreover, multiple linear regression was adopted by 23% of the analyzed manuscripts, whereas statistical analysis and data mining were the choices in 27% of manuscripts. Logistic regression accounted for 27% of the revised manuscripts. Also, machine learning techniques accounted for 19% of the revised manuscripts. Finally, the remaining 4% corresponded to the other intelligent techniques. We noticed four points.

Firstly, the studies (S1, S2, S4, S5, and S21) relied on multiple linear regression where S1 presented a model to predict defects in software projects to enhance the quality of software testing. This study seeks to find a suitable model to predict software defects to save effort, costs, and software companies' time. The results of this study show that R square and standard errors are 0.91 and 5.90%, respectively. S2 presented a model for predicting defects in software projects to improve the testing process in those projects. Besides, the adjusted R square in multiple linear regression is 90%. S4 presented a framework to predict defect density in open-source software projects. The results of this study show that

the R square in multiple linear regression is 0.86. S5 presented a model to predict faults in software projects. Furthermore, the results of this study show that R square and adjusted R square are 83% and 80%, respectively. S21 presented a review study to detect defects in a software project. It also seeks to find an optimal model to detect defects efficiently to save costs and time. Also, this study confirmed that regression models have achieved high results in terms of accuracy in detecting defects of software projects.

Secondly, the studies (S6, S7, S8, S9, and S10) relied on logistic regression, where S6 presented an approach to improve the quality of software projects by detecting bugs in software projects efficiently. Also, the standard error in the proposed statistical technique is 0.24. S7 presented a study to detect defects in software projects in the early stage to save effort, money, and time. This study also depends on statistical techniques such as correlation coefficients and logistic regression. The results show that the accuracy in logistic regression is 91.2%, and the correlation coefficient is 0.95. S8 presented a model for predicting defects in software projects. The result of this study shows that the standard error in logistic regression is 0.19. S9 presented an empirical model to predict fault in software projects. This study also depends on the binary logistic regression technique to predict defects in software projects. The results also show that the precision, recall, and f1 measures are 0.65, 0.9, and 0.79. S10 presented

a study to predict software defects by using logistic regression just in time. The results of this study show that the proposed technique is better than the state-of-the-art methods in terms of accuracy. The accuracy of the proposed technique is 0.73.

TABLE VI. INTELLIGENT AND STATISTICAL TECHNIQUES IN SOFTWARE DEFECT PROJECT

NO	Multiple Linear Regression	Logistic Regression	Statistical Analysis	Data Mining	Machine Learning	Other
S1	✓	-	-	-	-	-
S2	✓	-	-	-	-	-
S3	-	-	✓	-	-	-
S4	✓	-	-	-	-	-
S5	✓	-	-	-	-	-
S6	-	✓	-	-	-	-
S7	-	✓	-	-	-	✓
S8	-	✓	-	-	-	-
S9	-	✓	-	-	-	-
S10	-	✓	-	-	-	-
S11	-	-	-	✓	-	-
S12	-	-	✓	-	-	-
S13	-	-	-	-	✓	✓
S14	-	-	-	✓	-	-
S15	-	-	-	-	✓	✓
S16	-	-	-	-	✓	-
S17	-	-	✓	-	-	-
S18	✓	✓	-	-	✓	-
S19	-	-	-	-	-	✓
S20	-	-	-	-	✓	-
S21	✓	✓	-	-	-	-
S22	-	-	-	-	-	✓
S23	-	-	-	-	-	✓
S24	-	-	✓	-	-	-
S25	-	-	✓	-	-	-
S26	-	-	-	-	-	✓

Thirdly, the studies (S3, S11, S12, S14, S17, S24, S25) relied on statistical analysis and data mining techniques where S3 presented an approach to forecasting defects in software projects. It also depends on statistical regression such as multiple linear regression to predict defects in those projects. Besides, the adjusted R square in statistical regression is 98.6%, and the correlation coefficient is 0.98. S11 presented a model to extract software static defects by using data mining techniques. The results of this study show that the accuracy in Association Rules, Decision Tree, Naive Bayes, and Neural Network is 77.2%, 76.6%, 73.2%, and 73.2%, respectively. Thus, Association Rules is better than Decision Tree, Naive Bayes, and Neural Network in terms of accuracy. S12 presented a study to improve the quality of software projects using statistical analysis. The results of this study were

evaluated in terms of projection of errors (total errors) and cumulative projection of severity errors (e.g., series, moderate and minor). It also shows that total errors in 2016 are more than in 2015 by 1.5%.

Moreover, most severity errors are minor types. S14 presented a study to predict defects in legacy industrial software using data mining techniques. The results of this study show that the area under the curve (AUC) in Random Forest, Logistic Regression, Decision Tree, Naive Bayes, and a combination of Random Forest + Logistic regression is 0.73, 0.72, 0.66, 0.67, and 0.75. Thus, a combination of Random Forest + Logistic regression is better than Random Forest, Logistic Regression, Decision Tree, Naive Bayes. S17 presented an approach to improve software quality and cost minimization using statistical analysis. The results of this study were evaluated in terms of standard error. The standard error in the statistical model is 0.13. S24 presented a study to evaluate the impact of automated feature selection techniques on the interpretation of defect models. This study investigated 12 automated feature selection techniques in terms of consistency, correlation, performance, computational cost. By analyzing 14 publicly-available defect datasets, the results showed that the most important inconsistent metrics are highly correlated with the automated Spearman correlation of 0.85–1. S25 presented a study to predict defects in software models. This study applied the Mathews Correlation Coefficient-MCC to avoid defects in software models. MCC in F-score is less than 0.01. Therefore, the proposed technique is better than the state-of-the-art methods in terms of MCC.

Fourthly, the studies (S13, S15, S16, S18, S20) relied on machine learning techniques where S13 presented a model to predict software defects by using an enhanced genetic algorithm. The results of this study were evaluated in terms of precision. It also confirmed that precision in enhanced genetic algorithm, genetic algorithm, and neural network is 0.93, 0.81, and 0.80, respectively. Thus, the enhanced genetic algorithm is better than the genetic algorithm and neural network. S15 presented a model to predict effective faults in software projects using extreme learning machines with various kernel methods (e.g., Linear kernel, Polynomial kernel, and Sigmoid kernel). The results of this study were evaluated in terms of accuracy metrics. The accuracy in the linear kernel, Polynomial kernel, and Sigmoid kernel is 0.88, 0.93, and 0.91. Thus, an extreme learning machine using the Polynomial kernel is better than linear kernel and Sigmoid kernel. S16 presented a model to predict universal defects in software projects using clustering techniques. The results of this study were evaluated in terms of AUC. The AUC in K-mean clustering is 0.76. S18 presented a model to detect defects in a software project. This study depends on object-oriented metrics. It also relies on many intelligent techniques such as linear regression (LR), logistic regression (LG), random forest (RF), support vector machine (SVM), and neural network (NN). The results of this study were evaluated in terms of AUC. The AUC in LR, LG, RF, SVM and NN is 0.86, 0.94, 0.91, 0.90 and 0.90. Thus, LG is better than LR, RF, SVM, and NN. S20 presented a review analysis to predict defects in a software project. This study depends on many metrics, such as product and process metrics. It also introduced a

comparative analysis between Neural Network, Naive Bayes, Deep Forest technique. This study relies on previous works in the analysis of these techniques. Besides, this study confirmed that Deep Forest is better than Neural Network, Naive Bayes in terms of error rate.

Fifthly, the studies (S19, S22, S23, and S26) relied on other intelligent and statistical techniques where S19 presented an approach to predict many faults in a software system by using a genetic algorithm. The results of this study were evaluated in terms of error rate and recall. The error rate and recall in the genetic algorithm are 0.11, 0.91, respectively. S22 presented a new technique in software defect prediction by Complexity-based Oversampling. This paper relied on three main factors: a line of code, number of children, and weighted method per class. By analyzing the results, the proposed technique is better than the other oversampling techniques under the statistical Wilcoxon rank-sum test and Cliff's effect size. S23 presented a framework to predict software defect type using concept-based classification. This paper's main objective is to minimize the labeled training data's dependence for automation of the software defect type classification task. The results show that the proposed framework outperforms the state-of-the-art semi-supervised [LeDEx] in terms of the F1 score. F1 score in the proposed framework and LeDEx is 63.16% and 62.30%, respectively. S26 presented a study to assess the software prediction model by using Receiver Operating Characteristic. The results showed that the proposed technique is better than all other state-of-the-art methods in terms of recall and accuracy by 0.4 and 0.8, respectively.

The literature study also analyzed the performance evaluation metrics in the scope of our RQ3. Results are shown in Table VII and Table VIII. 21% of the selected manuscripts (S10,11,15, 9, 13, and 21) adopted accuracy and precision. 21% of them (S9, 11, 19, 23, and 25) selected only recall and F1 score. The error rate was used by 30% of the analyzed manuscripts (S1, 6, 7, 8, 17, 19, 20, 22, 24, and 26). 15% of the manuscripts adopted the R Square measure (S1, 2, 3, 4, and 5). We also realized that 13% (S12 S14, S16, and S18) did not use any defined evaluation metric.

Our research helped us to determine several research gaps. It was only possible to identified a few manuscripts (S11 and S13) tackling specific metrics impacting defects in software projects. For example, some studies (S5, S6, S9, S18, and S21) are concentrated on the OOP metric in general, with no mention of the line count of code and the number of developers. There are only simple manuscripts (S14, S20, S23, and S24) regarding finding defects in all types of software projects (small, medium, and large projects). However, stakeholders in software companies seem to find this topic pertinent and are willing not only to enhance software efficiency in those projects but interested to predict early defects in software projects to save costs and money. The results of this survey also showed a significant gap in the field of "intelligent and statistical models," particularly relating to the automatic prediction of defects in software projects. Some of the most promising algorithms are not yet being utilized.

Only a few studies (S18 and S21) tackle the application of "hybrid statistical and intelligent techniques, for instance, logistic regression with multiple linear regression and regression analysis with deep learning," which is a promising technique for forecasting defects in software projects. Moreover, there is a lack of official studies to identify critical factors that influence defects in software projects.

TABLE VII. SAMPLE OF PERFORMANCE METRICS RATE IN PREVIOUS WORK

	Performance Metrics	Rate
1	Accuracy and precision	21%
2	Recall and F1 Score	21%
3	Error Rate	30%
4	R Square Measure	15%
5	Other	13%

TABLE VIII. MAJORITY OF PERFORMANCE METRICS USED IN SOFTWARE DEFECT PROJECTS

NO	Accura cy	Precisio n	Recal l	F1 scor e	Erro r Rate	R- Squar e	Othe r
S1	-	-	-	-	✓	✓	-
S2	-	-	-	-	-	✓	-
S3	-	-	-	-	-	✓	-
S4	-	-	-	-	-	✓	-
S5	-	-	-	-	-	✓	-
S6	-	-	-	-	✓	-	-
S7	-	-	-	-	✓	-	-
S8	-	-	-	-	✓	-	-
S9	-	✓	✓	✓	-	-	-
S10	✓	-	-	-	-	-	-
S11	✓	✓	✓	✓	-	-	-
S12	-	-	-	-	-	-	✓
S13	-	✓	-	-	-	-	-
S14	-	-	-	-	-	-	✓
S15	✓	-	-	-	-	-	-
S16	-	-	-	-	-	-	✓
S17	-	-	-	-	✓	-	-
S18	-	-	-	-	-	-	✓
S19	-	-	✓	-	✓	-	-
S20	-	-	-	-	✓	-	-
S21	✓	-	-	-	-	-	-
S22	-	-	-	-	✓	-	-
S23	-	-	-	✓	-	-	-
S24	-	-	-	-	✓	-	-
S25	-	-	-	✓	-	-	-
S26	-	-	-	-	✓	-	-

IV. PROPOSED MODEL

Proposal of a new proposed model based on a statistical model able to predict defects in software projects. This section presents an approach for a statistical model able to predict defects in software projects. The proposed model has been used in several scientific data science researches like is the case of [7]. As shown in Fig. 4, the detailed the proposed model will cover the following phases:

- State-of-the-art analysis: Review the literature to extract important metrics, data sources, mathematical and computational approaches used for predicting defects of software projects.
- Data collection: data is collected from the NASA data sets online. We have two reasons to select the NASA Data set. The first reason is it is too hard to collect huge data from software companies to reveal the defects in software projects. The second reason for selecting Nasa is based on its vast and high-quality data. It explains the static measures and other variables that are used to detect static defects in software projects. It also shows a binary variable indicating whether the module is defective or not.
- Data Analysis and Pre-Processing: Analyze the data in detail and, if necessary, transform it to expose its information content better. Different mathematical techniques may be used, namely, outlier removal, discretization, reduction of the number of variables, and/or dimensionality (adopting regression models).
- Feature selection: determine critical metrics and detect defects that will be adopted in the proposed IST study by using logistic regression and multiple linear regression. Create a mapping between logistic regression and multiple linear regression to determine the final list of critical metrics capable of predicting defects in software projects.
- Build a model: present a statistical model capable of predicting defects in software projects using multiple linear regression and logistic regression.
- Training and verification model: train the model with data set and verify its ability to predict defects in software projects.
- Also, we will present a comparison between logistic regression and multiple linear regression by using the final list of critical metrics to determine which one is better than the other in terms of accuracy, precision, recall, F1 measure, and error rate.

Following this holistic approach, we built a methodology composed of five phases, as shown in Fig. 4.

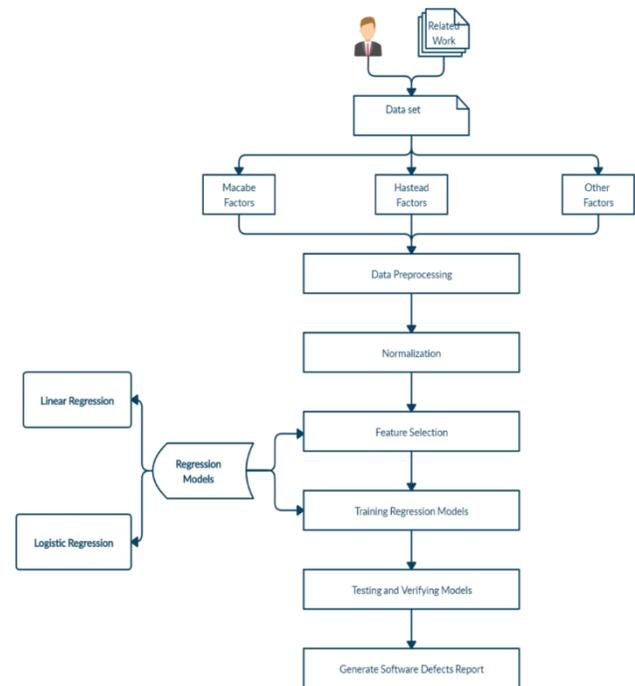


Fig. 4. A Proposed Statistical Model for Software Defects Prediction.

V. CONCLUSION

This paper presented a systematic review on the topic of revealing defects in software projects, concentrating on finding replies to our research questions, a diplomatic map was used to find the most used terminology in the statistical technique's software projects domains. By following a Prisma approach in our systematic review, we started by determining 627 papers and ended with VP analyses of 26 papers. The research questions covered three major points. Firstly, we identified the factors of our metrics that influence revealing defects in software projects. Secondly, we concentrated our research on identifying the production techniques used in the context. After, we determined the evaluation criteria used by those techniques. Thus, there is still a chance for enhancement regarding our topic to use statistical and intelligent techniques to reveal defects in software projects.

Finally, a new methodology based on a statistical model able to predict defects in software projects was proposed.

This study succeeded in identifying the critical factors that affect the detection of defects in the programs. Statistical analysis is executed by four methods, which are MLR-CDF, MLR-PLSDF, LR-CDF, and LR-PLSDF. LR-CDF outperforms on all the proposed methods in order to accuracy and standard error. In addition, LR-CDF outperforms on state-of-the-art methods (Association rule, Decision tree, Naive Bayes, and neural network) related to the accuracy by 9.1%, 10.3%, 13.1%, and 13.1%, respectively.

The study has some limitations. it was restricted by the search keywords selected and the time of the manuscripts (last six years). In addition, it utilized a fixed number of electronic sources. Furthermore, this study only handled English scientific papers, and we cannot warranty to have picked all the worthy substance for our review.

It is recommended as future work to utilize other techniques in terms of improving the model accuracy and identifying critical factors for revealing defects in software projects.

REFERENCES

- [1] Y. Koroglu et al., "Defect prediction on a legacy industrial software: A case study on software with few defects," *Proc. - Int. Conf. Softw. Eng.*, vol. 17-May-201, pp. 14–20, 2016, doi: 10.1145/2896839.2896843.
- [2] A. Abdelaziz Mohamed, N. Ramadan Darwish, and H. Ahmed Hefny, "Towards a Machine Learning Model for Predicting Failure of Agile Software Projects," *Int. J. Comput. Appl.*, vol. 168, no. 6, pp. 975–8887, 2017.
- [3] M. Sirshar, "Comparative Analysis of Software Defect Prediction Techniques," no. December, p. 456頁、453頁、603頁, 2019.
- [4] D. Sharma and P. Chandra, "Identification of latent variables using factor analysis and multiple linear regression for software fault prediction," *Int. J. Syst. Assur. Eng. Manag.*, vol. 10, no. 6, pp. 1453–1473, 2019, doi: 10.1007/s13198-019-00896-5.
- [5] V. S. Sukanya and S. Saraswathy, "An Enhanced Evolutionary Model for Software Defect Prediction," vol. 7, no. 10, pp. 15323–15328, 2017.
- [6] S. S. Rathore and S. Kumar, "Predicting number of faults in software system using genetic programming," *Procedia Comput. Sci.*, vol. 62, no. Scse, pp. 303–311, 2015, doi: 10.1016/j.procs.2015.08.454.
- [7] A. H. Yousef, "Extracting software static defect models using data mining," *Ain Shams Eng. J.*, vol. 6, no. 1, pp. 133–144, 2015, doi: 10.1016/j.asej.2014.09.007.
- [8] J. A. Moral-Muñoz, E. Herrera-Viedma, A. Santisteban-Espejo, and M. J. Cobo, "Software tools for conducting bibliometric analysis in science: An up-to-date review," *Prof. la Inf.*, vol. 29, no. 1, pp. 1–20, 2020, doi: 10.3145/epi.2020.ene.03.
- [9] D. Moher et al., "Preferred reporting items for systematic reviews and meta-analyses: The PRISMA statement," *PLoS Medicine*, vol. 6, no. 7, 2009, doi: 10.1371/journal.pmed.1000097.
- [10] S. N. U., "Software Testing Defect Prediction Model - a Practical Approach," *Int. J. Res. Eng. Technol.*, vol. 02, no. 05, pp. 741–745, 2013, doi: 10.15623/ijret.2013.0205001.
- [11] M. Dhiuddin and S. Ibrahim, "A Prediction Model for System Testing Defects using Regression Analysis," *Int. J. Soft Comput. Softw. Eng.*, vol. 2, no. 7, pp. 55–68, 2012, doi: 10.7321/jscse.v2.n7.6.
- [12] E. A. Felix and S. P. Lee, "Integrated Approach to Software Defect Prediction," *IEEE Access*, vol. 5, pp. 21524–21547, 2017, doi: 10.1109/ACCESS.2017.2759180.
- [13] D. Verma and S. Kumar, "Prediction of defect density for open source software using repository metrics," *J. Web Eng.*, vol. 16, no. 3–4, pp. 294–311, 2017.
- [14] D. Sharma and P. Chandra, "Identification of latent variables using factor analysis and multiple linear regression for software fault prediction," *Int. J. Syst. Assur. Eng. Manag.*, vol. 10, no. 6, pp. 1453–1473, 2019, doi: 10.1007/s13198-019-00896-5.
- [15] O. Sari and O. Kalipsiz, "Bug prediction for an ATM monitoring software use of logistic regression analysis for bug prediction," *ICEIS 2015 - 17th Int. Conf. Enterp. Inf. Syst. Proc.*, vol. 2, pp. 382–387, 2015, doi: 10.5220/0005382803820387.
- [16] G. Mauša, T. G. Grbac, L. Brezočnik, V. Podgorelec, and M. Heričko, "Software metrics as identifiers of defect occurrence severity," *CEUR Workshop Proc.*, vol. 2508, no. September, pp. 22–25, 2019.
- [17] P. He, B. Li, X. Liu, J. Chen, and Y. Ma, "An empirical study on software defect prediction with a simplified metric set," *Inf. Softw. Technol.*, vol. 59, no. February, pp. 170–190, 2015, doi: 10.1016/j.infsof.2014.11.006.
- [18] M. K. Dhillon, P. B. Singh, and P. J. Singh, "Empirical Model for Fault Prediction On the Basis of Regression Analysis," *Int. J. Sci. Res.*, vol. 5, no. 6, pp. 163–168, 2016, doi: 10.21275/v5i6.nov164139.
- [19] X. Chen, Y. Zhao, Q. Wang, and Z. Yuan, "MULTI: Multi-objective effort-aware just-in-time software defect prediction," *Inf. Softw. Technol.*, vol. 93, pp. 1–13, 2018, doi: 10.1016/j.infsof.2017.08.004.
- [20] N. Of, "S Tatistical a Nalysis of R Ainfal I Nsurance," vol. 89, no. 5, pp. 1248–1254, 2007, doi: 10.1111/j.1467-8276.2007.01092.x.
- [21] V. S. Sukanya and S. Saraswathy, "An Enhanced Evolutionary Model for Software Defect Prediction," vol. 7, no. 10, pp. 15323–15328, 2017.
- [22] Y. Koroglu et al., "Defect prediction on a legacy industrial software: A case study on software with few defects," *Proc. - Int. Conf. Softw. Eng.*, vol. 17-May-201, pp. 14–20, 2016, doi: 10.1145/2896839.2896843.
- [23] L. Kumar, A. Tirkey, and S. K. Rath, "An effective fault prediction model developed using an extreme learning machine with various kernel methods," *Front. Inf. Technol. Electron. Eng.*, vol. 19, no. 7, pp. 864–888, 2018, doi: 10.1631/FITEE.1601501.
- [24] F. Zhang, A. Mockus, I. Keivanloo, and Y. Zou, "Towards building a universal defect prediction model with rank transformed predictors," *Empir. Softw. Eng.*, vol. 21, no. 5, pp. 2107–2145, 2016, doi: 10.1007/s10664-015-9396-2.
- [25] A. K. Marandi and D. A. Khan, "An approach of statistical methods for improve software quality and cost minimization," *Int. J. Appl. Eng. Res.*, vol. 12, no. 6, pp. 1054–1061, 2017.
- [26] G. K. Rajbahadur, S. Wang, Y. Kamei, and A. E. Hassan, "The impact of using regression models to build defect classifiers," *IEEE Int. Work. Conf. Min. Softw. Repos.*, pp. 135–145, 2017, doi: 10.1109/MSR.2017.4.
- [27] S. S. Rathore and S. Kumar, "Predicting number of faults in software system using genetic programming," *Procedia Comput. Sci.*, vol. 62, no. Scse, pp. 303–311, 2015, doi: 10.1016/j.procs.2015.08.454.
- [28] M. Sirshar, "Comparative Analysis of Software Defect Prediction Techniques," no. December, p. 456頁、453頁、603頁, 2019.
- [29] M. S. Rawat and S. K. Dubey, "Software Defect Prediction Models for Quality Improvement: A Literature Study," *Int. J. Comput. Sci. Issues*, vol. 9, no. 5, pp. 288–296, 2012.
- [30] S. Feng et al., "COSTE: Complexity-based OverSampling TEchnique to alleviate the class imbalance problem in software defect prediction," *Inf. Softw. Technol.*, vol. 129, no. September 2020, p. 106432, 2020, doi: 10.1016/j.infsof.2020.106432.
- [31] S. Patil and B. Ravindran, "Predicting software defect type using concept-based classification," *Empir. Softw. Eng.*, vol. 25, no. 2, pp. 1341–1378, 2020, doi: 10.1007/s10664-019-09779-6.
- [32] J. Jiarpakdee, C. Tantithamthavorn, and C. Treude, "The impact of automated feature selection techniques on the interpretation of defect models," *Empir. Softw. Eng.*, vol. 25, no. 5, pp. 3590–3638, 2020, doi: 10.1007/s10664-020-09848-1.
- [33] A. A. Bangash, H. Sahar, A. Hindle, and K. Ali, "On the time-based conclusion stability of cross-project defect prediction models," *Empir. Softw. Eng.*, 2020, doi: 10.1007/s10664-020-09878-9.
- [34] S. Morasca and L. Lavazza, "On the assessment of software defect prediction models via ROC curves," *Empir. Softw. Eng.*, vol. 25, no. 5, pp. 3977–4019, 2020, doi: 10.1007/s10664-020-09861-4.

A Hybrid Deep Neural Network for Human Activity Recognition based on IoT Sensors

Zakaria BENHAILI*, Youssef BALOUKI, Lahcen MOUMOUN

Hassan First University of Settat, Faculty of Sciences and Techniques, Mathematics
Computer Science and Engineering Sciences Laboratory (MISI), 26000 Settat, Morocco

Abstract—Internet of things (IOT) sensors, has received a lot of interest in recent years due to the rise of application demands in domains like ubiquitous and context-aware computing, activity surveillance, ambient assistive living and more specifically in Human activity recognition. The recent development in deep learning allows to extract high-level features automatically, and eliminates the reliance on traditional machine learning techniques, which depended heavily on hand crafted features. In this paper, we introduce a network that can identify a variety of everyday human actions that can be carried out in a smart home environment, by using raw signals generated from Internet of Thing's motion sensors. We design our architecture basing on a combination of convolutional neural network (CNN) and Gated recurrent unit (GRU) layers. The CNN is first deployed to extract local and scale-invariance features, then the GRU layers are used to extract sequential temporal dependencies. We tested our model called (CNGRU) on three public datasets. It achieves an accuracy better or comparable to existing state of the art models.

Keywords—IoT; deep learning; CNN; GRU; CNGRU; human activity recognition

I. INTRODUCTION

The Internet of Things (IoT) is a technology that has a lot of potential, it presents a platform where sensors and devices can communicate seamlessly within a smart environment. Each year, the number of IoT supporting devices increases; sectors such as transport, healthcare, security, smart cities, education, agriculture, and many others have already benefited from its development. This will result in a generation of applications capable of completing complex sensing and recognition tasks to support a new world of human-things interactions. The recognition of human activities is a field that presents an interaction between computers and humans which has been promoted recently by the expansion of artificial intelligence. This progress has reached a stage that has allowed it to integrate several fields, to the point that we find its applications in everyday life. In the field of security by making surveillance more intelligent [1]. In smart homes by improving the security and monitoring the health condition of the residents [2], and increasing the degree of independence and quality of life, especially for the elderly [3]. HAR is present as well in the field of healthcare, by the deploy of a combination of one or more techniques of recognition that notifies the medical staff once an intervention is necessary [4].

This widespread availability is owing to significant efforts to reduce the size of the electronic components and create sensors that can be included in smartphones, smart watches,

and other wearable internet of things devices.

Depending on the type of sensors used, we categorize activity recognition into vision-based or sensor-based recognition. The first category deploys cameras to obtain images and videos and use it to detect and classify activities, however it faces challenges as image variation, object deformation, mobility constraints imposed by visual sensors, besides other problems related to power consumption and privacy. On the other hand, sensor based recognition which is based on acceleration sensors, gyroscope sensors, geomagnetic sensors and others, are simple to use and generate relatively accurate and reliable data. The classic approaches require a lot of data pre-processing and domain knowledge for feature engineering, which will be necessary at every change of dataset, and limit the generalization of the model.

Recently, Deep learning has achieved good performances and it has accumulated successes in image, speech, and natural language processing, and today it is introduced in human activity recognition, to profit from its capacity to learn complex movements, by abstracting features automatically from raw data without being handcrafted. Deep learning's layer-by-layer structure enables it to progressively learn features from simple to complex, which is effective in the analyse of multimodal sensory data. The various architectures of deep learning are capable of encoding these features from diverse perspectives. For example, CNNs can capture local multimodal sensory connections, where RNNs can extract each temporal dependency and learn information incrementally across multiple time intervals.

We achieve sensor-based HAR through four major steps, the first is data collection, followed by data segmentation, then feature selection or extracting features, and last the classification of the activity. Most of the previous works in HAR are based in their approaches on a manual feature engineering, which already requires an expert knowledge, the method proposed in this article does not require any design or creation of features, it exploits directly the data generated by the accelerometer and gyroscope. This is the key contributions of our work:

We propose CNGRU, an end to end Network for HAR capable of automatically extracting and learning features from raw data without pre-processing.

We deploy a combination of two types of neural networks: convolutional and gated recurrent units.

*Corresponding Author.

The network permits to recognize various activities and gestures, recorded using different types and combinations of sensors. The experience on three most widely used open datasets, proves that we reach comparable, or better results than previous methods, which demonstrates the generalization capability of the model.

We organize our paper as follows: Section II reviews related works of human activity recognition. In Section III, we propose our model for HAR. Section IV presents and examines the experimental results. And last in Section V, we draw out our conclusion.

II. REVIEW OF LITERATURE

Prior studies on human activity recognition have been conducted utilizing open-access datasets available on the internet. Mainly the UCI HAR dataset was exploited alone or with other datasets like Opportunity[5], WISDM V1.1 [6], PAMAP2[7]. Consequently, this availability of data facilitated the design and evaluation of the activity recognition approaches based on motion sensors. Whereas some works are based on the investigation of feature selection in order to achieve higher accuracies, others attempted to avoid this design and engineering task by utilizing the capacity of deep learning models. Convolution neural network is the most common model in the approaches proposed in the literature, researchers exploit its ability to capture local connections, as well as the recurrent neural network and its variants capable of capturing temporal dependencies between signal readings. And in other works those two networks are fused or cascaded to learn the most important features.

The authors in [8] have proposed a hybrid architecture, which combines LSTM and CNN. After preprocessing data, they fed it to two LSTM layers for temporal feature extraction, while the spatial features were extracted by two other convolution layers.

Deep et al [8] used the UCI HAR dataset to test their model composed of CNN followed by an LSTM network. They have achieved better recognition scores compared to simple LSTM architecture. On the same dataset, Hernández et al [9] presented the idea of using bidirectional LSTM networks, to recognize the six activities of this dataset. They attain a high recognition performance, except for static activities: laying and standing. Ahmad et al [10] introduced a new approach based on an architecture called multi-head CNN to recognize human activities, The fundamental idea is to employ three CNNs, each supplied by three streams: overall acceleration, body acceleration, and body gyroscope. The results of these parallel CNNs are then integrated and transmitted to another LSTM layer, resulting in a high recognition accuracy. Sikder et al [11] used frequency's and power's features of raw activity signals, and they feed each stream of them to a CNN channel, the result is concatenated for classification, finally an accuracy of 95.25% is obtained on UCI HAR.

Other works have explored the effect of deepness on recognition, the authors in [12] proposed an HDL: Hierarchical Deep Learning Model capable of recognizing activities with an accuracy of 97.95 % on the UCI HAR

dataset, their model is composed of several BLSTM layers, which are used to capture information from the original data, CNN layers came afterwards to learn features from the output of the last BLSTM layer, and classification is obtained in the end using a Softmax layer. Xu et al [13] have proposed InnoHAR, a network which, takes advantage of Inception-like modules to make feature extraction, combined with GRU for sequential temporal dependencies extraction, Gao et al [14] proposed a method called DanHAR designed for challenging scenarios where there are multi-modal sensors. Their model uses a hybrid approach that fuses information using a dual-attention mechanism with CNN, which improved the ability to capture temporal and spatial patterns, resulting in a better performance while keeping the number of parameters small.

Teng et al [15] proposed a network based on convolutional neurons with a local loss after each CNN module, they compared a baseline model containing three CNN layers and one Fully Connected layer, with the same model having the first time similarity matching loss, a second time cross-entropy loss and the third time a combination between the two previous losses. Sena et al [16] divided the data into several inputs according to the type of sensor, then for each of them they built a deep CNN to extract temporal scales and features. Their method employs a DCNN, which is made up of two convolutional layers followed by a Maxpooling layer. In the end all the DCNN ensemble are merged using late fusion method. A different approach used by Bokhari et al [17], who exploited Channel State Information (CSI) to estimate and classify activities performed in an indoor environment using a deep Gated Recurrent network (DGRU).

III. MATERIALS AND METHODS

Even if the conventional HAR methods have reached good scores, their reliance on handcrafted and their need to heavy data preprocessing methods limits their scalability to other datasets. Convolutional Neural Networks, Recurrent Neural Networks, and their combinations enabled for the creation of shallow and deep models in an end-to-end technique, resulting in high recognition scores in complicated task solving.

A. Convolutional Neural Network

This architecture is based on the convolutional layer, which performs the convolution operation on the input by multiplying it by the weights of a filter and then summing it to find the value corresponding to that position. The output of this linear operation is injected into a nonlinear activation function g and can be expressed as:

$$a_{i,j} = g(\sum_{m=1}^L \sum_{n=1}^k W_{m,n} \cdot x_{i+m,j+n} + b) \quad (1)$$

Where, $x_{i+m,j+n}$ is the activation of the higher neurons linked to the neuron (i, j) , $W_{m,n}$ is a matrix with a size of $L \cdot K$ and containing the weights of the convolution filter, and b is the bias [18].

the convolutional network is a type of neural network which is mainly constituted of convolutional layer, but other layers like Maxpooling and Fully connected layers can also be present and stacked one after another to add depth and build an hierarchical network [19]. For feature extraction the convolutional layer and the Maxpooling layer can be deployed

together as a single part, whereas the second part which has the role of classifying the resulting feature vectors is dedicated to the Fully connected layer, and it typically contains a number of nodes equal to the number of classes [20].

B. Gated Recurrent Unit

Conventional Recurrent Neural Network suffers from the issue of vanishing gradient when the network cannot transmit convenient gradient information back to the input layers, making the optimization difficult and prohibiting them from learning long term dependencies [21]. Short-term memory units [22] (LSTMs) and recently gated recurrent units (GRUs) [23] are two modifications of RNN designed to solve this problem. Where LSTM have the state of the art performance, it needs more inference time and processing. In our work we studied using GRUs, which are simpler than LSTM, have fewer parameters, and give a good trade-off between speed and performance [24]. The recurrent transition of GRU are obtained by:

$$z_t = \sigma(W_z[h_{t-1}, x_t]) \tag{2}$$

$$r_t = \sigma(W_r[h_{t-1}, x_t]) \tag{3}$$

$$\hat{h}_t = \tanh(W[r_t \odot h_{t-1}, x_t]) \tag{4}$$

$$h_t = (1 - z_t) \odot h_{t-1} + z_t \odot \hat{h}_t \tag{5}$$

Where $\{W_z, W_r, W\}$ designate the recurrent weights. h_t, \hat{h}_t are hidden states. σ denotes sigmoid function. And \odot component-wise or Hadamard multiplication. z_t is the update gate and r_t is the reset gate.

The update gate z_t determines the degree of similarity between the hidden state h_t and the new hidden state \hat{h}_t and if the update is performed. The reset gate r_t is used to regulate how much of the prior state we wish to retain. if r_t , is equal to 1 it means that we keep information from the previous state, otherwise, this latter state is neglected.

C. Overview

Activity recognition is considered a classification problem, the signals extracted from motion sensors are time series data, in our approach Convolutional neural networks are used on these raw signals to avoid the requirement for feature engineering and to take advantage of local dependency and correlation between signal measurements [25]. The extraction of temporal features is the next stage. Because Simple RNN

has a vanishing gradient problem, we opted to run signals through three consecutive GRU layers. We chose GRU because of its ability to deal with extended sequences and its time efficiency [26].

D. Proposed Architecture

Our architecture is inspired by LeNet 5 [27], it benefits from its simplicity and straightforwardness, the original network uses a pair of convolutional and average pooling layers, followed by a flattening layer, two fully-connected layers and last a Softmax classifier. It was initially designed for handwriting and printed characters' recognition. We made the following change: we divided the layers into two groups: convolution layers and dense layers. We reduced the number of units in the last layer, replaced two-dimensional convolution and two-dimensional average pooling with one-dimensional convolution and one-dimensional average pooling, and finally injected what we called a GRU block in between.

Different GRU block configurations were tested and evaluated in order to select the one with the highest accuracy. TABLE I contains the configuration of each injected block.

The first GRU block contains only one layer with 100 units, then a dropout layer of 20%, this architecture has the advantage of being simple, and light, its training was fast, but unfortunately it cannot recognize well all the activities. To solve this problem, we added another layer to the first one, and we kept the number of nodes for each of them at 100 nodes, then we preserved the 20% dropout after each layer, the results showed an increase in accuracy of more than 2%. In the third architecture, we wanted to test the effect of deepness on the initial network, in fact in GRU block 3 we increased the number of nodes in the first two layers to 128 nodes, then we added a third one with 64 nodes, while using Batch Normalization instead of the dropout after each layer, the experimental results for each network (CNN + GRU bloc) is presented in TABLE II. We find that the third network has the best accuracy, it means that adding three GRU layers, gives the model the capability to better extract the sequential temporal dependencies, while batch normalization layers served better in reducing Overfitting than dropout. This improvement in accuracy is also accompanied by a reduction in the number of parameters from 455,566 to 427,950. Fig. 1 illustrates the final architecture, Fig. 2 presents the diagram of the proposed solution in this paper.

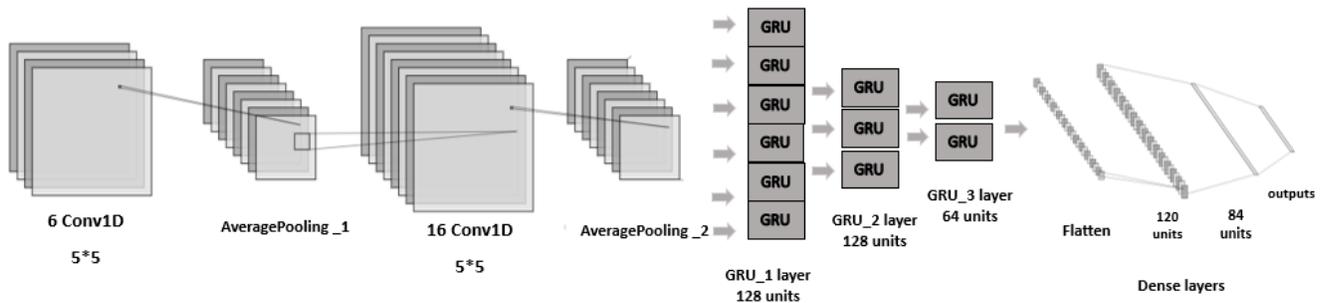


Fig. 1. The Proposed Network.

TABLE I. DEFINITION OF GRU BLOCKS

GRU block	Layers
Architecture 1	1 GRU layer (100 units) + 20% dropout.
Architecture 2	2 GRU layer (100 units) +20% dropout after each layer.
Architecture 3	2 GRU layers (128 units) +1 GRU layer (64 units) +batch Normalization after each layer.

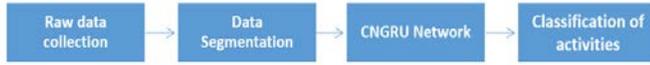


Fig. 2. Steps to Recognize Activities from Raw Data.

Several recent studies have demonstrated that a one-dimensional convolutional neural network is well suited for the analysis and extraction of discriminative features from data time series generated by sensors such as accelerometers and gyroscopes, and that it has the ability to learn an internal representation of data sequences [28]. Average pooling is often used instead of Maxpooling since it can extract features more smoothly. As mentioned earlier the 128-128-64 combination of GRU layers nodes, proved to outperform the 100-100 and 100 node combinations used in the other two architectures. We used the Adam optimizer with a learning rate fixed at 0.001, tested batch sizes of 32, 64, and 128, and finally chose 64 since it produced the best results. We trained the model for 1000 epochs and we used early stopping. TABLE III contains a definition of each layer and the parameters used in this our network.

TABLE II. TEST ACCURACY, TIME PER EPOCH, AND THE NUMBER OF PARAMETERS FOR UCI-HAR

Network	Accuracy	Time	Parameters
cnn + architecture 1	94.87 %	1s	68,866
cnn + architecture 2	96.20 %	7s	455,566
cnn+ architecture 3	96.77 %	17s	427,950

TABLE III. DEFINITION OF EACH LAYER AND THE PARAMETERS USED IN THIS OUR NETWORK

Layer	Parameters
convolution_1	Kernel=5, stride=1, filters=6, activation= tanh
average pooling_1	-
convolution_2	Kernel=5, stride=1, filters=16, activation= tanh
average pooling 2	-
gru_1	128 units + batch normalization_1
gru_2	128 units + batch normalization_2
gru_3	64 units + batch normalization_3
Flatten layer	-
dense layer_1	120 units , activation= tanh
dense layer_2	84 units, activation = tanh
dense layer_3	6 units, activation = softmax

IV. RESULTS AND DISCUSSION

A. Evaluation Methodology

We ran tests on three publicly available datasets. Here is a short description of each one:

UCI HAR [29]: This dataset was gathered by 30 users aged 19-48 who wore smartphones around their waists while performing a series of activities. The information gathered is classified into five activity classes, three of which are static activities (standing, sitting, and lying) and the others are dynamic (walking, going upstairs, and going downstairs). The accelerometer and gyroscope embedded in the phone (Samsung Galaxy SII) enabled the measurement of three-axial linear acceleration as well as three-axial angular velocity.

WISDM V1.1 [6]: is a dataset collected by using only one IMU (accelerometer), the chosen activities were selected carefully, depending on their performance regularity in daily life. Those activities are Walking, Jogging, Upstairs, Downstairs, Sitting, Standing. This dataset has approximately the same activities as UCI, Fig. 3 contains a description of its activities.

SKODA [30]: this dataset has been recorded using only one type of IMU, in a manufacturing scenario and covers the problem of recognizing the activities of assembly-line workers in a car production environment. A worker carried a number of sensors while performing manual quality checks for the correct assembly of parts in newly built cars. 10 resulting hand movements are considered. TABLE IV contains various recording information about all the datasets used in this work.

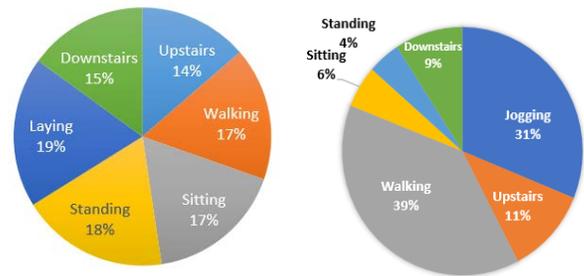


Fig. 3. Activity Description of UCI in the Left and WISDM v1.1 in the Right.

TABLE IV. DEFINITION OF THE CHARACTERISTICS OF THE DATASETS

dataset	activities	subject	place	sampling rate	samples
WISDM	6	36	thigh	20 hz	1.098.207
UCI HAR	6	30	waist	50 hz	10.298
SKODA	10	1	arms	98 hz	~701.440

B. Performance Measure

When we were evaluating our model, we noticed the lack of an evaluation standard. Various evaluation metrics are used to measure and compare the human activity recognition performance. The main ones are accuracy, recall, F-measure, Area under the Curve (AUC). Where some works use F-measure, other authors prefer accuracy. This diversity tends to make finding the state of the art model difficult. The diversity

of validation protocol should also be taken into consideration when dividing data into training/test/validation since it impacts the recognition results and comparison. The parameters we used to compare the model's performance are defined as follows:

$$Accuracy = \frac{TP+TN}{TP+TN+FP+FN} \quad (6)$$

$$Precision = \frac{TP}{TP+FP} \quad (7)$$

$$Recall = \frac{TP}{TP+FN} \quad (8)$$

$$F - Measure = 2 \times \frac{Precision \times Recall}{Precision+Recall} \quad (9)$$

(Where, T: True, P: Positives, F: False, N: Negatives). We use also Confusion Matrix, to have a summarized view about the performance of the classification, and to see the errors being made its type, and where the confusion occurs.

C. Results

We ran several tests on two other datasets to evaluate the performance and validate the efficiency of the proposed method. We used WISDM V1.1 and SKODA, the first one contains activities similar to UCI, while the second one contains a different type of gesture. We present the detailed results for UCI which was exploited in the design and tuning of our model, then we compare the results obtained with WISDM V1.1 at the level of each activity, and last we evaluate our approach on SKODA.

UCI HAR's signals were pre-processed by filtering noise then sampling in a fixed-width sliding windows of 2.56 sec and 50% overlap, again we chose to take 21 subjects for training and 9 for testing. We fed our network with data in a specific shape. Accuracy and loss over each epoch are used for evaluation. We trained the model through 1000 epochs, then we used early stopping technique to end training when the validation accuracy stops increasing. All the datasets were uploaded to Google drive, and we used for the experiment Google Colaboratory. Our model achieved an accuracy of 96.77 %. As shown in TABLE V, this value is comparable to the state of the art, and other works that use handcrafted features, classical machine learning algorithms, unsupervised machine learning algorithms or models composed of a combination of previous methods.

To show the correspondence between the predicted labels and the true ones, we used the confusion matrix illustrated in Fig. 4. It shows that we achieve good recognition for all activities. We see that the static action LAYING is easily identified, with an accuracy of 100% and it's unconfused with any other activity. The dynamic activities WALKING_UP and WALKING are also well recognized, but for STANDING and SITTING their accuracies are relatively smaller and consequently the total score of the model is reduced, furthermore we remark that they are often confused with each other's, this could be explained by the similarity of the signals of those two classes.

The second experiment was on WISDM V1.1 using raw data again, this time we evaluated our results, using K-fold cross-validation, to allow for a reasonable comparison with

preceding works. The model can predict all activities with great accuracy. The overall accuracy is (98.21%), this result is close to previous works on the same dataset done by Alsheikh et al [39] with a hybrid model using deep learning and hidden Markov models DL-HMM (98.23%). It improves accuracy over ensemble learning method [40], and slightly above the model proposed by Ravi et al [41] on the basis of shallow CNN architecture.

TABLE V. COMPARISON WITH OTHER WORKS ON UCI-HAR

Approach	Accuracy (%)
Ensemble method of HMM[31]	83.51
Two stage continuous HMM[32]	91.76
Hierarchical continuous HMM[33]	93.18
Our model	96.776
Multichannel Dilated CNN[34]	95.49
Deep Res Bidir-LSTM [35]	93.6
Handcrafted features +SVM [36]	89
FFT+1D-CNN[37]	95.75
1D CNN [37]	94.79
Stacked auto encoder +SVM [38]	92.16

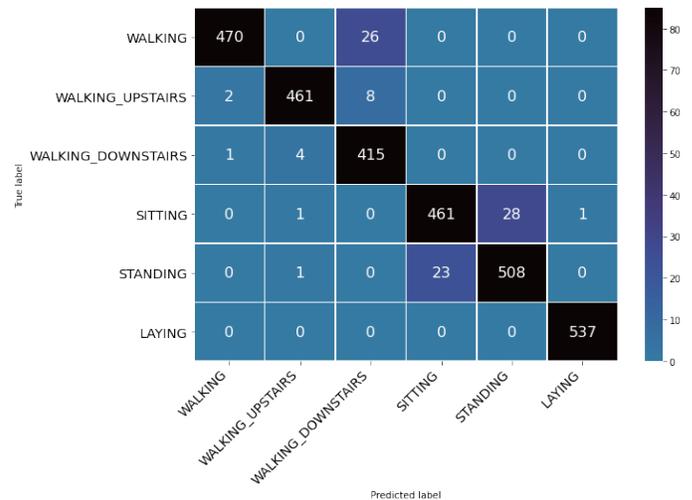


Fig. 4. Confusion Matrix for UCI HAR.

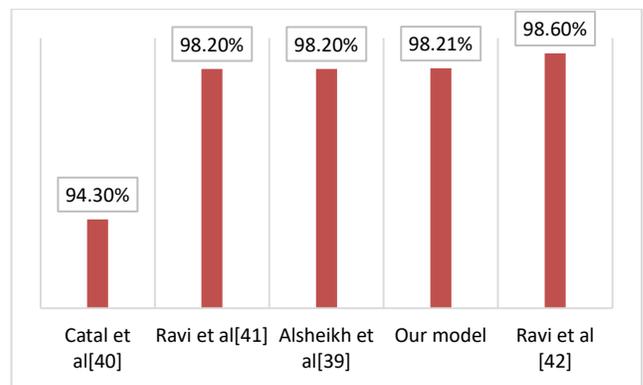


Fig. 5. Comparison between Accuracies of Previous Works on WISDM v1.1.

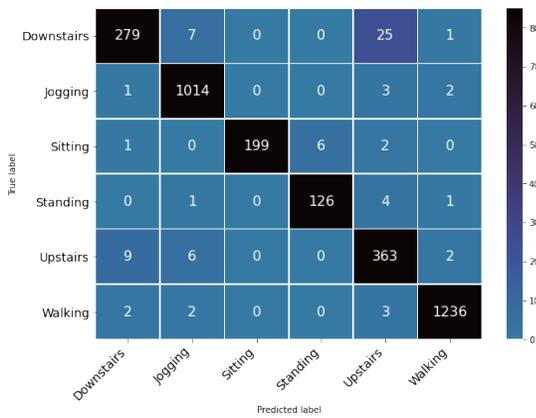


Fig. 6. Confusion Matrix for WISDM V1.1.

Fig. 5 contains a comparison with works on the same dataset. We mention that all results reported in this table are evaluated using 10-fold the cross-validation technique.

The confusion Matrix of WISDM V1.1 dataset is presented in Fig. 6 we can see that Walking and Sitting achieved a recognition close to 100%. We also note that the relative lack of sample for the two Sitting and Standing classes did not affect their recognition, which means that the change in orientation of the sensor on the thigh is easily detectable and learned, helping in result to better identify each class. Jogging is an activity that requires the movement of the whole body from point A to point B, is well identified. Where Walking Upstairs and Downstairs are often confused with each other, this indicates that the model has difficulty distinguishing between these types of movements.

In this part we will compare the ability of our model to detect each activity belonging to UCI HAR and WISDM V1.1, and compare it to other models. We chose these activities because they are the most regularly performed in daily life, and they are recorded differently in both datasets. This comparison should help us to understand the relevance of our approach.

UCI HAR and WISDM V1.1, datasets both contain 6 activities, 5 are the same, and two are different (jogging and laying). Dividing activities into two categories: static and dynamic, can lead to understand the behavior of the model. We will compare and evaluate each activity according to its F1 score, since we have an imbalance between classes.

We observe that the static activities sitting standing and laying, are differentiable by the model among the others even if we change the dataset, this indicates its aptitude to detect those movements despite using only an accelerometer instead of its combination with a gyroscope. We deduct also that the location of sensors does not affect the detection of those activities. the other remaining activities "walking downstairs", "Jogging", "walking Upstairs", and "Walking" are dynamic and they present the vast majority of the data in WISDM V1.1, and almost half of UCI HAR dataset. Jogging and Walking are well identified 99% of the time in WISDM V1.1, and 96% in UCI HAR (Walking). The lowest score achieved is 93% in WISDM V1.1, it indicates that the model does not manage to detect with ease the Downstairs class.

TABLE VI. PER ACTIVITY COMPARISON

Activity	F1 score					
	WISDM V1.1			UCI HAR		
	Our method	Ravi et al [42]	Ronao et al [37]	Lin et al [34]	Zhao et al [35]	Our method
Downstairs	92.99	95.14	99.49	97.16	93.7	95.37
Jogging	99	99.50	-	-	-	-
Sitting	98.50	98.14	87.68	91.14	89.15	94.50
Standing	98.50	97.64	91.37	93.47	90.87	95
Upstairs	94.50	95.30	99.50	96.65	93.96	98.50
Walking	99	99.30	99.44	95.09	94.53	96.96
Laying	-	-	90.55	99.26	99.75	1

Considering the number of sensors, we remark that the use of a single accelerometer alone did not provide the necessary information to identify the dynamic actions which are related to climbing or descending, specifically moving downstairs or upstairs because they obtain the lowest score among classes and even for the other works presented in TABLE VI. On the other hand, we note that the recording in UCI HAR realized with both a gyroscope and an accelerometer allowed a good detection despite the small number of samples, as indicated in TABLE IV.

In WISDM V1.1 dataset the most recognized classes are jogging and walking, followed by walking upstairs in UCI HAR dataset, and the lowest score is for walking downstairs which reaches 93%.

Comparing our results with other approaches, we see that our network can classify activities in a similar way or better than other works using feature engineering, like the spectrogram domain of the time series signal, or hierarchical continuous hidden Markov model or using complex end to end deep learning networks.

In this part we want to test our model on a dataset that does not contain the same characteristics of the two previous ones. As previously mentioned Skoda contains gestures made with the hand in an assembly environment. Performed by a single subject and one type of sensors, it contains 10 gesture classes, to evaluate our work and compare it with others we used the 10-fold cross-validation process. The accuracy of our network is 96%. Fig. 7 shows that it outperforms other works previously done on the same dataset. The classification results are shown in Fig. 8 as a form of a confusion matrix. In this matrix we visualize that the model recognizes all the activities with a high score, except for the activity "close both left Front door" which is confused with "opening left front door" and "closing left front door". We see also that the NULL class causes the largest confusion.

Class names: 0:'Null Class',1:'Write on Notepad',2:'Open Hood', 3:'Close Hood', 4:'Check Gaps on the Front Door', 5:'Open Left Front Door',6:'Close Left Front Door',7:'Close Both Left Front Door',8:'Check Trunk Gaps',9:'Open and Close Trunk', 10:'Check Steering Wheel'.

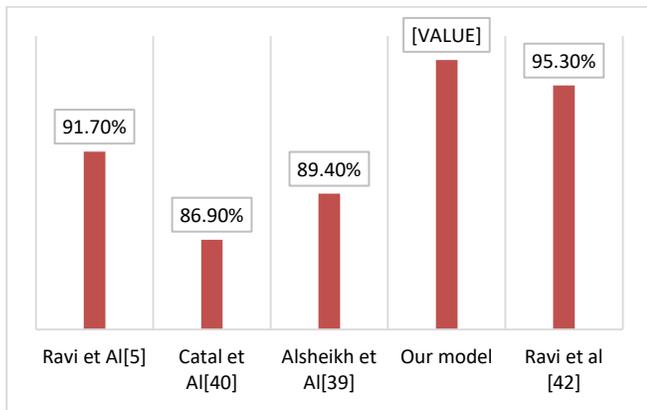


Fig. 7. Comparison between Accuracies of other Works on Skoda.

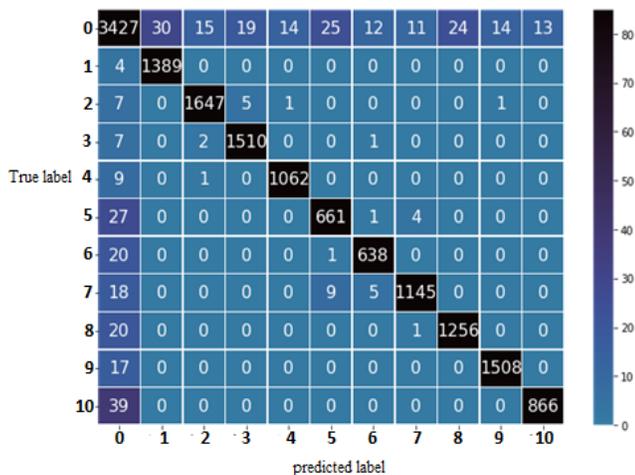


Fig. 8. Confusion Matrix for Skoda.

V. CONCLUSION

In this paper we aimed to integrate Internet of Things (IoT) technology and deep learning to recognize human activities. We presented CNGRU, a new structure that combines convolution layers with GRU. This architecture is able to learn features automatically from raw data, unlike previous works based on handcrafted features. The effectiveness of this architecture is proved by experimenting on three datasets containing a variety of activity classes and recorded using different sensors. We achieved 96.77% on UCI-HAR, 98.21% on WISDM V1.1, and 96.70% on SKODA. This final result is superior than or close to existing state-of-the-art approaches that use shallow or deep designs or classical methods.

Future works will investigate a resource efficient implementation of this network for IoT devices, and explore other datasets that contains more complex activities.

REFERENCES

[1] S.-R. Ke, H. L. U. Thuc, Y.-J. Lee, J.-N. Hwang, J.-H. Yoo, and K.-H. Choi, "A Review on Video-Based Human Activity Recognition," *Computers*, vol. 2, no. 2, Art. no. 2, Jun. 2013, doi: 10.3390/computers2020088.

[2] H. D. Mehr, H. Polat, and A. Cetin, "Resident activity recognition in smart homes by using artificial neural networks," in 2016 4th International Istanbul Smart Grid Congress and Fair (ICSG), Istanbul, Turkey, Apr. 2016, pp. 1–5. doi: 10.1109/SGCF.2016.7492428.

[3] G. Sebestyen, I. Stoica, and A. Hangan, "Human activity recognition and monitoring for elderly people," in 2016 IEEE 12th International Conference on Intelligent Computer Communication and Processing (ICCP), Sep. 2016, pp. 341–347. doi: 10.1109/ICCP.2016.7737171.

[4] S. Ranasinghe, F. Al Machot, and H. C. Mayr, "A review on applications of activity recognition systems with regard to performance and evaluation," *Int. J. Distrib. Sens. Netw.*, vol. 12, no. 8, p. 1550147716665520, Aug. 2016, doi: 10.1177/1550147716665520.

[5] D. Roggen et al., "Collecting complex activity datasets in highly rich networked sensor environments," in 2010 Seventh International Conference on Networked Sensing Systems (INSS), Jun. 2010, pp. 233–240. doi: 10.1109/INSS.2010.5573462.

[6] J. R. Kwapisz, G. M. Weiss, and S. A. Moore, "Activity recognition using cell phone accelerometers," *ACM SIGKDD Explor. Newsl.*, vol. 12, no. 2, pp. 74–82, Mar. 2011, doi: 10.1145/1964897.1964918.

[7] A. Reiss and D. Stricker, "Introducing a New Benchmarked Dataset for Activity Monitoring," Jun. 2012, pp. 108–109. doi: 10.1109/ISWC.2012.13.

[8] S. Deep and X. Zheng, "Hybrid Model Featuring CNN and LSTM Architecture for Human Activity Recognition on Smartphone Sensor Data," in 2019 20th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), Dec. 2019, pp. 259–264. doi: 10.1109/PDCAT46702.2019.00055.

[9] F. Hernández, L. F. Suárez, J. Villamizar, and M. Altuve, "Human Activity Recognition on Smartphones Using a Bidirectional LSTM Network," in 2019 XXII Symposium on Image, Signal Processing and Artificial Vision (STSIVA), Apr. 2019, pp. 1–5. doi: 10.1109/STSIVA.2019.8730249.

[10] W. Ahmad, B. M. Kazmi, and H. Ali, "Human Activity Recognition using Multi-Head CNN followed by LSTM," in 2019 15th International Conference on Emerging Technologies (ICET), Peshawar, Pakistan, Dec. 2019, pp. 1–6. doi: 10.1109/ICET48972.2019.8994412.

[11] N. Sikder, M. S. Chowdhury, A. S. M. Arif, and A. Nahid, "Human Activity Recognition Using Multichannel Convolutional Neural Network," in 2019 5th International Conference on Advances in Electrical Engineering (ICAEE), Sep. 2019, pp. 560–565. doi: 10.1109/ICAEE48663.2019.8975649.

[12] T. Su, H. Sun, C. Ma, L. Jiang, and T. Xu, "HDL: Hierarchical Deep Learning Model based Human Activity Recognition using Smartphone Sensors," in 2019 International Joint Conference on Neural Networks (IJCNN), Jul. 2019, pp. 1–8. doi: 10.1109/IJCNN.2019.8851889.

[13] C. Xu, D. Chai, J. He, X. Zhang, and S. Duan, "InnoHAR: A Deep Neural Network for Complex Human Activity Recognition," *IEEE Access*, vol. 7, pp. 9893–9902, 2019, doi: 10.1109/ACCESS.2018.2890675.

[14] W. Gao, L. Zhang, Q. Teng, J. He, and H. Wu, "DanHAR: Dual Attention Network for multimodal human activity recognition using wearable sensors," *Appl. Soft Comput.*, vol. 111, p. 107728, Nov. 2021, doi: 10.1016/j.asoc.2021.107728.

[15] Q. Teng, K. Wang, L. Zhang, and J. He, "The Layer-Wise Training Convolutional Neural Networks Using Local Loss for Sensor-Based Human Activity Recognition," *IEEE Sens. J.*, vol. 20, no. 13, pp. 7265–7274, Jul. 2020, doi: 10.1109/JSEN.2020.2978772.

[16] J. Sena, J. Barreto, C. Caetano, G. Cramer, and W. R. Schwartz, "Human activity recognition based on smartphone and wearable sensors using multiscale DCNN ensemble," *Neurocomputing*, vol. 444, pp. 226–243, Jul. 2021, doi: 10.1016/j.neucom.2020.04.151.

[17] S. M. Bokhari, S. Sohaib, A. R. Khan, M. Shafi, and A. ur R. Khan, "DGRU based human activity recognition using channel state information," *Measurement*, vol. 167, p. 108245, Jan. 2021, doi: 10.1016/j.measurement.2020.108245.

[18] J. Gu et al., "Recent advances in convolutional neural networks," *Pattern Recognit.*, vol. 77, pp. 354–377, May 2018, doi: 10.1016/j.patcog.2017.10.013.

[19] K. O'Shea and R. Nash, "An Introduction to Convolutional Neural Networks," *ArXiv151108458 Cs*, Dec. 2015.

[20] Y. Chen, H. Jiang, C. Li, X. Jia, and P. Ghamisi, "Deep Feature Extraction and Classification of Hyperspectral Images Based on Convolutional Neural Networks," *IEEE Trans. Geosci. Remote Sens.*,

- vol. 54, no. 10, pp. 6232–6251, Oct. 2016, doi: 10.1109/TGRS.2016.2584107.
- [21] T. Mikolov, A. Joulin, S. Chopra, M. Mathieu, and M. Ranzato, “Learning Longer Memory in Recurrent Neural Networks,” ArXiv14127753 Cs, Apr. 2015.
- [22] S. Hochreiter and J. Schmidhuber, “Long Short-Term Memory,” *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997, doi: 10.1162/neco.1997.9.8.1735.
- [23] K. Cho et al., “Learning Phrase Representations using RNN Encoder–Decoder for Statistical Machine Translation,” in *Proceedings of the 2014 Conference on Empirical Methods in Natural Language Processing (EMNLP)*, Doha, Qatar, Oct. 2014, pp. 1724–1734. doi: 10.3115/v1/D14-1179.
- [24] S. Khandelwal, B. Lecouteux, and L. Besacier, “COMPARING GRU AND LSTM FOR AUTOMATIC SPEECH RECOGNITION,” LIG, Research Report, Jan. 2016. [Online]. Available: <https://hal.archives-ouvertes.fr/hal-01633254>.
- [25] N. Y. Hammerla, S. Halloran, and T. Plötz, “Deep, convolutional, and recurrent models for human activity recognition using wearables,” in *Proceedings of the Twenty-Fifth International Joint Conference on Artificial Intelligence*, New York, New York, USA, Jul. 2016, pp. 1533–1540.
- [26] J. Chung, C. Gulcehre, K. Cho, and Y. Bengio, “Empirical evaluation of gated recurrent neural networks on sequence modeling,” *NIPS 2014 Workshop Deep Learn.* Dec. 2014, 2014.
- [27] Y. Lecun, L. Bottou, Y. Bengio, and P. Haffner, “Gradient-based learning applied to document recognition,” *Proc. IEEE*, vol. 86, no. 11, pp. 2278–2324, Nov. 1998, doi: 10.1109/5.726791.
- [28] J. Brownlee, “1D Convolutional Neural Network Models for Human Activity Recognition,” *Machine Learning Mastery*, Sep. 20, 2018. <https://machinelearningmastery.com/cnn-models-for-human-activity-recognition-time-series-classification/>.
- [29] D. Anguita, A. Ghio, L. Oneto, X. Parra, and J. L. Reyes-Ortiz, “A Public Domain Dataset for Human Activity Recognition using Smartphones,” presented at the 21th European Symposium on Artificial Neural Networks, Computational Intelligence and Machine Learning, Bruges, Belgium, Apr. 2013.
- [30] P. Zappi et al., “Activity Recognition from On-Body Sensors: Accuracy-Power Trade-Off by Dynamic Sensor Selection,” in *Wireless Sensor Networks*, Berlin, Heidelberg, 2008, pp. 17–33. doi: 10.1007/978-3-540-77690-1_2.
- [31] Y.-J. Kim, B. Kang, and D. Kim, “Hidden Markov Model Ensemble for Activity Recognition Using Tri-Axis Accelerometer,” *2015 IEEE Int. Conf. Syst. Man Cybern.*, 2015, doi: 10.1109/SMC.2015.528.
- [32] C. A. Ronao and S. B. Cho, “Human activity recognition using smartphone sensors with two-stage continuous hidden markov models: 2014 10th International Conference on Natural Computation, ICNC 2014,” *2014 10th Int. Conf. Nat. Comput. ICNC 2014*, pp. 681–686, 2014, doi: 10.1109/ICNC.2014.6975918.
- [33] C. A. Ronao and S.-B. Cho, “Recognizing human activities from smartphone sensors using hierarchical continuous hidden Markov models,” *Int. J. Distrib. Sens. Netw.*, vol. 13, no. 1, p. 1550147716683687, Jan. 2017, doi: 10.1177/1550147716683687.
- [34] Y. Lin and J. Wu, “A Novel Multichannel Dilated Convolution Neural Network for Human Activity Recognition,” *Math. Probl. Eng.*, vol. 2020, p. e5426532, Jul. 2020, doi: 10.1155/2020/5426532.
- [35] Y. Zhao, R. Yang, G. Chevalier, X. Xu, and Z. Zhang, “Deep Residual Bidir-LSTM for Human Activity Recognition Using Wearable Sensors,” *Math. Probl. Eng.*, vol. 2018, p. e7316954, Dec. 2018, doi: 10.1155/2018/7316954.
- [36] D. Anguita, A. Ghio, L. Oneto, X. Parra, and J. L. Reyes-Ortiz, “Human Activity Recognition on Smartphones Using a Multiclass Hardware-Friendly Support Vector Machine,” in *Ambient Assisted Living and Home Care*, Berlin, Heidelberg, 2012, pp. 216–223. doi: 10.1007/978-3-642-35395-6_30.
- [37] C. A. Ronao and S.-B. Cho, “Human activity recognition with smartphone sensors using deep learning neural networks,” *Expert Syst. Appl.*, vol. 59, pp. 235–244, Oct. 2016, doi: 10.1016/j.eswa.2016.04.032.
- [38] Y. Li, D. Shi, B. Ding, and D. Liu, “Unsupervised Feature Learning for Human Activity Recognition Using Smartphone Sensors,” in *Mining Intelligence and Knowledge Exploration*, Cham, 2014, pp. 99–107.
- [39] M. A. Alsheikh, A. Selim, D. Niyato, L. Doyle, S. Lin, and H.-P. Tan, “Deep Activity Recognition Models with Triaxial Accelerometers,” ArXiv151104664 Cs, Oct. 2016, [Online]. Available: <http://arxiv.org/abs/1511.04664>.
- [40] C. Catal, S. Tufekci, E. Pirit, and G. Kocabag, “On the use of ensemble of classifiers for accelerometer-based activity recognition,” *Appl. Soft Comput.*, vol. 37, pp. 1018–1022, Dec. 2015, doi: 10.1016/j.asoc.2015.01.025.
- [41] D. Ravi, C. Wong, B. Lo, and G.-Z. Yang, “Deep learning for human activity recognition: A resource efficient implementation on low-power devices,” in *2016 IEEE 13th International Conference on Wearable and Implantable Body Sensor Networks (BSN)*, Jun. 2016, pp. 71–76. doi: 10.1109/BSN.2016.7516235.
- [42] D. Ravi, C. Wong, B. Lo, and G.-Z. Yang, “A Deep Learning Approach to on-Node Sensor Data Analytics for Mobile or Wearable Devices,” *IEEE J. Biomed. Health Inform.*, vol. 21, no. 1, pp. 56–64, Jan. 2017, doi: 10.1109/JBHI.2016.2633287.

Bioinformatics Research Through Image Processing of Histopathological Response to Stonefish Venom

Mohammad Wahsha^{1*}

Marine Science Station, The University of Jordan
Aqaba Branch, Jordan

Heider A. M. Wahsheh²

Department of Information Systems
College of Computer Sciences and Information Technology
King Faisal University, Al-Ahsa, Saudi Arabia

Wissam Hayek³, Maroof Khalaf⁵, Tariq Al-Najjar⁶

Faculty of Basic and Marine Sciences
The University of Jordan, Aqaba Branch, Jordan

Haya Al-Tarawneh⁴

Control Health Division
Aqaba Special Economic Zone Authority
Aqaba, Jordan

Abstract—The present study utilizes coastal and environmental engineering to investigate the histopathological effects of *Synanceia verrucosa* venom on Albino BALB/c mice. *S. verrucosa* is the most hazardous venomous marine fish that belong to the family Synanceiidae, generally known as the "Reef Stonefish". Crude venom was collected from venom glands of the dorsal spines of stonefish samples taken from the Jordanian coastline of the Gulf of Aqaba, Red Sea. The mice were given intramuscular injections of the venom. Consequently, the research evaluated the acute toxicity and influence on selected serum biomarker enzymes, as well as possible histological alterations of the soleus skeletal muscles. The mice 24 h LD₅₀ was 0.107 µg toxin/kg mouse body weight. After the treatment using venom sublethal dose, the serum biomarkers, including Lactate dehydrogenase (LDH) and Alanine aminotransferase (ALT), were significantly improved ($P \leq 0.05$). In addition, Lipid Peroxidation (LPO) contents were significantly increased ($P \leq 0.05$) after venom treatment. Moreover, we combined routine medical procedures and artificial intelligence-assisted image analysis for a rapid qualitative and quantitative diagnosis of stonefish injury, based on the histophotography of mice tissue samples during the observation period (1, 2, and 3 hours respectively). The novelty of our method is that we could detect severe and mild damage with an accuracy of 93% and 91%, respectively. The most histological abnormalities in muscles were the great variety in diameters, content, and widespread among randomly distributed muscle fibres. In addition, loss of the tissue's striated appearance was noticed in toxin-treated groups compared with the control group. Consequently, our findings indicate the Stonefish's harmful influences that may endanger human life and highlight the need for appropriate measures to be considered. This, in turn, can ensure beach safety in the Gulf of Aqaba.

Keywords—*Synanceia verrucosa*; Gulf of Aqaba; artificial intelligence; marine biotoxins

I. INTRODUCTION

Injuries by stingrays from dangerous marine organisms are common in coastal and lakesides regions worldwide [1]. These injuries can threaten life and affect body organs and systems [2]. According to several reports, there is a potential for more severe injuries, particularly with stonefish and

stingray envenomation [3]. Stonefish belong to the genus *Synanceia*, considered one of the most venomous fish in the world. It can be found in tropical waters (Pacific Ocean, Indian Ocean, and the Red Sea) [3, 4]. The stonefish defense system comprises 17 spines covered with thick skin supported by venom glands [5, 6]. It is found in the shallow water near the bottom [7]. Using its pectoral fins, Stonefish can rapidly dredge in the mud or the seabed sand in which it settles down and lays motionless [8]. It has a solid ability to camouflage and blend in so perfectly with its surroundings, enhancing its hiding ability [6, 7]. Their ability to hide under the sand or between coral makes them challenging to detect and avoid, which increases the chances of injury by their stings [4]. [9] reported two cases of injuries from Stonefish in the north of Australia; one of these cases occurred with a 16 years old girl who presented hysterical screaming from pain severity. She impaled her big toe on the spine of a fish in the water. There was a puncture wound on the tip of the toe. The whole toe was cyanosed and swollen. Large doses of pethidine failed to control her pain. A ring block was inserted in the toe, and the Stonefish antivenom was administered with good effect. She was discharged the next day and did not suffer a sequel.

In general, injuries from the venom of the stonefish sting diversify considerably. It can vary from intense pain, which may persist for several hours or even days, redness and swelling in the sting site followed by shock, pulmonary edema, hypotension, bradycardia, arrhythmia, cardiovascular collapse, muscles weakness, paralysis, convulsions, to occasional death in severe cases [5, 10]. Damage to cells can occur as a result of stresses such as toxins and venoms [8]. Most observable cellular changes and cell deaths occur due to biochemical changes within the cell [11]. Releasing the intracellular enzymes has been a marker of cell damage in various injury cases [12]. Increasing ALT activity level has been associated with organ toxicities [13]. LDH is a cytoplasmic enzyme that catalyzes lactate oxidation into pyruvate and reverses, predominantly in muscle tissues [11]. Histology is also crucial in pathology; it characterizes changes or disease phenotypes and diagnoses their causes [14]. Limited studies estimate the effect of piscine venoms on muscle. For example, [15] study the impact of *Scatophagus*

Argus (family: Scatophagidae) venom on gastrocnemius muscle, were the venom-induced significant local tissue damage characterized by pain, edema, and necrosis and induced a rapid increment in serum creatine kinase and lactate dehydrogenase (LDH) showing the myotoxicity of venom.

Therefore, in this study, we aimed to evaluate the toxicity of stonefish venom on mice muscles using biochemical, histological, and image processing analysis.

II. MATERIAL AND METHODS

A. Chemicals and Fish Sample

All chemicals and reagents were of analytical grade and purchased from Sigma–Aldrich unless otherwise indicated. At least ten stonefish samples were collected by SCUBA diving from the northern side of the Gulf of Aqaba. Collected fish were identified as *Synanceia verrucosa* based on [7]. Fish were kept alive under the control condition in an oxygenated seawater aquarium at the Aquaculture unit of the Marine Science Station (MSS) located along the Jordanian Gulf of Aqaba.

B. Experimental Animal

Male Balb *c*/mice 6-7 weeks old (average body weight 25gm) were used. Mice were obtained from the animal house at Yarmouk University located on the northern side of Jordan. They were maintained on a standard laboratory diet and tap water during the experiment period. The sampling activities on animals (fish and mice) were conducted after taking the required permissions from relevant public authorities and agreeing with the animal care and use legislations at the MSS.

C. Isolation of Fish Crude Venom

Crude venom was collected by inserting the rubber caps of test tubes into the dorsal spine of the sampled fish, considering reaching a suitable distance in the spine to extrude the required high viscous venom. A volume of 0.3-0.4 ml of venom was dissolved in 1ml phosphate buffer saline to get milky diluted venom. The concentration of the venom was calculated using the Bradford method as recommended by [4]. The extracted soluble crude venom was immediately stored in a dark container at -20 °C for further biochemical and histological analysis. The concentration of the extracted venom was determined following [8].

D. LD₅₀ Determination

A modified up and down method was used to evaluate the intramuscular injection (i.m) LD₅₀ value of the extracted venom using Balb/*c* mice in laboratory conditions [4]. A stock solution of crude stonefish venom was diluted several times (up to 30 times V/V). The experiment was set into triplicate groups of healthy mice (n=3). Mice were observed for 24h and symptoms of toxicity such as modifications for regular activities and the death time of injected mice were recorded.

E. Mice Bioassay and Experimental Model

Sixty male Balb/*c* mice were divided into two main groups: The first group (C) was the control group, intramuscular injected (i.m) with phosphate buffer saline

without venom administration (15 mice). The second group (T) was the toxin-treated groups (45 mice); mice were administered by intramuscular injection (i.m) with 107 µg stonefish venom/kg mouse body weight (according to LD₅₀ value) and divided into three sub-groups: (a) Fifteen mice were killed after 1hr (T1). (b) Fifteen mice were killed after 2hrs. (T2) and (c) Fifteen mice were killed after 3hrs. (T3).

Blood samples were collected into a vial without anticoagulant from each mouse via cardiac puncture. The serum was separated by centrifugation at 3000X g for 30 min and kept at -4°C for the enzyme activity assays. The levels of serum lactate dehydrogenase (LDH) and Alanine aminotransferase (ALT) were measured at Sukaina Specialized Medical Labs in Amman, Jordan, using Sigma-Aldrich activity assay kits.

Moreover, soleus muscles were removed immediately after decapitation. They were divided into two groups: The first group was perfused with normal saline containing heparin and homogenized with phosphate buffer saline (pH 7.2). The perfused samples were kept in dark plastic bottles and stored at -20°C for the LPO assay. The lipid peroxidation levels of the skeletal tissues were analyzed based on [16]. The second group was served for the microscope study and analysis. Small pieces of the heart were treated with formalin for fixation from all groups. Heart portions were dehydrated and embedded according to the procedures described by [17]. Tissue sections (7µm) were stained using Hematoxylin and Eosin (H&E) and analyzed under the light microscope, according to [17, 18].

F. Histopathological Image Analysis using Image-Processing Techniques

Consequently, our obtained digitized sections of muscle tissue histopathology were amenable to the application of computerized image analysis and machine learning techniques. Besides, Artificial intelligence for image analysis has been utilized to distinguish possible muscle tissue injury after exposure to stonefish venom.

The model framework was designed on the assumption that its outputs were based on the following indices:

- Collect dataset of histopathological and benign images.
- Extract Features.
- Evaluate the artificial intelligence model using prediction quality metrics.

At least one hundred histological photographs have been used to build the model dataset; since then, this dataset has been computerized based on three-class labels; Mild, Moderate, and Severe. Artificial intelligence applies an image filter to extract image features such as corners, edges, colors, histograms, regions of interest points, and ridges [19]. Furthermore, the Support Vector Machine (SVM) algorithm was applied to build a model that analyses our histophotograph and classifies them into the three main classes (Mild, Moderate, and Severe). Prediction quality metrics were also applied to evaluate the performance of the SVM model,

which includes: True Positive (TP), True Negative (TN), False Positive (FP), False Negative (FN), Precision, Recall, and F-Measure (F-M) [20, 21]. The following formulas present the main metrics:

$$Accuracy_i = \frac{TP + TN}{TP + FP + TN + FN} \quad (1)$$

$$Recall_i = \frac{TP}{TP + FN} \quad (2)$$

$$Precision_i = \frac{TP}{TP + FP} \quad (3)$$

$$F - measure = \frac{2TP}{2TP + FP + FN} \quad (4)$$

G. Statistical Analysis

Statistical analysis was based on ANOVA and is presented as means \pm S.D. Statistical significance was considered at a p-value of 0.05 or less. The data were analyzed statistically using Sigma Stat statistical software version 3.5.

III. RESULTS

The stonefish crude venom concentration was calculated using the standard curve to be 4.47 $\mu\text{g}/\text{ml}$. The approximate LD_{50} of the extracted toxin was 107 μg venom/kg mouse body weight. The behavior of the venomous treated mice could be clearly distinguished by losing their energetic activity, nausea and vomiting, diarrhea, vertigo, fainting, convulsions, and spastic paralysis in the late stage.

A. Effect of the Stonefish Venom on the Enzymatic Profile

The changes in serum biochemical markers LDH and ALT levels are presented in Fig. 1 and 2, respectively. In treated mice with the venom, the serum LDH and ALT levels showed significant ($P \leq 0.05$) increased after 1 hour of venom administration and continued to rise until three hours. Moreover, it was notable that the effect of stonefish venom on mice's skeletal muscles was time-dependent. As shown in Fig. 1: the treated groups produced nearly one-fold after 1 hour, 12 and 21-fold after 2 and 3 hours after venom exposure, respectively.

Fig. 1 presents the LDH activity in mice muscle tissue. C: Control group, T1: Toxin group after 1hr, T2: Toxin group after 2hrs and T3: Toxin group after 3hrs, for mice tissues from muscle. Presented data are mean values (units per liter) for each group of mice \pm S.D.

Correspondingly, the mice muscles that received stonefish venom revealed an increase in ALT value by a fold of almost 9 in the case of T1 and T2 when compared to the control group (Fig. 2). A further increase was shown as 13-fold in toxin group T3 compared with the controls ($P \leq 0.05$).

Fig. 1 presents the trend of change in ALT activity in tissues of mice muscle. C: Control, T1: Toxin group after 1hr, T2: Toxin group after 2hrs and T3: Toxin group after 3hrs.

Presented data are mean values (units per liter) for each group of mice \pm S.D.

On the other hand, Malondialdehyde (MDA) produced oxidative damage to lipids. MDA concentration in tissue homogenate is mainly used as a biomarker for tissue damage. Control mice (group C) exhibited normal lipid peroxidation (MDA) levels, 7.3 $\mu\text{M}/\text{g}$ in muscles homogenate. However, after that venom administration, a dramatic irregular trend of MDA production was observed due to rapid and severe tissue damage (Fig. 3).

Fig. 3 shows the trend of change in MDA mean concentration (μMg^{-1}) for mice muscles. C: Control mice group, T1: Toxin group after 1hr, T2: Toxin group after 2hrs and T3: Toxin group after 3hrs, presented value are mean value \pm S.D. (n= 7).

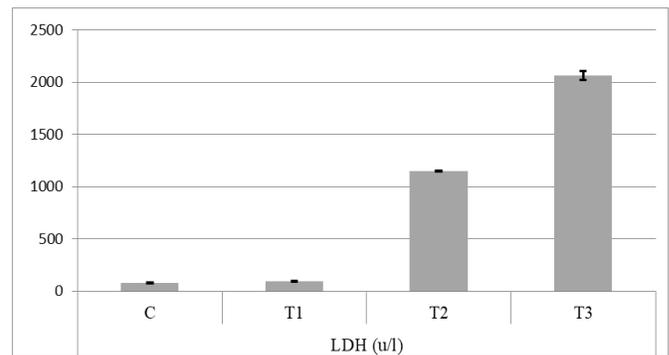


Fig. 1. The Treated Groups after Venom Exposure, respectively.

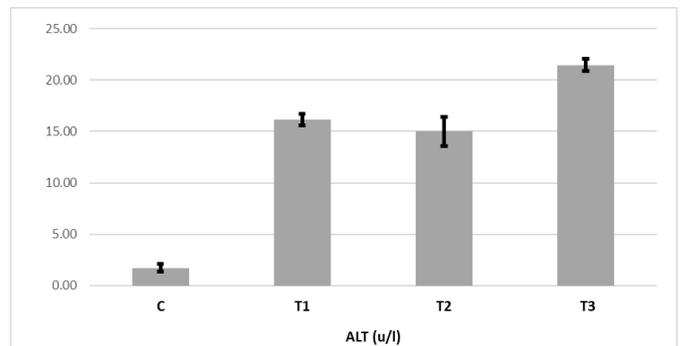


Fig. 2. The Trend of Change in ALT Activity in Tissues of Mice Muscle.

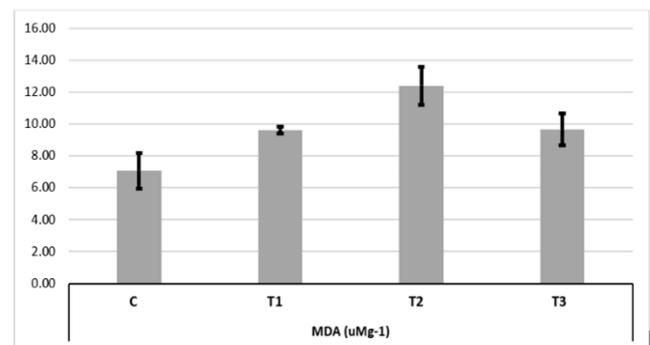


Fig. 3. The Trend of Change in MDA means Concentration (μMg^{-1}) for Mice Muscles.

B. Histopathological Observations

We have revealed that the histo-structure of the skeletal muscle is highly disturbed under the influence of the stonefish venom. The most apparent histological abnormalities in muscles were the great variety of diameters, content, and widespread among randomly distributed muscle fibres. In addition, loss of the fibers' striated appearance can appear in venom-treated groups compared with the control group (Fig. 4). Muscle fibers of the control group show higher content and widespread fibres compared with the treatment groups. (H&E, 10X). C: Control group, T1: Toxin group at 1hr, T2: Toxin group at 2hrs, T3: Toxin group at 3hrs. *: Inflammation.

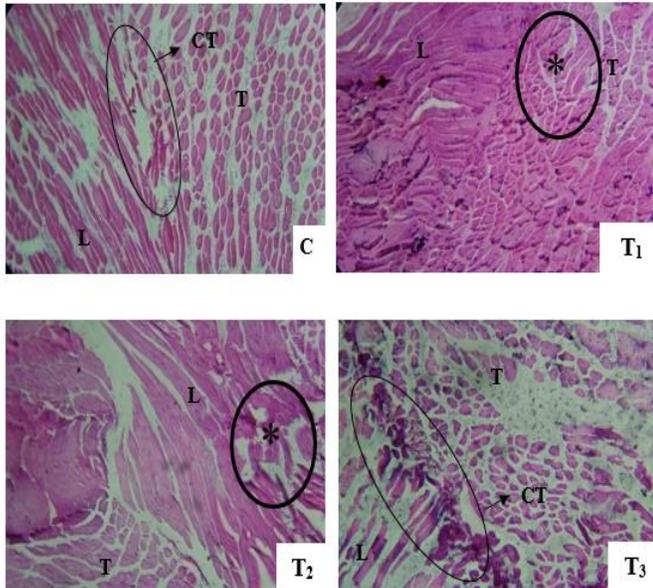


Fig. 4. The Histopathological Changes in Muscles of Venom Injected (LD₅₀) Mice Compared with the Control Mice.

Moreover, Fig. 5 illustrated the histopathological changes in muscles of venom-treated mice compared with the control group.

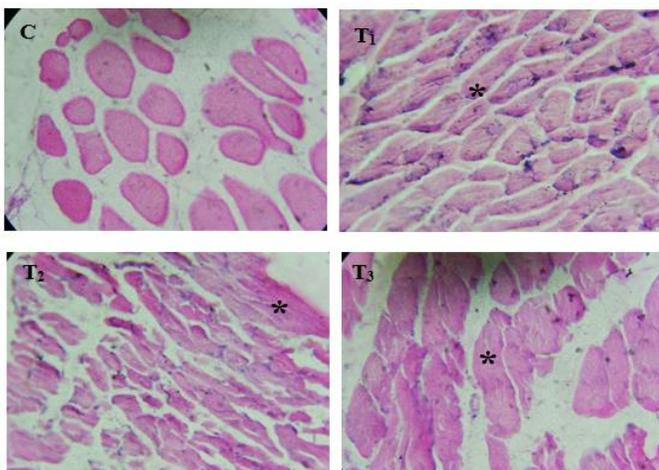


Fig. 5. The Histopathological Changes in Muscles of Venom-Treated (LD₅₀) Mice Compared with the Control Mice.

Control mice muscle reveals a widespread in muscle fibres. Venom treated muscles showing inflammation, degradations, and loss of the striated appearance of the protein fibers. (H&E, 40X). C: Control group, T1: Toxin group at 1hr, T2: Toxin group at 2hrs, T3: Toxin group at 3hrs. *: Inflammation.

C. Histopathological Image Analysis

Previous sections demonstrated the experimentally routine procedures for evaluating the possible harmful effects of stonefish venom on male BALB/c mice's skeletal muscles. Although the histopathological photographs' investigation was performed manually, this technique is time-consuming and depends on the investigator's experience. Therefore, artificial intelligence-assisted image analysis was suggested for qualitative and quantitative diagnosis of skeletal muscle tissues in order to overcome the time challenge. Consequently, our results showed that the SVM model accuracy could detect severe and mild damage with 93% and 91%, respectively, according to the used dataset with promising accuracy results. Table I shows the SVM model's detailed prediction metrics.

TABLE I. DETAILED RESULTS OF THE SVM MODEL

Class	TP	FP	Precision	Recall	F-M
Mild	0.80	0.077	0.80	0.80	0.80
Moderate	0.909	0.040	0.909	0.909	0.909
Severe	0.933	0.48	0.933	0.933	0.933
Weighted Average	0.889	0.053	0.889	0.889	0.889

TP: True Positive, FP: False Positive, and F-M: F-Measure

True Positive classifies images correctly to their original class labels, while False Positive incorrectly classifies images. Precision reflects the ratio of relevant images through the retrieved. Recall means the percentage of the relevant images that the model retrieved. The F-Measure is the harmonious average of precision and recall. It is a composed metric that penalizes extreme values and provides a single measurement for a system that illustrates optimization. The SVM results showed that artificial intelligence offers accurate models to be applied in the natural environment. Therefore, it can support researchers and medicals in recognizing the appearance of particular health issues after stonefish envenomation and assist in the production of fast, reliable, and economical technologies.

IV. DISCUSSION

This study investigates the adverse effect of stonefish crude venom using biochemical and histological approaches on mice muscles. Serum LDH values showed a significant increase ($P \leq 0.05$) by 12 and 21-fold in the T2 and T3 groups, respectively, compared with the control group. These results are reasonable in which a suitable explanation could be rendered by the regulatory mechanism of LDH in the muscles. LDH is regulated by the relative concentrations of its substrates [11, 22]. LDH becomes more active under periods of extreme muscular output due to the increase in substrates for the LDH reaction [4, 22]. When skeletal muscles are forced to produce high levels of energy, the demand for

Adenosine Triphosphate (ATP) in regards to aerobic ATP supply leads to an accumulation of free Adenosine Diphosphate (ADP), Adenosine Monophosphate (AMP), and inorganic phosphate (Pi) [22]. The subsequent glycolytic flux, specifically the production of Nicotinamide adenine dinucleotide (NADH) and pyruvate, exceeds the capacity for pyruvate dehydrogenase and other shuttle enzymes to metabolize pyruvate. The flux through LDH increases in response to increased pyruvate and NADH to metabolize pyruvate into lactate [22-24].

Furthermore, the results show a significant increase in ALT activity after stonefish venom injection, proving muscle toxicity and cell-damaging, which agreed with [12] and [13]. Moreover, the results showed an increase in MDA level in the homogenate tissue of the toxin groups, as highly reactive molecules are responsible for the development of several and different diseases [23, 25]. Our finding proves that there are cytotoxicity and cellular damage, in agreement with [26, 27].

The most apparent histological abnormalities in muscle tissue are reflected by losing their striated appearance. In addition, there was a variation in the diameters, content, widespread among randomly distributed muscle fibres and inflammation in fibres. Thus, our histological studies confirmed that the stonefish venom produced marked pathological changes consistent with extensive damage to the muscle fibers of the mice. The latter finding agrees with a similar study by [5], where it was reported that the protease-related activities of stonefish crude venoms are probably responsible for tissue necrosis and the spread of venom toxicity. It usually consists of depolarising action (stress-inducing imbalance) of cell membrane on both nerve and muscle tissues, and that their effects differ only quantitatively [25, 28, 29]. Based on our findings, we hypothesized the role of stonefish venom in cell signaling (ROS dependent) that might interact with the biological consequences processes.

As presented previously, histological photomicrographs can be procured by using technoscientific digital cameras connected with a microscope to identify tissue formation and structure abnormalities under the microscope. Recently, automated artificial intelligence algorithms can be utilized to distinguish abnormal characteristics based on a specific symptom. In agreement with other related studies [30, 31, 32], artificial intelligence has shown dramatic growth in environmental monitoring and medical health applications, mainly in enhancing histopathology imagery, which can provide a breeding ground for developing bioinformatics applications in various fields.

V. CONCLUSION

Our observations on rapid skeletal muscle damage and inflammation induced by stonefish venom permit us to highlight the need to maintain adequate antivenom stocks in the hospitals in Aqaba. Moreover, we illustrated the benefits of using digital image processing techniques for stonefish histology image analysis by developing a predictive set of tools to aid researchers and medicals in identifying the appearance of specific health problems after stonefish envenomation and provide fast, reliable, and economical technologies. Further coastal and environmental engineering

investigations on dangerous marine organisms: their distribution, habitat, and ecotoxicity along the Jordanian coast of the Gulf of Aqaba, can prove to be promising towards ensuring beach safety in the Gulf of Aqaba.

REFERENCES

- [1] V. Haddad, H.O. Stolf, J.Y. Risk, F.O. França, and J.L.C. Cardoso, "Report of 15 injuries caused by lionfish (*Pterois volitans*) in aquarists in Brazil: a critical assessment of the severity of envenomations," *Journal of venomous animals and toxins including tropical diseases*, vol. 21, pp. 1-7, 2015.
- [2] M. Wahsha, H. Al-Tarawneh, M. Khalaf, W. Hayek, M. Sbaih, and T. Al-Najjar, "Cardiovascular responses to Stonefish *Synanceia verrucosa* venom in balb/c mice," *Fresenius Environmental Bulletin*, vol. 30(2), pp. 891-898, 2021.
- [3] S.L. Saggiomo, C. Firth, D.T. Wilson, J. Seymour, J.J. Miles, Y. Wong, "The Geographic Distribution, Venom Components, Pathology and Treatments of Stonefish (*Synanceia* spp.) Venom," *Marine Drugs*, vol. 19(6), pp. 302, 2021.
- [4] A. Khalil, M. Wahsha, K. Khadra, M. Khalaf, and T. Al-Najjar, "Biochemical and histopathological effects of the stonefish (*Synanceia verrucosa*) venom in rats," *Toxicol*, vol. 142, pp. 45-51, 2018.
- [5] K.M. Poon, C.H.V. Ng, M.L. Tse, "A 10-year retrospective review of stonefish sting injury in Hong Kong," *Hong Kong Journal of Emergency Medicine*, vol. 27, pp. 300-303, 2020.
- [6] F. V. Campos, T. N. Menezes, P. F. Malacarne, F. L. Costa, G. B. Naumann, H. L. Gomes, and S. G. Figueiredo, "A review on the *Scorpaena plumieri* fish venom and its bioactive compounds," *Journal of Venomous Animals and Toxins including Tropical Diseases*, vol. 22, pp. 1-9, 2017.
- [7] M. Khalaf, and A. Disi, "Fishes of the Gulf of Aqaba," *Isted. Marine Science Station Publication*, pp. 64-68, Jordan, 1997.
- [8] M. Wahsha, H. Al-Tarawneh, M. Khalaf, T. Al-Najjar, and W. Al-Zyoud, "Histological and functional renal alterations caused by *Synanceia verrucosa* venom in Mice," *Fresenius Environmental Bulletin*, vol. 28(7), pp. 5294-5300, 2019.
- [9] G. Taylor, "Toxic fish spine injury: Lessons from 11 years' experience," *Spms Journal*, vol. 30(1), pp. 7-8, 2000.
- [10] T.Y. Chen, Y.H. Chang, H.P. Lin, S.T. Chen, and D.F. Hwang, "Proteomic Identification of Stonefish *Synanceja verrucosa* Venom," *Journal of Food and Nutrition Research*, vol. 3(8), pp. 526-539, 2015.
- [11] M. Wahsha, S. Al-Jassabi, M. Azirun, and K. Abdul-Aziz, "Biochemical screening of Hesperidin and Naringin against liver damage in Balb/c mice exposed to Microcystin-LR," *Middle East Journal of Scientific Research*, vol. 6(4), pp. 354-359, 2010.
- [12] M. Kteifan, M. Wahsha, and F. Al-Horani, "Assessing stress response of *Stylophora pistillata* towards oil and phosphate pollution in the Gulf of Aqaba, using molecular and biochemical markers," *Chemistry and Ecology*, vol. 33(4), pp. 281-294, 2017.
- [13] J. Ozer, M. Ratner, M. Shaw, W. Bailey, and S. Schomaker, "The current state of serum biomarkers of hepatotoxicity," *Toxicology*, vol. 245(3), pp. 194-205, 2008.
- [14] P. M. Treuting, and S. M. Dintzis, "Comparative Anatomy and Histology: A Mouse and Human Atlas," 1st ed USA, Elsevier, 2012.
- [15] G. Sivan, K. Venketasvaran, and C. K. Radhakrishnan, "Characterisation of biological activity of *Scatophagus argus* venom," *Toxicol*, vol. 56(6), pp. 914-925, 2010.
- [16] M. Wahsha, C. Bini, S. Fontana, A. Wahsha, and D. Zilioli, "Toxicity assessment of contaminated soils from a mining area in Northeast Italy by using lipid peroxidation assay," *Journal of Geochemical Exploration*, vol. 113, pp.112-117, 2012.
- [17] H. Alhaj, "Principles of histology," 1st ed. Amman, Dar Almaseera for publishing, distribution and printing, 2013.
- [18] H. Alhaj, "Optical Microscopic Preparations," 1st ed. Amman, Dar Almaseera for publishing, distribution and printing, 2010.
- [19] H. Wahsheh, and M. Al-Zahrani, "Secure Real-Time Computational Intelligence System Against Malicious QR Code Links," *International Journal of Computers Communications & Control*, 16(3), pp. 1-9, 2021.

- [20] S. Abdulateef, M. Mahmuddin, and N. Harun, "Shadow Identification in Food Images using Extreme Learning Machine," International Journal of Advanced Computer Science and Applications(IJACSA), vol. 8(8), pp. 68-74, 2017.
- [21] H. Herle, and P. K V, "Relative Merits of Data Mining Algorithms of Chronic Kidney Diseases," International Journal of Advanced Computer Science and Applications(IJACSA), 12(6), 2021.
- [22] L. Spriet, R. Howlett, and G. Heigenhauser, "An enzymatic approach to lactate production in human skeletal muscle during exercise," Medicine and science in sports and exercise, vol. 32(4), pp. 756-763, 2000.
- [23] M. Wahsha, and S. Al-Jassabi, "The role of Silymarin in the protection of mice liver damage against Microcystin-LR toxicity," Jordan Journal of Biological Sciences, vol. 2(2), pp. 63-68, 2009.
- [24] M. Wahsha, T. Al-Najjar, H. Al-Tarawneh, M. Khalaf, and S. Amer, "Biochemical and histological observations of lung injury after stonefish (*Synanceia verrucosa*) envenomation in BALB/c mice," Fresenius Environmental Bulletin, vol. 26(12), pp. 7204-7208, 2017.
- [25] S. Bordbar, A. Ebrahimpour, A. Abdul Hamid, M. Y Abdul Manap, F. Anwar, and N. Saari, "The improvement of the endogenous antioxidant property of stone fish (*Actinopyga lecanora*) tissue using enzymatic proteolysis," Biomed Research International, pp. 1-9, 2013.
- [26] E. Niki, "Lipid peroxidation: physiological levels and dual biological effects," Free Radical Biology and Medicine, vol. 47(5), pp. 469-484, 2009.
- [27] R. Ziegman, P. Alewood, "Bioactive components in fish venoms," Toxins, 7(5): pp. 1497-531, 2015.
- [28] J.Y.L. Lee, L.C. Teoh, S.P.M. Leo, "Stonefish envenomations of the hand—A local marine hazard: A series of 8 cases and review of the literature," Academy of Medicine Singapore, vol. 33, pp. 515-520, 2004.
- [29] R.J. Harris, and R.A. Jenner, "Evolutionary ecology of fish venom: adaptations and consequences of evolving a venom system," Toxins, vol. 11(2), pp. 1-21, 2019.
- [30] H. Wahsheh, and M. Al-Zahrani, "Secure and Usable QR Codes for Healthcare Systems: The Case of Covid-19 Pandemic," 12th International Conference on Information and Communication Systems (ICICS), pp. 324-329, 2021.
- [31] S. Ayyad, M. Shehata, A. Shalaby, A. El-Ghar, M. Ghazal, M. El-Melegy, and A. El-Baz, "Role of AI and Histopathological Images in Detecting Prostate Cancer: A Survey," Sensors, vol. 21(8), pp. 2586, 2021.
- [32] T. Tiyyarattanachai, T. Apiparakoon, S. Marukatat, S. Sukcharoen, N. Geratikornsupuk, N. Anukulkarnkusol, P. Mekaroonkamol, N. Tanpowpong, P. Sarakul, R. Rerknimitr, and R. Chaiteerakij, "Development and validation of artificial intelligence to detect and diagnose liver lesions from ultrasound images," PLoS ONE, vol. 16(6), e0252882, 2021.

Real Time Distributed and Decentralized Peer-to-Peer Protocol for Swarm Robots

Mahmoud Almostafa RABBAH¹, Nabila RABBAH², Hicham BELHADAOU³, Mounir RIFI⁴
RITM Laboratory, ESTC, Hassan II University, Casablanca, Morocco^{1,3,4}
Laboratory of Complex Cyber Physical Systems, ENSAM, Hassan II University, Casablanca, Morocco²

Abstract—This contribution proposes an approach to enhance the capability of robotic agents to join the Internet of Things (IoT) and act autonomously in extreme and hostile environment. This capability will help in the development in environments where the connectivity, availability, and responsiveness of the devices are subject to variations and noises. A real time distributed and decentralized Peer-to-Peer protocol was designed to allow Autonomous Unmanned Surface Vessels (AUSV) extend their context awareness. The developed Middleware allows a real time communication and is designed to run on top of a Real Time Operating System (RTOS). Furthermore, the proposed Middleware will give researchers access to a large amount of data collected by sensors, and thus solve one of the major problems encountered while training artificial intelligence models which is the lack of sufficient data.

Keywords—Autonomous robots; smart objects; peer-to-peer; real time communication; ROS2; ZeroMQ; middleware

I. INTRODUCTION

In the past, static robots, such as industrial arms, were used to perform repetitive tasks in a production line where the environment is well controlled and known in advance, at that time, collaboration between robots was not a priority. However, we are increasingly seeing the emergence of applications involving a swarm robot that share a common ultimate goal, e.g., The Autonomous Unmanned Surface Vessels (AUSV) or Unmanned Ground and Aerial Robots that must achieve missions like first responders, coast guards, area search, target detection and tracking, formations, rendezvous [1-3].

From these facts, the research on collaborative robots has increased considerably, and many researchers have started to make their focus on the internal design of the robot's context awareness [4-5], and the trend is to use Mobile Robots in hostile environments where the stability of the surrounding conditions and the connectivity is limited.

Mobile Robots require collaborative capabilities to achieve complex missions on hostile environment, e.g., AUSV may need to collaborate to build a mesh network where each AUSV serves as a network node. However, most of proposed AUSV was designed to operate in an already known environment and are not designed to adapt themselves to the new changes in the context.

We propose middleware for collaboration, communication, device hardening for deployments in extreme environments. We explore Multi Agent Systems (MAS) as a solution to

enhance the collaboration by increasing autonomy, flexibility, and composability of robotic agents with the IoT devices available on their surrounding environment to promote the self-awareness of those agents. Not only the sensing and actuation are considered, but we also look at the distribution of decision-making in term of collaboration between the components of the application.

Our proposed Middleware named Collaborative Open Platform for Distributed Artificial Intelligence (COPDAI) allows a real time communication between a community of robots while supporting link and component degradation. The community takes distributed decisions that position agents on strategic locations to mitigate the risk of disconnection. Position depends also on the capabilities such as sensing and actuating. Agents are interconnected and they maintain this interconnection as principal vehicle of communication among them in a peer-to-peer mode.

Another problem that COPDAI will try to solve is the difficulty of having access to sufficient data to train artificial intelligence models, COPDAI will promote the sharing of sensor data and the trained models within the scientific community, as well as within the mobile robots.

II. RELATED WORK

In recent study [6] authors presented multiple node communication mechanisms: Simple message, Ports, Topics, Events and services, and based on pre-established criteria, they compared several Robotics Software Framework (RSF) to evaluate the coverage of each of them to defined criteria. It is worth mentioning that robotic systems are often designed over an Ethernet. Field Buses, such as CANBus, I2C, EtherCAT, Serial lines, FireWire, PROFIBUS, and even PCI are often used. Unfortunately, most RSFs and MASs use only the IP protocol.

Generally, the MAS was used for its great flexibility and the ability to reuse components in different projects. Several patterns have been proposed for its implementation in Multi-Robot Systems, proving a gain in development time [7], in this Work Jade Middleware was used to ensure communication.

Agents distribution can be categorized into three forms [8]: Embedded agents at the robot level, agents located at a server level or hybrid distribution: Intelligence and computational agents are external to the robot, and acquisition and control agents are embedded.

In [9], the authors worked on the control of soccer robots, three schemes based on the multi-agent system paradigm were established: the first scheme is based on the control of the robots from a remote computer, in this configuration the robots had no embedded intelligence, the second scheme is based on a distributed architecture where the vision and the decision are done on a central computer and the control of the motors is delegated to embedded systems attached to the robots, the third scheme allows a greater autonomy of the robots where the acquisition of the sensor data, the decision as well as the control of the motors are done at the level of the robot, in addition to an eventual communication between robots.

In [10] the authors have proposed a distributed knowledge base, this base is shared between them. The agents are organized in a hierarchical way and in case of errors that occur in an agent belonging to the lower level, the agents of the higher level replan the trajectory of the robot.

In [11], the authors based their middleware on the Real-time CORBA specification [12] which extends the basic CORBA model to support real-time constructs. A client/server model was adopted, and the predictability improvement was based on Real-time CORBA mechanisms such as: thread-pooling and priority assignment.

In [13], the authors focused on the support of networking and middleware of mobile embedded systems, a communication protocol named TDMA allowed the transmission of data and manage the uncertainty related to the communication, in addition a shared memory named RTDB was defined to allow the agents to share data.

The authors in [14] developed a Humanoid Robot using XBotCore middleware, for real time communication, the middleware use EtherCAT protocol, and the software was built on the top of Xenomai RTOS, the middleware was designed to satisfy 1 kHz control frequency and implement four tasks in real time behavior among other: robot kinematic chain, robot joints, robot Force/Torque sensors. In [15], a middleware based on the concept of control kernel has been developed. Different types of nodes have been designed on top of two protocols namely: CAN bus and Ethernet, the nodes have different capabilities and can provide different types of services depending on their computing power. Lightweight nodes communicate on top of CAN bus and powerful nodes on top of Ethernet.

Also, in [16] we studied 14 Middlewares which are either oriented to robotics applications or smart objects applications, we concluded that most of the Middlewares do not meet the real time constraint like: UBIWARE [17], LMAARS [18], ACOSO [19], Voyager [20], JCAF [21], Aura [22], UBIWARE [23], LMAARS [24] and SOCRADES [25], while others suffer from a centralized architecture like ROS [26], ICARS [27], COROS [28].

III. COPDAI COMMUNICATION ARCHITECTURE

This Each sensor, actuator or decision module can be attached to the robot body or located in its external environment; we will represent each of these components by a node.

Due to the constraint of the hostile environment, our architecture must be robust to the instability of the physical communication links, thus each node can appear and disappear at any time, the Middleware must allow each node to detect the presence of the other nodes and must implement a recovery mechanism in case of communication failure.

In addition to that, our architecture must not have a Single Point of Failure (SPOF): the degradation of a node must not compromise the whole robot's mission, or at least we must be able to switch to a safe position, for that the architecture must be decentralized, we propose a Peer-to-Peer communication between the nodes.

Also, we need to allow distributed computing between nodes: thus, a node that is located on a computer/server with more resources (CPU, RAM...) can contribute to the computations that a node located on an embedded board with limited resources cannot do by itself.

In addition to that, the constraint of real time requires us to define a priority between the transmitted messages, and thus allow the node to process these messages with a minimum level of guarantee and a predictable behavior.

Finally, the middleware must promote collaboration within the scientific community through the sharing of content and collected data during experiments (sensor data, actuators data...) and optionally results or the trained model.

We distinguish four families of possible communication between these nodes among others (Fig. 1):

- Inter-robot communication:
 - Communication between nodes located in the same embedded card / computer.
 - Communication between nodes located in separate embedded cards / computers.
- Communication between robots.
- Communication between robots and smart objects.
- Content sharing (images, videos...) between researchers / robots.

During the design of the communication layer of COPDAI Middleware, we had to provide answers to the following functional requirements:

- Discovery: How can the nodes recognize each other, knowing that they can be located on the same embedded board or on remote embedded boards?
- Presence: How do we track the appearance and disappearance of nodes? Are we going to use a central component as advocated by multi-agent systems or are we going to use a distributed mechanism with partial knowledge of the topology?
- Connectivity: How do we connect one node to another? Are we going to use ethernet communication (on the same segment or on different network segments) or are we going to use inter-process communication (IPC)?

- Point-to-Point messaging: How to send a message from one node to another? Using a central system such as a message broker, or direct communication?
- Group messaging: How we can do group messaging? Use push/pull pattern or use publish/subscribe pattern?
- Real Time communication: How to prioritize critical messages and ensure that they are processed in real time?
- Content distribution: How to send the data collected by the robot embedded system (sensor data, execution data or engine logs...)? Are we going to use a decentralized protocol like (FileMQ [29], IPFS [30] ...)? Or are we going to use server-centric protocols like (FTP, HTTP...)?
- Bridging: How we can do wide area bridging?
- Security: How nodes protect the information they carry? And how to secure messages and content during the exchange operation?
- Test & Simulation: How do we simulate large numbers of nodes? Are we going use real embedded systems? Or are we going provide a way to do a software simulation?
- Distributed logging: What strategy to adopt to trace communications and collect logs from the nodes in order to detect possible failures or to debug?

A. Transport Layer

We choose the concurrency framework ZeroMQ [31] as transport layer, it gives us sockets that carry atomic messages across various transports, among others: IPC and TCP, researchers evaluate the performance of OpenDDS, ORTE and ZeroMQ middleware in terms of latency and scalability, they choose the publish/subscribe pattern to study those middleware performances and results show that ZeroMQ has the best performance with minimal latency [32]. Also, researchers here [33-34] have found that ZeroMQ scales much better and can smoothly handle high data loads and even bursts of requests, which was not the case in their old middleware version based on CORBA.

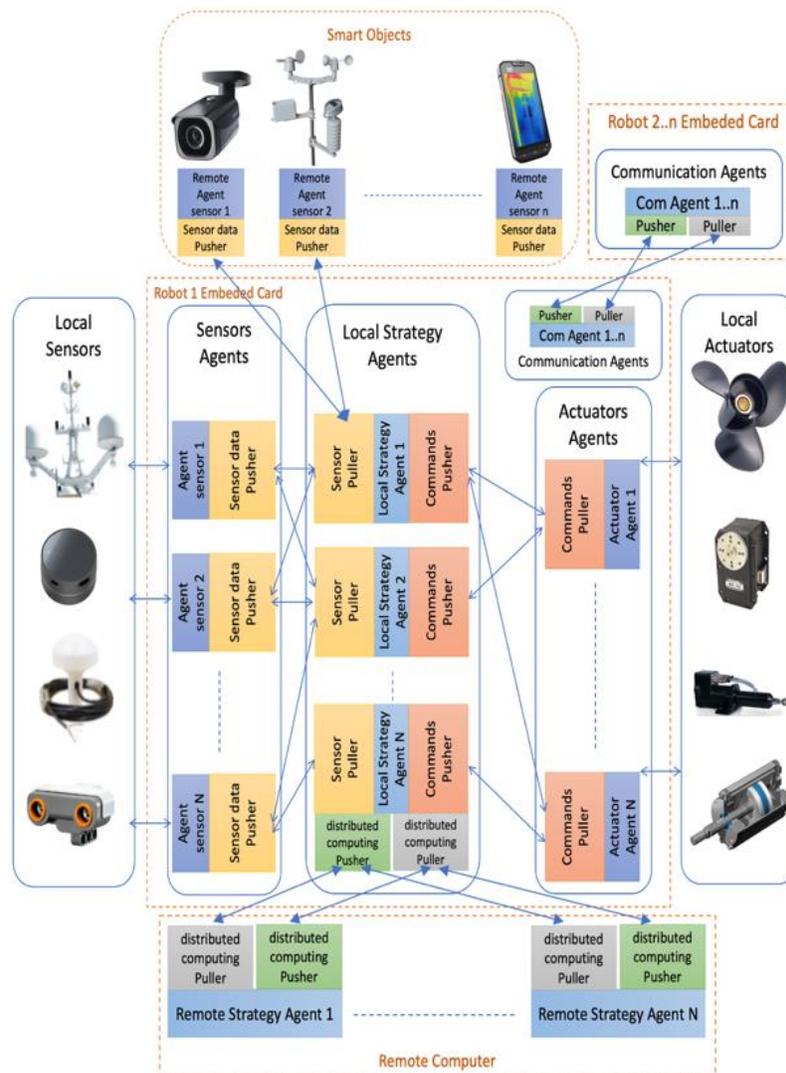


Fig. 1. Communication Families between COPDAI Nodes.

B. Transport Mechanisms

COPDAI will support in its first version the following transport mechanisms: TCP/IP, UDP/IP, and IPC, other mechanisms will be supported in the future releases such as Bluetooth, Serial wire and Acoustic communications.

Nodes within the same embedded card/computer will use IPC to communicate with each other and nodes located on different embedded boards/computers will communicate using IP protocols.

We were inspired by the ZeroMQ Realtime Exchange Protocol (ZRE) which governs how a group of peers on a network discover each other, organize into groups, and send each other events [35]. ZRE runs over the ZeroMQ Message Transfer Protocol (ZMTP). ZRE has been designed to run in smart home and can accept a limited number of nodes: each node establishes a connection to the other ones, which means if we have N nodes we are going to have $\frac{N \times (N-1)}{2}$ connections, which can cause the saturation of a network quickly. Another problem is that ZRE support only IP communication which represents an unjustifiable overhead in our case for the nodes that must communicate within the same embedded card / computer. And finally, ZRE has not implemented any notion of service.

COPDAI supports 4 Messaging types:

- Node to Node messaging: Nodes that belong to the same hierarchical group, and that are located on the same physical medium (embedded card / network segment) can communicate directly in Peer-to-Peer.
- Topic messaging: it is the case where some nodes want share message about the same topic.
- Hierarchical messaging: Nodes are organized in groups that accept a maximum number k of members, each group contains a leader, communication between

members of the same group is direct, but communication between two nodes belonging to different groups must go through the respective leaders of each group,

- Bridging messaging: Communication between nodes belonging to two physical boundaries (two embedded cards or two Network segments) passes through a dedicated node, this node is elected among the group leaders.

Fig. 2 shows a use case of communication types with k=3, if we compare ZRE with COPDAI in this use case, in Network Segment 1 we have only 3 IP connections instead of 171 using ZRE, also ZRE does not allow communication between nodes in segment 1 and 2:

C. Discovery on the Same Machine

In a specific folder location, within the user home directory, each node creates a file with its UUID as file name. Each $\Delta_t - \epsilon$ the node modifies its file timestamp.

Each Δ_t nodes list the files whose last modification date is less than Δ_t , and so, they will be able to know the new nodes that have just appeared or those that have disappeared (Fig. 3).

D. Discovery over IP

We want to keep back compatibility with the ZRE protocol for discovery over IP Protocol, so we are going to use the same mechanism: ZRE uses UDP IPv4 beacon broadcasts to discover nodes. Each ZRE node shall listen to the ZRE discovery service which is UDP port 5670. Each ZRE node SHALL broadcast, at regular intervals, on UDP port 5670 a beacon that identifies itself to any listening nodes on the network [35].

The header shall consist of the letters ‘Z’, ‘R’, and ‘E’, followed by the beacon version number, which shall be %x01.

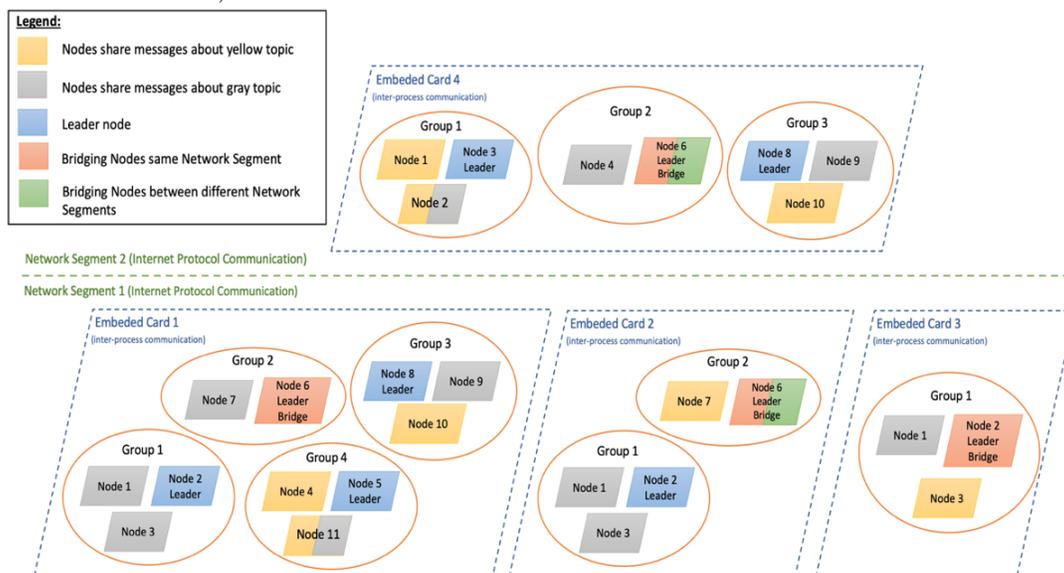


Fig. 2. COPDAI Communication Types with Groups that Accept at Maximum 3 Members.

Name	Date Modified
dealer	Today at 05:04
router	Today at 05:04
4ae7823c-1300-41c0-9c90-9e3a9afdb4c0	Today at 05:04
5c7bffd6-5bb6-4d39-ba0a-e4862451ded6	Today at 05:04
6d599c78-2f46-4a65-9723-ae33edcf6836	Today at 05:04
22f8bd03-47be-4242-9d5c-a0f6e9d2a962	Today at 05:04
73d80114-7f8d-4530-a4a8-3b0106272b80	Today at 05:04
81fd2700-0dca-4932-8365-b95a6eb4f8fa	Today at 05:04
99c280cb-1d8f-4bab-93fc-9e7730b0b5cc	Today at 05:04
184d2010-d6e6-44b1-ad84-eccc45e1eacf	Today at 05:04
79272d9d-66a9-4bf5-b74b-1b16e2caf362	Today at 05:04
e3313e47-8146-40cb-89e1-b4f4d7a1801a	Today at 05:04

Fig. 3. IPC Discovery Files.

The body shall consist of the sender's 16-octet UUID, followed by a two-byte mailbox port number in network order. If the port is non-zero this signals that the peer will accept ZeroMQ TCP connections on that port number. If the port is zero, this signals that the peer is disconnecting from the network. The body contains also another two-byte mailbox port number for real time communication channel, and since in our case the Bridge node hides behind it several nodes which should be discoverable to the outside world, we will extend the ZRE beacon so that the body contains UUIDs of these nodes (Fig. 4).

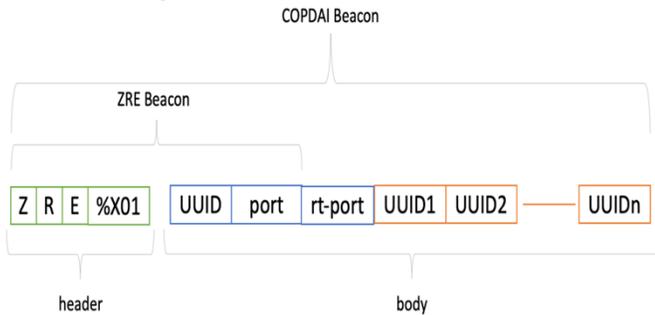


Fig. 4. COPDAI Beacon Message.

Node that receives a valid beacon with a non-zero port number will be considered as a new peer.

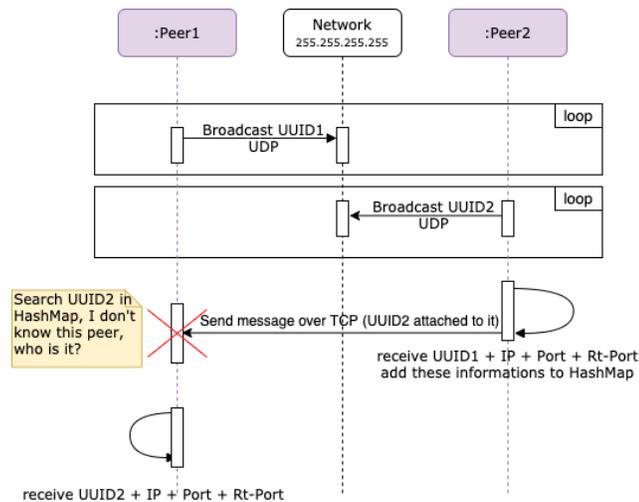


Fig. 5. Use Case where we can receive a Message before Receiving a Beacon from Peer.

UDP messages are limited to 1500 bytes on LANs and 512 bytes on Internet, so the bridge node cannot handle more than 92 nodes in LANs and 30 nodes in Internet, if the bridge node reaches its limit, a new one is elected and handle the rest of the nodes.

Another problem is that bridge node can get the first beacon from a peer after it starts to receive messages from it, so in this situation we got a message from a node that we don't know its IP address and port (Fig. 5).

So, we must consider discovery over TCP: Our first command to any new peer to which we connect is an "Hello" command with our IP address and ports. Below the steps we will follow:

- If we receive a UDP beacon from a new peer, we connect to the peer through a TCP socket.
- Each message must contain the UUID of the sender.
- If it's a Hello message, we connect back to that peer if not already connected to it.
- If it's any other message, we must already be connected to the peer, if it is not the case, we raise an assertion.
- We send messages to each peer using the per-peer socket, which must be connected.
- When we connect to a peer, we also tell our Node that the peer exists.
- Every time we get a message from a peer, we treat that as a heartbeat.

Fig. 6 shows the message format for the "Hello" command throw IP.

```
hello = signature %d1 version sequence endpoint groups status name headers
signature = %AA %A2 ; two octets
version = number-1 ; Version number (2)
sequence = number-2 ; Cyclic sequence number
endpoint = string ; Sender connect endpoint
standpoint = string ; Sender real time endpoint
uuids_services = strings ; list of nodes under the sender's responsibility with svc
groups = strings ; List of groups sender is in
status = number-1 ; Sender groups status value
services = strings ; List of services offered by the sender
name = string ; Sender public name
headers = dictionary ; Sender header properties
```

Fig. 6. COPDAI Hello Message throw IP.

Below we explain the signification of each part of the "Hello" Message:

- 1) Part 1: It is an Event Type (4 bytes), it is equal to %d1,
- 2) Part 2: It is the signature which let us control the received message is a COPDAI Message, must always equal to %xAAA2,
- 3) Part 3: It is the protocol version.
- 4) Part 4: It is a sequence number which will allow our node to check if there were any lost messages between the current received message and the last received one, for each peer.
- 5) Part 5: It is a string that concatenates the IP address of the peer and its port, the endpoint is specified as "tcp://ipaddress:mailbox".

- 6) Part 6: It is a string that concatenates the IP address of the peer and its real time port, the rtpoint is specified as "tcp://ipaddress:rt-mailbox".
- 7) Part 7: list of UUIDs nodes under the responsibility of the sender and for each UUID list of proposed services.
- 8) Part 8: List of groups to which the peer belongs.
- 9) Part 9: The "group status sequence" is a one-octet number that is incremented each time the peer joins or leaves a group. Each peer may use this to assert the accuracy of its own group management information.
- 10) Part 10: List of services offered by the sender.
- 11) Part 11: A Human friendly peer's name.
- 12) Part 12: Headers is a hash table (Key/Value HashMap) of additional information that the peer can eventually send.

E. Detecting Disappearances over IP

Several reasons can come into play and distort the decision that a peer has really disappeared: due to high TCP traffic the UDP packets can be dropped (which causes a high latency before getting the beacon) or a high latency before getting a message on top of the TCP and which is also considered as heartbeat.

To overcome this problem, if we don't get a beacon from the peer after a while, we switch to TCP heartbeats which consist of sending a PING command and receiving a PING_OK response, the PING command is described in ZRE protocol as follow (Fig. 7).

```
ping      = signature %d6 version sequence
version  = number-1          ; Version number (2)
sequence = number-2          ; Cyclic sequence number
```

Fig. 7. PING Command Sent to a Peer if it Disappears [35].

Bellow we explain the signification of the new part of the "PING" Message:

- Part 1: It is an Event Type (4 bytes), t is equal to %d6.

If the Peer is still alive it must respond with a PING_OK as described in Fig. 8:

```
ping_ok   = signature %d7 version sequence
version   = number-1          ; Version number (2)
sequence  = number-2          ; Cyclic sequence number
```

Fig. 8. PING OK Message that a Peer Send to Confirm it is Still Alive [35].

Bellow we explain the signification of the new part of the "PING OK" Message:

- Part 1: It is an Event Type (4 bytes), it is equal to %d7

F. Greeting Message over IPC

The following (Fig. 9) illustrates the Hello message in case of IPC Communication:

```
hello     = signature %d8 version sequence endpoint groups status name headers
signature = %xAA %xA2          ; two octets
version   = number-1          ; Version number (2)
sequence  = number-2          ; Cyclic sequence number
uuids_services = strings      ; list of nodes under the sender's responsibility with svc
groups    = strings          ; List of groups sender is in
status    = number-1         ; Sender groups status value
services  = strings          ; List of services offered by the sender
name      = string           ; Sender public name
headers   = dictionary       ; Sender header properties
```

Fig. 9. COPDAI Hello Message over IPC.

Bellow we explain the signification of the new part of the "Hello" Message over IPC:

- Part 1: It is an Event Type (4 bytes), it is equal to %d8.

G. Topology Heartbeating

Fig. 10 shows a typical example of the links between nodes in the COPDAI Middleware, nodes of the same hierarchical group communicate with each other and with their leader, leaders communicate with each other and with the Bridge Node, and finally Bridge Nodes communicate with each other.

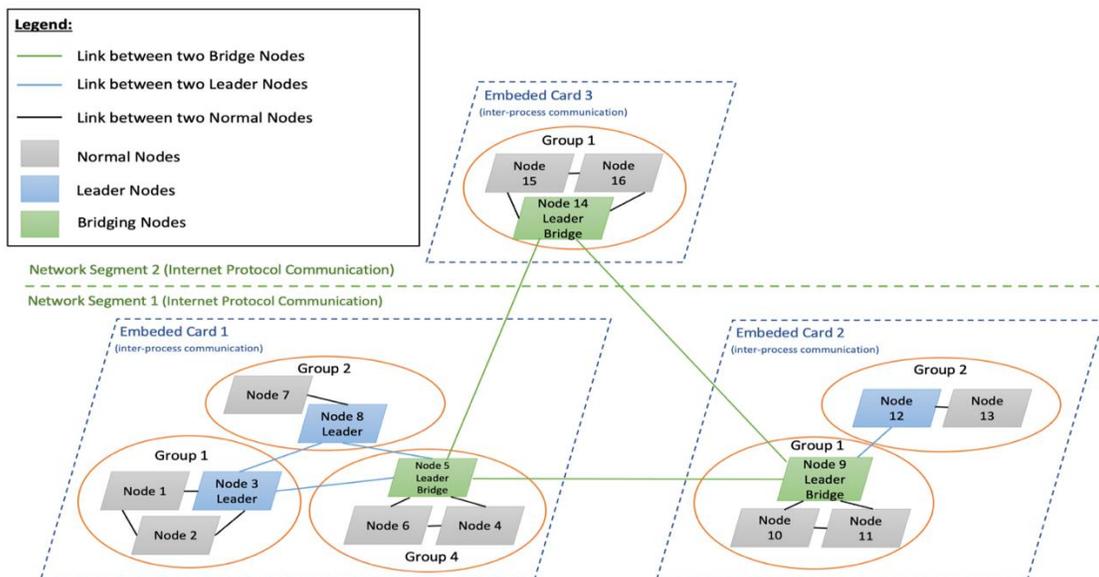


Fig. 10. Typical Communication Topology between COPDAI Nodes.

Each time the leader detects that there is a change in the nodes under its responsibility, e.g., a node in the group has disappeared, a new node has joined its group, it will notify the other leaders by sending the following message (Fig. 11):

```

topology      = signature %d9 version sequence topology status
signature     = %xAA %xA2          ; two octets
version       = number-1          ; Version number (2)
sequence     = number-2          ; Cyclic sequence number
uids_services = strings           ; List of nodes under the sender's responsibility with svc
groups        = strings           ; List of groups sender is in
status        = number-1          ; Sender groups status value
services      = strings           ; List of services offered by the sender
    
```

Fig. 11. COPDAI Topology Heartbeating Message.

Bellow we explain the signification of new part of the "Topology Heartbeating" Message:

- Part 1: It is an Event Type (4 bytes), it is equal to %d9

Bridge Node being itself a Leader, it is responsible for notifying the other Leaders in the same machine by any change in its group.

A Bridge Node is elected among the Leaders, so it is responsible for the propagation of the topology to others Bridge Nodes once a change has happened at the level of its group, or at the level of a group of another leader, the message (Fig. 11) is sent to others Bridge Nodes, with the difference that it concatenates all the nodes present on the machine with their respective services and not only the nodes that belong to its group.

In the opposite direction, once a Bridge Node receives a topology message from another one, it notifies the Leaders on its machine using the following message format (Fig. 12), in the same way the leaders propagate this message to each member of their group:

```

topology      = signature %d9 version sequence topology status
signature     = %xAA %xA2          ; two octets
version       = number-1          ; Version number (2)
sequence     = number-2          ; Cyclic sequence number
uids_services = strings           ; List of nodes under the sender's responsibility with svc
groups        = strings           ; List of groups sender is in
status        = number-1          ; Sender groups status value
services      = strings           ; List of services offered by the sender
    
```

Fig. 12. Remote Bridge Node Topology Heartbeating Message.

Bellow we explain the signification of new parts of the "Remote Bridge Node Topology Heartbeating" Message:

- Part 1: It is an Event Type (4 bytes), it is equal to %d10.
- Part 5: Remote Bridge Node UUID
- Part 6: List of UUIDs nodes under the responsibility of the Remote Bridge Node and for each UUID list of proposed services.
- Part 7: List of groups to which the Remote Bridge Node belongs.
- Part 9: List of services offered by the Remote Bridge Node.

H. Communication between Two Peers

One of the problems we have encountered in trying to have true Peer-to-Peer communication is that ZeroMQ socket is not symmetric, to overcome this problem, we have adopted the harmony pattern: For the outgoing messages, we are going to use a DEALER socket per peer so we can safely send messages.

For the ingoing messages, we choose the ROUTER socket, and so, the Harmony pattern comes down to these components (Fig. 13 and 14):

- One UDP socket where we listen to the broadcasted beacons (In case of Bridge Node).
- One ROUTER socket that we bind to an ephemeral port, and where we receive incoming messages from peers.
- One DEALER socket per peer that we connect to the peer's ROUTER socket.
- One ROUTER socket (named RT-ROUTER) that we bind to an ephemeral port, and where we receive incoming messages from peers which must be processed in real time (we suppose here that the Node is a type of RTCyclicNode and the listener is decorated properly to behave in real time (more details in our recent contribution [36]).
- One DEALER socket (named RT-DEALER) per peer that we connect to the peer's RT-ROUTER socket.
- Reading from our ROUTER/RT-ROUTER socket.
- Writing to the peer's DEALER/RT-DEALER socket.

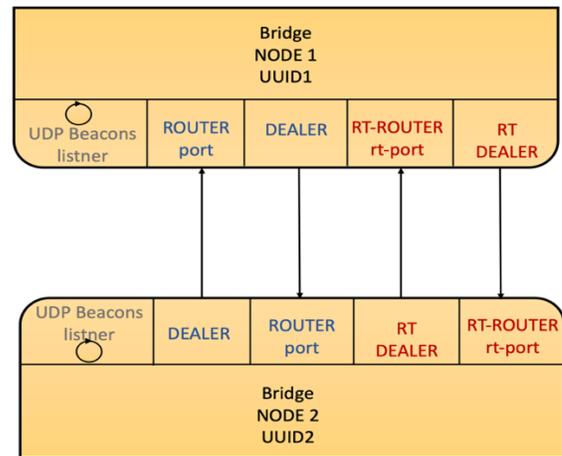


Fig. 13. Sockets used in each COPDAI Bridge Node (IP Communication).

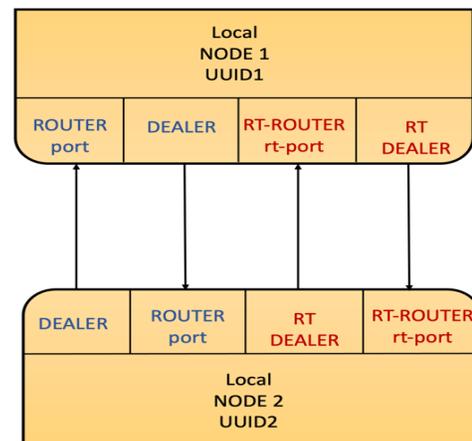


Fig. 14. Sockets used in each COPDAI Local Node (IPC Communication).

If the peer disappears and comes back with a different IP address and/or port, we have to disconnect our DEALER sockets and reconnect to the new ports.

In the case of IPC communication, a folder hierarchy was adopted as shown in (Fig. 15), a file is created in a folder named "dealer" which will be used as a medium for the DEALER socket, another file will be created in the folder "dealer/rt" for real time communication, the same tree structure is adopted for the ROUTER and RT-ROUTER sockets.



Fig. 15. IPC Sockets Folder Hierarchy.

The exchanged message between peers in the same hierarchical group is in this format (Fig. 16).

whisper	=	signature	%d2	version	sequence	content
version	=	number-1				; Version number (2)
service	=	string				; The service name to invoke
sequence	=	number-2				; Cyclic sequence number
content	=	msg				; Wrapped message content

Fig. 16. Format of a Message Exchanged between two Nodes in Same Hierarchical Group.

Bellow we explain the signification of new parts of the Message exchanged between two nodes:

- Part 1: It is an Event Type (4 bytes); it is equal to %d2.
- Part 3: the service name to invoke.
- Part 6: the content message which is serialized using Protocol buffer [37] (it is the serialized object we are going pass to the service as a parameter).

I. COPDAI Node Topology Knowledge Management

Each node according to its position in the COPDAI hierarchy (Normal Node, Leader or Bridge), maintains some knowledge about the current topology:

- All Nodes maintains at least:
 - Peers UUIDs.
 - For each Peer UUID list of services offered by it.
 - For each Peer the list of groups to which it belongs.
 - For each Peer its Manager UUID (can be the UUID of a Leader or a Bridge Node).

- For each Peer the time when it starts running (used in election).
- List of Services.
- For each Service list of Peers offering it.
- For each Peer the outgoing message sequence (for assertion and Quality of Service (QoS)).
- For each Peer the incoming message sequence (for assertion and QoS).
- For each Peer group status sequence (for assertion and QoS).
- Timestamp when this node start running (used in election).
- The last time the node signaled its presence to the outside world (used in election).
- The Normal Node maintains also:
 - The UUID of the Leader Node that is responsible for it.
- The Leader Node maintains also:
 - Same Machine Leaders UUIDs.
 - The UUID of the Bridge Node that is responsible for it.
- Bridge Node maintains also:
 - Same Machine Leaders UUIDs.
 - Bridges Nodes UUIDs.
 - For each Bridge Node: The Endpoint, port, rt-port.

J. Message Routing

When a node wants to send a message to another node which does not belong to its hierarchical group, it constructs the message (Fig. 17) and sends it to the leader, if the leader finds that this node is managed by another leader on the same machine it sends the message to it, this last one transmits the message to the target node, if not, it transmits the message to the Bridge Node on the local Machine, this one will send the message to the Bridge Node which manages the target node, and thus the message is routed until it reaches its destination, an example is illustrated in Fig. 18:

route	=	signature	%d11	version	routing	content
version	=	number-1				; Version number (2)
target_uuid	=	string				; Target Node UUID
service	=	string				; The service name to invoke
sequence	=	number-2				; Cyclic sequence number
content	=	msg				; Wrapped message content

Fig. 17. COPDAI Routing Message Format.

Bellow we explain the signification of new parts of the routing message:

- Part 1: It is an Event Type (4 bytes), it is equal to %d11.
- Part 3: The target peer.

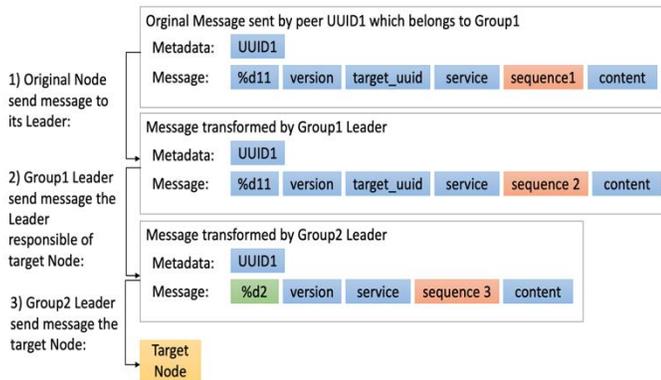


Fig. 18. Example of Routing Message between Nodes that doesn't belong to the same Hierarchical Group.

K. Group Messaging

For group messaging we want to be able to join and leave groups, discover the existing of nodes in other groups and send a message at once to several nodes belonging to the same group. This gives us some new protocol commands:

JOIN - we send this to all peers when we join a group (Fig. 19):

```

join          = signature %d4 version sequence group status
version       = number-1           ; Version number (2)
sequence      = number-2           ; Cyclic sequence number
group         = string              ; Name of group
status        = number-1           ; Sender groups status value
    
```

Fig. 19. Group Join Message Format [35].

- Below we explain the signification of new parts of the join message:
- Part 1: It is an Event Type (4 bytes), it is equal to %d4.
- Part 4: the group the node wants to join.

LEAVE - we send this to all peers when we leave a group (Fig. 20).

```

leave         = signature %d5 version sequence group status
version       = number-1           ; Version number (2)
sequence      = number-2           ; Cyclic sequence number
group         = string              ; Name of group
status        = number-1           ; Sender groups status value
    
```

Fig. 20. Leaving Group Message Format [35].

Below we explain the signification of new parts of the leave message:

- Part 1: It is an Event Type (4 bytes), it is equal to %d5,
- Part 4: the group the node wants to leave.

The following Fig. 21 illustrates the format of a message that will be sent to a group.

```

shout         = signature %d3 version sequence group content
version       = number-1           ; Version number (2)
sequence      = number-2           ; Cyclic sequence number
group         = string              ; Group to send to
service       = string              ; The service name to invoke
content       = msg                 ; Wrapped message content
    
```

Fig. 21. Multi-part Message Format for Group Messaging

Below we explain the signification of new parts of the multi-part message format:

- Part 1: It is an Event Type (4 bytes), if it is equal to %d3.
- Part 4: the group the node wants to send to it the message.
- Part 5: the service name to invoke.
- Part 6: Message content.

When a Leader receive a JOIN or LEAVE or a multi-part message it propagates it to other Leaders, the same for a Bridge Node if it receives a JOIN or LEAVE or multi-part message it propagates it to others Bridge Nodes.

Leaders and Bridge Nodes also are responsible for propagating this message to the Nodes they manage.

L. Election and Membership

1) When a node starts the first time, it sends a request to find a free group to all nodes in the same machine (Fig. 22).

2) If a leader receives a group search request, and if there is free space in its group, it reserves a space for the requester and sends an invitation (Fig. 23).

3) Once an invitation is received, the node sends a request to join the leader group (it must return the same invitation code received in the previous step) (Fig. 24).

4) Then the leader sends a confirmation with the name of the group that the node has just become one of its members (Fig. 25).

```

shout         = signature %d3 version sequence group content
version       = number-1           ; Version number (2)
sequence      = number-2           ; Cyclic sequence number
group         = string              ; Group to send to
service       = string              ; The service name to invoke
content       = msg                 ; Wrapped message content
    
```

Fig. 22. Search Free Group Message Format.

```

shout         = signature %d3 version sequence group content
version       = number-1           ; Version number (2)
sequence      = number-2           ; Cyclic sequence number
group         = string              ; Group to send to
service       = string              ; The service name to invoke
content       = msg                 ; Wrapped message content
    
```

Fig. 23. Leader Invitation Message Format.

```
shout      = signature %d3 version sequence group content
version    = number-1          ; Version number (2)
sequence  = number-2          ; Cyclic sequence number
group      = string            ; Group to send to
service    = string            ; The service name to invoke
content    = msg               ; Wrapped message content
```

Fig. 24. Membership Request Format.

```
shout      = signature %d3 version sequence group content
version    = number-1          ; Version number (2)
sequence  = number-2          ; Cyclic sequence number
group      = string            ; Group to send to
service    = string            ; The service name to invoke
content    = msg               ; Wrapped message content
```

Fig. 25. Membership Confirmation Message Format

5) Once this is done the node sends a "JOIN" message to notify everyone that it has just joined the group (Fig. 19), and after that it creates the necessary IPC sockets with other group's members.

Note: All these operations are time-stamped, if it takes times to receive a response, the operation is cancelled, and the process is resumed.

6) If the node doesn't receive any response from leaders, or if it has failed to become a member of a group after a configurable amount of time, the node creates a new group, joins it, and sends JOIN command to outside world, after that it becomes the leader of this new group it notifies peers with the following message (Fig. 26).

7) If Leaders receive a "LEADERSHIP" message, they send back a congratulation message, and specify which one of them is the Bridge Node (Fig. 27).

8) Once the Leader receives a congratulation message, it creates the necessary IPC sockets with the other Leader.

9) If after a while, the Leader doesn't receive any congratulation message, it considers itself as a Bridge Node, creates the necessary TCP sockets and starts listening on the UDP port to detect other Bridge Nodes over IP.

10) If a leader disappears, the rest of the nodes in the group start elections by exchanging between them the following message containing their start date (Fig. 28): the node that started first becomes the new leader and continues the process explained in step 6.

11) Each node saves/updates the last time it signalled its presence to the outside world, if it was a while since it notifies peers about its presence (a pre-parameterized value in COPDAI Middleware), and if it was a Leader, it concludes that he is no longer the leader and considers itself as a normal node and starts the process again from step 1.

12) If a Bridge Node disappears, the rest of the Leaders start elections by exchanging between them the message shown in (Fig. 28): The Leader that started first becomes the new Bridge Node and continues the process from step 9. The new Bridge Node is responsible of propagating the new topology to the outside world (Fig. 11).

```
shout      = signature %d3 version sequence group content
version    = number-1          ; Version number (2)
sequence  = number-2          ; Cyclic sequence number
group      = string            ; Group to send to
service    = string            ; The service name to invoke
content    = msg               ; Wrapped message content
```

Fig. 26. Leadership Announcement Message.

```
shout      = signature %d3 version sequence group content
version    = number-1          ; Version number (2)
sequence  = number-2          ; Cyclic sequence number
group      = string            ; Group to send to
service    = string            ; The service name to invoke
content    = msg               ; Wrapped message content
```

Fig. 27. Leaders Congratulation Message Format.

```
shout      = signature %d3 version sequence group content
version    = number-1          ; Version number (2)
sequence  = number-2          ; Cyclic sequence number
group      = string            ; Group to send to
service    = string            ; The service name to invoke
content    = msg               ; Wrapped message content
```

Fig. 28. Election Message Format.

M. Content Sharing

We used the InterPlanetary File System (IPFS) [38] which is a peer-to-peer distributed file system that stores and retrieves files in a BitTorrent-like way.

So, to allow sharing of data captured by sensors (images, videos...) or artificial intelligence models between researchers / robots, we installed in each machine the ipfs daemon which connects it to the global distributed network by running the following commands:

```
$> ipfs init (1)
```

```
$> ipfs daemon (2)
```

IPFS requires 512MiB of memory and the installation takes only 12MB, if the machine doesn't have the necessary resources, we just ignore the IPFS installation.

The first time a node starts, it verifies if it has the ipfs capability by running the following command:

```
$> ipfs version (3)
```

If a node wants to add any file to the distributed file system, it just run:

```
$> ipfs add filename (4)
```

To allow nodes located on machines that do not have sufficient resources to share files, we run a dedicated COPDAI nodes (named IPFS Nodes) in servers that have enough resources, these nodes offer the "ipfs" service, and each node can send files to them using the "SEND MESSAGE" command (Fig. 16). The IPFS nodes persist the message content in file and after that, add it to the distributed file system (command 4).

After adding a file to ipfs, the command 4, returns a hash code, IPFS already offers the possibility to retrieve files via browser or command line interface (CLI) but it requires that we know already the hash code, to overcome this limitation, an event is fired associating each hash code with the UUID of the node that generated it and the file creation time, the event is sent to the distributed tracing system. In the future we plan to add an interface to brows the files by agents UUIDs / Names.

Researchers can share their content by just sharing the hash code.

N. Distributed Logging

In such a complex distributed system, tracing message between nodes is paramount, we have chosen Jaeger [39] for distributed transaction and monitoring. The tracing is based on the OpenTracing Semantic Specification [40].

IV. TESTS AND IMPLEMENTATION

A first version of COPDAI Middleware is already developed in python [41], as well as in java [42], also an Android version of the COPDAI agent has been developed [43] to allow any robot to benefit from the existing sensors on a smartphone (Accelerometer, GPS, GYROSCOPE, Magnetometer...) and this allowed us to validate our communication architecture as well as to extend the capabilities of the robot used in our contribution [44] (Fig. 29) after attaching the smartphone to its body.

To challenge our middleware, we compared its performance with ROS2 [45] which is the upgrade of ROS1 by utilizing the Data Distribution Service, the main goal of ROS2 is to provide the real time capability, it is under heavy development, it supports communication over IP, ROS2 doesn't support ARM board even though most mobile robots use embedded cards based on ARM architecture like (Jetson TX2, Raspberry Pi, BeagleBone, Orange Pi, ...), because they are energy efficient.

For each type of communication: COPDAI communication over IPC, COPDAI Real Time communication over IPC, Real Time communication over IP and communication using ROS2, we measured the latency that a message takes to pass from one node to another, we studied the following three scenarios: a node communicates only with one other node, a node communicates with 10 nodes and a node communicates with 100 nodes at the same time, for each scenario we sent 10k messages, to limit network noise, all nodes were deployed on the same machine (Asus Zephyrus ROG, CPU Pentium i7 2.3GHz, RAM 16 GB) the RTOS used: Ubuntu 20.04 Patched to PREEMPT_RT.

Table I illustrates the average latencies in each scenario, we notice that for the scenario of the real time communication using the COPDAI middleware on top of IPC the average latency did not change greatly by increasing from 10 nodes to 100 nodes, which shows a great stability of the system, on the other hand we notice that the average latency climbed in an exponential way in the case of ROS2, same for the case of the communication using COPDAI RT over IP or COPDAI over IPC the average latency is stable and robust to the scaling up.

Table II illustrates the maximum latencies obtained in each scenario, the highest latency was obtained when communicating between 100 nodes using ROS2 with more than 6 minutes of delay between sending and receiving the message, while we notice that the maximum latency in the case of using COPDAI RT over IP did not exceed 9 seconds and 7 seconds over IPC.

Table III illustrates the minimum latencies obtained in each scenario, communication between two nodes using COPDAI RT over IPC give the best result we also notice that in the case of 100 nodes for the same protocol we obtain a good result.

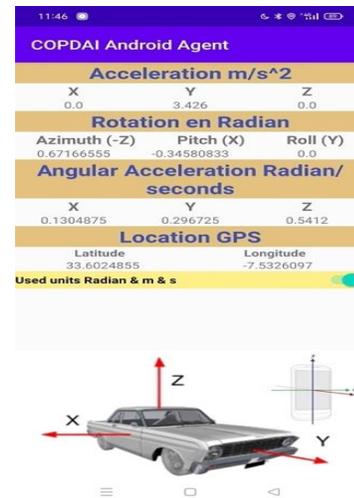


Fig. 29. COPDAI Android Agent which Enhance Robot's Capabilities by Sharing Sensors Data.

TABLE I. AVERAGE LATENCIES IN (MS)

	One Node	10 Nodes	100 Nodes
COPDAI RT Over IPC	164.853	182.592	183.27
COPDAI RT Over IP	180.98	169.352	179.751
COPDAI Over IPC	200.878	201.494	198.819
ROS 2	306.636	415.334	1381.091

TABLE II. MAXIMUM LATENCIES IN (MS)

	One Node	10 Nodes	100 Nodes
COPDAI RT Over IPC	305.277	840.438	6865.242
COPDAI RT Over IP	389.717	1120.752	8817.04
COPDAI Over IPC	379.308	562.39	2322.554
ROS 2	51170.058	90730.255	412285.491

TABLE III. MINIMUM LATENCIES IN (MS)

	One Node	10 Nodes	100 Nodes
COPDAI RT Over IPC	58.415	93.261	77.486
COPDAI RT Over IP	58.754	80.507	78.305
COPDAI Over IPC	103.863	109.328	111.111
ROS 2	181.098	163.54	273.133

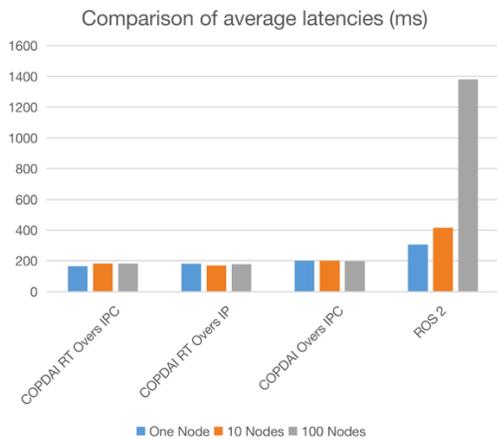


Fig. 30. Average Latency in Proportion with the Number of Nodes and the Communication Mechanism used.

As shown in Fig. 30, our middleware shows a very good performance, it scales efficiently, the real-time communication on IPC is the most optimized, which justifies our choice of such a mechanism for a communication within the same machine, and in general the real-time communication shows a great stability.

V. CONCLUSION

In this paper, a distributed, decentralized, real-time Peer-to-Peer protocol has been designed to allow robots and smart objects to act autonomously and improve their capabilities, COPDAI Middleware allows so, the Autonomous Unmanned Surface Vessels share their knowledge in extreme and hostile environments where links and components are subject to degradation. The designed protocol allows COPDAI nodes to build a mesh network and be aware of their environment. In addition, COPDAI solves the problem of the difficulty to have access to enough data and effectively train artificial intelligence models, by easily enabling the sharing of collected sensor data among the members of the scientific community. A first version of this Middleware has been developed in python, java and Android. We were also able to increase the perception capabilities of a mobile robot by attaching to its body an Android smartphone where COPDAI nodes are deployed, nodes collect mobile sensor data (Accelerometer, GPS, GYROSCOPE, Magnetometer...) and push them to the node deployed on the robot's embedded card. We compared the performance of COPDAI and the ROS2 Middleware. we found that COPDAI has a lower latency and better response time, in addition to a more stable communication when scaling the number of deployed nodes.

In our next work, we will look at the security of communication between nodes, and we will detail discovery and communication for nodes that are behind Firewalls or Routers.

REFERENCES

[1] Vander Hook, J., Seto, W., Nguyen, V., Hasnain, Z., Gallagher, L., Halpin-Chan, T., Varahamurthy, V., & Angulo, M. (2019). Autonomous swarms of high speed maneuvering surface vessels for the central test evaluation improvement program. In *Unmanned Systems Technology XXI* (pp. 110210M). <https://doi.org/10.1117/12.2518554>.

[2] Esposito, J., Feemster, M., & Smith, E. (2008). Cooperative manipulation on the water using a swarm of autonomous tugboats. In *2008 IEEE International Conference on Robotics and Automation* (pp. 1501–1506). <https://doi.org/10.1109/ROBOT.2008.4543414>.

[3] Langerwisch, M., Wittmann, T., Thamke, S., Remmersmann, T., Tiderko, A., & Wagner, B. (2013). Heterogeneous teams of unmanned ground and aerial robots for reconnaissance and surveillance—a field experiment. In *2013 IEEE International Symposium on Safety, Security, and Rescue Robotics (SSRR)* (pp. 1–6). <https://doi.org/10.1109/SSRR.2013.6719320>.

[4] Patil, D., Upadhye, M., Kazi, F., & Singh, N. (2015). Multi robot communication and target tracking system with controller design and implementation of swarm robot using arduino. In *2015 International Conference on Industrial Instrumentation and Control (IIC)* (pp. 412–416). <https://doi.org/10.1109/IIC.2015.7150777>.

[5] Broberg, J., Hede, S., Mikkelsen, S., Pedersen, J., Sørensen, C., Madsen, P., & Borch, O. (2009). Collaboration Layer for Robots in Mobile Ad-hoc Networks. *IFAC Proceedings Volumes*, 42(22), 103–110. <https://doi.org/10.3182/20091006-3-US-4006.00018>.

[6] Inigo-Blasco, P., Diaz-del-Rio, F., Romero-Ternero, M., Cagigas-Muñiz, D., & Vicente-Diaz, S. (2012). Robotics software frameworks for multi-agent robotic systems development. *Robotics and Autonomous Systems*, 60(6), 803–821. <https://doi.org/10.1016/j.robot.2012.02.004>.

[7] Chella, A., Cossentino, M., Gaglio, S., Sabatucci, L., & Seidita, V. (2010). Agent-oriented software patterns for rapid and affordable robot programming. *Journal of systems and software*, 83(4), 557–573. <https://doi.org/10.1016/j.jss.2009.10.035>.

[8] Kim, J.H., & Vadakkepat, P. (2000). Multi-agent systems: a survey from the robot-soccer perspective. *Intelligent Automation & Soft Computing*, 6(1), 3–17. <https://doi.org/10.1080/10798587.2000.10768155>.

[9] Kim, J.H., Shim, H.S., Kim, H.S., Jung, M.J., Choi, I.H., & Kim, J.O. (1997). A cooperative multi-agent system and its real time application to robot soccer. In *Proceedings of International Conference on Robotics and Automation* (pp. 638–643). <https://doi.org/10.1109/ROBOT.1997.620108>.

[10] Kalkhoff, W. (1995). Agent-Oriented Robot Task Transformation. In *Proceedings of Tenth International Symposium on Intelligent Control* (pp. 242–247). <https://doi.org/10.1109/ISIC.1995.525066>.

[11] Kuo, Y.h., & MacDonald, B. (2004). Designing a distributed real-time software framework for robotics. In *Australasian Conference on Robotics and Automation (ACRA)*. Canberra.

[12] Schmidt, D. G., and Fred Kuhns. "An overview of the real-time CORBA specification." *Computer* 33.6 (2000): 56-63.

[13] Almeida, L., Santos, F., & Oliveira, L. (2016). Structuring communications for mobile cyber-physical systems. In *Management of Cyber Physical Objects in the Future Internet of Things* (pp. 51-76). Springer, Cham. https://doi.org/10.1007/978-3-319-26869-9_3.

[14] Muratore, L., Laurenzi, A., Hoffman, E., Rocchi, A., Caldwell, D., & Tsagarakis, N. (2017). Xbotcore: A real-time cross-robot software platform. In *2017 First IEEE International Conference on Robotic Computing (IRC)* (pp. 77–80). <https://doi.org/10.1109/IRC.2017.45>.

[15] Munoz, M., Munera, E., Blanes, J., Simo, J., & Benet, G. (2013). Event driven middleware for distributed system control. *XXXIV Jornadas de Automatica*, 8.

[16] Rabbah, M., Rabbah, N., Belhadaoui, H., & Rifi, M. (2016). Challenges facing middleware for mobile robots in smart environment. *Int. J. Sci. Eng. Res*, 7(11), 33–40.

[17] Katasonov, A., Kaykova, O., Khriyenko, O., Nikitin, S., & Terziyan, V. (2008). Smart semantic middleware for the internet of things. In *International Conference on Informatics in Control, Automation and Robotics* (pp. 169–178).

[18] Choi, J., Cho, Y., Choi, J., & Choi, J. (2014). A layered middleware architecture for automated robot services. *International Journal of Distributed Sensor Networks*, 10(5), 201063. <https://doi.org/10.1155/2014/201063>.

[19] Fortino, G., Guerrieri, A., Lacopo, M., Lucia, M., & Russo, W. (2013). An agent-based middleware for cooperating smart objects. In *International Conference on Practical Applications of Agents and Multi-*

- Agent Systems (pp. 387–398). https://doi.org/10.1007/978-3-642-38061-7_36.
- [20] Savidis, A., & Stephanidis, C. (2003). Dynamic environment-adapted mobile interfaces: the Voyager Toolkit. Stephanidis, C.(Ed.), 4, 489–493.
- [21] Dey, A., Abowd, G., & Salber, D. (2001). A conceptual framework and a toolkit for supporting the rapid prototyping of context-aware applications. *Human-Computer Interaction*, 16(2-4), 97–166. https://doi.org/10.1207/S15327051HCI16234_02.
- [22] Brooks, R. (1997). The intelligent room project. In *Proceedings Second International Conference on Cognitive Technology Humanizing the Information Age* (pp. 271–278). <https://doi.org/10.1109/CT.1997.617707>.
- [23] Katasonov, A., Kaykova, O., Khriyenko, O., Nikitin, S., & Terziyan, V. (2008). Smart semantic middleware for the internet of things. In *International Conference on Informatics in Control, Automation and Robotics* (pp. 169–178).
- [24] Choi, J., Cho, Y., Choi, J., & Choi, J. (2014). A layered middleware architecture for automated robot services. *International Journal of Distributed Sensor Networks*, 10(5), 201063. <https://doi.org/10.1155/2014/201063>.
- [25] Spiess, P., Karnouskos, S., Guinard, D., Savio, D., Baecker, O., De Souza, L., & Trifa, V. (2009). SOA-based integration of the internet of things in enterprise services. In *2009 IEEE international conference on web services* (pp. 968–975). <https://doi.org/10.1109/ICWS.2009.98>.
- [26] Quigley, M., Conley, K., Gerkey, B., Faust, J., Foote, T., Leibs, J., Wheeler, R., Ng, A., & others (2009). ROS: an open-source Robot Operating System. In *ICRA workshop on open source software* (pp. 5).
- [27] Suh, Y.H., Lee, K.W., & Cho, E.S. (2013). A device abstraction framework for the robotic mediator collaborating with smart environments. In *2013 IEEE 16th International Conference on Computational Science and Engineering* (pp. 460–467). <https://doi.org/10.1109/CSE.2013.75>.
- [28] Koubâa, A., Sriti, M. F., Bennaceur, H., Ammar, A., Javed, Y., Alajlan, M., ... & Shakshuki, E. (2015). Coros: A multi-agent software architecture for cooperative and autonomous service robots. In *Cooperative Robots and Sensor Networks 2015* (pp. 3-30). Springer, Cham. https://doi.org/10.1007/978-3-319-18299-5_1.
- [29] <https://rfc.zeromq.org/spec/19/> (2021).
- [30] Benet, J. (2014). Ipfs-content addressed, versioned, p2p file system. arXiv preprint arXiv:1407.3561.
- [31] ZeroMQ, <https://zeromq.org/> (2021).
- [32] Rizano, T., Abeni, L., & Palopoli, L. (2013). Experimental evaluation of the real-time performance of publish-subscribe middlewares.
- [33] Lauener, J., & Sliwinski, W. (2017, October). How to design & implement a modern communication middleware based on ZeroMQ. In *Proc of ICALEPCS* (Vol. 17, pp. 45-51).
- [34] Chang, H. J. (2015). A multi-agent message transfer architecture based on the messaging middleware zeromq. *KIISE Transactions on Computing Practices*, 21(4), 290-298. <https://doi.org/10.5626/KTCP.2015.21.4.290>.
- [35] <https://rfc.zeromq.org/spec/36/> (2021).
- [36] Mahmoud Almostafa, R., Nabila, R., Hicham, B., & Mounir, R. (2018). Python in Real Time Application for Mobile Robot. *Smart Application and Data Analysis for Smart Cities (SADASC'18)*. <http://dx.doi.org/10.2139/ssrn.3179445>.
- [37] <https://developers.google.com/protocol-buffers/> (2021).
- [38] <https://ipfs.io> (2021).
- [39] <https://www.jaegertracing.io> (2021).
- [40] <https://github.com/opentracing/specification/blob/master/specification.md> (2021).
- [41] <https://github.com/mrabbah/copdaipythonagent> (2021).
- [42] <https://github.com/mrabbah/jyre> (2021).
- [43] <https://github.com/mrabbah/copdaiandroidagent> (2021).
- [44] Rabbah, M. A., Rabbah, N., Belhadaoui, H., & Rifi, M. (2017, October). Designing middleware over real time operating system for mobile robot. In *First International Conference on Real Time Intelligent Systems* (pp. 419-425). Springer, Cham. https://doi.org/10.1007/978-3-319-91337-7_37.
- [45] Maruyama, Y., Kato, S., & Azumi, T. (2016, October). Exploring the performance of ROS2. In *Proceedings of the 13th International Conference on Embedded Software* (pp. 1-10). <https://doi.org/10.1145/2968478.2968502>.

Improving Customer Churn Classification with Ensemble Stacking Method

Mohd Khalid Awang, Mokhairi Makhtar, Norlina Udin, Nur Farraliza Mansor
Faculty of Informatics and Computing, Universiti Sultan Zainal Abidin,
22000 Tembil, Terengganu, Malaysia

Abstract—Due to the high cost of acquiring new customers, accurate customer churn classification is critical in any company. The telecommunications industry has employed single classifiers to classify customer churn; however, the classification accuracy remains low. Nevertheless, combining several classifiers' decisions improves classification accuracy. This article attempts to enhance ensemble integration via stack generalisation. This paper proposed a stacking ensemble based on six different learning algorithms as the base-classifiers and tested on five different meta-model classifiers. We compared the performance of the proposed stacking ensemble model with single classifiers, bagging and boosting ensemble. The performances of the models were evaluated with accuracy, precision, recall and ROC criteria. The findings of the experiments demonstrated that the proposed stacking ensemble model resulted in the improvement of the customer churn classification. Based on the results of the experiments, it indicates that the prediction accuracy, precision, recall and ROC of the proposed stacking ensemble with MLP meta-model outperformed other single classifiers and ensemble methods for the customer churn dataset.

Keywords—Stacking ensemble; customer churn prediction; bagging; boosting

I. INTRODUCTION

The rapid development of wireless telecommunications has altered the course of Malaysia's telecommunications industry [1]. Customers may choose and switch between the packages of various service providers. Churn is a term used to describe the behaviour of customers who switch service providers, and it has become a significant issue for Malaysian network providers.

Numerous researchers have attempted to develop various classifiers to predict customer churn, including the decision tree [2], genetic algorithm [3], and regression analysis [4]. However, the conventional approach of using single classifiers for churn prediction is ineffective. It should be improved, as various uncertainty factors such as customer service, network coverage, product quality, packaging prices, and reception quality can all contribute to customer churn [5].

Furthermore, a set of classifier methods referred to as the ensemble method may be used to improve prediction accuracy. The ensemble approach performs better than individual classifiers because of their divergence or independent character. The ensemble technique combines the choices of many classifiers to enhance classification performance [6].

Multi-classifier ensemble techniques, also known as many classifiers, are machine learning algorithms that include training many base classifiers and then aggregating their output to get the highest possible prediction accuracy [7]. Combining the predictions of several classifiers, such as bagging [8], boosting [9], stacking [10] and ensemble selection [11], maybe a practical approach for improving classification performance.

The rest of this article is structured as follows: Section 2 discusses the review of related literature, including ensemble methods such as bagging, boosting, and stacking. Section 3 covers the research methodology, including the data set and the proposed ensemble stacking. Section 4 presents the experimental setup and results from the discussion. The conclusion of this research is discussed in Section 5.

II. LITERATURE REVIEW

A. Predictive Analytics

Predictive analytics is the most often used technique of predicting customer turnover in the business world. When it comes to predictive modelling, it is a model that can be used to forecast or estimate the target values of future instances [12]. In the context of this research, it is described as the process of forecasting or identifying consumers who are likely to abandon their current purchases in the near future [13].

Predictive analytics is made up of a variety of techniques such as statistical prediction modelling, machine learning modelling, and data mining that analyse previous information and make predictions about future events or something completely new and unknown [14]. Predictive modelling is a technique in which a classifier is usually built based on certain information in order to anticipate the result of a given situation. In accordance with [15], predictive modelling may be divided into four subcategories, as follows:

- 1) Classification is used when the predicted result is categorical in nature.
- 2) A regression analysis is used when the prediction results in a numerical value as the result of the analysis.
- 3) Clustering is the term used to describe the process of grouping a certain collection of items based on their characteristics as a result of the analysis.
- 4) When the result is the discovery of intriguing connections between data, this is referred to as association rules.

Predictive models are frequently employed in business because they may detect threats and opportunities by identifying trends in historical and transactional data that are inherent in the database. When used correctly, predictive models may discover connections between numerous variables, allowing for risk assessment or possibly linked with a set of particular circumstances, and therefore assist in the decision-making process for a transaction, among other things [16]. Predictive models are capable of overcoming some of the challenges associated with conventional data analysis, such as dealing with large amounts of data and characteristics with a high degree of dimensionality. Making an effective prediction model requires a number of steps that must be completed in order for it to be successful. These steps include data preparation, data quality checking, feature selection, modelling, prediction, and data analysis. It is sometimes called data mining or knowledge discovery to refer to the whole process [12].

B. Data Mining

According to [16], data mining is a logical process used to mine a vast quantity of information to discover a significant piece of information. In order to get information that is usable, quicker, and more productive [17], data mining methods must be used due to the availability of vast quantities of data and the difficulty of the information retrieval process being prohibitively complex. Apart from that, when compared to statistical techniques, this strategy has emerged as one of the most effective options for forecasting future trends [18]. This data mining method has been successfully used in a variety of important sectors. For example, the need for physicians to enhance their prediction models for specific patients necessitates the use of data mining methods to build and improve risk models [18]. There are a variety of data mining methods accessible, each with a different level of appropriateness based on the domain application. Business data mining applications, such as customer churn forecasts, have great promise and are already in widespread usage and application [19]. A potential client who wishes to terminate the service is identified and detected automatically using this tool. Classification, regression, grouping, and association are just a few of the tasks that are involved in data mining [16].

Classification is one of the most important tasks in the field of data mining. Because the output of the predictive model falls into one of two categories (churn or non-churn), the categorisation activity is regarded in this research as customer churn classification. The goal of customer churn classification is to explain the relationships between a variety of variables, such as the customer profile, call history, and payment information. Essentially, there are twenty (20) characteristics that identify the most significant variables that lead to client turnover [20]. When predicting the behaviour of a new unknown consumer, the relationships between characteristics are taken into consideration.

C. Classification in Data Mining

Classification is described as a component of functional learning that assigns a new object to one of many predefined classes. Classification is a two-step process that begins with the creation and training of a classifier model using any

classification method. Then, in the second phase, the model is evaluated using a set of test data to determine the classifier's performance and accuracy. Classification is a general term that refers to the process of defining class labels for a data set whose class labels are unknown. Classification techniques are employed in knowledge discovery applications for a variety of purposes, including categorising financial market movements and automatically identifying interesting items in big picture collections [16].

D. Classification Algorithms in Data Mining

When doing data analysis or data mining, classification is a fundamental activity that involves the development of a classifier [12]. It is possible to create a classifier by using a collection of characteristics to describe instances and then assigning them a class label. Classifier induction from data sets including previously classified cases is a fundamental issue in machine learning. Various functional representations, such as decision trees, decision lists, neural networks, decision graphs and rules, are used in a variety of methods to solve this issue.

E. Ensemble Methods

A key concept of the ensemble technique is that it seeks to combine ideas from many individual classifiers in order to get superior results that complement one another [21]. The majority of prior research agrees that accuracy increases when employing an ensemble approach rather than a single classifier, with the condition that the mixers in the combinations must be accurate and varied in order for the accuracy to improve [17], [22]. The idea of this ensemble technique is comparable to the concept of the decision-making process, in which individuals are urged to have a conversation with their colleagues before making any decisions about anything. Before making any major choices, it is common for people to seek second or third views. In general, before a decision is made, individual opinions that may be slightly different from each other will be considered, and then their opinions will be combined to reach the final decision [23]–[25].

The results of ensemble techniques are a set of complementary hypotheses whose predictions are consistent with the evidence that has been seen. When multiple classifiers are fitted to the training data, or when a single classifier is fitted under different training circumstances, these hypotheses are generated. For example, the ensemble approach may be implemented by including randomisation methods into the learning algorithm or by using a variety of heuristics for the estimate of the classifier parameters. In the next step, the ensemble prediction is calculated using averaging or voting procedures to combine the choices of the various components in the ensemble to produce a single prediction [26], [27]. In a discrete variable environment, voting rules are nothing more than simple averages.

F. The Fundamental of Ensemble Methods Data

The ensemble approach for classification problems is shown in Fig. 1, which shows a typical structure. Each phase of the framework is split into four sections, which are as follows:

- 1) Training set.
- 2) Base inducer.
- 3) Diversity generator.
- 4) Combiner or composer.

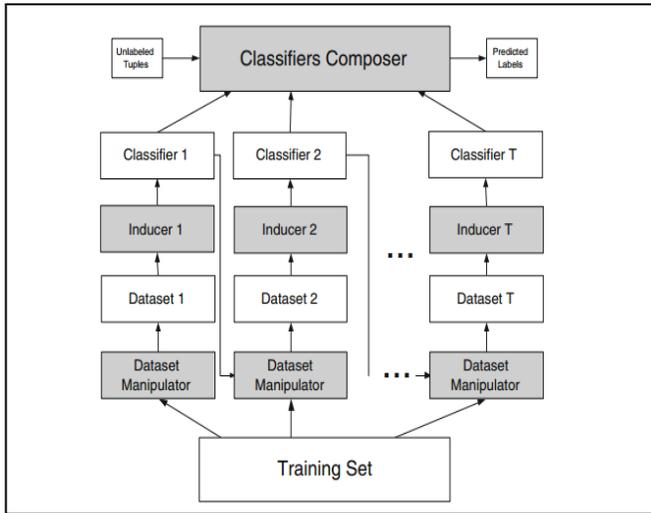


Fig. 1. Ensemble Framework.

The selection of the data set for the training set was the first step in the ensemble's development. Following the selection of the training data set, the subsequent phase involves the generation of the base inducer or ensemble creation, during which the classification algorithms are chosen and trained using the training data set. The diversity generator will guarantee that the basic classifiers have a diverse set of characteristics. At the end of the process, the several classifiers are merged to create the final ensemble.

A study by [28] identifies three kinds of motivations for why ensemble techniques may be better than a single classifier in certain situations. Fig. 2 depicts the problems that need to be addressed.

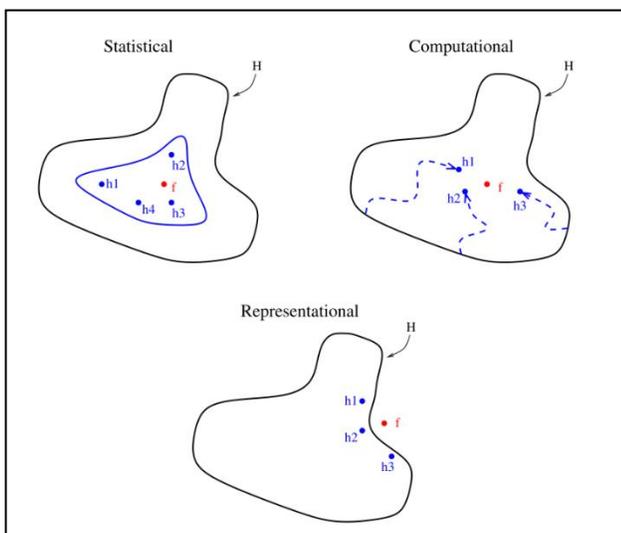


Fig. 2. Three Fundamental Reasons why an Ensemble may Work Better than a Single Classifier.

Statistical issue: When the hypothesis space is too vast to investigate and the available training data is restricted, statistical problems emerge, and there may be many hypotheses that provide the same accuracy on the training data. The issue arises when the learning algorithm selects one of these hypotheses, and there is a chance that the selected hypothesis is incorrect, and therefore the system will be unable to accurately predict future data. Ensemble techniques, on the other hand, suggested combining various ideas, as illustrated in Fig. 2. Combining the hypotheses may minimise or eliminate the statistical issue, as well as the danger of selecting the incorrect hypothesis [29].

Computational issue: A machine learning algorithm, such as a neural network or decision tree, may become trapped in local optima because of the way the search progresses. Finding the optimal hypothesis is always challenging, even if there are ample training data. Instead of searching sequentially from a single location, we use an ensemble approach where we begin at several remote sources. The resulting approximation is thus likely to be closer to the true unknown hypothesis. According to the findings presented in Fig. 2, selecting the incorrect local minimum's risk may be reduced [30].

Representational issue: Even for the vast majority of machine learning problems, no hypothesis can accurately represent the unknown hypothesis in the hypothesis space. When using the ensemble technique, the results presented in Fig. 2 may be feasible to represent even more functions. Since the learning algorithm may be able to formulate a more accurate approximation to the unknown hypothesis, it may be able to get a more accurate solution [28].

Generally, conventional learning methods fail to address difficulties pertaining to the three issues of statistical, constitutional, and representational in nature [29]. In the statistical domain, "high variance" issues are defined as situations in which traditional learning methods fail to address statistical problems. In contrast, the failure of conventional learning methods in computing problems is referred to as a "high variance calculation." A further distinction may be made between classifiers and learning algorithms that suffer from representational problems and those that suffer from a very "high bias." Because of this, ensemble techniques have the potential to mitigate or eliminate the three major shortcomings of conventional learning algorithms.

It is possible to divide the ensemble methods into two main phases: the construction phase and the merging phase. There are at least two main phases in each of the ensemble methods, according to [5]. The creation of ensemble categories should be the first step in the ensemble's growth. It is associated with the combination of the predictions of each classification in an ensemble that the second phase, known as ensemble integration or combination, is performed. However, some researchers recommend ensemble methods that are divided into three phases [5]. Ensemble construction, ensemble trimming, and ensemble combination are the three phases.

1) When the ensemble building phases are completed, they create a collection of heterogeneous base learner classifiers that are used to predict the final output using a given learning technique.

2) As part of the ensemble pruning phase, some fundamental classifiers are eliminated using a variety of mathematical techniques in order to improve the overall accuracy of the ensemble.

3) The third step is the selection and combining of ensembles. During the ensemble selection and combination phase, the filtered learner models are combined to form a single or subset of classifiers, which may provide results that are more accurate than the average of all the individuals' basic classifiers. The template is used to format your paper and style the text. All margins, column widths, line spaces, and text fonts are prescribed; please do not alter them. You may note peculiarities.

G. Homogeneous Ensemble

The term homogeneous refers to the employment of the same learning technique. Various variables are utilised in the same learning process to create different homogeneous models that are generated from different executions [5], and boosting are two popular methods for creating homogeneous models. The approaches for constructing a homogenous ensemble are as follows:

- 1) Manipulation of the learning algorithm's parameters.
- 2) Injection of randomness into the learning process; or
- 3) Manipulation of the training cases; or
- 4) Manipulation of the input characteristics and classifier outputs.

Bagging

"Bootstrap" is implied by the term "bagging" [31]. Bagging is based on two basic principles: bootstrap and aggregate. Because the use of several independent base classifiers generally results in a substantial decrease in error, the basis classifiers must be as self-contained as possible. Bagging encourages diversity and variety of classifications by randomly using a part of training data sets to train each classifier in the ensemble. There must be no overlap between the data sets used. The random forest approach, for example, combines this methodology with random decision-making trees to get very high classification accuracy.

Boosting

The boosting algorithm's strength rests in its ability to turn weak categories into strong classifiers. The weak classifier is somewhat better than random predictions, whereas the strong classifier is intuitively close to the optimum performance. The method's origins may be traced back to a basic question: can weak and strong classifiers be combined to achieve a perfect result? Because the number of poor classifiers usually exceeds the high criterion, this idea is very important. According to the boost, every bad classification may be upgraded to strong classification. Getting a bad learner is very easy, while getting a strong learner is more challenging [32].

H. Stacking Ensemble

On two aspects, stacking differs from bagging and boosting. First, stacking often takes into account heterogeneous weak learners, while bagging and boosting mostly take into account, homogeneous weak learners. Second, stacking uses a meta-model to combine the basic models, while bagging and boosting use stochastic methods to combine weak learners.

The heterogeneous ensemble model is created when the classifier uses multiple learning methods on the same data set [33]. Because of the many learning methods, the classifier has a variety of perspectives and predictions. This technique is one way to create many ensembles while guaranteeing excellent ensemble merging outcomes. Each algorithm has its own set of benefits and drawbacks. For example, as compared to the nearest k-neighbor method, neural networks are stronger for noise. The use of a combination of categories may improve categorisation performance. The boosting algorithm's strength rests in its ability to turn weak categories into strong classifiers. The weak classifier is somewhat better than random predictions, whereas the strong classifier is intuitively close to the optimum performance.

I. Literature Review on Customer Churn

Future customer behaviour prediction is one of the most important tasks in company operations, as it serves as the foundation for all strategic choices and planning. According to [34], customer retention leads to higher revenues while simultaneously lowering marketing expenses when compared to selling to new clients. Rather than seeking additional clients who would raise expenses, the long-term profitability is determined by maintaining the appropriate customer base. With growing rivalry from strong rivals in the telecommunications sector, client retention and loyalty management problems are becoming essential. Predicting client behaviour is very difficult due to the fact that they are human and that their happiness is dependent on the quality of customer service and goods provided to them. In order to forecast customer turnover, several academics have attempted to develop different classifiers. These include the decision tree, support vector machine (SVM), neural network, and logistic regression, among others. In the present state of prediction models, most methods are based on single classifiers, which have poor accuracy. The use of numerous classifiers is introduced in some recent studies; however, the methods used are based on various combinations that make use of all the basic classifiers in order to create the final outcome. The common algorithms of the single classifier and the multiple classifiers method in customer churn models are discussed in detail in the following sub-section of this document.

J. Single Classifiers Approach in Customer Churn Prediction

The models of customer attrition prediction that are most often used by researchers are presented in this subsection. Single classifiers such as logistic regression models, decision tree models, support vector machine models, Bayesian models, and artificial neural network models are among the most often used.

Churners were predicted using decision trees and logistic regression, according to a study conducted by [35]. The researchers concluded that logistics regression is an appropriate choice of classifier for incorporating domain knowledge into the model because, in the analysis of the two sets of data, model performance remains relatively stable even after the introduction of domain restrictions when the AUC measure is taken into consideration.

Based on a dataset collected from the 2009 KDD Cup, [36] presented a J48 decision tree and logistic regression. Customers of a French telecoms firm are studied to determine their marketing preferences. They discovered that the accuracy achieved with the decision tree method was much greater than that obtained with the logistic regression technique, indicating that the decision tree technique is superior.

According to [37] study, linear models, such as logistic regression, are a good choice for modelling customer churn prediction, while decision trees are unstable and should not be used. A linear model, according to the study, has a higher level of stability than decision trees, which tend to age quickly and see their performance deteriorate because of this.

Comparison between logistic regression with other algorithms was performed by [38], who sought to discover the most accurate predictors of churn and to assess the accuracy of various data mining methods; their findings were also confirmed. When compared to decision trees and neural networks models, logistic regression demonstrated better performance in their research.

Unlike the decision tree, logistic regression, and other classification algorithms, the neural network, which replicates our human thinking, is a new kind of classification method. It is possible to forecast customer turnover using the neural network learning algorithm in several different ways. Using a Feed Forward Back Propagation (FFBP) Neural Network, [39] developed a classification model for classification problems. The highest level of precision was reached with a 92.35 percent rate of success. There are three neurons in the hidden layer of the prediction model and two neurons in the output layer for churners, and no neurons for non-churners. In order to achieve a balance between churn and non-churn customers, no data pre-processing or sampling technique was used in the proposed model, which includes all characteristics.

The study by [40] asserted that a neural network could achieve maximum output accuracy and demonstrate that it is superior to decision trees and logistic regression. They also claimed that a neural network could achieve maximum output accuracy and demonstrate that it is superior to decision trees and logistic regression. The efficiency of the algorithm, on the other hand, is not only determined by the accuracy of the output but also by other variables such as the time required to make a prediction and the amount of memory resources required to accomplish the job. Although the neural network algorithm was successful in generating high accuracy in this research, the time required and the amount of memory used by the neural network method were both excessive.

The authors of a research [41] developed the particle classification optimisation-based Back Propagation neural

network for telecoms customer churn prediction (PBCCP) method, which was published in Nature Communications. They conducted extensive tests with large amounts of telecommunications data and concluded that the PBCCP algorithm provides a significant increase in accuracy when predicting customer turnover when compared to existing classification methods. The author in [42] conducted research in which they used decision trees, artificial neural networks, and support vector machines (SVM) to reduce customer turnover for an Iranian mobile business. Specifically, they discovered that the neural network model outperformed alternative categorisation methods. However, according to [38], logistic regression outperforms the neural network method in terms of accuracy. However, a study conducted by [41] found that decision trees outperformed neural network models on a churn data set for a Taiwanese telecom firm and that this was the case even after controlling for other factors.

The support vector machine (SVM), which has full theoretical underpinnings, is extensively utilised in a broad range of applications. The author in [42] developed a hierarchical reference model for SVM-based classification in customer churn prediction, which is based on a hierarchical reference model. Their experimental design comprised a variety of different classifiers, including logistic regression, classification, and regression trees, among other things. SVM outperformed all other classifiers, according to the researchers, in terms of predictive performance. This result on SVM has also been supported by other research, such as the one conducted by which examined the performance of neural networks, support vector machines, and Bayesian networks. The data set includes all 21 characteristics, and no data pre-processing or sampling methods were employed in the collection of the data. The results of the tests indicate that SVM outperforms all other algorithms used in the experiments. Customer churn prediction accuracy is also influenced by feature factors. One of the model's drawbacks is that it did not make use of any feature selection methods, and it is probable that the accuracy of predictions will be improved if the variable selection is carried out.

K. Ensemble Method Approach in Customer Churn

Customers churn prediction models have been improved by using ensemble methods, which have been suggested by academics to enhance their predictive ability. [43] published one of the first ensemble methods used in a customer churn prediction model, which was one of the first to be used. Back-propagation artificial neural networks and self-organising maps were suggested by the authors as hybrid artificial neural network models, which are a combination of both. It was discovered via the experiments that ensemble models beat the basic model of a single neural network when it came to the accuracy of predictions, the total number of predictions, the total number of errors, and the total number of predictions per second. In particular, the artificial neural network hybrid models perform to their highest potential.

Enhancing is an ensemble technique that tries to create a strong classifier from a collection of weak classifiers in a given situation. Based on these findings, [44] investigated the effects of boosting customer churn prediction models by

utilising logistic regression as a base learner and building separate customer churn prediction models for each cluster of customers. It is compared against a single logistic regression model to see how well it works. Following the results of the experimental assessment, it was discovered that boosting outperformed any single logistics regression model.

A hybrid model based on clustering and ensemble classifiers has been proposed, which was used in several studies [45]. In particular, the self-organising map clustering method, as well as four additional classifier techniques, such as the support vector machine, the decision tree, artificial neural networks, and K-nearest neighbours, were utilised in this study. The authors created 14 models, and the ensemble classifier incorporates all of the basic classifiers. They then examined the accuracy, sensitivity, and specification performance of the various models they created. Compared to other single classification models, the findings indicated that combining the self-organising map with heterogeneous boosting produced the highest performance.

Customers churn prediction was made possible by [46], who developed an intelligent hybrid model based on Particle Swarm Optimization and a Feedforward neural network. If the suggested ensemble model is used in conjunction with other states of the art classification methods, the assessment outcomes of churn consumers are shown to be substantially improved. Another significant result from the proposed model is that the weights of the input characteristics were automatically allocated and optimised by the algorithm. Despite this, it gave weight to each of the input characteristics, and no feature selection was performed prior to the ensemble building process. The second disadvantage of the model is that it makes use of all the basic classifiers in the ensemble combination. An ensemble may be composed of models that are both homogeneous and heterogeneous in nature. This section will go into more depth on each of these major categories, which are homogeneous and heterogeneous, respectively.

III. METHODOLOGY

This study is based on a customer dataset obtained from one of the local telecoms providers. There are a total of 272 entries in the datasets, which were subsequently split into two groups: training and testing. Table I includes the specifics of the dataset's input characteristics as well as the label for the dataset's output. The output indicates if the client is a churner or not.

A. Proposed Stacking Ensemble

As shown in Fig. 3, stacking utilises the meta-classifier idea (level-2 classifier) to aggregate the output of the basic classifiers (level-1 classifiers).

Cross-validation is used to prevent overfitting. The following is a broad explanation of the suggested stacking model:

- 1) Split the customer dataset into training and testing datasets.
- 2) For the training dataset and split them into k-folds. (test for k=5, k=10, and k=20)

- 3) For each of the 1st level models (Base classifiers model, test for model 1 to model 6)
 - a) Train a base model on the k-1 parts
 - b) Prediction is made on the kth part.
- 4) Training data set predictions are employed as features for the 2nd level model (meta-model).
- 5) Then the predictions are made on the test dataset.

TABLE I. THE CUSTOMER CHURN DATASET

Input Features
input X1= The State Code
input X2= The Account length
input X3= The Area code
input X4= The Customer Phone number
input X5= Choice of International Plan
input X6= Choice of Voice Mail Plan
input X7= The Number of voice mail messages
input X8= The Total day minutes
input X9= The Number of day calls
input X10= The Total day charge
input X11=The Total evening minutes
input X12= The Number of evening calls
input X13=The Total evening charge
input X14= The Total night minutes
input X15= The Number of night calls
input X16= The Total night charge
input X17= The Total international minutes
input X18=The number of international calls
input X19= The Total international charge
input X20=The number of calls to customer service
Output Feature
Y1=actual result

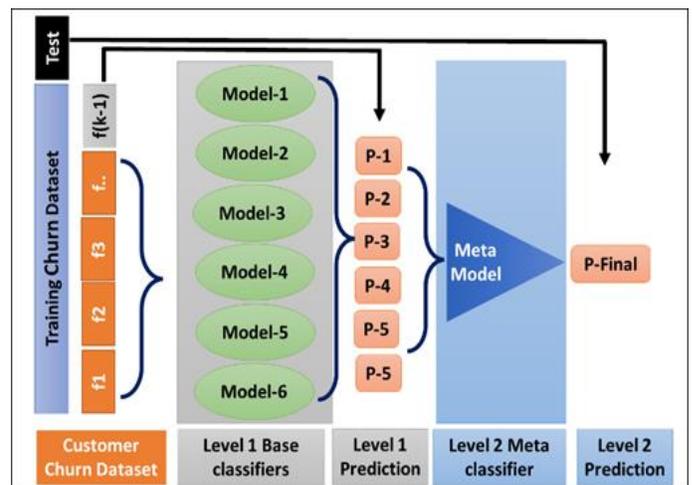


Fig. 3. The Proposed Ensemble Stacking Model for Customer Churn.

B. Level-1 Base Classifiers Construction

The study began with the creation of a level1 model, which is the base classifiers. The first step in creating a successful ensemble technique is to create a varied set of base classifiers in the repository. Different learning algorithms are often used to generate base models, which in turn form the basis of ensembles. Therefore, these ensembles included several kinds of models, all of which provide a desirable degree of variety when it comes to predictions. The pool of classifiers in this study is made up of heterogeneous classifiers created using six different classification learning methods. The selected learning algorithms are as follows:

- 1) Model-1 = KNeighborsClassifier()
- 2) Model-2 = DecisionTreeClassifier()
- 3) Model-3 = SVC()
- 4) Model-4 = GaussianNB()
- 5) Model-5 = AdaBoostClassifier()
- 6) Model-6 = BaggingClassifier

The outputs of the level-1 base classifiers are then used to train a level-2 meta-classifier.

C. Level-2 Meta Classifier Construction

Normally, the meta-model is constructed based on a basic linear model, such as linear regression or logistic regression for regression issues or classification problems. However, any machine learning model or algorithm may act as the meta learner. In this research, various learning algorithms have been employed to evaluate their classification performance and aims to find the best meta-learner model. The selected meta-learners are listed as follows:

- 1) Meta-Model-1 = KNeighborsClassifier()
- 2) Meta-Model-2 = MLPClassifier ()
- 3) Meta-Model-3 = SVC()
- 4) Meta-Model-4 = GaussianNB()
- 5) Meta-Model-5 = LogisticRegression()

D. Performance Measurements

The performance of classifiers is an essential part of data mining activities. Generally, the most common performance measure in classification tasks is the percentage of accuracy, which describes the ratio of a total number of correct classifications over the total number of cases. Accuracy is considered an excellent statistic, but only when we have symmetrical datasets with near-identical values for false positives and false negatives. Therefore, we should consider additional factors while evaluating our model's performance. In this experiment, we will consider four types of performance measurements which are as follows:

- 1) Accuracy
- 2) Precision
- 3) Recall
- 4) ROC

Accuracy equals $TP+TN/TP+FP+FN+TN$

Precision - Precision is defined as the ratio of properly predicted positive observations to anticipated positive

observations in total. This statistic answers the query, "Of all customers classified as churned, how many really churned?" Precision refers to the low incidence of false positives.

Precision is equal to $TP/TP+FP$.

Recall (Sensitivity) - Recall is defined as the ratio of properly predicted positive observations to all observed positive observations in the actual class - yes. The recall question is: How many customers who really churned did we label?

Recall equals to $TP/TP+FN$.

ROC - The receiver operating characteristic curve (ROC curve) is a performance metric for classifying issues at different threshold levels. The receiver operating characteristic (ROC) curve indicates the degree or measure of separability, whereas the area under the curve (AUC) represents the degree or measure of separability. It indicates the degree to which the model can discriminate between classes. The larger the AUC, the more accurately the model predicts 0 classes as 0 and 1 classes as 1. For example, the higher the AUC, the more accurate the model is at differentiating churners from non-churners. The ROC curve is created by plotting the true positive rate (TPR) against the false positive rate (FPR) at various threshold settings.

IV. RESULT AND DISCUSSION

To examine the performance of the classification algorithms, we utilised a variety of performance measures. Accuracy, precision, recall, sensitivity, and the ROC curve are the measures in question. The accuracy metric indicates the proportion of properly classified instances; however, it is insufficient for evaluating the classifier's performance. Table II and Fig. 4 show the overall performance of the base model, while Table III presents the performance of different meta-models.

Based on Table II and Fig. 4, we could notice that the best base model is DecisionTreeClassifier with an accuracy of 93.5 percent, precision of 95.1 percent, recall of 93.6 percent and ROC of 94.0 percent. The BaggingClassifier, on the other hand, has an amazing ROC performance of 95.1 percent, but its accuracy of 90.4 percent is somewhat lower than that of the DecisionTreeClassifier.

TABLE II. THE OVERALL PERFORMANCE OF BASE-MODEL CLASSIFIERS

Level 1 – Base-model Classifier	Performance Measurement			
	Accuracy	Precision	Recall	ROC
KNeighborsClassifier	66.3	69.8	73.3	81.6
DecisionTreeClassifier	93.6	95.1	93.6	94.0
SupportVectorMachine	57.4	57.4	1.0	0.5
GaussianNB	65.7	67.2	79.9	72.9
AdaBoostClassifier	86.7	88.5	88.7	92.8
BaggingClassifier	90.4	92.3	89.5	95.1

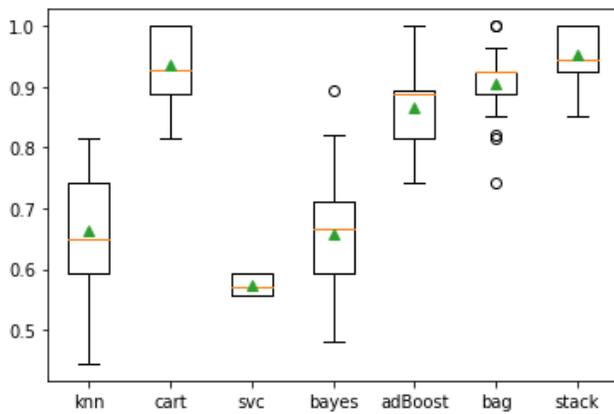


Fig. 4. The Performance of Stacking Ensemble.

Another finding in Table II is that there are few single classifiers with low accuracies, such as the SupportVectorMachine (with a 57.4 percent accuracy), perform poorly compared to other classifiers. The same low performance is also revealed by KNeighborsClassifier and GaussianNB classifiers. Therefore, these ensembles included several kinds of models, all of which provide a desirable degree of variety when it comes to predictions. Consequently, we may suppose that our base-model pool is made up of both excellent and bad classifiers and that the rule of meta-model at the next level is to merge them in order to create a superior model.

TABLE III. THE OVERALL PERFORMANCE OF LEVEL2, META-MODEL CLASSIFIERS

Level 2 – Meta-model Classifier	Performance Measurement			
	Accuracy	Precision	Recall	ROC
Stacking Ensemble (KNeighborsClassifier)	94.3	94.7	94.3	95.5
Stacking Ensemble (MultiLayerPerceptron)	95.4	95.9	94.9	97.8
Stacking Ensemble (SupportVectorMachine)	93.9	94.9	95.7	97.2
Stacking Ensemble (GaussianNB)	94.5	95.5	95.1	96.4
Stacking Ensemble (LogisticRegression)	95.3	95.9	95.1	96.8

Based on Table III, we have developed, tested and compared with the six base-model classifiers, KNeighborsClassifier, DecisionTreeClassifier, SupportVectorMachine, GaussianNB, bagging, and boosting, our proposed stacking ensemble classifier has achieved excellent classification results. All meta-models of stacking ensemble classifiers gained significantly better performance than individual classifiers, bagging and boosting.

The Stacking Ensemble (SupportVectorMachine) is the weakest meta-model, with an accuracy of 93.9 percent, although it performs better than the best model in the base-model (DecisionTreeClassifier). According to Table III, the

Stacking Ensemble (MultiLayerPerceptron) meta-model classifier surpassed all other models with a classification accuracy of 95.4 percent. In addition, it had the highest ROC of 97.8 percent. Stacking Ensemble (LogisticRegression) performance might also be considered since it attained almost the same accuracy (95.3 percent) as the top meta-model.

The proposed stacking ensemble method to classify customer churn has a high performance since the base classifiers are stacked, combining their predictive power. Different classifiers in this model compensate for the shortcomings of other classifiers, resulting in an overall improvement in performance. The suggested stacking ensemble is a one-of-a-kind combination of heterogeneous base classifiers and meta classifiers that perform best at classification.

V. CONCLUSION

In this study, we employed six different learning algorithms as the base classifiers, and we tested several different meta-model classifiers. It was discovered that the MultiLayerPerceptron meta-model classifier performed the best among the other classifiers. A large number of research studies are being conducted in the area of ensembles of classifiers, and many of them are proposing various kinds of classifiers at the base level and at the meta-level, depending on the type of application being investigated. This study contributes to the area of data mining research by suggesting an effective combination of base and meta-level classifiers for a customer churn classification. Thus, this study strongly indicates that the proposed ensemble stacking model outperformed any single classifiers, bagging and boosting ensemble, which is also in accordance with the previous research findings in other application areas.

When compared to single and ensemble techniques for predicting customer churn, our proposed ensemble stacking model has proven to be superior. However, we have only tested our proposed model on the selected customer churn dataset, and we intend to validate it on additional datasets in the future, both in terms of customer churn datasets and other types of datasets, in order to determine whether our approach can be applied to different kinds of problems.

REFERENCES

- [1] M. A. Hajar, D. N. Ibrahim, and M. A. Al-shara, "Value Innovation in the Malaysian Telecommunications Service Industry: Case Study," in International Conference of Reliable Information and Communication Technology, 2018, pp. 892–901.
- [2] A. De Caigny, K. Coussement, and K. W. De Bock, "A new hybrid classification algorithm for customer churn prediction based on logistic regression and decision trees," Eur. J. Oper. Res., vol. 269, no. 2, pp. 760–772, 2018.
- [3] E. Stripling, S. vanden Broucke, K. Antonio, B. Baesens, and M. Snoeck, "Profit maximising logistic model for customer churn prediction using genetic algorithms," Swarm Evol. Comput., vol. 40, pp. 116–130, 2018.
- [4] H. Jain, A. Khunteta, and S. Srivastava, "Churn Prediction in Telecommunication using Logistic Regression and Logit Boost," Procedia Comput. Sci., vol. 167, no. 2019, pp. 101–112, 2020.
- [5] N. N. Y. Vo, S. Liu, X. Li, and G. Xu, "Leveraging unstructured call log data for customer churn prediction," Knowledge-Based Syst., vol. 212, p. 106586, 2021.

- [6] L. Rokach, *Pattern Classification Using Ensemble Methods*. World Scientific, 2010.
- [7] L. Rokach, "Ensemble-based classifiers," *Artif. Intell. Rev.*, vol. 33, no. 1–2, pp. 1–39, 2010.
- [8] Q. L. Zhao and Y. H. Jiang, "Incremental learning based on ensemble pruning," in *2011 Eighth International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 2011, pp. 377–381.
- [9] D. Opitz and R. Maclin, "Popular Ensemble Methods: An Empirical Study," *J. Artif. Intell. Res.*, vol. 11, pp. 169–198, 1999.
- [10] U. Sultan et al., "Master Machine Learning Algorithms: discover how they work and implement them from scratch.," *Appl. Soft Comput. J.*, vol. 77, pp. 188–204, 2016.
- [11] Y. Yang, G. Wang, Z. Zhang, and K. Tian, "A novel emotion recognition approach based on ensemble learning and rough set theory," *9th IEEE Int. Conf. Cogn. Informatics*, pp. 46–52, 2010.
- [12] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, "The KDD process for extracting useful knowledge from volumes of data," *Commun. ACM*, vol. 39, no. 11, pp. 27–34, 1996.
- [13] V. Lazarov and M. Capota, "Churn Prediction," *TUM Comput. Sci.*, 2007.
- [14] X. Wu, T. Ma, J. Cao, Y. Tian, and A. Alabdulkarim, "A comparative study of clustering ensemble algorithms," *Comput. Electr. Eng.*, vol. 68, no. August 2017, pp. 603–615, 2018.
- [15] C. Elkan, *Predictive analytics and data mining*. 2010.
- [16] U. Fayyad, G. Piatetsky-Shapiro, and P. Smyth, "From Data Mining to Knowledge Discovery in Databases," *AI Mag.*, vol. 17, no. 3, p. 37, 1996.
- [17] I. H. Witten and E. Frank, "Data Mining: Practical Machine Learning Tools and Techniques," *Data Min. Pract. Mach. Learn. Tools Tech.*, 2016.
- [18] T. G. Dietterich, "Ensemble methods in machine learning," *Lect. Notes Comput. Sci.*, vol. 1857, pp. 1–15, 2000.
- [19] A. A. Ahmed, "Methods For Customer Retention In Telecom Industries," 2017.
- [20] M. K. Awang, M. R. Ismail, M. Makhtar, and M. A. Nordin, "Performance Comparison of Neural Network Training Algorithms for Modeling Customer Churn Prediction," p. 94.
- [21] M. Mohamad, M. Y. M. Saman, and N. A. Hamid, "Complexity Approximation of Classification Task for Large Dataset Ensemble Artificial Neural Networks," *Lect. Notes Electr. Eng.*, vol. 520, no. April, pp. 195–202, 2019.
- [22] M. Mohamad, M. Y. M. Saman, and M. S. Hitam, "The use of output combiners in enhancing the performance of large data for ANNs," *IAENG Int. J. Comput. Sci.*, vol. 41, no. 1, pp. 38–47, 2014.
- [23] R. Polikar, "Ensemble based systems in decision making," *Circuits Syst. Mag. IEEE*, vol. 6, no. 3, pp. 21–45, 2006.
- [24] C. F. Tsai and M. Y. Chen, "Variable selection by association rules for customer churn prediction of multimedia on demand," *Expert Syst. Appl.*, vol. 37, no. 3, pp. 2006–2015, 2010.
- [25] R. Rosly, M. Makhtar, M. K. Awang, and M. A. Nordin, "The Study on the Accuracy of Classifiers for Water Quality Application," *Int. J. u- e-Serv. Sci. Technol.*, vol. 8, no. 3, pp. 145–154, 2015.
- [26] M. Wozniak and M. Zmyslony, "Chosen problems of designing effective multiple classifier systems," in *2010 International Conference on Computer Information Systems and Industrial Management Applications, CISIM 2010*, 2010, pp. 42–47.
- [27] M. Makhtar, D. C. Neagu, and M. J. Ridley, "Comparing multi-class classifiers: On the similarity of confusion matrices for predictive toxicology applications," *Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 6936 LNCS, pp. 252–261, 2011.
- [28] T. G. Dietterich, "Machine-learning research," *AI Mag.*, vol. 18, no. 4, pp. 97–136, 1997.
- [29] Zhi-Hua Zhou, *Ensemble Methods Foundations and Algorithms*. Cambridge, UK AIMS: Chapman & Hall/CRC, 2014.
- [30] Z. Zhou and W. Tang, "Selective ensemble of decision trees," *Lect. Notes Comput. Sci.*, vol. 2639, pp. 476–483, 2003.
- [31] L. Breiman, "Bagging Predictors," *Mach. Learn.*, vol. 24, no. 421, pp. 123–140, 1996.
- [32] Y. Freund, "Boosting a weak learning algorithm by majority," *Inf. Comput.*, vol. 121, no. 2, pp. 256–285, 1995.
- [33] G. Tsoumakas, L. Angelis, and I. Vlahavas, "Selective fusion of heterogeneous classifiers," *Intell. Data Anal.*, vol. 9, no. 6, pp. 511–525, 2005.
- [34] E. Ascarza, "Retention Futility: Targeting High-Risk Customers Might Be Ineffective," *J. Mark. Res.*, vol. 55, no. 1, pp. 80–95, 2016.
- [35] E. Lima, C. Mues, and B. Baesens, "Domain knowledge integration in data mining using decision tables: case studies in churn prediction," *J. Oper. Res. Soc.*, vol. 60, pp. 1096–1106, 2009.
- [36] K. Dahiya, "Customer Churn Analysis in Telecom Industry," *4th Int. Conf. Reliab. Infocom Technol. Optim. (ICRITO)(Trends Futur. Dir.*, pp. 1–6, 2015.
- [37] M. Owczarczuk, "Churn models for prepaid customers in the cellular telecommunication industry using large data marts," *Expert Syst. Appl.*, vol. 37, no. 6, pp. 4710–4712, 2010.
- [38] A. A. Khan, S. Jamwal, and M. M. Sepehri, "Applying Data Mining to Customer Churn Prediction in an Internet Service Provider," *Int. J. Comput. Appl.*, vol. 9, no. 7, pp. 8–14, 2010.
- [39] S. Babu, N. R. Ananthanarayanan, and V. Ramesh, "A Study on Efficiency of Decision Tree and Multi Layer Perceptron to Predict the Customer Churn in Telecommunication using WEKA," *Int. J. Comput. Appl.*, vol. 140, no. 4, pp. 26–30, 2016.
- [40] S. Khodabandehlou and M. Zivari Rahman, "Comparison of supervised machine learning techniques for customer churn prediction based on analysis of customer behavior," *J. Syst. Inf. Technol.*, vol. 19, no. 1–2, pp. 65–93, 2017.
- [41] C. F. Tsai and M. Y. Chen, "Variable selection by association rules for customer churn prediction of multimedia on demand," *Expert Syst. Appl.*, vol. 37, no. 3, pp. 2006–2015, 2010.
- [42] S. Lessmann and S. Voß, "Computational Intelligence and Information Management A reference model for customer-centric data mining with support vector machines," *Eur. J. Oper. Res.*, vol. 199, no. 2, pp. 520–530, 2009.
- [43] F. T. Chih and H. L. Yu, "Data mining techniques in customer churn prediction," *Recent Patents Comput. Sci.*, vol. 3, no. 1, pp. 28–32, 2010.
- [44] N. Lu, H. Lin, J. Lu, and G. Zhang, "A customer churn prediction model in telecom industry using boosting," *IEEE Trans. Ind. Informatics*, vol. 10, no. 2, pp. 1659–1665, 2014.
- [45] M. Fathian, Y. Hoseinpoor, and B. Minaei, "Offering a hybrid approach of data mining to predict the customer churn based on bagging and boosting methods," *Kybernetes*, vol. 45, no. 5, pp. 732–743, 2016.
- [46] H. Faris, "A hybrid swarm intelligent neural network model for customer churn prediction and identifying the influencing factors," *Inf.*, vol. 9, no. 11, pp. 1–18, 2018.

Enhancing the Takhrij Al-Hadith based on Contextual Similarity using BERT Embeddings

Emha Taufiq Luthfi¹, Zeratul Izzah Mohd Yusoh², Burhanuddin Mohd Aboobaid³

Faculty of Computer Science, Universitas Amikom Yogyakarta, Yogyakarta, Indonesia¹

Faculty of Information, Communication and Technology, Universiti Teknikal Malaysia Melaka, Melaka, Malaysia^{2, 3}

Abstract—Muslims are required to conduct Takhrij to validate the truth of Hadith text, especially when it is obtained from online media. Typically, the traditional Takhrij processes are conducted by experts and apply to Arabic Hadith text. This study introduces a contextual similarity model based on BERT Embedding to handle Takhrij on Indonesian Hadith Text. This study examines the effectiveness of BERT Fine-Tuning on the six pre-trained models to produce embedding models. The result shows that BERT Fine-Tuning improves the embedding model average accuracy by 47.67%, with a mean of 0.956845. The most high-grade accuracy was the BERT embedding built based on the indobenchmark/indobert-large-p2 pre-trained model on 1.00. In addition, the manual evaluation achieved 91.67% accuracy.

Keywords—Hadith text; Takhrij; natural language processing; text-similarity; word embedding; BERT fine-tuning

I. INTRODUCTION

With the growth of information on the Internet, nowadays, most people, including Muslims, use online media as a primary source of information or knowledge. Most Muslims have adopted online media as a direct reference for exploring religious content, including those seeking verses of Qurán or Hadith. The problem is, not all information or knowledge on the Internet are verified for its correctness and authenticity [1].

The primary sources of Islamic law are the Qurán and Hadith [2][3]. Qurán is God's significantly trustworthy and unchanged Holy Book, which has been used as Islamic main reference for more than 14 eras since its revelation [4]. Hadith is an Islamic rule derived from the accumulation of the Prophet Muhammad PBUH's expressions, behaviors, judgments, or character [5][6]. Unlike the Holy Qurán, the Hadith distributed among Muslims are not all trustworthy [7]. Thus, Muslims need to authenticate the correctness of the Hadith, especially when it is from online media.

The approach in validating the correctness of the Hadith is referred as criticism of Hadith [8]. Three Hadith studies support Hadith's criticism: (1) Musthalah Hadith's study; (2) Study of Takhrij and Dirasah Sanad; and (3) Study of Thurud Fahmil Hadith. To recognize a Hadith's authenticity status, a Muslim must perform a Takhrij. Takhrij refers to the examination of the existence of the Hadith in the Hadith Books (its initial sources) such as Kutub al-Sittah, the Six Canonical Books of Hadith, Muwatta Imam Malik, and others. There is some prior research that describes and employs Takhrij al-Hadith to define the status of Hadith. According to [9], Takhrij is performed to meet several objectives as follows: (1) Origin

text (Masdar al-Hadith), (2) Authority of Hadith, (3) Narrators Bonds (Sanad), (4) Hadith Manuscript (Matn), (5) Hadith status in other references (specifying Shawahid or witnesses and Mutaba'at or follow-up), (6) Narrator's profile (al-Jarh wa Ta'dil), (7) Levels of Hadith according to the Sanad, (8) Levels of Hadith according to the Matn and (9) juristic ruling of Hadith (Hukm al-Hadith). [10][11] describes several methods of Takhrij based on the book written by Mahmud al-Thahhan entitled Usul al-Takhrij Dirasah wa al-Asânid:

- 1) Matn's first-word method.
- 2) The Word indexing method.
- 3) The Companion name index method.
- 4) The Hadith theme method.
- 5) The search method is based on Hadith status.
- 6) The search method is based on multiple Matn or Sanad conditions.
- 7) Digital searching via computer CDs or the Internet.

The Takhrij methods numbered 1-6 above are classical methods. In tune with digitalization growth, method number 7 has arisen [12].

Table I summarized the methods, and it can be formed that the Takhrij is a process for obtaining the original Hadith Text through numerous techniques. Table I also shows that traditional Takhrij requires human expertise in the process. Fig. 1 shows the illustration of the Takhrij process.

From the expert's point of view, Takhrij must be based on Arabic Hadith texts to avoid distortion on the Hadith translation. As such, performing Takhrij for other language, such as Indonesian, presents additional challenges.

For illustration, Table II shows two examples of Matn Hadith (highlighted in grey) that are different in sentence but have identical context. As we analyzed deeper; there are several different uses of the word that bring same meaning (bold in Table II), as manifested in Table III. These present a challenge in the Takhrij process to confirm the Hadith authenticity, where the translations are textually diverse though contextually identical.

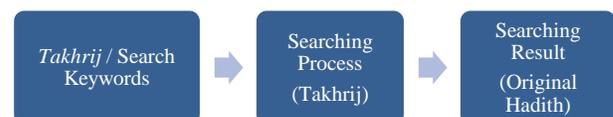


Fig. 1. Takhrij Process Illustration.

TABLE I. TRADITIONAL TAKHRIJ METHODS

1. Hadith Matn's first-word method.	
	Takhrij References: (1) <i>Al-Jami' Al-Shaghir Min Hadis Al-Basyir Al-Nadzir</i> , (2) <i>Faydh Al-Qadir Bi Syarh Al-Jami' Al-Shaghir</i> , (3) <i>Al-Fathu Al-Kabir Fi Dhammi Al-Ziya'dah Ila Al-Jami' Al-Shaghir</i> , (4) <i>Jam'u Al-Jawami' or Al-Jam'i Al-Kabir</i>
	Strength: The intended Hadith will likely be discovered right away.
	Weakness: An inaccuracy in the pronunciations of the first word employed becomes an obstacle to obtaining the Hadith.
2. The Word indexing method.	
	Takhrij References: <i>Al-Mu'jam Al-Mufahras Li Al-Faadz Al-Hadis An-Nabawy</i>
	Strengths: (1) Speed up Hadith exploration; (2) Limit searchable Hadith to specific master books by specifying the name of the book, juz, and pages; and (3) Allow Hadith to search through any words in the index.
	Weakness: (1) Must be able to speak Arabic and have sufficient scientific knowledge; (2) Does not mention the narrators from among the Companions; and (3) On occasion, a Hadith cannot be reached with a single word and must be found using other words.
3. The Companion name index method.	
	Takhrij References: A. The Books of <i>Al-Athr'af</i>: (1) <i>Tuhfatu Al-Asyraf Bi Ma'rifati Al-Athr'af</i> , (2) <i>Al-Nukat Al Zhiraaf 'Ala Al-Athraaf</i> B. The Books of <i>Al-Musnad</i>: (1) <i>Musnad Al-Imam Ahmad Bin Hanbal</i>
	Strength: (1) Shorten Takhrij by introducing Hadith Scholars who narrated their books; (2) Allow Takhrij on all Sanads.
	Weakness: Less effective without prior knowledge of the Hadith's narrators.
4. The Hadith theme method.	
	Takhrij References: (1) <i>Kanzu al-'Ummaal</i> , (2) <i>Miftah Kunuz al-Sunnah</i> , (3) <i>Al-Mughny 'An Hamli al-Asfar</i> , (4) <i>Nashbu al-Rayah</i> , (5) <i>Al-Dirayah</i> , (6) <i>Muntaqaa al-Akhbar</i> , (7) <i>Al-Durr al-Mansur</i> , etc
	Strength: Knowledge of the Hadith's content is required.
	Weakness: Occasionally, the theme of Hadith cannot be defined, or the theme defined by researchers and book compilers is different.
5. The search method is based on Hadith status.	
	Takhrij References: A. Mutawatir Hadith: (1) <i>Al-Azhar Al-Mutanatsirah fi Al-Akhbar Al-Mutawatirah</i> , B. Qudsi Hadith: (1) <i>Al-Ittihafat al-Saniyyah fi al-Ahadis al-Qudsiyyah</i> , C. Popular Hadith: (1) <i>Al-Maqasid al-Hasanah</i> , (2) <i>Kasyful Khofa' Wa Muzilul Ilbas</i> , D. Mursal Hadith: (1) <i>Al-Marasil</i> , E. Maudhu' Hadith: (1) <i>Tanzih asy-Syari'ah al-Marfu'ah 'an al-Ahadis asy-Syani'ah al-Maudhu'ah</i> , (2) <i>Al-Masnu fi Al-Hadis Maudhu</i>
	Strength: Probably would facilitate the Takhrij since most of the Hadith contained in a paper based on its characteristics are very few, so it does not require more complicated reasoning.
	Weakness: Due to the small number of hadiths included, the scope is minimal.
6. The search method is based on multiple Matn or Sanad conditions.	
	Takhrij References: <i>Rijalul Hadith Book</i>

TABLE II. AN EXAMPLE OF TAKHRIJ HADITH

The Hadith of an-Nawawi	Takhrij References
<i>Dari Amirul Mukminin Abu Hafsh, Umar bin Khaththab, ia berkata bahwa dirinya pernah mendengar Rasulullah bersabda, "Sesungguhnya, amal itu bergantung pada niatnya. Dan sesungguhnya seseorang hanya akan mendapatkan sesuatu sesuai dengan yang diniatkannya itu. Siapa yang hijrahnya karena Allah dan Rasul-Nya maka ia akan mendapat Allah dan Rasul-Nya. Dan siapa yang hijrahnya karena dunia yang ingin didapatkannya atau wanita yang ingin dinikahinya maka ia akan mendapatkan sesuai dengan yang ditujuinya itu."</i>	<i>Telah menceritakan kepada kami [Al Humaidi Abdullah bin Az Zubair] dia berkata, Telah menceritakan kepada kami [Sufyan] yang berkata, bahwa Telah menceritakan kepada kami [Yahya bin Sa'id Al Anshari] berkata, telah mengabarkan kepada kami [Muhammad bin Ibrahim At Taimi], bahwa dia pernah mendengar [Alqamah bin Waqash Al Laitsi] berkata; saya pernah mendengar [Umar bin Al Khaththab] diatas mimbar berkata; saya mendengar Rasulullah shallallahu 'alaihi wasallam bersabda: "Semua perbuatan tergantung niatnya, dan (balasan) bagi tiap-tiap orang (tergantung) apa yang diniatkan; Barangsiapa niat hijrahnya karena dunia yang ingin digapainya atau karena seorang perempuan yang ingin dinikahinya, maka hijrahnya adalah kepada apa dia diniatkan" (Shahih Bukhari 1)</i>

TABLE III. AN EXAMPLE OF HOW WORDS ARE USED IN HADITH

The Hadith of an-Nawawi	Takhrij References
<i>amal</i>	<i>perbuatan</i>
<i>mendapatkan sesuatu</i>	<i>balasan</i>
<i>dan siapa</i>	<i>barangsiapa</i>
<i>didapatkannya</i>	<i>digapainya</i>
<i>ditujuinya</i>	<i>diniatkan</i>

This paper employs semi-supervised BERT (Bidirectional Encoder Representations from Transformers) word embedding with a feed-forward neural network classifier to produce a Hadith text representation and determine its contextual similarity level. This work focuses on Hadith in the Indonesian language. The rest of the paper is structured as follows: Section II presents the previous work related to the contextual similarities. Section III about the theoretical definition of the text similarities, BERT, and the evaluation parameters used. Then Section IV describes the proposed model in this study. The results of this research examination are then discussed in Section V. Finally, Section VI explains the conclusion and directions for future research.

II. RELATED WORK

Review on existing works shows that there are several work on word embedding techniques. Authors in [13] established a model that employs word2vec word embeddings, i.e., CBOW and Skrip-gram, innovated with SVM, for classifying the sentiment of social media tweets according to the context. This study shows that skip-gram 100-dimension achieved best classification performance with the values of precision, recall, f-score sequentially 64.4%, 58%, 61.1%.

Several other studies have applied BERT word embedding. The study by [14] utilized BERT sentence embedding for building automatic essay scoring. The outcome indicates that the BERT sentence embedding reaches an F1-score of 82.9%. Similarly, authors in [15] proposes a neural network with a pre-trained language model, M-BERT, that acts as an embedding layer to detect clickbait headlines. Evaluated with 5-fold cross-validation, it has an accuracy score of 91.4%, f1-score of 91.4%, a precision score of 91.6%, and ROC-AUC of 92%. Another study in [16] employs Latent Dirichlet Allocation and BERT embeddings to conduct topic modeling for graduate students' articles collected from the internet. The proposed model reached an average of 92.6% success rate for classifying the appropriate subject documents.

The study in [17] proposed INDOBERT, a novel Indonesian pre-trained language model, to evaluate and benchmark it across INDOLEM. The INDOLEM dataset covers several Indonesian language tasks, including word-forming and sentence-forming, word-meaning, and conversation. The results show that INDOBERT produces novel achievements in most of the tasks in INDOLEM. Authors in [18] introduces a novel model to recognize hate speech in Indonesian Twitter texts. The SVM and RFDT have been applied as machine learning approaches while BiGRU and pre-trained IndoBERT with BiGRU operate as deep learning strategies. The result shows that BiGRU and IndoBERT plus without stop word deletion obtained the most excellent accuracy of 84.77%.

Although several studies have successfully demonstrated the use of BERT word embedding, there is lack of studies on the contextual similarity between conducting Takhrij al-Hadith with Indonesian Hadith text.

III. FUNDAMENTAL THEORY

A. Text Similarities

Text similarity is an extensively applied method for obtaining relatedness between two texts [19]. A mechanism for representing text is required to measure the text-similarity of the natural language. Machines are incapable of understanding the notions of words. The usual technique for representing text is term vectors, in which terms or phrases are converted into vectors of real numbers [20].

Fig. 2 illustrates the variety of text representation forms. Work in [21] presents the weakness of traditional word embeddings, i.e., they carry no contextual representation of 'comparable' words. Furthermore, it raises a 'sparse' matrix problem on an extensive vocabulary. On the contrary, Word2Vec in Skip-Gram or CBOW can attract the semantic (contextual) representation. However, the 'sparse' matrix is still an obstacle to an extensive vocabulary.

B. BERT

BERT (Bidirectional Encoder Representations from Transformers) is a pre-trained transformer form that can be fine-tuned with a single supplementary output layer. BERT fine-tuned the ability to generate various NLP tasks with new state-of-the-art outcomes for a broad range of assignments, including question answering, sentence classification, and sentence-pair regression, without significant task-particular architecture modification [22][23]. Fig. 3 shows the BERT architecture.

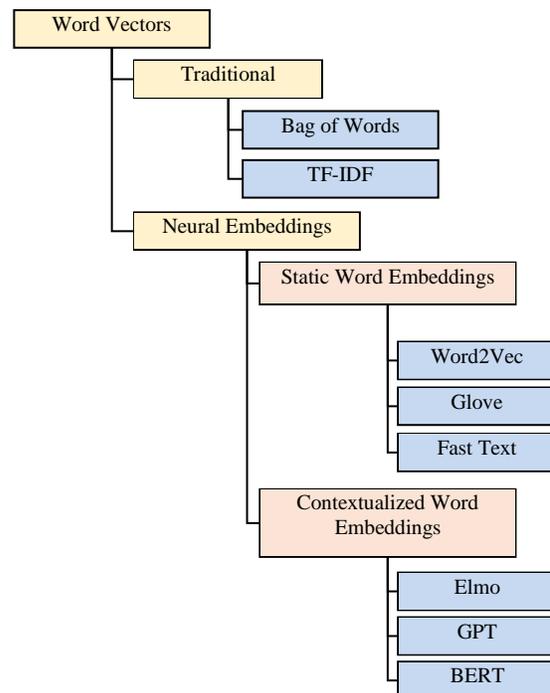


Fig. 2. Word Vectors Text Representation.

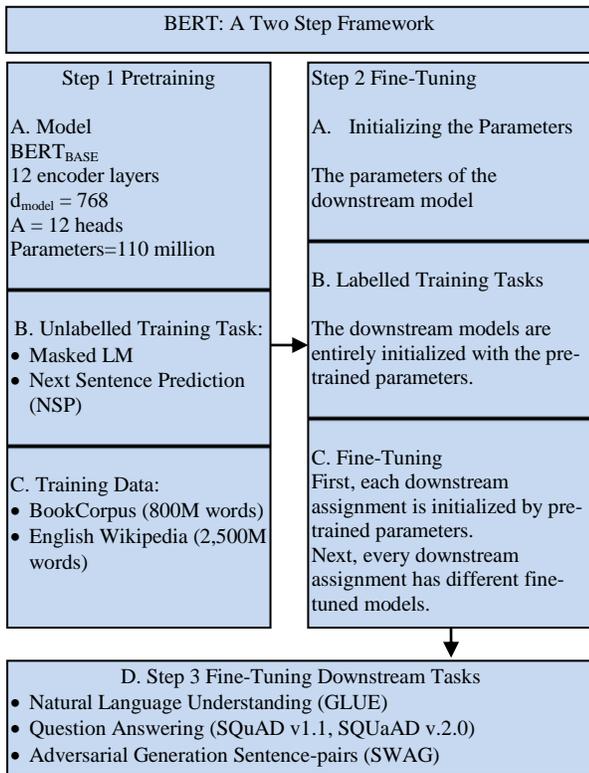


Fig. 3. BERT Architecture.

A feature-based or fine-tuning approach can assign pre-trained language representations for downstream assignments [22]. Fine-tuning is simple as the transformer self-attention mechanism provides BERT with the ability to perform various downstream assignments on a single text or text pair by exchanging suitable inputs and outputs. Every assignment only requires providing the assignment-particular inputs and outputs inside BERT also fine-tune entire parameters end-to-end.

C. Evaluation Parameters

The evaluation of performances plays a crucial role in the development of classification models [24]. BERT Fine-Tuning employs Categorical Cross-Entropy Loss, also called Softmax Loss, as a loss function to calculate the distance within the current output of the algorithm and the expected output. It is a Softmax activation plus a Cross-Entropy loss, as shown in Fig. 4 [25].

Softmax output activation function:

$$f(s)_i = \frac{e^{s_i}}{\sum_j^C e^{s_j}} \quad (1)$$

Cross-Entropy Loss:

$$CE = -\sum_i^C t_i \log(f(s)_i) \quad (2)$$



Fig. 4. Categorical Cross-Entropy Loss Illustration.

Accuracy metrics operate to measure the number of accurate predictions to the total number of input specimens. The accuracy metric defined as [26]:

$$Acc = \frac{True\ Positive + True\ Negative}{Total\ Sample} \quad (3)$$

IV. PROPOSED MODEL

A. Methodology

The methodological approach practiced in this study is compiled in Fig. 5. The first step is gathering and preparing Hadith text as a dataset for training and testing the model. This study focuses on Hadith text that correlated to the Forty Hadith of al-Imam an-Nawawi. Ten unprocessed Hadith texts were gathered from [27] as Hadith texts to be tracked (Takhrij). Furthermore, fifty raw Hadith texts were gathered from <https://carihadis.com> as Takhrij references. The datasets are distributed as 70% training and 30% testing data. Table IV shows the specimens of raw Hadith text.

The second step is data pre-processing. Here are three sub-steps that are (a) text standardization, (b) eliminating undesirable items from Hadith text, and (c) data labeling. Fig. 6 shows the flow of the data pre-processing process in detail.

Table V shows the specimen of Hadith text resulting from pre-processing sub-step point a and point b.

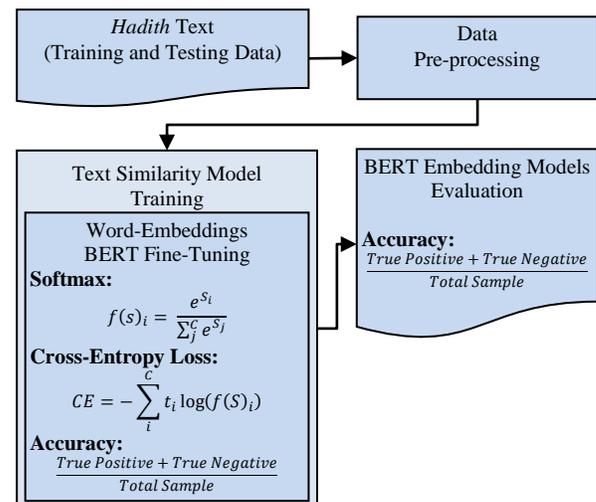


Fig. 5. Proposed Methodology.

TABLE IV. AN EXAMPLE OF RAW HADITH TEXT

The <i>Hadith</i> of <i>an-Nawawi</i>	<i>Takhrij</i> References
<p>Dari Amirul Mukminin Abu Hafsh, Umar bin Khaththab, ia berkata bahwa dirinya pernah mendengar Rasulullah bersabda, "Sesungguhnya, amal itu bergantung pada niatnya. Dan sesungguhnya seseorang hanya akan mendapatkan sesuatu sesuai dengan yang diniatkannya itu. Siapa yang hijrahnya karena Allah dan Rasul-Nya maka ia akan mendapat Allah dan Rasul-Nya. Dan siapa yang hijrahnya karena dunia yang ingin didupakannya atau wanita yang ingin dinikahinya maka ia akan mendapatkan sesuai dengan yang ditujunya itu."</p>	<p>Telah menceritakan kepada kami [Al Humaidi Abdullah bin Az Zubair] dia berkata, Telah menceritakan kepada kami [Sufyan] yang berkata, bahwa Telah menceritakan kepada kami [Yahya bin Sa'id Al Anshari] berkata, telah mengabarkan kepada kami [Muhammad bin Ibrahim At Taimi], bahwa dia pernah mendengar [Alqamah bin Waqash Al Laitsi] berkata; saya pernah mendengar [Umar bin Al Khaththab] diatas mimbar berkata; saya mendengar Rasulullah shallallahu 'alaihi wasallam bersabda: "Semua perbuatan tergantung niatnya, dan (balasan) bagi tiap-tiap orang (tergantung) apa yang diniatkan; Barangsiapa niat hijrahnya karena dunia yang ingin digapainya atau karena seorang perempuan yang ingin dinikahinya, maka hijrahnya adalah kepada apa dia diniatkan" (Shahih Bukhari 1)</p>
	<p>Telah menceritakan kepada kami [Abdullah bin Maslamah] berkata, telah mengabarkan kepada kami [Malik] dari [Yahya bin Sa'id] dari [Muhammad bin Ibrahim] dari [Alqamah bin Waqash] dari [Umar], bahwa Rasulullah shallallahu 'alaihi wasallam bersabda: "Semua perbuatan tergantung niatnya, dan (balasan) bagi tiap-tiap orang (tergantung) apa yang diniatkan; barangsiapa niat hijrahnya karena Allah dan Rasul-Nya, maka hijrahnya adalah kepada Allah dan Rasul-Nya. Barangsiapa niat hijrahnya karena dunia yang ingin digapainya atau karena seorang perempuan yang ingin dinikahinya, maka hijrahnya adalah kepada apa dia diniatkan.". (Shahih Bukhari 53)</p>
	<p>Telah menceritakan kepada kami [Muhammad bin Katsir], telah mengabarkan kepada kami [Sufyan], telah menceritakan kepadaku [Yahya bin Sa'id] dari [Muhammad bin Ibrahim At Taimi] dari [Alqamah bin Waqqash Al Laitsi], ia berkata; aku mendengar [Umar bin Al Khaththab] berkata; Rasulullah shallallahu 'alaihi wasallam bersabda: "Sesungguhnya amalan itu tergantung kepada niatnya, dan bagi setiap orang akan mendapatkan sesuai apa yang telah ia niatkan. Barangsiapa yang hijrahnya kepada Allah dan RasulNya, maka hijrahnya adalah kepada Allah dan RasulallahNya, dan barangsiapa yang hijrahnya untuk dunia yang hendak ia dapatkan atau karena seorang wanita yang akan ia nikahi, maka hijrahnya akan mendapatkan sesuai apa yang ia maksudkan." (Sunan Abu Daud 1882)</p>

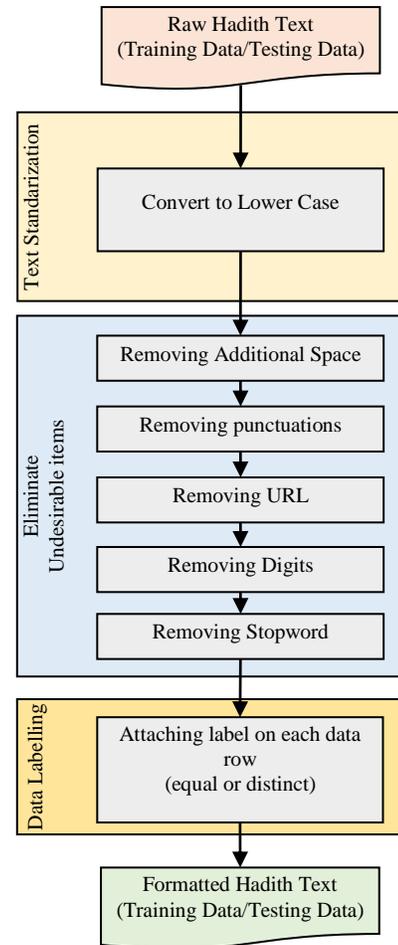


Fig. 6. Data Pre-Processing Flow.

TABLE V. EXAMPLE OF OUTPUT OF TEXT STANDARDIZATION AND ELIMINATE UNDESIRABLE ITEMS PROCESS

Status, Hadith1, Hadith2
<p>equal, dari ummul mukminin ummu abdillah aisyah ia berkata bahwa rasulullah bersabda siapa saja yang mengadaada dalam perkara agama kami ini sesuatu yang bukan bagian darinya maka ia tertolak dalam riwayat muslim yang lain disebutkan siapa saja yang mengerjakan suatu amalan yang tidak ada keterangannya dari kami maka ia ditolak, telah menceritakan kepada kami abu marwan muhammad bin utsman al utsmi berkata telah menceritakan kepada kami ibrahim bin sad bin ibrahim bin abdurrahman bin auf dari bapaknya dari al qasim bin muhammad dari aisyah berkata rasulullah shallallahu alaihi wasallam bersabda barangsiapa membuat perkara baru dalam urusan kami yang tidak termasuk darinya maka dia tertolak</p>
<p>distinct, dari abu hurairah abdurrahman bin shakhr berkata bahwa ia pernah mendengar rasulullah bersabda apa yang kularang jauhilah dan apa yang kuperintah lakukanlah semampu kalian sesungguhnya yang membinasakan umatumat sebelum kalian adalah mereka banyak bertanya dan berselisih dengan nabi, telah menceritakan kepada kami abu marwan muhammad bin utsman al utsmi berkata telah menceritakan kepada kami ibrahim bin sad bin ibrahim bin abdurrahman bin auf dari bapaknya dari al qasim bin muhammad dari aisyah berkata rasulullah shallallahu alaihi wasallam bersabda barangsiapa membuat perkara baru dalam urusan kami yang tidak termasuk darinya maka dia tertolak</p>

The third step is to build the BERT Embedding for contextual similarities model. The model is built with the exercises on top of some semi-supervised BERT models that employ BERT Fine-Tuning. A precise fine-tuning approach is needed to fit the BERT to NLP tasks in contextual similarities (Takhrij).

This study investigates the fine-tuning of five different BERT pre-trained models. The target model is a single label classification model and trained with several parameters, which are:

- Maximum length: None
- Batch Size: 32
- Epochs: 100
- Classification labels: Equal and Distinct
- Dense Layer: 2 Layers
- Dense Activation: SoftMax
- Loss function: Categorical Crossentropy
- Loss metrics: Accuracy

Fig. 7 illustrates the built model.

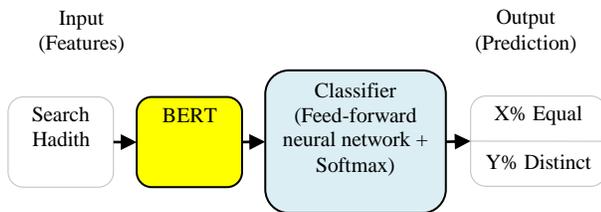


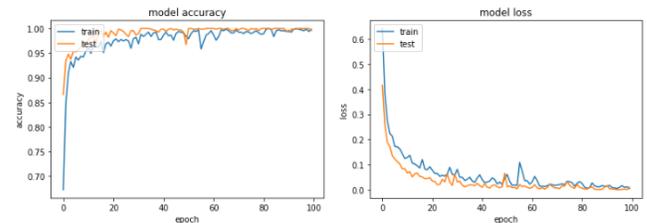
Fig. 7. BERT Model Illustration.

V. RESULT

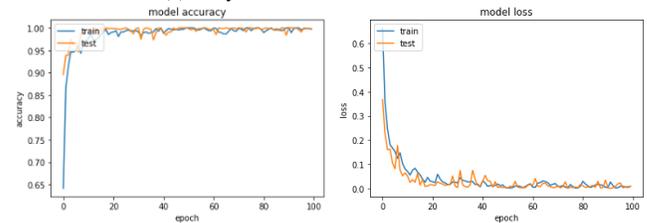
The BERT embedding model fine-tuning process is reported in Fig. 8, optimizing loss and accuracy values on each training and testing process iteration.

Table VI shows the accuracy result of the model built on the top of five different BERT pre-trained models. The BERT pre-trained model has choices that support the Indonesian language. The outcomes indicate that the BERT embedding model for contextual similarities gained average accuracy of 0.480060 and 0.956845 after fine-tuning, increasing by 0.4767886. The BERT pre-trained model indobenchmark/indobert-large-p2 achieved the best accuracy.

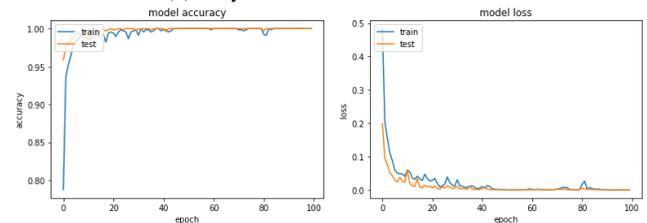
The fine-tune BERT embedding built on indobenchmark/indobert-large-p2 was then evaluated by manually comparing two texts of The Hadith of an-Nawawi with the Hadith text from the original books of Hadith. The result indicates an accuracy of 91.67%, as seen in Table VII.



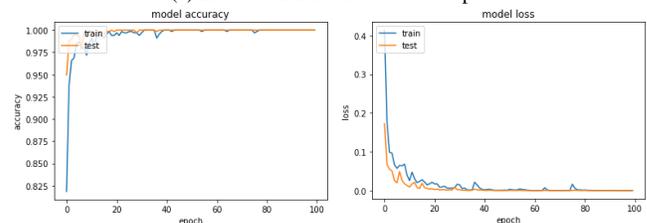
(a) Cahya/Bert-base-Indonesian-522M.



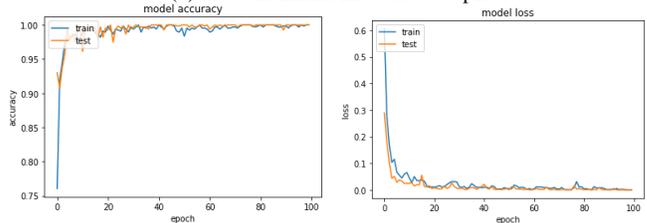
(b) Cahya/Bert-base-Indonesian-1.5G.



(c) Indobenchmark/Indobert-base-p1.



(d) Indobenchmark/Indobert-base-p2.



(e) Indobenchmark/Indobert-Large-p2.

Fig. 8. BERT Model Accuracy of Train and Test Process.

TABLE VI. MODEL ACCURACY

BERT pre-trained	Accuracy without Fine-Tuning	Accuracy with Fine-Tuning	Fine-Tuning Improvement
cahya/bert-base-indonesian-522M	0.626488	0.825893	0.199405
cahya/bert-base-indonesian-1.5G	0.630952	0.962798	0.331845
indobenchmark/indobert-base-p1	0.391369	0.997024	0.605655
indobenchmark/indobert-base-p2	0.373512	0.998512	0.625000
indobenchmark/indobert-large-p2	0.377976	1.000000	0.622024
Average	0.480060	0.956845	0.476786

TABLE VII. MANUAL EVALUATION

Takhrij Hadith Text	Sources Hadith Text	Results	Status
The Hadith of an-Nawawi 1	Shahih Bukhari 1	Equal 1.00	✓
	Shahih Bukhari 53	Equal 1.00	✓
	Shahih Muslim 3530	Equal 1.00	✓
	Sunan Abu Daud 1882	Equal 1.00	✓
	Sunan Ibnu Majah 4217	Equal 1.00	✓
	Sunan Nasai 74	Equal 1.00	✓
	Sunan Daruquthni 128	Equal 1.00	✓
	Shahih Ibnu Hibban 388	Equal 1.00	✓
	Shahih Muslim 10	Distinct 1.00	✓
	Shahih Muslim 11	Equal 0.58	✗
	Sunan Nasai 4904	Equal: 0.54	✗
	Sunan Nasai 4905	Distinct 0.99	✓
The Hadith of an-Nawawi 2	Shahih Bukhari 1	Distinct 1.00	✓
	Shahih Bukhari 53	Distinct 1.00	✓
	Shahih Muslim 3530	Distinct 1.00	✓
	Sunan Abu Daud 1882	Distinct 1.00	✓
	Sunan Ibnu Majah 4217	Distinct 1.00	✓
	Sunan Nasai 74	Distinct 1.00	✓
	Sunan Daruquthni 128	Distinct 0.99	✓
	Shahih Ibnu Hibban 388	Distinct 0.99	✓
	Shahih Muslim 10	Equal 0.91	✓
	Shahih Muslim 11	Equal 0.97	✓
	Sunan Nasai 4904	Equal 0.95	✓
	Sunan Nasai 4905	Equal 0.93	✓

VI. CONCLUSION AND FUTURE WORK

In this paper, a semi-supervised BERT word embedding with a feed-forward neural network classifier is proposed and implemented to produce a Hadith text representation and determine its contextual similarity level. This work focuses mainly for Hadith in the Indonesian text. The BERT fine-tuning raised average accuracy by 47.67%, with a 0.956845 mean accuracy in the training process. The pre-trained model Indobenchmark/indobert-large-p2 achieved the highest accuracy with training 1.00. The final manual evaluation achieved 91.67% accuracy on the Hadith contextual similarity identification. It means the proposed model in this study reaches the highest performance when used to conduct Hadith Takhrij (searching) for Indonesia Hadith text. As a future development of this experiment, there are some directions to be studied. The first direction is to extend the number of Hadith texts as an experiment dataset. That is needed because Hadith text is known to have some different Sanad and Matn structures. Another direction is in the order of automatic recognition of parts of the Hadith text. Identify its Sanad or Matn and then classify the Hadith text based on its structure.

REFERENCES

- [1] R. Baru, S. Hadzrullathfi, S. Omar, and B. Ibrahim, "Identifying False Hadith Guidelines," *Malaysian J. Islam. Stud.*, vol. 1, pp. 62–73, 2017.
- [2] S. R. Mohammad Najib, N. Abd Rahman, N. Kamal Ismail, N. Alias, Z. Mohamed Nor, and M. N. Alias, "Comparative Study of Machine Learning Approach on Malay Translated Hadith Text Classification based on Sanad," *MATEC Web Conf.*, vol. 135, p. 00066, 2017.
- [3] N. A. P. Rostam and N. H. A. H. Malim, "Text categorisation in Quran and Hadith: Overcoming the interrelation challenges using machine learning and term weighting," *J. King Saud Univ. - Comput. Inf. Sci.*, Mar. 2019.
- [4] Muahammad Khurram Khan and M.Alginahi Yaser, "The Holy Quran Digitization: Challenges and Concerns," *Life Sci. J.*, vol. 10, no. 2, pp. 156–164, 2013.
- [5] Ayub, "Matn Criticism and Its Role in The Evaluation of Hadith Authenticity," (*International J. Islam. Stud. Humanit.*, no. March, pp. 1–4, 2018.
- [6] A. Mahmood, H. Ullah, F. K., M. Ramzan, and M. Ilyas, "A Multilingual Datasets Repository of the Hadith Content," *Int. J. Adv. Comput. Sci. Appl.*, vol. 9, no. 2, 2018.
- [7] E. T. Luthfi, N. Suryana, and A. S. H. Basari, "Digital Hadith Authentication: a Literature Review and Analysis," *J. Theor. Appl. Inf. Technol.*, vol. 96, no. 15, 2018.
- [8] T. Rohman and U. Huda, "Methodology of Hadith Research : The Study of Hadith Criticism Metode Penelitian Hadis: Studi tentang Kritik Hadis," vol. 2, no. 1, pp. 73–84, 2019.
- [9] I. Suliaman et al., "The convenience of takhrij al-hadith through ICT apps: An exploratory analysis on selected hadith website and mobile apps," *Int. J. Civ. Eng. Technol.*, vol. 9, no. 11, pp. 2649–2660, 2018.
- [10] A. Rahman, "Pengenalan Atas Takhrij Hadis," *Riwayah J. Stud. Hadis*, vol. 2, no. 1, p. 146, 2017.
- [11] A. Izzan, *Studi Takhrij Hadis: Kajian Tentang Metodologi Takhrij dan Kegiatan Penelitian Hadis, Pertama*. Bandung: Tafakur, 2012.
- [12] Istianah and S. Wahyuningsih, "The hadith digitization in millennial era: A study at center for hadith studies, Indonesia," *Qudus Int. J. Islam. Stud.*, vol. 7, no. 1, pp. 25–44, 2019.
- [13] F. W. Kurniawan and W. Maharani, "Indonesian Twitter Sentiment Analysis Using Word2Vec," *2020 Int. Conf. Data Sci. Its Appl. ICoDSA 2020*, pp. 9–14, 2020.
- [14] R. A. Rajagede, "Improving Automatic Essay Scoring for Indonesian Language using Simpler Model and Richer Feature," *Kinet. Game Technol. Inf. Syst. Comput. Network, Comput. Electron. Control*, vol. 4, pp. 11–18, 2021.
- [15] M. N. Fakhruzzaman, S. Z. Jannah, R. A. Ningrum, and I. Fahmiyah, "Clickbait Headline Detection in Indonesian News Sites using Multilingual Bidirectional Encoder Representations from Transformers (M-BERT)," 2021.
- [16] S. M. Ozdemirci and M. Turan, "Case Study on well-known Topic Modeling Methods for Document Classification," *Proc. 6th Int. Conf. Inven. Comput. Technol. ICICT 2021*, pp. 1304–1309, 2021.
- [17] F. Koto, A. Rahimi, J. H. Lau, and T. Baldwin, "IndoLEM and IndoBERT: A Benchmark Dataset and Pre-trained Language Model for Indonesian NLP," pp. 757–770, 2021.
- [18] A. Marpaung, R. Rismala, and H. Nurrahmi, "Hate Speech Detection in Indonesian Twitter Texts using Bidirectional Gated Recurrent Unit," *KST 2021 - 2021 13th Int. Conf. Knowl. Smart Technol.*, pp. 186–190, 2021.
- [19] S. Viji, D. Tayal, and A. Jain, "A Machine Learning Approach for Automated Evaluation of Short Answers Using Text Similarity Based on WordNet Graphs," *Wirel. Pers. Commun.*, no. 0123456789, 2019.
- [20] A. Bornstein, "Beyond Word Embeddings Part 2." [Online]. Available: <https://towardsdatascience.com/beyond-word-embeddings-part-2-word-vectors-nlp-modeling-from-bow-to-bert-4ebd4711d0ec>. [Accessed: 19-May-2021].

- [21] R. K. Gupta, "Journey to BERT : Part 1," *medium.com*, 2020. [Online]. Available: <https://medium.com/swlh/journey-to-bert-part-1-a89413855a10>. [Accessed: 08-Aug-2021].
- [22] M. C. Kenton, L. Kristina, and J. Devlin, "BERT: Pre-training of Deep Bidirectional Transformers for Language Understanding," no. *Mlm*, 1953.
- [23] N. Reimers and I. Gurevych, "Sentence-BERT: Sentence embeddings using siamese BERT-networks," *EMNLP-IJCNLP 2019 - 2019 Conf. Empir. Methods Nat. Lang. Process. 9th Int. Jt. Conf. Nat. Lang. Process. Proc. Conf.*, pp. 3982–3992, 2020.
- [24] Y. Liu, Y. Zhou, S. Wen, and C. Tang, "A Strategy on Selecting Performance Metrics for Classifier Evaluation," *Int. J. Mob. Comput. Multimed. Commun.*, vol. 6, no. 4, pp. 20–35, 2014.
- [25] R. Gómez Bruballa, "Understanding Categorical Cross-Entropy Loss, Binary Cross-Entropy Loss, Softmax Loss, Logistic Loss, Focal Loss and all those confusing names," 2018. [Online]. Available: https://gomburu.github.io/2018/05/23/cross_entropy_loss/. [Accessed: 29-Aug-2021].
- [26] Ž. Vujović, "Classification Model Evaluation Metrics," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 6, pp. 599–606, 2021.
- [27] M. D. Al-Bugha and M. Mistu, *Al-Wafi: Syarah Hadis Arba'in Imam An-Nawawi (Edisi Indonesia)*. Jakarta: Qisthi Press, 2014.

UX Testing for Mobile Learning Applications of Deaf Children

Normala Mohamad¹

Department of General Studies
MARA Vocational Institute Beseri
Perlis, Malaysia

Nor Laily Hashim²

School of Computing
Universiti Utara Malaysia
Kedah, Malaysia

Abstract—Many studies are focusing on deaf children mobile learning. However, they are not concentrating on user experience (UX) testing. Current UX testing is based on existing UX evaluation models that are hard to apply due to the comprehensive measurements and lack of description on how to conduct evaluation for a more specific mobile learning process. Moreover, the existing UX evaluation models are not highlighted to be applied in testing UX for deaf children's mobile learning. Hence, this paper proposed questions for UX testing for deaf children's mobile learning to explore UX issues in offering an enjoyable learning application. Smileyometer is used to capture the data from deaf children after using a selected mobile learning application, KoTBaM and Learning Fakih. This study involves deaf children aged 7 – 12 years old familiar with the mobile application. The survey is divided into two sections: i) demographic information and ii) 24 questions that the respondent must answer using a smileyometer. The survey included 38 deaf children from Malaysian Deaf School. The participating deaf children completed the questionnaires with the assistance of their teachers after using the mobile learning application in the classroom. Yet, various issues needed to be addressed in order to improve the deaf children's user experience. Special exercises should be developed for deaf children connected to their school syllabus to consolidate their knowledge and self-learn everywhere. Furthermore, games elements should be adapted so the deaf children are able to learn while playing.

Keywords—User experience; UX testing; UX dimension; UX metrics; mobile learning application; deaf children; smileyometer

I. INTRODUCTION

UX testing is a method to measure how easy an application is. It is also performed by actual users for a selected application [1]. In determining the experience that occurs when a user interacts with a system [2], the result from this test can be employed in a system's design [3]. As Moran (2019) indicated, UX testing can determine if there are any problems in the design of an application, any parts that do not cover users' meet and learning about user behaviour [1]. Through the UX testing's result, the mobile learning application can be constructed appropriately focusing on end-user [2]. In addition, most mobile learning applications developed specifically for deaf children are less used than common applications for general users [4]. Deaf children require less effort to complete tasks and spend less time understanding the flow of mobile learning, which directly contributes to determining their UX.

Furthermore, there is a lack of UX testing for deaf children's mobile applications [5]. Thus, in order to perform UX testing that focuses on deaf children's mobile learning, appropriate questions that focus on the subject are essential [6]. It enhances UX questionnaires such as UEQ [7] and meCUE [8], which are developed for general UX testing. It is one of the efforts to provide equal rights and opportunities to this community. Thus, disabled children should not be left behind in adapting self-learning to ensure equal opportunities like ordinary children.

In Malaysia, disabilities are classified into few categories, such as mute, deaf, blind, mental disability, and physical disability [9]. Likewise, this study focuses on deaf children since the number of deaf people is increasing yearly [10] and is expected to grow to 700 million in 2050 [11]. On the other hand, [12] reported that in 2025, the number of smartphone users will increase to 30.74 million in Malaysia. The deaf community may contribute to growing these statistics. Thus, UX of the deaf should be a highlight in developing an excellent mobile learning application.

Mobile learning application has proven to increase learning interest and motivate deaf children [10]. Moreover, in the Covid-19 pandemic, deaf children have to self-learn to ensure they are not left behind in their education even though the pandemic situation. Hence, mobile learning applications become a vital aid for them to learn and do revision. Consequently, UX testing has to be done to ensure the deaf mobile learning applications are entirely designed and give a good experience for them. Indirectly, it will overcome the less-used issues of existing deaf children mobile learning [4].

The UX testing can be conducted efficiently if the assessment is focused on mobile learning applications for deaf children [6]. Therefore, some questions are adopted from UEQ [7] and meCUE [8], where both of these instruments contain general UX questionnaires.[13] in their work have proposed usability questionnaires for deaf mobile application interfaces. All the questions are modified to make them related to deaf children's mobile learning. These questions are applied during the UX testing where children will answer them using Smileyometer after they have used the selected mobile learning applications. Smileyometer is a familiar method used for study among children [14] [15]. The deaf children are assisted by their teachers to complete the smileyometer since the researchers are not allowed to communicate directly with the deaf children in the classroom. The deaf children are more

comfortable with their teachers than outsiders [16] [17]. Thus, the questionnaires are distributed through their teachers, who briefed them about the UX testing process.

There are many previous UX studies among children but very few of them concentrated on disabled children, especially deaf children. Thus, this study is needed to measure the UX among deaf children using mobile applications designed specifically for them. However, this study is limited to testing on children who are deaf only since there are many types of deafness in Malaysia. According to the Social Welfare Department of Malaysia (2018), deafness can be classified into three, which are deaf only, deaf and dumb, and deaf with other disabilities [9]. Thus, the participants for this study will be selected among the deaf-only children by their teacher.

This paper is aim to test the UX of mobile learning application for deaf children. Hence, it was organized as follows: introduction, background, material and method, results and discussions, and conclusion.

II. BACKGROUND

This section covers past studies regarding UX of mobile learning for children since UX among disabled children is very few [5] and selection questions related to UX dimensions suggested in previous studies. The background of smileyometer as an instrument in collecting data is also explained in this section. It is also supported by some previous studies that applied this fun toolkit [18].

There are many studies involved in UX testing among children, such as [15][17][19]. Those studies are used selected mobile learning applications during UX testing sessions. [15] were studied about ascertaining the UX of Word Mania among kids at UUM International School, Sintok Malaysia. Nevertheless, this study has not applied any questionnaires even though they use a smileyometer to capture the data. Based on their finding, the kids need more time to answer the questions in Word Mania. Thus, the simplest task should be involved in children's mobile learning applications.

While [17] had test UX among 64 children aged 7-12 years old using Fantasy Land. The children are required to answer UEQ questionnaires. However, some questions are difficult to understand since advanced terms are involved, so [17] have to explain the terms using simple sentences that suit the children's age. Thus, the UEQ questionnaires should be improvised to suit the capabilities of the children. For the same purpose of study, [19] also studied UX among children using mobile technology. They are motivated to learn it since there is a lack of UX studies regarding educational applications such as science and mathematics. So, this study is to explore the hedonic factors such as enjoyable, exciting, upsetting, and confusing experiences. [19] found that gender, culture, and religion are important matters that affect the children's experience.

On the other hand, there are minimal UX testing among deaf children. [20] studied UX testing among attention deficit hyperactivity disorder (ADHD) children. The UX testing was involved ADHD children from Mexico. Due to the covid-19 pandemic, the children had very limited face-to-face activities

in school. Thus, [20] design a learning application using virtual reality (VR) technology. The children feel like in a face-to-face class when they are using this application. [20] obtained satisfactory experience among ADHD children who are using the VR educational application. While [21] were studied UX testing among autistic children in comparing three prototypes of learning applications. Smileyometer, fun sorter, and again-again table are used to collect data in this study. Smileyometer has been applied before and after the study. The children are given around 5-10 minutes to play with the application before completing the instrument. Based on this study, [21] concludes that very few different experiences among the three prototypes and few usability issues to the specific prototype.

Many research cover UX of mobile learning among children, which recommended some dimensions such as emotion [21][22][23][24][26], satisfaction [22][23][24][25], efficiency [17][22][23][25], and effectiveness [22][23][26]. Likewise, deaf accessibility is also considered as a dimension in developing the questions for this study since it is highlighted on the deaf itself [13]. As mentioned earlier, studies regarding the UX testing of mobile learning among disabled children are minimal [2]. Thus, the mentioned studies were taken based on targeting children.

Most of the studies related to children use smileyometer in capturing the data [26]. Smileyometer is being chosen, and it was believed in capturing data from children [27]. Smileyometer is one of the fun toolkits besides fun sorter and again-again table. It was introduced by Janet C. Read [18] in 2006.

There are five emojis, as shown in Fig. 1. These emojis represent scores chosen by the participant. The smileyometer scale has five primary emotional states to choose from as portrayed in Fig. 1: From the left: (a) Awful; (b) Not Very Good; (c) Okay; (d) Really Good; (e) Fantastic. Every question is provided with smileyometer. For example, if a participant chooses an awful emoji, the participant strongly disagrees with the question. In contrast, if a fantastic emoji is remarked, the participant strongly agrees with the question.

Several studies applied smileyometer, such as evaluating the user experience of playful interactive learning interfaces with children [14], ascertaining the UX of the word mania mobile app for children using fun toolkit v3 [15], and understanding the fidelity effect when evaluating games with children [21]. Moreover, smileyometer is used in highlighting the children's momentum feeling [25]. Hence, smileyometer is chosen for this study in evaluating the UX of mobile learning for deaf children. Based on previous research that using smileyometer proved that this is the interactive scale in obtaining data from children [25].

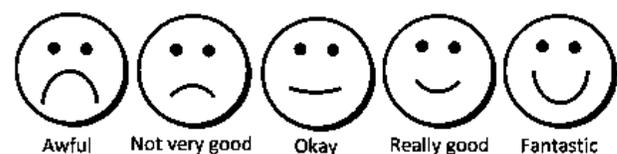


Fig. 1. Smileyometer Tating Scale.

Two mobile learning applications for deaf children, which are KoTBaM and Learning Fakh, were chosen. KoTBaM is a learning application developed based on Bahasa Isyarat Komunikasi for deaf children in Malaysian Deaf School [28]. The participants might feel easy to understand content of KoTBaM since they have learned about the content in school. Besides, some videos on constructing sentences using sign languages were provided too, giving participants more attention to learning [29]. While Learning Fakh is a learning game application for deaf children developed based on the Fakh method [30]. The Fakh method is a technique applied by the teachers in Malaysian Deaf School in teaching Hijahiyah letters using sign languages. It has quizzes elements to make the lesson fun as claimed by González et al. that enjoyment should be provided to avoid boredom and improve effective state among the children [31]. The quizzes are divided into three levels which are easy, medium, and hard. These two applications are chosen since the content of the application are related to lesson in school. Besides that, there are also recommended by the teachers of deaf children.

Besides that, as stated earlier, the UX dimensions can be a reference for this study in developing UX metrics for UX testing of deaf children's mobile learning. Since smileyometer was very familiar in previous UX studies among children, it also measured the UX among deaf children. Hence, a set of questionnaires have been developed based on the dimensions applied in previous studies. It was discussed thoroughly in the next section.

III. MATERIAL AND METHOD

This study aims to evaluate the UX of deaf children's mobile learning by the actual user, and it was briefly explained in this section. The process of identifying the selected questions is out of the scope of this paper. This study was performed to measure UX for two learning applications which are KoTBaM and Learning Fakh using smileyometer and adheres to [24] UX testing approach on how to conduct UX test in a classroom environment which is used by many past researchers [14][17][25] and finds an approachable method. There are three steps involved in evaluating UX of deaf children's mobile learning applications for this study.

A. Identifying the Participants

A total of 38 deaf children aged between 7 to 12 years old has been recruited from Malaysian Deaf School. The pupils are screened based on their experience of working on mobile and mobile applications. According to Lazar et al., 10 participants are substantial for this study since they are deaf and considered disabled people [32]. Purposive sampling is used in this study which common approach in identifying a user in UX [33]. Purposive sampling means that participants are selected based on the needs of the study. This approach was applied in a previous study that involved a deaf sample, such as [7][17][18]. Teachers select the deaf participants based on their familiarity in using mobile learning applications.

B. Instrument's Development

A set of questionnaires are adapted from UEQ [7], meCUE [8], and questionnaires from [13] that are supported to five

dimensions, as shown in Table I. The arrangement of words and understandability of the questionnaires for the participants are checked by an expert who is an author of textbook Bahasa Isyarat [28] in Malaysian Deaf School. The questionnaires use smileyometer scale to tick by the participants after interacting with the KoTBaM and Learning Fakh.

Twenty-four survey questions are designed for this study. The questions are based on existing UX questionnaires, as mentioned earlier in the previous section. The metrics depend on five dimensions: emotion, satisfaction, efficiency, effectiveness, and deaf accessibility. The distribution number of questions is stated in Table I.

TABLE I. QUESTIONNAIRE CONTENT ON UX DIMENSIONS OF DEAF CHILDREN MOBILE LEARNING

Dimension	No. of question
Satisfaction	4
Deaf accessibility	4
Efficiency	7
Effectiveness	4
Emotion	5

According to Table I, five questions regarding emotion dimension, four questions about satisfaction, deaf accessibility, and effectiveness dimensions, while seven focus on the efficiency dimension. All the questions are going for a reliability test to know how reliable the questions are. The test uses SPSS to get the Cronbach alpha value. According to Sekaran, a reliability coefficient of 0.70 or higher is considered acceptable, while 0.90 to 1.00 consider having excellent coefficient reliability among the items in the questionnaire. Reliable coefficient survey questions for this study is 0.967 as shown in Table II. Thus, it was considered acceptable to use in this study [34].

C. Test Administration

Participants have been given a brief description of the UX testing conducted. Since the participants are deaf, Malaysian Deaf School teachers become translators throughout the evaluation process. All the participating documents have been passed to the teachers during the briefing session. It is because the researchers are not permitted to meet the participants directly due to the covid-19 pandemic. The Malaysia Ministry of Education limits physical activities to curb the transmission of the virus. Therefore, translators are given space in translating the instructions into sign language for the participants. Two mobile learning applications, KoTBaM and Learning Fakh are involved during the session. The participants are given 5 to 10 minutes to use every learning application. They are allowed to end the session early if they are feeling bored while using the application. Once participants understand and agree, testing is conducted. The participants are required to answer the survey and assist by their teacher.

D. Data Collection and Data Analysis Method

Every dimension has been tested through the questionnaires during the UX testing session. The feedback has been analyzed using the mean value for each dimension

involved, as suggested by [8] to compare the two learning applications. The mean value can be determined which applications are giving good UX based on the dimensions analyzed. Thus, the analyzed result can be used as guidance to improve the design of the learning application in the future.

TABLE II. UX QUESTIONNAIRE OF DEAF CHILDREN MOBILE LEARNING

Dimension	Items	Mean	Standard Deviation	Cronbach's alpha
Satisfaction	Suitability of the content for deaf children learning	3.867	1.157	0.967
	Following the syllabus of deaf children learning	3.800	1.246	
	Repetition to use the apps	3.933	1.118	
	Feel to use the apps daily	4.033	1.134	
Deaf Accessibility	Vibration/flash helps as alerting	4.100	1.189	
	The alerting used is very useful	3.600	1.108	
	Help video is very helpful	3.750	1.144	
	Text translation is very convenient in assisting understanding	3.900	1.203	
Efficiency	Easy to achieve the learning goals	3.867	1.228	
	Less time needed to understand the usage of menu/button	3.817	1.214	
	Less effort to complete the task	4.083	1.046	
	Novelties of content	4.033	1.089	
	Innovativeness of the task provided by the apps	4.000	1.042	
	Readability of the content	3.933	1.039	
	Easy to learn the content	3.867	1.096	
Effectiveness	Clearness of the content	3.817	1.066	
	Able to perform all tasks given by the learning apps	3.900	1.175	
	Correctness of apps flow	3.733	1.103	
	Easy apps handling	3.733	1.118	
Emotion	To what extent the colour and font used are pleasing in appearance	4.100	1.189	
	The stylish of the apps	3.600	1.108	
	The apps creatively design	3.750	1.144	
	Feel happy and knowledgeable with apps experience	3.900	1.203	
	Enjoy with the presentation of the learning apps.	4.100	1.189	

IV. RESULT AND DISCUSSION

This section reports the result of UX testing. They are classified into two (2) sub-sections, which are 1) demographic information and 2) data results. The data was examined through SPSS to report on the results. The data analysis yields a comparison of which learning application gives better UX for deaf children.

A. Demographic Information

This part aims to assess the demographic analysis of the users involved in the UX testing in terms of gender and age.

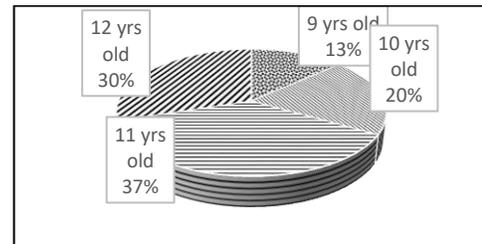


Fig. 2. Demographic Information on Age.

For the UX testing, 38 aged ranged between 7 and 12 years old participants were chosen due to the availability of the selected schools. Most participants are age 11 years old, stating 37% followed by 30% for participants aged 12 years old. At the same time, participants aged ten and nine years old have shown 20 % and 13% of the participants involved (Fig. 2).

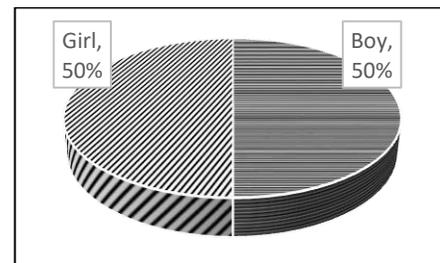


Fig. 3. Demographic Information on Gender.

The participants are from three Malaysian Deaf Schools (MDS): MDS Johor Bahru, MDS Perlis, and MDS Temenggong, Segamat. As shown in Fig. 3, 50% were boys while the rest were girls. Among them, MDS Perlis participants were the highest, consisting of 43%, MDS Johor Bahru were 40% of a total participant, and finally, MDS Temenggong, Segamat comprised 17% of overall participants (refer Fig. 4).

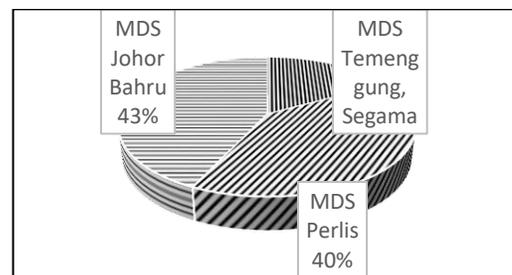


Fig. 4. Overall Participants.

B. Data Analysis Result

The data was collected through survey questions (refer to Table II) that were rated by the participants using smileyometer. The data have been analyzed by each dimension involved in this model through their mean value. It is also presented in a graphical bar chart to show the comparison between criteria in the dimension. Meanwhile, the results are also presented in comparison between two learning applications: Learning Fakih and KoTBaM. Learning Fakih is a prototype for a mobile learning application, while KoTBaM is a learning application that has been published and can be downloaded from the play store.

As presented in Fig. 5, two mobile learning applications have been evaluated for UX testing among deaf children. The mean value is shown based on the dimension involved. The effectiveness dimension for KoTBaM has stated the highest mean value, which is 4.4, compared to the highest mean value for Learning Fakih, which is 3.75 that stated in the emotion dimension. The satisfaction dimension stated the lowest mean value for both applications, 3.69 for KoTBaM and 3.4 for Learning Fakih. However, all mean values for KoTBaM are higher than Learning Fakih, as reported in Fig. 5. In this case, it can be summarized that majority of the deaf children will choose KoTBaM compared to Learning Fakih since all the mean values on all dimensions for KoTBaM are higher.

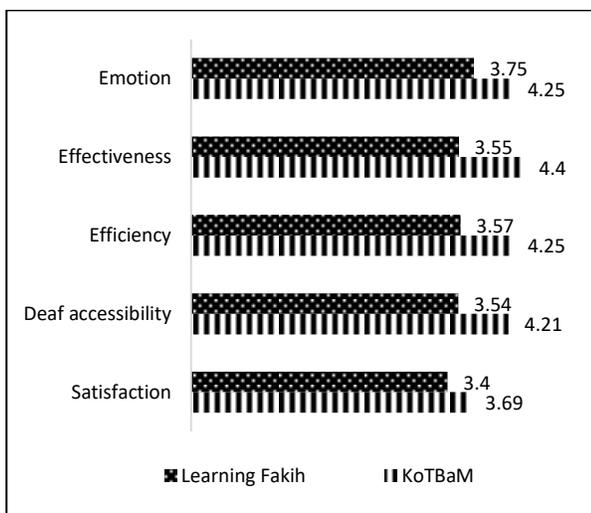


Fig. 5. Result of UX Testing by Dimensions.

Based on personal communication between the teachers who conduct the UX testing session, the deaf children are quite slow to answer quizzes at the hard level provided in Learning Fakih. It may be difficult for them to remember [35] the sequence of Hijahiyah letters and baris orderly. It may make the questions quite difficult for them to answer since they cannot remember new things quickly. Likewise, they were pretty enjoyed the learning since they are able to play it while learning. Hence, repetition is significant to remember and memorize the thing that they had learned.

Furthermore, KoTBaM is more accessible for deaf children compared to Learning Fakih. Deaf children need guidance, and it was provided in KoTBaM but not in Learning Fakih. KoTBaM provides a user manual to guide deaf children

on how to use the learning application. On the other hand, the user manual also can be a reference for the normal user such as teachers or parents of deaf children in using the deaf learning application. These features may make deaf children feel more confident to use it. It may contribute to the mean value of deaf accessibility for KoTBaM being higher than Learning Fakih.

Moreover, the contents in KoTBaM are based on the syllabus that deaf children have learned in their schools. It looks like the deaf children do revision for the subject through KoTBaM. Every word in the contents of KoTBaM is provided with videos of sign language compared to Learning Fakih, which only provides images of the hand gestures of the sign language. The contents do not focus only on the topic, but other lessons included like alphabets, numbers, and name of animals. The sign languages are provided only for *hijahiyah* letters but not for others. The deaf children might be confused about the content since it involves many subjects. Therefore, the Learning Fakih is not practical for deaf children, affecting the mean value of the effectiveness dimension rated by the participants.

However, there are no quizzes or exercises provided by KoTBaM, but there were some quizzes in Learning Fakih. Quizzes and exercises may need to test the understandability of the deaf children about their learning. The deaf children do not perform the quizzes in Learning Fakih since they feel that it is so hard for them to choose the correct answer. As claimed by Marschark & Spencer, the deaf children are slower four times than normal children [35]. Thus, the exercise provided should be easier and simpler for them.

V. CONCLUSION

In conclusion, the survey questions of this study can be a guideline to measure for a more pleasant and practical deaf children's mobile learning besides can be improved the basis of learning for this special education children. Besides that, the result also can be a reference for UX practitioners and mobile application developers in designing a practical and enjoyable mobile learning application for deaf children. However, the results are evaluated among deaf children only and to be applied on another two variants of the deaf, which are deaf and dumb, and deaf with other disabilities.

In addition, these survey questions can also be applied for UX testing for other mobile learning applications for deaf children. The proposed dimensions in this work are customized and highlighted on deaf accessibility. Hence, other disabilities are not recommended to utilize this survey. The result may not be accurate if these dimension are tested for other disabilities since different disabilities may need different accessibility features to support learning using mobile applications. In the future, the authors may extend this study to investigate how these dimensions are associated to one another in measuring a UX for mobile learning application for deaf children.

ACKNOWLEDGMENT

The authors would like to thank everyone involved directly or indirectly with this project, especially research grant under Fundamental Research Grant Scheme

(FRGS/1/2020/ICT10/UUM/02/1), for financial support throughout the research study. Also, Majlis Amanah Rakyat and Ministry of Education (MOE) for their collaborations in the literature work. Besides that, special thanks to Mdm. Hazirah Abdul Pisal, Mdm. Rodhiha Ma'rof, and Mdm. Mahyani Masri from the selected Malaysian Deaf School for involving in the UX testing process.

REFERENCES

- [1] Moran, K., "Usability testing 101", 2019. <https://www.nngroup.com/articles/usability-testing-101/>
- [2] ISO 9241-11, "Ergonomics of human-system interaction" 2018. In International Organization for Standardization.
- [3] Dix, A., Finlay, J., Abowd, G. D., and Beale, R. "Human-Computer Interaction" (Third edit). Pearson Education, 2004.
- [4] Yeratziotis, A., and Panayiotis, Z., "Interactive Software Technology for Deaf Users: Mapping the HCI Research Landscape that Focuses on Accessibility" Universal Access in Human-Computer Interaction. Access to Today's Technologies: 9th International Conference, vol. 9175, no. 8, pp. 253–264, 2015.
- [5] Kraveva, R., and Kravev, V., "An Evaluation of The Mobile Apps for Children with Special Education Needs Based on The Utility Function Metrics", International Journal on Advanced Science, Engineering and Information Technology, vol. 8, no. 6, pp. 2269-2277, 2018.
- [6] Chen, Z., and Zhu, S., "The research of mobile application user experience and assessment model", in Proceedings of 2011 International Conference on Computer Science and Network Technology, pp. 2832-2835, 2011.
- [7] Schrepp, M., "User Experience Questionnaire Handbook. User Experience Questionnaire", 2019. <https://www.ueq-online.org/Material/Handbook.pdf>
- [8] Minge, M., Thüring, M., Wagner, I., and Kuhr, C. V., "The meCUE questionnaire: a modular tool for measuring user experience", Advances in Ergonomics Modeling, Usability & Special Populations, pp. 115-128, 2016.
- [9] Social Welfare Department Malaysia, "Pendaftaran Orang Kurang Upaya (OKU)", 2021. <https://www.jkm.gov.my/jkm/index.php?r=portal/left&id=UnN2U3dtUHhacVN4aHNpPbUIPayt2QT09>.
- [10] Bitar, H., Alsulami, R., and Alahmadi, S., "Building and evaluating an Android mobile App for people with hearing disabilities in Saudi Arabia to provide a real-time video transcript: a design science research study", Romanian Journal of Information Technology and Automatic Control, vol. 31, no. 3, pp. 109–122, 2021.
- [11] World Health organization, "WHO: 1 in 4 people projected to have hearing problems by 2050 World Health Organization", 2021. <https://www.who.int/news/item/02-03-2021-who-1-in-4-people-projected-to-have-hearing-problems-by-2050>.
- [12] Statista, "Number of Smartphone Users in Malaysia from 2010 to 2020 and A Forecast Up to 2025, 2021. <https://www.statista.com/statistics/494587/smartphone-users-in-malaysia/>.
- [13] Nathan, S. S., "A Usability Evaluation Model for Hearing Impaired Mobile Applications Interfaces", University Utara Malaysia, 2017.
- [14] Alhussayen, A., Alrashed, W., and Indriasari, E., "Evaluating the user experience of playful interactive learning interfaces with children", Procedia Manufacturing, vol. 3, no. 2015, pp. 2318–2324, 2015.
- [15] Hussain, A., Mkpjojiogu, E. O. C., Kamal, F. M., and Lateef, H. M., "Ascertaining the UX of the word mania mobile app for children using fun toolkit v3", International Journal of Recent Technology and Engineering, vol. 8, no. 2 Special Issue 2, pp. 202–205, 2019.
- [16] Mich, O., "Evaluation of Software Tools with Deaf Children", in ASSETS'09, pp. 235–236, 2019.
- [17] Mispa, K., Mansor, E. I., and Kamaruddin, A., "Evaluating Children ' s User Experience (UX) Towards Mobile Application : the Fantasy Land Prototype", in Proceedings The 5th ACM In Cooperation International Conference in HCI and UX, pp. 46–54, 2019.
- [18] Read, J. C., and MacFarlane, S., "Using the fun toolkit and other survey methods to gather opinions in Child Computer Interaction", in Proceeding of the 2006 Conference on Interaction Design and Children, pp. 81–88, 2006.
- [19] Khlaif, Z. N., Itmazi, J., Farid, S., Shaqour, A. Z., and Kouraïchi, B., "Exploring children experience with educational mobile technology", Research in Learning Technology, vol. 27, 2019.
- [20] Reyes, H. C., Arteaga, J. M., Condori, K. V., and González, M. L. B., "A Lean UX Process Model for Virtual Reality Environments Considering ADHD in Pupils at Elementary School in COVID-19 Contingency", Sensors, vol. 21, no. 11, pp. 1–21, 2021.
- [21] Sim, G., Cassidy, B., and Read, J. C., "Understanding the fidelity effect when evaluating games with children", in ACM International Conference Proceeding Series, pp. 193–200, 2013.
- [22] Cano, S., Arteaga, J. M., Collazos, C. A., and Amador, V. B., "Model for Analysis of Serious Games for Literacy in Deaf Children from a User Experience Approach", in Proceedings of the XVI International Conference on Human Computer Interaction, pp. 1–9, 2015.
- [23] Cano, S., Collazos, C. A., Flórez Aristizábal, L., Gonzalez, C. S., and Moreira, F., "Towards a methodology for user experience assessment of serious games with children with cochlear implants", Telematics and Informatics, vol. 35, no. 4, pp. 993–1004, 2018.
- [24] Susanne, M., Roman, B., & Markku, T., "Evaluating User Experience of Autistic Children through Video Observation", in CHI 2013: Changing Perspectives, pp. 463–468, 2013.
- [25] Ibrahim, N., Fatimah, W., Ahmad, W., and Shafie, A., "User experience study on folktales mobile application for children's education", in 9th International Conference on Next Generation Mobile Applications, Services and Technologies, pp. 353-358, 2015.
- [26] Read, J. C., "Evaluating Artefacts with Children : Age and Technology Effects in the Reporting of Expected and Experienced Fun", International Conference on Multimodal Interaction., pp. 241–247, 2012.
- [27] Bernhaupt, R., "User Experience Evaluation Methods in the Games Development Life Cycle", In Game User Experience Evaluation: Human-Computer Interaction Series, pp. 1–8, 2015.
- [28] Ma'rof, R., Ahmad, N. A., and Mesnan, M. N. A., "Bahasa Isyarat Komunikasi (Buku Aktiviti)", Dewan Bahasa dan Pustaka, 2016.
- [29] Alias, A., Azahari, M. H., and Ismail, A. I., "Enhancing Learning Ability Among Deaf Students By Using Interactive Images", International Journal of Education and Research, vol. 3, no. 3, pp. 285–296, 2015.
- [30] Hussain, A., Jomhari, N., Kamal, F.M., and Mohamad, N., "mFakih: Modelling Mobile Learning Game to Recite Quran for deaf Children", International Journal on Islamic Applications in Computer Science and Technology, Vol. 2, Issue 2, pp. 8-15 2014.
- [31] González-González, C., Toledo-Delgado, P., Collazos-Ordoñez, C., and González-Sánchez, J. L., "Design and analysis of collaborative interactions in social educational videogames", Computers in Human Behavior, vol. 31, no. 1, pp. 602–611, 2014.
- [32] Lazar, J., Feng, J. H., and Hochheiser, H., "Research Methods in Human-Computer Interaction", in Research Methods in Human-Computer Interaction. Pp. 493-518, 2017.
- [33] Gertz, G., and Boudreault, P., "Deaf Gain : Raising the stakes for human diversity", in A. Soloman (Ed.), The SAGE Deaf Studies Encyclopedia. University of Minnesota Press. 2016.
- [34] Sekaran, U., "Research methods for business: A skill building approach", John Wiley & Sons, New York, 2006.
- [35] Marschark, M., and Spencer, P. E., "The Oxford Handbook of Deaf Studies in Language", Oxford University Press, 2016.

The Regularization Effect of Pre-activation Batch Normalization on Convolutional Neural Network Performance for Face Recognition System Paper

Abu Sanusi Darma¹

University Sultan Zainal Abidin, Faculty of Informatics and Computing, Campus Besut, 22200, Terengganu, Malaysia¹
Al-Qalam University Katsina, School of Natural & Applied Sciences, Department of Mathematical Sciences, P.M.B. 2137, Katsina, Nigeria¹

Fatma Susilawati Binti Mohamad²

University Sultan Zainal Abidin
Faculty of Informatics and Computing
Campus Besut, 22200
Terengganu, Malaysia

Abstract—Face recognition is of pronounced significance to real-world applications such as video surveillance systems, human computing interaction, and security systems. This biometric authenticating system encompasses rich real human face characteristics. As such, it has been one of the important research topics in computer vision. Face recognition systems based on deep learning approaches suffer from internal covariate shift problems that cause gradients to explode or gradient disappearance, which leads to improper network training. Improper network training causes network overfitting and computational load. This reduces recognition accuracy and slows down network speed. This paper proposes a modified pre-activation batch normalization convolutional neural network by adding a batch normalization layer after each convolutional layer within each of the four convolutional units of the proposed model. The performance of the proposed model is validated with a new dataset, AS-Darmaset, which is built out of two publicly available databases. This paper compared the convergence behavior of four different CNN models: the Pre-activation Batch Normalization CNN model, the Traditional CNN without Batch Normalization, the Post-Activation Batch Normalization CNN model, and the Sparse Batch Normalization CNN Architecture. The evaluation results show that the recognition performance of Pre-activation BN CNN has training and validation accuracies of 100.00% and 99.87%, the Post activation Batch normalization has 100.00% and 99.81%, and the traditional CNN without BN has 96.50% and 98.93%. The sparse batch normalization CNN has 96.25% and 97.60% success rate, respectively. The result shows that the Pre-activation BN CNN model is more effective than the other three deep learning models.

Keywords—Face recognition; pre-active batch normalization; convolutional neural network

I. INTRODUCTION

Face recognition systems have witnessed a lot of recent advancements in terms of selective human-machine interfaces, such as the future ATM authentication and authorization system, driving licenses identification and verification, and so on [1]. Although face biometric authentication systems have made significant progress and are now widely used in a variety of applications such as criminal investigation, lie detection systems, clinical medicine, distance education, security systems, access control, video surveillance, commercial areas,

and even use in social networks such as Facebook [2, 3]. The standard tradition machine learning for face recognition are still plagued by a slew of issues and are only effective in a limited number of scenarios. In terms of major intrapersonal changes in illumination, facial expressions, posture, occlusions, views, and other factors, that lead their performance begins to deteriorate [4]. Furthermore, light intensity, the number of light sources, light direction, and camera angle are all unpredictable. However, these methods extract a small number of image features in lower recognition accuracy, which cannot satisfy human face recognition in complex conditions [5]. With deep learning-based approaches for image feature extraction, superior performance has been achieved. Convolutional Neural Network has become a popular method for face recognition system. The CNN, which automatically extracts a variety of features of the image and classify, has good robustness to complex environments [2]. The architecture of CNN is inspired by biological processes and loosely based on the responses of the neurons in the receptive field of the human brain visual context [7]. Convolutional Neural Networks (CNN) are usually composed of convolutional layer, normalization layer, activation layer, max-pooling layer, and fully connected layers [8]. The driving factor for their successes has been the abundance of available data via the internet and the huge efforts of the research community to create large hand label dataset such as ImageNet [9]. A recent improvement called batch normalization [8], accelerate the learning process by computing batch statistic, it makes normalization an internal part of the model architecture. These changes allow for much faster convergences, diminishes the impact of model initialization, and act as a regularization method [10].

In this paper, we explore the impact of key architectural elements of a convolutional neural network. These are the batch normalization and dropout layers in the context of pre-active batch normalization architecture of convolutional neural networks [11].

II. MAJOR CONTRIBUTION

The main contribution of this paper is to enhance the performance of Convolutional neural network architecture for face recognition with a higher recognition rate. In this research, we built an improved Pre-active Batch Normalization CNN

algorithm by applying a batch normalization layer immediately after each convolutional layer before the non-linear (ReLU) activation function to perform the normalization operation thereby reducing the internal covariate shift. We again added a dropout layer in between the two fully connected layers to help improve the network performance. The general structure of the proposed model is made up of four (4) convolutional units, one dropout layer, two fully connected layers, one softmax layer, and one classification layer. First, confirm that you have the correct template for your paper size.

The rest of this paper is organized as follows: Section discusses various works of literature. The proposed research methodology is highlighted in Section IV. Sections V and VI present the research experiments. Finally, Section VII consists of the research paper conclusions.

III. RELATED WORK OF LITERATURES

Compare to previous literature work, our main contribution is the application of four batch normalization layers to the four convolutional units of a simple convolutional neural network for face recognition application. A dropout layer is also added in between the two fully connected layers. This is done to prevent gradient exploding or gradient disappearance, prevent network overfitting and increase performance with higher recognition accuracy. Convolution Neural Network was first proposed by LeCun and it was firstly applied in handwriting recognition [12]. Literature [3] proposed a modified CNN architecture for face recognition application by adding two normalization layers for the output of the first and last convolutional layers to accelerate the network. The result showed a satisfying recognition rate of 98.8%. Literature [2]. Explored the efficiency of a new sparse batch normalization CNN to overcome the problem of gradient disappearance and gradient exploration faced by the facial expression recognition model. There proposed model uses continuer convolution at the begging of the network to enhance the integrity of the facial regional features. Batch Normalization is sparsely added to facilitate network training. The experiment shows that the model has a sufficient performance of 96.87% recognition rate to satisfy the 7 classes of the express. Literature [13] proposed a CNN model for a real-time face recognition system. Model architecture has no batch normalization layer, but it has a dropout layer. The performance of the model architecture is evaluated by turning various parameters of the model to enhance the recognition rate. Maximum accuracy of 98.75% and 98.00% is obtained. Literature [14] proposed an end-to-end

face recognition system based on 3D face texture. Combining the geometric invariants, histogram of orientated gradient, and the fine-tuned Residual Neural Network. Batch Normalization is added to each convolutional layer to affine transformation on the input of each layer. The experimental results show that the best top 1 accuracy is up to 98.26% and the top 2 accuracy is 99.40% respectively. Literature [15] tested the performance of their proposed CNN for face recognition with three well-known image recognition methods PCA, LBPH, and KNN. Batch normalization and dropout are not employed in the model architecture. The experimental result shows that the proposed CNN has obtained the best recognition rate of 98.3%. The proposed method based on CNN outperforms the state-of-the-art methods. Literature [16] proposed to used and integrate deep learning CNN for human face Analytic and recognition for diversified applications. In their study the profound learning-based methodology of CNN with fuzzy logic is introduced, so the higher level of exactness in the face grin should be possible. With this method, the predictive feature of the human face can be used for a criminal investigation of the social analytics-based application. This model was training without a batch normalization layer. The model achieves a recognition accuracy of 98.12%. Literature [17] Evaluates the robustness of three well-known approaches by combining CNN as a powerful feature extraction algorithm followed by SVM as a high classifier and PCA for feature dimensional reduction technique. The result of the combined models provides a significant performance improvement and enhances recognition rate up to 95.2%.

IV. METHODOLOGY

A. Pre-Activation-BN-Convolution Neural Network (PABNCNN) Approach for Training and Features Classification

In this research, we aim to enhance the performance of the face recognition system, based on Deep Learning Convolutional Neural Network (CNN). The study proposed to reduce covariate shift, gradient disappearance and gradient explosion for better network convergence. Therefore, to achieving these aims the study proposed a new method called Pre-Activation Batch Normalization Algorithm. The method is powerful in preventing vanishing gradient and overfitting of the model. The proposed model is trained with Mini-Batch Stochastic Gradient Descent training algorithm. The block scheme of the proposed algorithm is shown in Fig. 1.

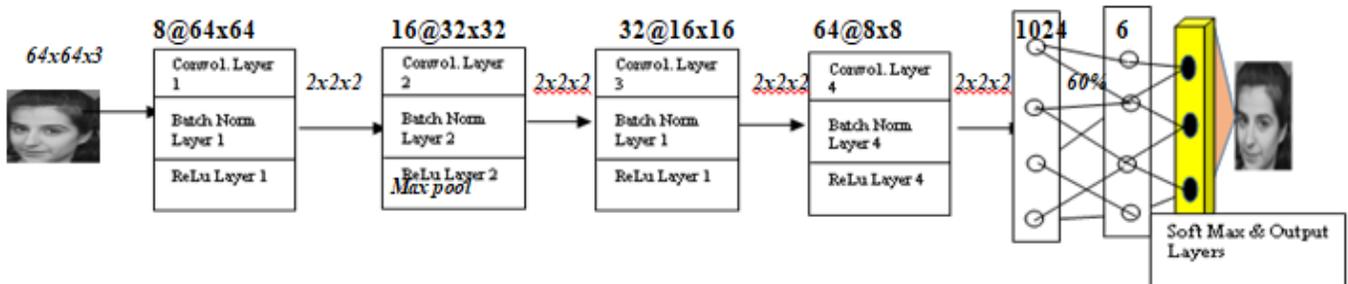


Fig. 1. The Structure of the Proposed Pre-Activation BN-CNN.

- Convolutional Neural Network (CNN)

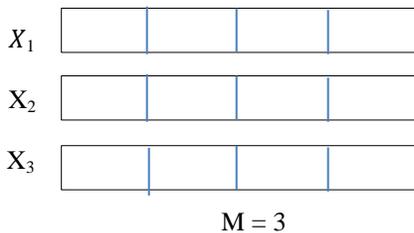
A CNN is made up of numerous layers with image processing activities that are built into its structure. This deep learning model was built using three structural representations: shared weights, local receptive field, and subsampling. The convolution kernel shapes shared weights to reduce the number of free parameters. For the feature maps at each layer, the convolution kernels are subjectively changed to build a noise filter as well as an edge detector. Both the convolution and subsampling kernels benefit from the local receptive field since it enchants a set of nearby pixels for further processing before transferring the result of a coarser resolution to the next convolutional layers. While reducing the feature map scope at the corresponding layer, the subsampling process involves local averaging [6]. A new trend in CNN comes with a batch normalization algorithm integrated into the architecture, thereby enhancing the network performance and training speed.

- Batch Normalization

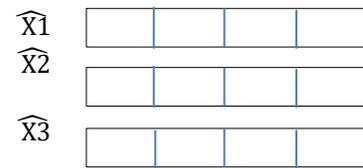
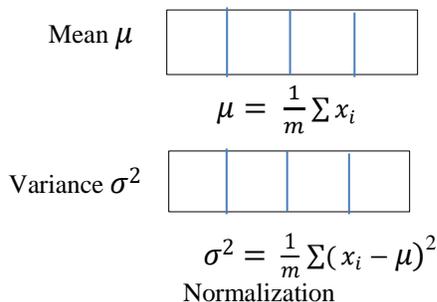
The goal of batch normalization is to achieve a stable distribution of activation values through training. Batch normalization has been established as a component in deep learning, largely helping to push the frontiers of computer vision [18]. BN normalized the means and variance computed within a mini-batch. This contributes tremendously to simplifying the optimization and enabling the network to converge [19]. Therefore, in batch normalization, the data distribution has the attribute that the mean of the data distribution is 0 and the variance is 1 [8]. The batch normalization performs well at medium and large batch sizes and has good generalization to multiple vision tasks [20]. Step of batch normalization operation can be presented as seen in Fig. 2.

- During Training

On a mini-batch feature X

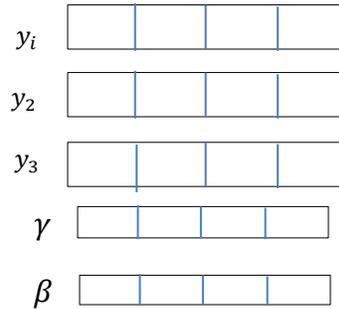


Calculate the mean and variance in the mini-batch



$$\widehat{X1} = \frac{X1 - \mu}{\sqrt{\sigma^2 + E}}$$

Scale and shift



$$y_i = \gamma * \widehat{X1} + \beta$$

Fig. 2. Figurative Representation of Batch Normalization Operation.

These can be represented in the formula below:

$$\mu = \frac{1}{m} \sum x_i$$

$$\sigma^2 = \frac{1}{m} \sum (x_i - \mu)^2$$

$$\widehat{X1} = \frac{x1 - \mu}{\sqrt{\sigma^2 + E}}$$

$$y_i = \gamma \widehat{X1} + \beta$$

Where μ is the mean value of the output layer l , and σ^2 is the variance value, while $\widehat{X1}$ is the normalization output obtained after subtracting the mean and dividing it by standard deviation $\frac{x1 - \mu}{\sqrt{\sigma^2 + E}}$, while y_i set the mean and variance to the new value. γ and β are learnable parameters.

With this operation by BN, after processing the problem of multiple layers, mutual coupling in network training weight updating can be solved, and the possibility of gradient disappearance or gradient explosion can be reduced.

B. The Design Principle of the Proposed Pre-activation BN-CNN Approach

The proposed Pre-activation BN-CNN consists of one input layer, four convolution units, one dropout layer, two fully connected layers, one Soft-Max layer, and one classification layer. The first convolution unit involves the first convolution layer labelled as C1 in Fig. 1. This layer is followed by the batch normalization layer, which is labelled as BN1, then the Rectifier linear unit (ReLU) activation function, which is labelled as R1, and the Max pooling (down sampling) layer, which is labelled as Mp1. The second convolution unit, the third, and the fourth all follow the same design format as the

first convolutional unit, having the batch normalization layer after each convolutional layer before the activation function.

In this paper, the relevant parameters of the proposed Pre-Activation Batch Normalization CNN Architecture are selected according to the proposed face images. The size of the input images is $64 \times 64 \times 3$. The four convolutional kernels' sizes are set to 3×3 , $K1 = 3$, $K2 = 3$, $K4 = 3$. All the convolutional strides, $S1$, $S2$, $S3$, and $S4$ are set to 1. In all the four convolutional units, we set the size of the convolutional layers as $C1 = 64$, $C2 = 32$, $C3 = 16$, $C4 = 8$. Each convolution layer is followed by a batch normalization layer before the activation function. Rectifier linear Unit (ReLU) is the activation function in all the four convolutional units, followed by a max-pooling layer for the down sampling operation. The operation has $k = 2$, with a stride of 2. This gives us the max-pooling result as $C1 = 64$, $C2 = 32$, $C3 = 16$, $C4 = 8$. All the feature maps $F1 = 8$, $F2 = 16$, $F3 = 32$, $F4 = 64$, and all the $C4 = 8 \times 8$ max pool to $4 \times 4 \times 64$, which were expanded into a one-dimensional vector and then connected to the first fully connected layer that is composed of 1024 neurons, a dropout is added between the first and second fully connected layers. And then 6 neurons are connected as the category of the six classes of different variations.

C. Data

This research paper proposed using two publicly available databases, namely the Label Faces in the Wild database and the Caltech 101_Object_Category database. These two databases are used to build a suitable database of 5280 face images, which we named AS_Darma. The 5280 face images were selected from the above two databases. The Label Faces in the Wild has 13,233 target face images of 5749 different individuals. In this database, there are 1680 individuals with two or more images. The remaining 4069 people have just single images. In the database, the image size in this database is 250×250 pixels and is in JPEG image format. Many of the images are in the r.g.b. color scheme. In this research, we selected 4,200 face images of 105 individuals. All of the selected images are in the same r.g.b. color scheme, resized to 64×64 pixel size in the same jpeg format, Fig. 3.

While the Caltech 101_Object_Category database has 450 face images of 27 unique subjects, The images are 325×495 pixels in jpeg format with a different expression, background, and light, but this research proposed cropping and resizing each face image to 64×64 pixels.

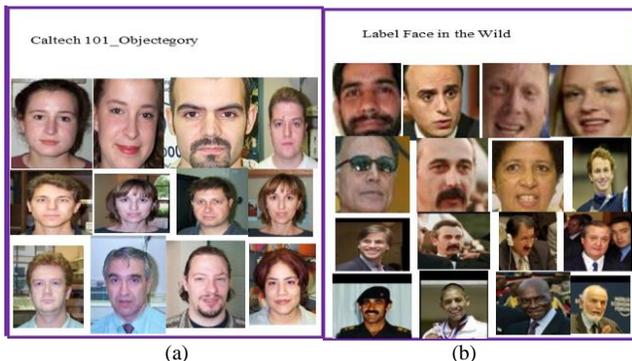


Fig. 3. (a) A Sample of Face Images from the Caltech 101_Object Category Database. (b) Label Face in the Wild Face Images.

In this research, we proposed using 5,280 human face images of 132 individuals. Each individual has 40 face images. To achieve this, we used dynamic data augmentation and preprocessing techniques to produce several synthetic images for each face image of an individual.

We produced 1,080 face images for 27 individuals from the Caltech 101_objects_categories database and 4,200 images for 105 individuals from the LFW. This gives us a total number of 5280. The 5280 images were split into $5280/100 \times 70 = 3,696$, which is 70%, and $5280/100 \times 30 = 1,584$, which is a 30% ratio. For both training and testing, 70% is for the training and the other 30% is for the testing. The 5280 images are used to form the proposed dataset called AS_Darmaset for the training and testing of the proposed deep learning architectures.

V. EXPERIMENT

This section provides an overview of the experimental setup that is used to verify the effect of our proposed Pre-Activation-Batch-normalization-CNN-Architecture [21]. The experiments were conducted using the newly built AS_Darmaset of 5280 face images. To understand the benefits of adopting a powerful deep learning batch normalization algorithm for enhancing the performance of the face recognition system. In this research, we compared the accuracy and loss errors produced by the four deep learning architectures of different batch normalization approaches. To help in determining the best and most robust batch normalization algorithm between the four models in terms of performance and recognition accuracy rate, the experiment will look at how these regularization techniques can improve network stability and performance.

MATLAB R2018b is used to develop and implement the four deep learning batch normalization CNN architectures. It is used for conducting the experiments as well. The Matlab software is used because it is the best programming tool for engineering and artificial intelligence systems. The architecture of our models is meant to run on the HP Elite Book 854w, Mobile Workstation. The CPU is an Intel Core i7 M620 @ 2.67GHz processor with internal physical memory of 8.00GB. Four experiments were conducted.

A. Experiment with Pre-activation Batch Normalization CNN Architecture

We first conducted the experiments using a Pre-activation Batch Normalization CNN architecture. With this batch normalization algorithm, the batch normalization layers are placed immediately after the convolutional layer in each convolutional unit of the network. This means that the batch norm layer is applied before each of the Rectifier Linear Unit (ReLU) activation functions. The performance of this architecture is evaluated using the proposed AS_Darmaset. In this research, the dataset is categorized into six classes of different face image variations. The six classes of variations include Facial Expiration, Facial Makeup, Occlusion, Old Age, Pose variation, and Younger Age variation. In each class, there are 880 face images of 22 individuals, and each person has 40 face images of size 64×64 pixels.

- Design Principle of Pre-activation Batch Normalization CNN Architecture.

Compute the input → Batch Norm → Applied Activation →
Compute Next layer input → Batch Nor → Applied
Activation

The performance of this model for face recognition is evaluated across six different classes of human face variation. Facial Expression, Makeup, i.e., cosmetic effects, occlusion, faces of older age, pose variation, and faces of younger age. There are 880 images in each of the different classes. Each class has 22 individuals, and each of the individuals has 40 face images of 64x64 pixel size.

Table I shows the information obtained from the training plot of the experiment, which shows the training accuracy, validation accuracy, training loss, and validation loss as illustrated in Fig. 4.

In the above figure, the first graph at the top shows the training accuracy (i.e., classification accuracy). The X-axis has 90 epochs and 810 iterations, while the Y-axis shows the accuracy values in percentages. The second graph at the bottom shows the loss function (cross-entropy loss). The training plot is for monitoring the status of the network. It shows how the network's accuracy is increasing. The upper side of the graph shows the performance accuracy, while the lower side of the graph shows the loss function. The graph shows the training matrices at each.

TABLE I. TRAINING PLOT DETAILS FOR PRE-ACTIVATION BATCH NORMALIZATION CNN TRAINING FROM THE SCRATCH

Parameters	Values
Training Accuracy	100.00%
Validation Accuracy	99.87%
Training Status	Completed
Elapsed Time	39 min 20 sec
Number of Epoch per Iteration	9
Mux. Number of Iteration	810
Validation Frequency	80 iteration

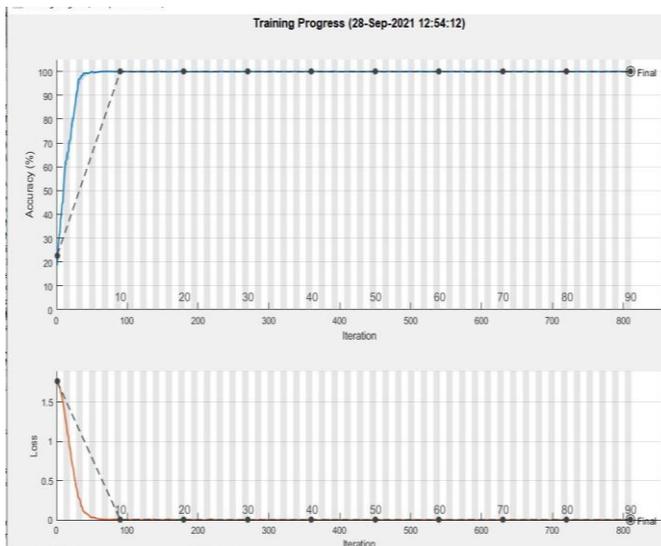


Fig. 4. Training Progress Plot Graph for Pre-Activation BN CNN Architecture.

Iteration: That is the estimation of the gradient [22]. The classification accuracy is represented by a light blue line, while the dark blue line represents the accuracy obtained by applying a smoothing algorithm to the training accuracy. While an interrupted black dotted line is defined as the classification accuracy of the whole validation dataset. At epoch 10 and iteration 90, the network started to converge with 100% training accuracy and validation accuracy of 99.87%. At epoch 80 and iteration 720, the training accuracy decreases to 99.75%, while the testing (validation) continues to maintain its accuracy value of 99.87%. Then, at epoch 84, iteration 750, the training accuracy improved to its normal 100% accuracy. Finally, the training and testing accuracies are 100% and 99.87%, respectively, at last epoch 90 and iteration 810 [21]. The Pre-Activation-CNN Architecture has yielded a better classification performance of 100% training accuracy and 99.87% validation accuracy. Without network overfitting, network convergence is successful. The loss function is shown on the second graph at the lower end. The light orange line is training loss, the smooth training loss is a dark dotted line, and the validation loss is a disrupted line, meaning the loss on each mini-batch and the validation dataset [23]. The figure shows that both the training and validation loss functions have converged to the minimum as the learning rate reached 1.600e-05. While the number of iterations reached 810 at 39 min 20 sec of training time.

B. Experiment with Traditional CNN Model without BN Algorithm

The traditional CNN model has a simple architecture of four convolutional units. In each of the units, there is one convolutional layer followed by a Rectifier linear unit (ReLU) activation function, then a max-pooling layer and a down sampling layer. This shows that there is no batch normalization algorithm in any of the four convolutional units. The architecture of this CNN is comprised of four (4) convolution layers, four (4) max-pooling layers, and two (2) fully connected layers. There is no batch normalization layer in the design principle of this model. The model was implanted in MATLAB R2018b and all the trainable parameters (i.e., layer weights and biases) were initialized with the Rectifier Linear Unit (ReLU) activation function at each convolutional process. Fig. 5, shows the training progress plot graph and the details regarding the training phase are listed in Table II below.

Table II shows the training details with training and validation accuracies of 96.50% and 98.93%, respectively as shown in the training graph below.

TABLE II. TRAINING PLOT DETAILS FOR PRE-ACTIVATION BATCH NORMALIZATION CNN TRAINING FROM THE SCRATCH

Parameters	Values
Training Accuracy	96.50%
Validation Accuracy	98.93%
Training Status	Completed
Elapsed Time	32 min 50 sec
Number of Epoch	9
Mux. Number of Iteration	810
Validation Frequency	80 iteration

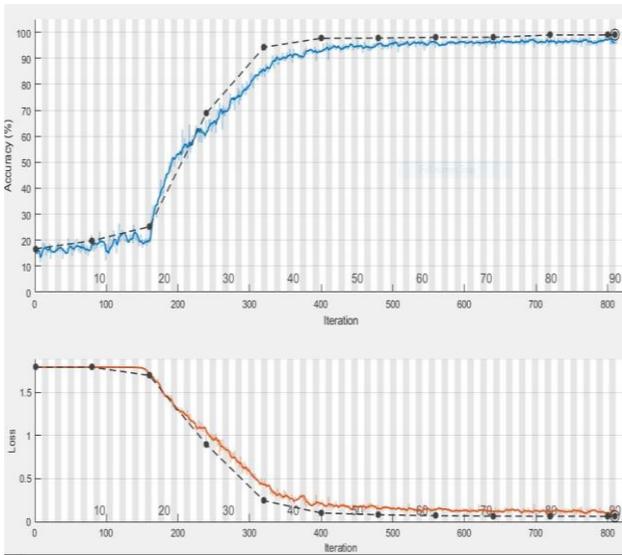


Fig. 5. Training Progress Plot Graph for Traditional CNN without BN Architecture.

In the above graph, the training and testing accuracies at epoch 1 and iteration 1 are initialised to 17.25% and 16.67%, respectively. The accuracy sharply increases at epoch 27 and iteration 240 to 62.00% and 69.00%, respectively. After epoch 50 and iteration 450, the accuracy reaches 93.50% and 97.66%. Similarly, at epoch 63, iteration 560, both the training and validation accuracies continue to increase to 96.50% and 98.04%. At epoch 78, iteration 700, the training accuracy decreased to 95.75%, while the testing accuracy of 98.04% was maintained. Finally, at the last epoch, 90 and iteration 810, the training and testing accuracies increased to 96.50% and 98.93%, respectively. The result is shown in the graph, which shows that the training data accuracy is higher than the testing dataset accuracy throughout the training process. This implies that there is large overfitting that occurred, particularly at the beginning of the training because the batch normalisation has not been implemented. While in the second graph, The training and testing losses, which represent the degree of differences between the model prediction and the real classes, decrease with increasing epoch number [23]. At epoch 1 and iteration 1, the training and testing losses were 1.7917 and 1.7918, respectively. While the number of epochs reaches the final stage, which is 90 epochs and 810 iterations, the training and testing losses were 0.1094 and 0.0628. This indicates that the model has overfitting and gradient disappearance caused by covariate shift.

C. Experiment with Post-activation Batch Normalization CNN Architecture

The Post-activation Batch Normalization CNN architecture has the following setup in the model design principle: Four (4) convolution layers, four (4) batch normalization layers, four (4) max-pooling layers, and two fully connected layers. In this architecture, the batch normalization layer is applied after each of the rectifier linear unit (Relu) activation functions within all four convolutional units. Table III shows the training details and Fig. 6: The Post-Activation Batch Normalization CNN Algorithm Training Progress Plot Graph.

TABLE III. TRAINING PLOT DETAILS FOR PRE-ACTIVATION BATCH NORMALIZATION CNN TRAINING FROM THE SCRATCH

Parameters	Values
Training Accuracy	100.00%
Validation Accuracy	99.81%
Training Status	Complete
Elapsed Time	39 min 8 sec
Number of Epoch per iteration	9
Mux. Number of Iteration	810
Validation Frequency	80

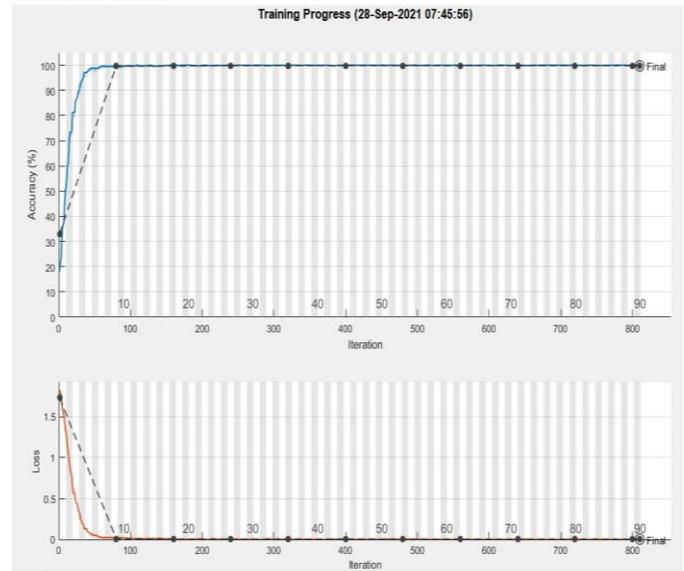


Fig. 6. Training Progress Plot Graph for Post-Activation-Batch-Normalization-CNN Model.

In the above training graph, it can be seen that the training and testing values at the initial epoch of 9 and iteration 80 have an accuracy value of 99.75% and 99.75%, respectively. Both the training and testing accuracies start to converge at epoch 18 and iteration 160 with the accuracy values of 100.00% and 99.68%. At epoch 27 and iteration 240, the training accuracy decreases to 99.75%, while the testing accuracy increases to 99.81%. At epoch 39 and iteration 350, the training accuracy reached 100.00% and the testing accuracy still maintained its accuracy value of 99.81. At the final epoch of 90 and iteration of 810, the training and testing accuracies continued to be 100.00% and 99.81%, respectively. The result shows that the testing dataset accuracy is close to that of the training dataset throughout the training process. This implies that no overfitting occurred and that the implementation of the batch normalization operation is working very well [24]. While in the lower part of the graph, which is the loss error curve, the training and testing losses, which represent the degree of differences between the model prediction and the real classes, decrease with increasing epoch number [23]. At epoch 1 and iteration 1, the training and loss errors were initialized as 1.7920 and 1.7915, respectively. While the number of epochs reaches its final stage, of epoch 90 and iteration 810, the training loss decreases to 0.0026 and the testing loss decreases to 0.0052. These show that both the training and validation loss

functions have convergence at the learning rate that reaches $1.600e-05$. So the network has no overfitting concerning its testing dataset since the training and testing loss values are closed.

D. Experiment with Sparse Batch Normalization CNN Architecture

The fourth model is a deep learning model with a sparse batch normalization architecture. This model was developed and used by [2]. The design principle of this deep learning model is characterized by the following:

An input layer convolutional layer 1; Convolutional layer 2, max-pooling layer, batch normalization layer; Convolutional layer 3, max pooling layer; Convolutional layer 4, max-pooling layer. It could be seen that the first convolutional layer unit has only the first convolutional layer, which has no operational layer attached to it. The batch normalization operation only takes place at the second convolution unit after the max-pooling operation. The third and fourth convolutional units have only convolutional layers with max-pooling layers each. It can be noticed that the architecture of this network does not utilize any activation function using the convolutional operation units. It only uses the soft-max function as an output function after the two fully connected layers within the output units of the network.

Table IV shows the training details and Fig. 7 shows the Sparse Batch Normalization CNN Architecture Training Progress Plot Graph.

The sparse Batch normalization model In Fig. 6, was implemented using MATLAB R2018b for the training and validation. This model runs around 270 epochs with 3 iterations per epoch and a batch size of 400. This is done to train this model with our proposed dataset very well [25]. Stochastic gradient descent and momentum term are the optimizers used for this model. The training graph in Fig. 6 above illustrates performance and classification accuracy and losses between both the training and validation phases with the number of epochs and iterations. At an initial learning rate of 0.0100, Epoch 1, and iteration 1, the training and validation accuracy values are initialized. The training and validation accuracy values reach 96.00% and 97.54%, respectively, at Epoch 107 and iteration 320.650increases %. Finally, at the last epoch of 270 and last iteration 810, the values of both the training and validation accuracies increase to 96.25% and 97.60%, respectively.

TABLE IV. TRAINING PLOT DETAILS FOR SPARSE BATCH NORMALIZATION CNN ARCHITECTURE TRAINING FROM THE SCRATCH

Parameters	Values
Training Accuracy	96.25%
Validation Accuracy	97.60%
Training Status	Complete
Elapsed Time	132 min 32sec
Number of Epoch per iteration	3
Mux. Number of Iteration	810
Validation Frequency	80

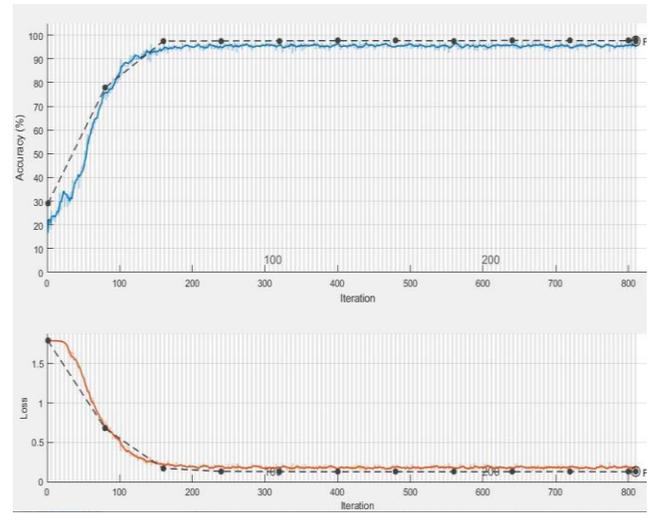


Fig. 7. Training Progress Plot Graph for Sparse Batch Normalization-CNN Architecture.

In the above training graph, the training and validation losses that represent the degree of differences between the model prediction and the real classes decrease with increasing epoch numbers [44]. At epoch1 and iteration 1, the training and validation losses were 1.7918 and 1.7913, respectively. At epoch 107 and iteration 320, the training and validation losses decrease to 0.1747 and 0.1335, respectively. While the number of epochs reaches its final stage, of epochs 270 and iteration 810, the training loss value increases to 0.1768, and the testing loss decreases to 0.1294. This result shows that the network has over fitted concerning its training and testing datasets since there are many differences between the loss values of the training and loss values of the testing dataset.

VI. COMPARISON OF THE TRAINING AND VALIDATION ACCURACIES AND LOSS ERRORS FOR DIFFERENT DEEP LEARNING CNN ARCHITECTURES

To find suitable deep learning CNN architectures for the proposed face recognition system, it is vital to recall the alleged effects of batch normalization, which can be broadly categorized as convergence speed and generalization performance improvement. In this paper, we trained and tested four different deep learning convNets with different model architectures. By comparing the experimental results of the four Fig. 9, comparison of Validation Accuracies of the deep learning ConvNet architectures, we will be able to rule out the robust ConvNet model that leads to higher classification performance and it will also rule out the type of model that leads to insignificant results. This section focuses on comparing the experimental results of the four deep learning models by observing the training and validation behavior of the different architectures [10]. Here we aim to isolate the effect of batch normalization in general, concerning our proposed Pre-Activation-Batch Normalization CNN Architecture. In this experiment, the Pre-Activation-BN-CNN-Architecture is abbreviated as PRACBNCNN, the Post-Activation-BN-CNN is presented as PSTACBNCNN, the Traditional-CNN-without-BN is denoted as TRCNNWITHOUTBN, and lastly, the Sparse-BN-CNN is represented as SPSBNCNN.

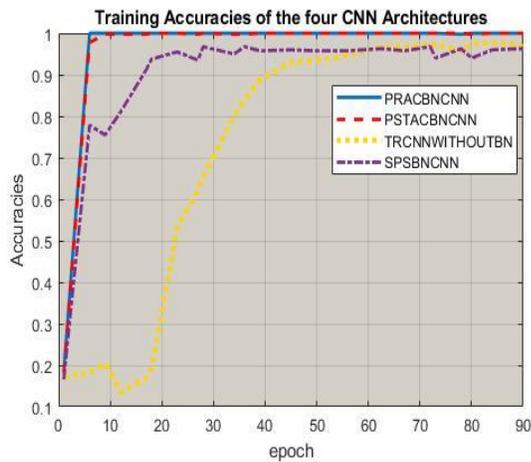


Fig. 8. Comparison of Training Accuracies of the Four CNN Architectures.

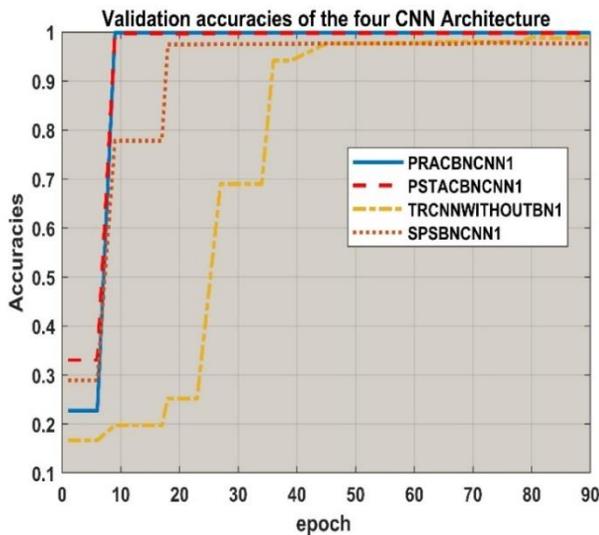


Fig. 9. Comparison of Validation Accuracies for the Four CNN Architectures.

Fig. 8 and Fig. 9 above show the training and validation accuracies overtime for all the four deep learning models. In terms of the training and validation accuracies, we can observe that both the Pre-activation-BN-CNN and Post-Activation-BN-CNN models have to reach overall accuracies in all cases by simply adding batch normalization before and after the rectifier linear unit activation function. The training and validation accuracies (solid blue lines) of the proposed Pre-active-BN-CNN follow by the Post-Activation-BN-CNN Training and validation accuracies (dotted red lines) consistently achieve higher accuracies and gained immediate convergence speed improvement on both the training and validation accuracy. While the Training and validation accuracies (zigzag dashed mustard lines) of the Traditional CNN without batch normalization architecture and that of Sparse Batch Normalization CNN (Fluctuated dotted purple line) are not ideal this is because there is a lot of overfitting. The results show that the training dataset of both TRCNNWITHOUTBN and SPSBNCNN are harder than validation datasets of the model. In the two figures the Pre-activation-BN-CNN model started to converge at epoch 10 with training and validation

accuracies of 100.00% and 99.87 respectively, the Post-Activation-BN-CNN started its convergence at epoch 18 with training and validation accuracies of 100.00% and 99.68%. On the other hand, the training and validation accuracies of Traditional-CNN-without-BN start to improve at 62 with 96.50% and 97.73%, respectively. The Accuracies of Sparse increases at epoch 23 with 95.50% and 97.47%. The training and validation results in the two figures tried to show that the performance of Post-Activation-BN-CNN is about the same as the Pre-Activation-BN-CNN, but the Pre-Activation-BN-CNN outperforms all the three deep learning CNN architectures. This is supported by the higher accuracy of each data. The training data has a curacy value of 100.00% and 99.87% on the Testing data [26].

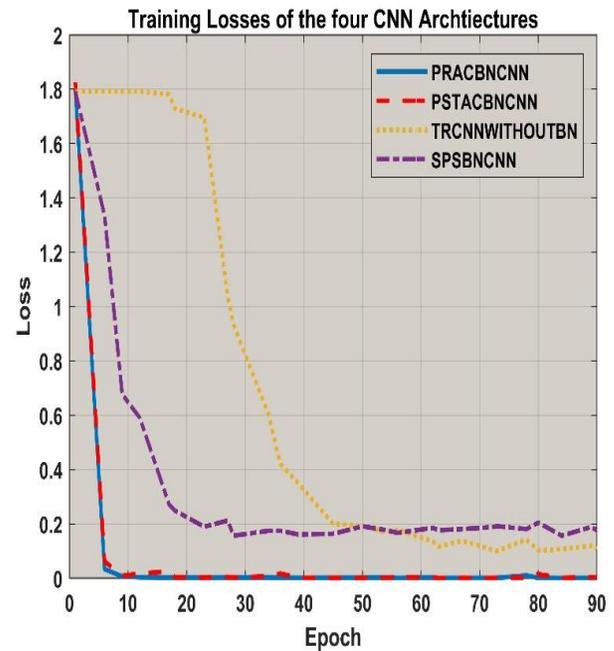


Fig. 10. Comparison of Training Losses for the Four CNN Architectures.

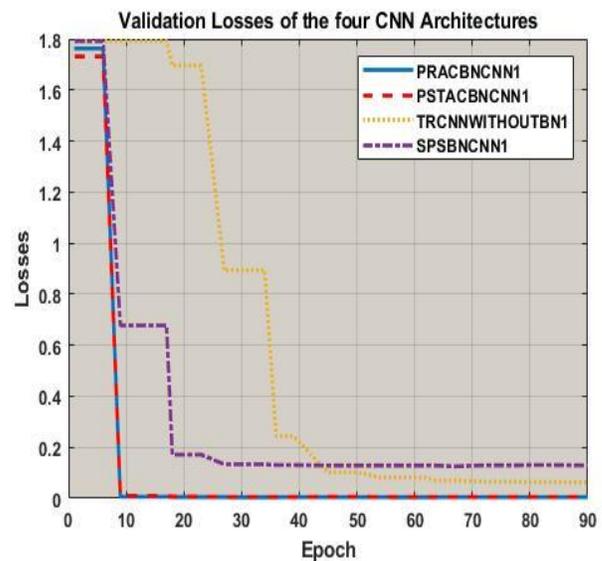


Fig. 11. Comparison for Validation Losses of the Four CNN Architectures.

The curve in Fig. 10 is the comparison of training loss error curve for the four CNN architectures, and the other graph in Fig. 11, is the validation loss error curve. Each with a different number of epochs ranging from 0 to 90. The two curves show the comparison results of the cross-entropy loss errors of the four deep learning models. By observing the losses over time of both the Pre-activation-BN-CNN- model and that of the Post-Activation-BN-CNN model we can see how the losses repeatedly fall to the lower level. In the figures, a noteworthy observation can be made at the begging of the training on the Traditional CNN without BN and Sparse BN CNN Networks. During the first phase of the training epochs training and validation losses of two models plateaus for the higher amount loss errors, until the gradient update escapes the unfavorable local minimum at epoch 72, iteration 640 with training and validation loss of 0.1059 and 0.653 for the Traditional CNN without BN.

While for the Sparse BN CNN model at epoch 84, 750 iterations with training and validation loss of 0.1565 and 0.1305 prospectively. The results show that the two models suffer from large covariate shifts, which lead to the network gradient disappearance and higher overfitting. In both the training and validation losses of the four models in the two graphs, we can see that there is separation between the models the Pre-activation BN-CNN training and validation loss errors (the solid blue lines) start to converge to the minimal error at epoch 10 with training and validation losses of 0.0067 and 0.0065. Finally, at the last epoch 90, the training and validation loss decreases to 0.0013 and 0.0048. While The Post-Activation-BN-CNN started to converges at epoch 18 and its last epoch 90 the training and validation loss decreases to 0.0026 and 0.0052 respectively. Fig. 9 and 10 illustrates the training and testing error rate of the proposed Pre-Activation Batch Normalization CNN Architecture, over 90 training Epochs, and 810 iterations. The training Errors are always lower than that produce by post Batch Normalization CNN and there is a higher split between the Pre-Activation-BN-CNN and the Traditional CNN without BN Architecture. In terms of the training and validation performance, Post-Activation Batch Normalization CNN architecture is about the same as Pre-Activation Batch Normalization Architecture, but Pre-Activation BN CNN Architecture has outperformed all of the other deep learning models. This can be seen in the two figures. The resulting training and validation loss values obtained from the Pre-Activation-BN-CNN are 0.0013 and 0.0048 when compare with the training and validation loss values of the other three models are very small. So that these values can be said to be quite low. This implies that the resulting model can be said to be able to classify well because it has lower loss error values and high accuracies values. This can be illustrated in Table V.

In the table, the Training and Testing of Different Deep Learning Models after 810 iterations, as in, the experiment results of the four deep learning CNN models are given. Some of the models have batch normalization layers and some without.

TABLE V. PERFORMANCE COMPARISON OF THE (FOUR) DIFFERENT DEEP LEARNING MODELS WITH AND WITHOUT BATCH NORMALIZATION LAYERS

Deep Learning Models	Face Recognition Accuracies Rate		
	Model Type	Training Accuracy	Validation Accuracy
Model 1	PRACBNCNN	100.00%	99.87%
Model 2	PSTACBNCNN	100.00%	99.81%
Model 3	TRCNNWITHUTBN	96.50%	98.93%
Model 4	SPSBNCNN	96.25%	97.60%

The batch normalization techniques give a classification improvement. The Pre-Activation-BN-CNN model performed better than the other three models, with training and validation accuracies of 100.00% and 99.87 as shown in the table. This is because the model architecture encompasses a batch normalization layer in each of the four convolutional units, which is placed before the Rectifier linear unit (ReLU) activation function. According to the training and validation results in the table, the Post-Activation is the next model with better training and validation accuracies of 100.00% and 99.81%. This model has a batch normalization layer in each of its four convolutional units after the rectified linear unit (ReLU) activation function. On the other hand, the table result shows that the traditional CNN has training and validation accuracies of 96.50% and 98.93%. This model has no batch normalization techniques in any of its four convolutional units, but it has the rectified linear unit in each of the convolution units. That is why its accuracy results outperformed those of the Sparse BN CNN model, which has the training and validation accuracies of 96.25% and 97.60% as shown in the table. This model has only one batch normalization layer at the second convolutional unit. The model has no rectifier linear unit (ReLU) activation function.

VII. PERFORMANCE EVALUATION MATRICS

It is critical to define performance measures that are appropriate for the job at hand when evaluating the performance of deep learning models. In this study, we proposed the most critical performance indicators for accuracy, precision, f-score, and recall, as given in the equations below, to analyze our results and to demonstrate that the above results explained in the preceding section are correct [26].

$$\text{Precision} = \frac{TP}{TP+FP} \tag{1}$$

$$\text{Recall} = \frac{TP}{TP+FN} \tag{2}$$

$$\text{Accuracy} = \frac{TP+TN}{TP+FP+TN+FN} \tag{3}$$

$$\text{F}_1\text{-Score} = \frac{2(\text{Precision}) * (\text{Recall})}{\text{Precision} + \text{Recall}} \tag{4}$$

TABLE VI. COMPARISON OF THE RESULTS FROM THE PERFORMANCE EVALUATION MATRICS

Deep Learning Models	Performance Evaluation				F ₁ -Score
	Model Type	Accuracy	Precision	Recall	
Model 1	PRACBNCNN	0.99873	0.9987	1.00	0.9993
Model 2	PSTACBNCNN	0.9981	0.9867	1.00	0.9990
Model 3	TRCNNWITHOUTB	0.98926	0.9892	0.994	0.9932
Model 4	SPSBNCNN	0.97601	0.97595	0.9899	0.9831

Performance graph

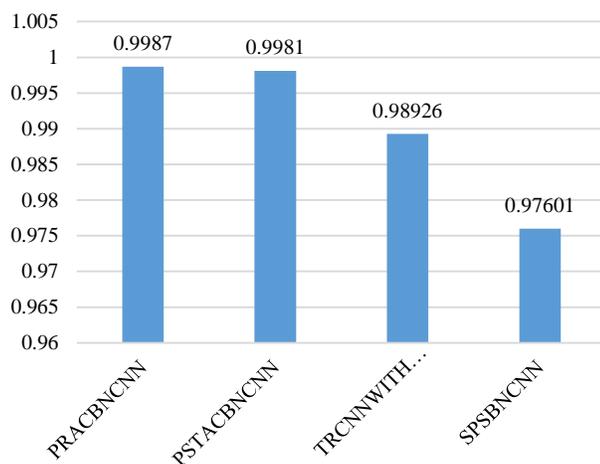


Fig. 12. Performance Evaluation Results.

As we mentioned in the above sections, this research aim to enhance the performance of the face recognition system, using a deep learning approach that involves a convolutional neural network (CNN). In order to evaluate the robustness of our proposed model we compared it result with the results of three other deep learning models. In this section in Table VI, we again compare the results in terms of Accuracy, Precision, Recall and F₁-Score to show the correctness of the previous explanations of our study results. These results were obtained after we evaluated the result obtained from the confusion matrices produce by each of the four models.

When observing the results in the table it can be seen that the PRACBNCNN model 1 is having the high accuracy of 0.99873 and precision of 0.9987. This goes along with the previous result in Table V, where the model has 99.87% validation accuracy. These results are represented in Fig. 12.

VIII. SUMMARY AND CONCLUSION

This research paper presented four deep convolutional neural network models. The architectural styles of the models were divided into two categories: The first architectures were deep learning CNN architectures with batch normalization techniques in each of the model convolutional units, and the

second deep learning architecture was deep learning models without batch normalization techniques. In this research, the best deep learning CNN architecture for recognizing human face images was obtained from the Pre-Activation-BN-CNN Architecture. This model is powered by a batch normalization layer at each of its four convolutional units. The batch normalization layers are all placed before the rectified linear units (Relu) activation function. The result of this research shows that placing the Batch Normalization layer before the ReLu activation function improved network classification power, as the model training and validation results showed 100.00% and 99.87%, respectively. This shows the regularization effect of the Pre-Activation-BN-CNN model over the other three CNN architectures for face recognition systems. In this research work, the application of the Pre-Activation-BN-CNN Architecture has enhanced the performance of the face recognition system. Therefore, reducing covariate shift prevents gradient disappearance and gradient exploration. This leads to better network convergence. The experiment results also show that having the rectified linear unit (Relu) activation function in a model architecture stabilizes network training and improves model classification. This is justified by comparing the results of the TRCNNWITHOUTBN, which has no batch normalization layer but has rectifier linear units, and the results of the SPSBNCNN, which has only one batch normalization layer at the second convolutional unit but has no rectifier linear activation unit. The training and validation accuracy of TRCNNWITHOUTBN are 96.50% and 98.93%, while that of SPSBNCNN is 96.25% and 97.60%, respectively.

IX. ACKNOWLEDGMENT

We would like to show our appreciation to the University Sultan Zainal Abidin, more especially the faculty of Informatics and computing, as well as the UNISZA Research Management Center (CRIEM) for their support on this research work financially and academically.

REFERENCES

- [1] S. D. Abu and F. S. Mohamad, "Approaches Of Deep Learning In Persuading The Contemporary Society For The Adoption Of New Trend Of AI Systems: A Review," Researchgate.Net, vol. 9, no. 12, pp. 163–177, 2020, [Online]. Available: https://www.researchgate.net/profile/Sanusi_Darma_Abu/publication/347784009_Approaches_Of_Deep_Learning_In_Persuading_The_Contemporary_Society_For_The_Adoption_Of_New_Trend_Of_AI_Systems_A_Review/links/5fe3d7aca6fdccdb8f71f6d/Approaches-Of-Deep-Learning-.
- [2] J. Cai, O. Chang, X. L. Tang, C. Xue, and C. Wei, "Facial Expression Recognition Method Based on Sparse Batch Normalization CNN," Chinese Control Conf. CCC, vol. 2018-July, pp. 9608–9613, 2018, DOI: 10.23919/ChiCC.2018.8483567.
- [3] Y. D. Coşkun, Musab, Ayşegül Uçar, Özal Yıldırım, "Face Recognition Based on Convolutional Neural Network," in International Conference of modern Electrical Energy System, 2017, no. January 2018, pp. 1–5, DOI: 10.1109/MEES.2017.8248937.
- [4] L. Shen and L. Bai, "A review on Gabor wavelets for face recognition," Pattern Anal. Appl., vol. 9, no. 2–3, pp. 273–292, 2006, DOI: 10.1007/s10044-006-0033-y.
- [5] P. N. Belhumeur, J. P. Hespanha, and D. J. Kriegman, "Eigenfaces vs. fisher face: Recognition using class specific linear projection," IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 7, pp. 711–720, 1997, DOI: 10.1109/34.598228.
- [6] S. A. Darma, F. Aliyu, and A. Kurfi, "The Role of Social Media in

- Empowering the Involvement of Women in Information Technology : A Case Study of Al-Qalam and U maru Musa Yar ' Adua Universities," vol. 2, no. 1, 2018.
- [7] D. H. H. A. T. N. WIESEL, "RECEPTIVE FIELDS AND FUNCTIONAL ARCHITECTURE OF MONKEY STRIATE CORTEX," *J. Physiol.*, vol. 195, no. 1, pp. 215–243, 2017.
- [8] S. I. C. Szegedy, "Australian Literary Journalism and 'Missing Voices': How Helen Garner finally resolves this recurring ethical tension," *Journal. Pract.*, vol. 10, no. 6, pp. 730–743, 2016, DOI: 10.1080/17512786.2015.1058180.
- [9] Jia Deng, Wei Dong, R. Socher, Li-Jia Li, Kai Li, and Li Fei-Fei, "ImageNet: A large-scale hierarchical image database," 2009 IEEE Conf. Comput. Vis. Pattern Recognit., no. May 2014, pp. 248–255, 2009, DOI: 10.1109/CVPRW.2009.5206848.
- [10] FABIAN SCHILLING, "The Effect of Batch Normalization on Deep Convolutional Neural Networks," 2016. [Online]. Available: <http://kth.diva-portal.org/smash/record.jsf?pid=diva2%3A955562&dsid=-5716>.
- [11] N. Gajhede, O. Beck, and H. Purwins, "Convolutional neural networks with batch normalization for classifying hi-hat, snare, and bass percussion sound samples," *ACM Int. Conf. Proceeding Ser.*, vol. 04-06-Octo, no. October 2016, pp. 111–115, 2016, DOI: 10.1145/2986416.2986453.
- [12] M. Bojarski et al., "End to End Learning for Self-Driving Cars," 2016, pp. 1–9.
- [13] K. B. Pranav and J. Manikandan, "Design and Evaluation of a Real-Time Face Recognition System using Convolutional Neural Networks," *Procedia Comput. Sci.*, vol. 171, no. 2019, pp. 1651–1659, 2020, DOI: 10.1016/j.procs.2020.04.177.
- [14] S. Zheng, R. W. O. Rahmat, F. Khalid, and N. A. Nasharuddin, "3D texture-based face recognition system using fine-tuned deep residual networks," *PeerJ Comput. Sci.*, vol. 2019, pp. 1–21, 2019, DOI: 10.7717/PEERJ-CS.236.
- [15] P. Kamencay, M. Benco, T. Mizdos, and R. Radiol, "A New Method for Face Recognition Using Convolutional Neural Network Face Recognition System – State of the Art," pp. 663–672, 2017, DOI: 10.15598/area.v15i4.2389.
- [16] O. A. H. Hayder Najm, Hayder Asaf, "An N EFFECTIVE IMPLEMENTATION OF F ACE R RECOGNITION USING," 2019.
- [17] M. K. Benkaddour and A. Bounoua, "Feature extraction and classification using deep convolutional neural networks, PCA and SVC for face recognition," *Trait. du Signal*, vol. 34, no. 1–2, pp. 77–91, 2017, DOI: 10.3166/TS.34.77-91.
- [18] W. Zaremba, I. Sutskever, and O. Vinyals, "Recurrent Neural Network Regularization," *Conf. Pap.*, no. 2013, pp. 1–8, 2015, [Online]. Available: <http://arxiv.org/abs/1409.2329>.
- [19] Y. Wu and K. He, "Group Normalization – Facebook Research," *Eccv*, no. Figure 1, 2018, [Online]. Available: <https://research.fb.com/publications/group-normalization/>.
- [20] X.-Y. Zhou et al., "Batch Group Normalization," 2020, [Online]. Available: <http://arxiv.org/abs/2012.02782>.
- [21] R. Lemlich, "Foam fractionation and allied techniques," *Ind. Eng. Chem. Res.*, vol. 60, no. 10, pp. 16–29, 2015, [Online]. Available: <http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Foam+Fractionation+and+Allied+Techniques#1>.
- [22] B. Eritzke, "A self-organizing network that can follow non-stationary distributions," *Lect. Notes Comput. Sci. (including Subsea. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics)*, vol. 1327, pp. 613–618, 1997, DOI: 10.1007/bfb0020222.
- [23] M. Shyu, S. Chen, and S. S. Iyengar, "A Survey on Deep Learning : Algorithms, Techniques," vol. 51, no. 5, 2018.
- [24] D. M. Ibrahim, N. M. Elshennawy, and A. M. Sarhan, "Deep-chest : Multi-classification deep learning model for diagnosing COVID-19, pneumonia, and lung cancer chest diseases," *Comput. Biol. Med.*, vol. 132, p. 104348, 2021, DOI: 10.1016/j.combiomed.2021.104348.
- [25] J. Yang and G. Yang, "Modified convolutional neural network based on the dropout and the stochastic gradient descent optimizer," *Algorithms*, vol. 11, no. 3, pp. 1–15, 2018, DOI: 10.3390/a11030028.
- [26] J. Alsamiri and K. Alsubhi, "Internet of things cyber attacks detection using machine learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 12, pp. 627–634, 2019, doi: 10.14569/ijacsa.2019.0101280.

Heuristics and Think-aloud Method for Evaluating the Usability of Game-based Language Learning

Kashif Ishaq^{1*}, Fadhilah Rosdi², Nor Azan Mat Zin³

Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia, Bangi, Malaysia

Adnan Abid⁴

School of Systems and Technology (SST)
University of Management and Technology, Lahore, Pakistan

Abstract—Digital learning environments are increasingly becoming popular in recent years. The rising usage of cell phones has invited researchers to design and develop learning applications and games for mobile phones. Specifically, game-based language learning is being promoted by researchers in many parts of the world. “Language Learning Serious Game (LLSG)” is based on a theoretical model constructed by the researcher that supports children learning English as a second language in a cultural context. The usability of such games is evaluated based on well-defined heuristics and other standard methods. This research aims to appraise the usability of LLSG through heuristics and think-aloud approaches while involving all essential stakeholders, including language experts, students, teachers, and game developers. The researcher proposed the heuristics in a cultural context, whereas the think-aloud review is compiled from the rigorous discussion session involving these stakeholders to evaluate the LLSG. The findings obtained from the heuristics evaluation reveal that the usability of LLSG is acceptable. On the other hand, various interesting suggestions and reviews were gathered from the discussion between experts and students. This evaluation will further improve the future versions of the game.

Keywords—Engagement; game-based; heuristic evaluation; language learning; motivation; think aloud; usability

I. INTRODUCTION

Digital learning provides the ability to incorporate skills and knowledge into a wide variety of academic scenarios. Several options are available for digital learning, which involves game-based learning that employs interactive video games with content. Learning through gamification has recently been established in collaboration with technical developments to improve gameplay, modern equipment, and new methods of motivating people to engage and communicate together. Video and mobile phone games are perceived to be the perfect venue for education nowadays. Games help learners achieve a more robust understanding by getting more fun, becoming more appealing, and placing learners in roles that enable them to reflect on their performance [1][2].

Game-based learning is a creative instructing tool that may benefit children specifically, even those left behind in their studies. These games are an entertainment tool with educational objectives, in which the players gain awareness and develop their abilities when playing [3]. Game-based learning in business, science, heritage, education, math, and languages has thrived [4][5][6][7]. Besides, a game-based

approach is used for assessments, learning, collaborations, individual learning, and creativity. A survey was conducted in which educational area was prominent to determine the significant gamified zones. It was also discovered that game-based learning encouraged the users [8][9].

A lot of games for language learning according to the cultural context have been developed and implemented successfully, i.e., Arab [10][11] Iran [12], Sudan [13], Singapore [14], China [15][16], Taiwan [17], Denmark [18], Italy [19][20], Greece [21], Korea [22], Romania [23], Spain [24][25]. Similarly, a mobile application, ‘Literacy and Numeracy Drive,’ was developed and implemented in the public sector schools of Punjab, Pakistan [26], but it was less effective in obtaining the intended learning outcomes [9] [27]. Thus, the researcher constructed a theoretical model for language learning in a cultural context [28]. Then to validate and evaluate the usability of the model, a game-based language learning application, ‘LLSG,’ was designed and developed according to the cultural context of public sector schools. The content and requirements for the game development were gathered from the extensive literature review and the stakeholders [9][27][93][95]. There are different methods to evaluate a game developed for language learning [29], but the usability testing method is commonly used for its evaluation [30] [31].

The usability assessment introduced by [30] [31] makes it easier for programmers to consider and enhance the usability and efficiency of the user interface for software applications. Improving the system's usability will strengthen the system's utilization. Additionally, a usability classical testing method is think-aloud, where one user works separately by expressing their decisions, expectations, thoughts, and feelings during application interaction. The evaluators can understand the reasons behind the action performed by the user with the system [32]. For usability assessment, researchers have used a heuristic assessment method devised by [30]. This assessment method is suitable for software evaluation since it is low-cost and realistic. Usability problems can be perceived better from the viewpoint of users and professionals as both assessment approaches are used. A variety of research has used both assessment approaches to measure the usability of game-based and e-learning systems. The findings suggested positively that the two methods were used concurrently [33-37]. This research aims to analyze the use of a game-based language learning application to understand its interface's positive and negative aspects to increase the quality and performance of its usage. The researcher followed both the usability evaluation

*Corresponding Author

methods: Experts' heuristics and think-aloud from teachers and students to identify the game's usability issues. The stakeholders appraised the game-based language learning application in the cultural context, suggesting minor changes to improve its quality for more effective usage. Incorporating Nielsen's ten indices with proposed heuristics [94] is another significant contribution of the study [38].

The rest of the article has been structured in the following manner: the related research work has been discussed in Section 2, whereas the evaluation process, including data collection for a language learning game, has been presented in Section 3. Results for the evaluation process have been discussed in Section 4, while the article concluded with its future work in Section 5.

II. LITERATURE REVIEW

The game-based learning and heuristic evaluation has been addressed in this section, as it is the main dominant element of this paper.

A. Game-based Learning

The study of [39] demonstrated that games could stimulate learners' interest and significantly improve one's learning. When gamification is applied to a game, it tends to make the game more affectionate, interactive, and progress [40][41][42]. Through modern technologies, immersive learning is enhanced with vivid interactive learning displays, which help to improve academic achievement [43]. If various gaming elements were integrated into digital instruction, students would pay attention to the multimedia material and experiences for a more extended period [44]. The study by [45] demonstrated that when multimedia games were integrated with gamification in a learning system, students understood the content, enhancing their willingness to take on the learning material. Other studies have shown that game-based learning with gamification could promote learners' motivation, participation, and success in the process [46-50]. There is compelling proof that a game-based learning experience may be helpful to learning acquisition.

The author in [51] developed a gamified e-learning system for blackboard, and an experiment was conducted to measure the learning outcome and performance of the experimental and control group, resulting in outperformed by the experimental group. Games are becoming increasingly popular in this modern age and are called "Education-al Games" or "Game-based learning." Game-based learning is a creative method of educating, improving learning, and excitement to cater to the requirements of numerous children, particularly those who are left behind. According to [52-56], the game-based application has been designated an instructional entertainment tool to encourage players to learn the skills during the play.

B. Game-based Language Learning

Electronic devices, such as smartphones, laptops, tablets, iPods, can serve as an effective and productive teaching resource for learners and lecturers in academia, especially when it comes to language learning through digital games [57]. Various studies have shown that gaming-based learning is valuable and revolutionary in the context of learning and

teaching. Thus, participants can help them increase their efficiency for language learning, improve their collaboration and maintain their effective outcomes. The findings showed that game-based learning had generated a highly efficient interactive learning environment, promoting student language skills [58]. Even though digital language learning games are generally represented by excitement, creativity, interest, surprise, domination, and immersive elements, they can boost students' attention, achievement, motivation, learning, and commitment [2] [58].

The author in [59] explored the effectiveness of the digital language learning game and found it more effective than the conventional teaching method in learning English. Similarly, [60] found that MMORPGs improved the dialogue ability in the English language. Teamwork, mutual understanding, and support were the elements in the dialogue. The study of [61] explored digital game-based language learning among learners and found its positive impact on language learning. The author in [62] used digital games in the Chinese context for the English language in the university. It was found that game-based learning reduced anxiety, reservedness and improved academic engagement. An experimental study was conducted to see the effectiveness of games used in English language class and got significant improvement output for the experimental group [63].

C. Theory of Usability

The author in [64] defined usability as a user who operates a particular object efficiently, quickly, and enjoys its operation. It has five features: satisfaction, memorability, error rate, performance, and learnability [30]. Moreover, usability was classified into satisfaction, effectiveness, and performance by International Organization for Standardization (ISO), but there was a lack of emphasis on user interface design, particularly for educational applications [65-66]. Furthermore, usability is divided into effectiveness, fastness, and safety [67]. Safety in this research was similar to the error rate recommended in the study of Nielsen. In contrast, fastness in the same analysis was identical to the effectiveness recommended by ISO and Nielsen. In addition to operating features, Preece and ISO concentrated on effectiveness, but the characteristics were not adequate. The effectiveness mentioned above in the Technology Acceptance Model (TAM) by [68] shows the functionality of a system and the possible impact accomplishment.

1) *Think-aloud theory*: The think-aloud technique involves the researchers speaking out their ideas to grasp further how the system functions. "Doing, thinking, and speaking" is another term to relate to the strategy as this method gives assessors the ability to offer their input by using the application. This data can yield essential knowledge to enhance the system's effectiveness because this technique has been one of the popular usability assessment approaches often used [69]. The benefits are that evaluators may efficiently conduct a thinking-aloud method, document intrinsically uncontrollable cognitive tasks, clearly grasp the direct reasons for utilizing challenges, and interact specifically with system

operations [70]. A diversity of experiments that used the think-aloud method in usability was successful [71-75].

2) *Heuristic evaluation*: A heuristic analysis [76] was performed on developing a user experience for an application and assessed usability based on previously learned skills. This assessment approach requires a limited sample of specialists to evaluate an interface to decide if the interface satisfies a series of standard operating indices and assess the product's technological suitability. The apparent benefit of this approach is that it does not require objective decisions, while assumptions and discussions are produced based on verified experience indices. With time constraints, making experts conduct the analysis would have doubled the impact, but half the time. This assessment is cost-effective and realistic, which eliminates the cognitive burdens of the evaluator, as well as heuristic assessment, which has proved to be a fruitful method for designing guidance architecture. During an assessment test, evaluators criticize and give recommendations for making the interface easy to use.

Similarly, this approach concentrates on usability problems and provides suggestions for the change of a system. Moreover, for the early stage of the usability life cycle, heuristic assessment by experts was suitable [76] since their more significant organizational expertise and advanced skills are required to conduct such evaluations. In the assessment process, experts recognize the experience of new participants to provide them with encounters that can arise between general users. For heuristic assessment, [94] proposed heuristics for LLSG given in Appendix A.

D. Current Studies for Heuristic Evaluation

In addition to the latest research findings on game-based learning, there are also usability tests for educational games. For usability review, three to five experts are more than appropriate for recognizing most usability issues. The general usability evaluation approach is ineffective because game design is separate from the application or system design. Some study has shown that computer video games require their heuristic structures. Therefore, several heuristics concerning video games were developed, who collected a series of heuristics for games from a case study and tested using Nielsen's heuristic and new guidance in the game industry [77][78][79]. Federoff's heuristics suffer from a lack of validation, clarity, and consistency. Additionally, these heuristics have minimal use throughout the design process [80][81].

A game-based application CAMEG was developed to teach students effectively and measure usability by taking a management information course. The researcher collected the data from a usability survey by taking student reviews and proposed an application suitable for learning [9]. A heuristic analysis was conducted with five human-computer interaction experts for the MOSAD application developed for the system, analysis, and development in a science subject. The findings revealed that MOSAD is a reliable and helpful application for revision purposes in higher education [5]. Similarly, a usability test was conducted for the primo discovery tool to detect user behavior patterns for library research. For this

purpose, gestures, verbal, and display behavior were analyzed through diagnostics usability evaluation to identify problems faced by users [9].

Video games are analyzed by the Playability Heuristic (PLAY), which involves three constraints [82], and this heuristic is required for three kinds of interactive games: first-person shooter, basic strategy, and action fantasy [78]. The heuristics are developed on a low generality case study by [82], but these heuristics are sometimes contradictory and vague [80]. The heuristics in PLAY are not appropriate for all game styles since each game style has its characteristics, structure, and usages [81]. The study of [83] analyzed the usability issues in interactive instructional games, giving particular attention to three aspects: the design (e.g., button, navigation), the process (e.g., ease of access, power, and learnability), and the gameplay (e.g., responsiveness). Their research utilized observation methods and interviews to examine usability issues from both users and non-users. The analysis of [84] measured the effectiveness of a virtual reality learning environment utilizing the widely recognized usability scale, and the findings revealed users' ratings of their perceptions and interests.

An investigation was performed for the effectiveness of an interactive video game on teaching digital engineering concepts in [85]. Students found the interactive tool to be a valuable educational platform and of strong usability. In the study of [71], the author analyzed the usability of a virtual environment health game about their feelings, decisions taken in the game, and responses to questions about player experiences through user interviews utilizing think-aloud analysis. In [86], the author conducted usability research using qualitative assessment and quantitative methodology to acquire users' impressions of college nursing subjects. Still, none of the aforementioned analyses consider experts reviews.

A review by [36] tested the usability of a writing pal application by utilizing various analysis approaches, including focus groups, vivo testing, module tests, and internal testing. The research contained student and teacher evaluations. Gamification instruction is a practical aspect in writing pal, which is meant to enhance students' proficiency in writing. The study [37] analyzed three interactive features: user interface acquaintance, navigation initiative, and VR environmental disturbances in instructional virtual reality technology games for geographical education. The experiment was performed on subjects like beginner players, advanced players, and professional players. The author of [33] conducted a usability analysis to test the usability of medical instructional games and simulations. A computer programmer built a specialist machine-dependent heuristic. A range of evaluation tools was used, such as examination, interviews, polls, and think-aloud. The study of [34] measured the usability of a web game-based learning application to teach users facial movements by heuristic testing utilizing the Nielson scale and user-think-aloud system to see user opinions, emotions, and viewpoints throughout the play. As outlined in this portion, various researchers have utilized different approaches and methods to test the usability of game-based educational resources. This study used both

heuristic evaluation and feedback through the think-aloud method for usability testing of LLSG.

III. METHODOLOGY

In this research, a heuristic evaluation and think-aloud method were used to decide which issues in the Graphical User Interface (GUI) of LLSG were inappropriate for language learners. The outcome allowed for developing a better-designed product, and the particular experts observed elements to recognize usability concerns.

Instructors, students, and a game developer were involved in the evaluation of the game. The instructors have good knowledge of assessing game content, and the designer has a strong understanding of the ability to determine the correct game elements. They evaluated a system to decide if it correctly followed known usability standards named “heuristics.” The Heuristic evaluation process consisted of three stages (Fig. 1 and Fig. 2). The first step was an analysis phase in which evaluators separately tested the game’s user interface by playing it on tablets. The second was a planning phase in which evaluators independently compile their list of identified issues for aggregation. In contrast, in the third phase, evaluators cooperate to produce a standard summary of usability problems. A prioritized list of usability issues was aggregated, compiled, and after review by the researcher, forwarded to the game developer for modification.

A. Sample of Study

According to [30] [87], approximately five to eight evaluators were required to conduct a heuristic evaluation. In this research, five professionals in the evaluation phase were involved with expertise and knowledge of English language teaching and game development. Moreover, twenty public sector school students were also part of this evaluation. The participants in the study were selected based on the convenience sampling technique. Table I describes the profile of experts.

Evaluator 1 was a female of 38-year-old with a Master in Education degree. She was familiar with mobile technology usage, videos, multimedia, and design and had experience in teaching and administration of 12 years. Evaluator 2 was a 43-year-old female with the degree of Bachelor in English language and known mobile technology and the experience of using it for 15 years at the school level. Evaluator 3 was a 33-year-old female with the degree of Bachelor in English language and has an understanding of computer technology with vast experience of teaching at various grades for 16 years. Evaluator 4 was a 31-year-old female with a Master in Education degree and attained a computer diploma from a professional institute. She had experience with computer and mobile technology teaching at grade ninth and tenth for 08 years. Lastly, Evaluator 5 was a male 29-year-old Game developer with a Bachelor in Computer Science degree and an expert in game and mobile application development. He was the senior developer in a Software house and played the role of team leader for the last five years. Twenty students (fifteen female and five male) from grade three of Government Girls High School were selected randomly for usability evaluation.

The mean age of the student evaluators was 11.6. Fig. 3a-3c shows the evaluation process of teachers and students.

B. Research Instrument

Usability is an important and emerging area in smartphone applications that cannot be avoided by proper software design. The researcher developed a language learning serious game in this study after constructing a theoretical model to measure its usability [5] [9]. For the usability perspective of a game-based application, a heuristic evaluation [30] was conducted from the stakeholders. The following instrument was used to conduct this research:

1) *Language learning serious game (LLSG)*: LLSG is a mobile-based and standalone game for English language learning consisted of Eight modules; “Sound,” “Singular/Plural,” “Uses (is/am/are),” “Action Words,” “Parts of Speech,” “Sentences,” “W Family,” and “Comprehension.”



Fig. 1. Heuristic Evaluation Process-1.

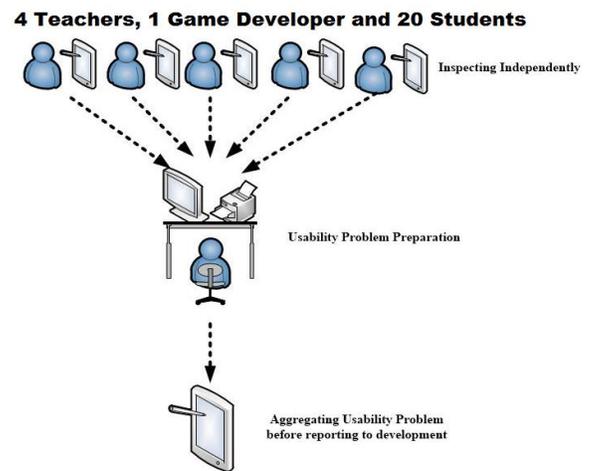


Fig. 2. Heuristic Evaluation Process-2.

TABLE I. PROFILE OF EVALUATORS

Sr. No.	Professional Role	User Experience (in Years)		
		Administration	Teaching at School	Games
1	Senior Headmistress	8	4	-
2	Teacher	5	15	-
3	Teacher	-	16	-
4	Teacher	-	08	-
5	Game Developer	-	-	8
6	Students	-	-	-



(a)

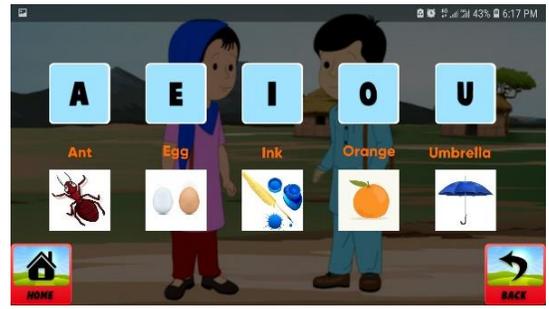


(b)



(c)

Fig. 3. (a). High-Fidelity Teacher Evaluation, (b). High-Fidelity Student Evaluation-1, (c). High-Fidelity Student Evaluation-2.



(b)



(c)



(d)



(e)



(a)



(f)



Fig. 4. (a) Main Menu, (b) Vowels, (c) Singular/Plural, (d) Singular/Plural Assessment, (e) Parts of Speech, (f) Parts of Speech Assessment, (g) Instruction after Mistakes, (h) Reward.

Fig. 4a shows the overview of the LLSG application containing all components offered in the game. For the learning, a user can click on any element, and the teacher will guide them to start with the first module, 'sounds,' in which a student will learn vowels (Fig. 4b), diagraphs, two/three letter sounds, and so on. Students can learn pronunciation by pressing the word/picture in the learning phase. After its completion, students can pick the assessment based on the complexity (Easy, Medium, and Advanced) to evaluate its progress. Fig. 4c and 4d are related to learning singular/plural and its assessment. Fig. 4e and 4f show the screenshot of parts of speech in which users need to click on the desired sub-module to learn noun, adjective, verb, pronoun, preposition, and assessments. As a user clicks on the assessment, they will proceed to their relevant exercises based on their complexity. Fig. 4g shows the instructions, as users make three mistakes while solving an exercise, will directly move back to its learning page to revise it. Finally, Fig. 4h shows the screenshot related to the assessment in which students can get correct or wrong attempts along with the remarks (Perfect/Good/Fair).

2) *Questionnaire*: For usability evaluation of LLGS, a questionnaire was administered based on a list of heuristics principles for interface design proposed by [94]. The questionnaire was categorized into three sections: demographic information in the first, heuristic for LLSG [94] for interface design at second, and expert comments in the third section were asked. When the evaluations were complete, the researchers compiled, interpreted, and evaluated the assessment findings. The heuristics in Appendix A for LLSG is illustrated.

3) *Technical tools (hardware & software)*: A laptop and a mouse as hardware equipment, unity as the primary development kit to develop the android package (.apk) of the game application, was used. A heuristic evaluation was performed by offline tasks for the application launched on the tablet provided by the school. The assessment phase was composed of many steps:

4) *Permission*: A departmental permission was required for the experiment and to collect data from a public sector school. The researcher wrote a letter to Chief Education Officer to get permission for the purpose under the supervision of the supervisor. After receiving approval from the stakeholders, the researcher set up a meeting with the professional evaluators and described the intention of the evaluation whereas, the researcher arranged a meeting with the game developer through a call to consult and clarify the evaluation objectives.

5) *Application demonstration*: The researcher explained how the applications work before presenting them to the experts then the questionnaire survey was handed over to the evaluators.

6) *Feedback*: The expert analyzed the LLSG application depending on the questions asked in the questionnaire. The next step was to collect a questionnaire from experts then compile data. The expert advice to strengthen the application and also commented on the issues. When the assessment was concluded, the review of the data proceeded immediately.

C. Evaluation Process

The current research used a heuristic evaluation methodology and think-aloud method approach, which allowed for low cost and simplicity. It made it more effective than other usability studies and effectively guided the experts to evaluate the game. The questionnaire was completed by five experts and twenty school students who practiced LLSG during the evaluation process. The evaluation was implemented in a classroom for students and the principal's office for teachers. Students completed their questionnaires with the help of a teacher.

The evaluation process took two hours for the teacher and three hours for students. Before the evaluation process, each game function was explained to them, and the researcher provided prompt responses to fix their issues.

Each evaluator independently assessed the language learning game using [76] and [88] heuristic assessment processes. Since each expert finished their assessment, they were allowed to speak openly amongst themselves on their experiences. Similarly, every student evaluator used LLSG and accomplished the questionnaire separately. Following usability testing, the evaluators reviewed the application to verify its reliability.

TABLE II. STEPS OF THINK-ALOUD APPROACH

Item #	Steps	Explanation
1	Explanation	The evaluators were briefed on the think-aloud research process and the most relevant usability concepts.
2	Practice	The evaluators experienced "speaking while thinking" to become familiar with the behavior model.
3	Execution	Shared the thoughts and suggestions with the other evaluators while the language learning game was running. The procedures of the activities were captured on film, and their viewpoints were documented; and
4	Protocol analysis	The author transcribed the voice samples.

The evaluators checked the application at least twice, the first time for thorough comprehension and the second time for ease of usage. The evaluators also used think-aloud methods to collect data when evaluating and using the game. Following the phases of the think-aloud method are defined in Table II.

This triangulation method was employed to enhance the validity and credibility of findings [89]. Data was gathered in different ways, and results were analyzed independently, but they needed to be compared. The researcher and co-researcher coded and evaluated the document using heuristics proposed by [94]. The evaluator checked the coding in-depth and updated it, focusing on the triangulation method for internal and external validity. It was further reviewed by the evaluator and the co-researcher for the efficiency of data transcription. Eventually, the study findings were combined with the participant's questionnaire responses and observations.

D. Validity and Reliability

This research employed the questionnaire after verifying the reliability and validity [3] [38] [90]. As determined by Cronbach's alpha, the reliability factor of each construct was higher than 0.8 based on the findings of 20 students. It showed perfect truthfulness for every structure and a sufficient internal consistency between all elements inside the construct. Furthermore, the following four factors were considered to enhance the confidence of the think-aloud method: validity, reliability, transferability, and credibility [91].

Triangulation of analysts was utilized in this research to ensure its reliability [92]. Three researchers individually examined data and evaluated their results. Additionally, a qualitative research technique specialist was present throughout the data processing process. Transparency was guaranteed by providing transcripts of a participant's think-aloud procedure and demonstrating how the data were coded and classified. Sampling techniques were also used in this research to increase transferability. Each think-aloud process was administered under identical circumstances to guarantee the reliability, and the researcher transcribed the data consistently. In addition, details have been provided on data collection and analysis methods. If required, the findings may be verified, as all the tape recordings, translations, and coding are preserved. As a result, truthfulness was achieved as well.

IV. RESULTS AND DISCUSSION

The results and discussion section were categorized into 1) Heuristic Evaluation results; and 2) teacher evaluators' comments and feedback.

TABLE III. HIGH-FIDELITY PROTOTYPE HEURISTIC EVALUATION RESULTS

Component	Item	Teacher Experts			Students		
		Yes	No	Not Sure	Yes	No	Not Sure
I	LHI1	100			100		
	LHI2	100			90		10
	LHI3	100			90		10
	LHI4	100			100		
	LHI5	100			100		
	LHI6	100			100		
	LHI7	100			100		
	LHI8	100			100		
	LHI9	100			100		
	LHI10	100			100		
	LHI11	100			100		
	LHI12	100			100		
GP	LHGP1	100			90		10
	LHGP2	100			100		
	LHGP3	100			100		
	LHGP4	100			100		
	LHGP5	100			100		
GM	LHGM1	100			100		
	LHGM2	100			100		
C	LHC1	100			90		10
	LHC2	100			100		
	LHC3	100			100		
	LHC4	100			100		
	LHC5	80		20	100		
	LHC6	100			100		
	LHC7	100			100		
	LHC8	100			100		
F	LHF1	100			100		
	LHF2	100			90		10
	LHF3	100			100		
LL	LHLL1	100			100		
	LHLL2	100			100		
	LHLL3	100			100		
	LHLL4	100			100		
	LHLL5	100			100		
	LHLL6	100			100		
CC	LHCC1	100			90		10
	LHCC2	100			100		
	LHCC3	100			100		
	LHCC4	100			100		
	LHCC5	100			80		
	LHCC6	100			100		
	LHCC7	100			100		
	LHCC8	100			100		
	LHCC9	100			100		
	LHCC10	100			100		
	LHCC11	100			100		

A. Heuristic Evaluation Result

The questionnaire was distributed between teachers and students to evaluate the high-fidelity prototype of LLSG, which was consisted of seven components and 47 elements. A descriptive analysis method to analyze the results of the heuristic evaluation questionnaire was used through Microsoft Excel. The authors [64] [88] specified that a heuristic evaluation result was a table or a list of usability issues presented in Table III. The individual agreement for each element was evaluated in terms of ‘Yes,’ ‘No,’ or ‘Not sure,’ and the frequency rates were calculated. The term ‘Not sure’ referred to any possibility that the expert is unsure about the item's answer.

The demographic information showed the teachers’ and students’ gender and age group, the study's respondents. Four (80%) female teachers and fifteen (75%) female students, whereas only one (20%) male (game developer) and five (25%) male students were the evaluators for the game. From the age perspective, one evaluator belonged to the age group of 25-30, two belonged to 30-35, and one was 35-40 and above 40 each. One student evaluator belonged to the age group of 7-8; the majority belonged to 9-10, and nine belonged to the age group of above 10.

(Language Heuristics-LH)

This section presented the results obtained from the heuristic evaluation and discussed with the feedback of the

experts. Table III shows the percentage score results from the descriptive data analysis. The majority of the heuristic evaluation elements scored 100% on average, whereas one element scored 80% from teachers’ experts, and five elements scored 90% with ‘not sure.’ In the Interface (I) component, as shown in Table IV, all the elements by all the teachers’ experts agreed 100%, and 90% of student evaluators were agreed with all the items except (LHI2, LHI3) as they were not sure about them. Therefore, the high-fidelity prototype interface design has no usability issues.

In the term gameplay (GP), all the teacher experts agreed with all the elements, whereas 90% of student evaluators were agreed with all the items except (LHGP1) as two evaluators responded with ‘Not sure’ comment. Regarding the game mechanics (GM), all the teachers and student evaluators were agreed 100% on all the elements. In content (C), all the elements were accepted by the evaluators except (LHC5) by one teacher’s expert and (LHC1) by two student evaluators. The experts agreed that game design content was adapted from the book (English curriculum) approved by the concerned authority. Furthermore, the content in the game was suitable for learning vocabulary and enhancing English comprehension. All the elements in the feedback (F) component was agreed by all teachers and student experts, with 100% mentioning that game provided instant feedback after solving the exercises with correct and wrong answers status.

TABLE IV. HIGH-FIDELITY PROTOTYPE HEURISTIC EVALUATION RESULTS BASED ON ITEMS

Components	Teachers’ Evaluators			Student Evaluators		
	No. of experts	Items	Marks	No. of experts	Items	Marks
I	5	(LHI1, LHI2, LHI3, LHI4, LHI5, LHI6, LHI7, LHI8, LHI9, LHI10, LHI11, LHI12)	Yes	18	(LHI1, LHI4, LHI5, LHI6, LHI7, LHI8, LHI9, LHI10, LHI11, LHI12)	Yes
				2	LHI2, LHI3,	Not Sure
GP	5	((LHGP1, LHGP2, LHGP3, LHGP4, LHGP5)	Yes	18	(LHGP2, LHGP3, LHGP4, LHGP5)	Yes
				2	(LHGP1)	Not Sure
GM	5	(LHGM1, LHGM2)	Yes	20	(LHGM1, LHGM2)	Yes
C	4	(LHC1, LHC2, LHC3, LHC4, LHC6, LHC7, LHC8)	Yes	18	(LHC2, LHC3, LHC4, LHC5, LHC6, LHC7, LHC8)	Yes
	1	(LHC5)	Not Sure	2	(LHC1)	Not Sure
F	5	(LHF1, LHF2, LHF3)	Yes	20	(LHF1, LHF2, LHF3)	Yes
LL	5	(LHLL1, LHLL2, LHLL3, LHLL4, LHLL5, LHLL6)	Yes	20	(LHLL1, LHLL2, LHLL3, LHLL4, LHLL5, LHLL6)	Yes
CC	4	(LHCC1, LHCC2, LHCC3, LHCC4, LHCC5, LHCC6, LHCC7, LHCC8, LHCC9, LHCC10, LHCC11)	Yes	18	(LHCC2, LHCC3, LHCC4, LHCC5, LHCC6, LHCC7, LHCC8, LHCC9, LHCC10, LHCC11)	Yes
				2	LHCC1	Not Sure

In the language learning section (LL), all the elements were agreed upon by all the teachers and student experts with 100% by expressing that English language learning becomes easy with the help of the game. It further helped students to improve their vocabulary and English comprehension in grade three. Lastly, in the cultural context (CC), all the elements by the teacher evaluators were agreed with 100%. In contrast, only one element (LHCC1) by two student experts were 'not sure' by the student evaluators. All the elements are considered effective for the game in a cultural context by the teachers and student evaluators. The experts' responses and comments who responded with 'Not sure' were considered, and the score of seven constructs of the LLSG (I, GP, GM, C, F, LL, and CC) was 90%.

After analyzing all the data from the stakeholders, the finding from the above tables shows that the game-based learning application developed for grade three students of public sector schools is useful and usable. Overall, the results obtained from the heuristic evaluation were very positive, indicating that the high-fidelity prototype had most of the required language learning, educational, and cultural context elements. All the items provided in the sections of heuristics were acceptable by the teacher and student evaluators, but in one section, teachers and students were not sure about the component of LLSG. After compiling the identified issues, it was found that the color scheme in the game interfaces needed minor revision. Some shortcuts of common actions were not available in the game. So, it is necessary to follow a standard for the interface's color scheme by adding common touchpad button shortcuts in the game where necessary.

B. Think-Aloud Method (Expert Review)

In addition to studying the observable factors, evaluators have given their input and reflected on what they considered the games' positive and negative features. The comments and feedback are given in Table V.

The comments of teacher evaluators and students focused on the game usability that makes sure it is efficient and useful for language learning. The modules provided in the LLSG were quite important and helpful for learning the English language in public sector schools. The sounds module helped to learn vowel, short vowel, and long vowel sounds along with its exercises. Singular/plural and uses of

is/am/are/has/have/was/were the second and third modules that provide the pictorial presentations of the topic with pronunciation. Similarly, parts of speech, action words, sentences, w family, and comprehension are the further modules available in the LLSG enriched with easy and interesting learning material and with pronunciation that helped to learn these topics efficiently. After learning the desired topic, an assessment with its difficulty level could be made to evaluate the performance and progress with the defined reward.

According to the feedback, there were minor corrections of the color scheme on various interfaces that needs to be changed as well as the 'Home' and 'Back' button needs alignment in the appropriate place of interfaces. The 'Hint' button is to get help from the students while attempting medium and advanced level exercises in the game was also missing on some interfaces that need to be added. The font size of the text has a vital part in any game application, whereas font size on some interfaces of LLSG required some corrections. Furthermore, cultural pictures in the text for practicing a topic to learn a language are very helpful, but in LLSG, these pictures from the text were missing that will be added while pronunciation was also missing in language learning practicing some exercises that needed to be resolved. Similarly, in some exercises, right and wrong attempts and reward system that motivates students to learn a language effectively were not working properly and required some corrections. However, the game developers' remarks are meant to change the graphical user experience of the device to enhance functionality that renders the system complete.

For effectiveness, the teacher evaluators and students reported that the LLSG is helpful, easy, and effective for learning English and achieving the desired learning outcome. The evaluators noted that the learning material (content) provided in the game is easy, understandable, and logical, especially the pictorial presentation which could help to understand the topic efficiently. Lastly, it was reported that LLSG is easy to use at home because it is a standalone application that does not require internet access, and it could be used at home with the help of parents with interest. The quick response after solving exercises helped and passionate to see the progress of the desired topic that causes motivation and more engagement with the game.

TABLE V. FEEDBACK AND COMMENTS

Construct/ Modules	Evaluation Comments		Action to be taken
	Expert	Students	
Sounds	The sound module allowed learning vowels, short vowels, and long vowels with pronunciation and colorful pictures.	This section helped to learn the sounds of vowels with pronunciation.	-
Singular/Plural	This module guided me to learn singular/plural with pictorial representation and assessment.	This section helped me to learn singular/plural with pictures and pronunciation.	-
Uses	The uses module helped to learn: is, am, are, has, have, had, was, were with pictures and pronunciations.	This module guided to use is, am, are, etc., in the sentences with pronunciation.	-
Action Words	Action words guided to identify the activity using pictures, pronunciations, and assessment.	In this section, the sentence is represented in pictorial form and can be pronounced.	-

Parts of Speech	This module helped to learn nouns, pronouns, verbs, adjectives, and prepositions separately with its easy, medium, advanced assessment.	This section helped to learn with pronunciation and pictures the noun, pronoun, verb, adjective, and preposition.	-
Sentences	This section guided to write a proper sentence structure with its assessment.	This section taught the sentence structure with capitalization and full stop.	-
W Family	This module helped to learn W's family (Why What, Where, Who, Whom) with pronunciation and assessment.	This section guided learning: why, what, where, who, whom with pronunciation and different assessment levels.	-
Comprehension	This module guided to understand the English long sentences with pictorial representation and pronunciation for easy understanding.	This section taught the understanding of long sentences with pictures and pronunciation.	-
Usability	<ol style="list-style-type: none"> The 'Home' and 'Back' buttons were not aligned on all interfaces, which caused a delay in using them. The 'Hint' button was missing in the medium level of exercise that supports the user. The font size was different in a few interfaces which is less readable. 	<ol style="list-style-type: none"> The 'Home' button was different on one screen and another on other screens. 'Hint' button that guided to solve a query was missing on some screens. The font size of the text was different on some screens. 	<ol style="list-style-type: none"> The home button will be aligned in the bottom right corner, and the Back button will be aligned in the bottom left corner. A hint button will be added to the appropriate screens (where missing). Font size in the game will be used according to a standard for the ease of users.
Content	<ol style="list-style-type: none"> Pictures were missing in the practicing topic. The alignment of questions in some exercises had disturbed, which was the cause of less efficient reading. Pronunciation was missing in some practicing exercises. 	<ol style="list-style-type: none"> Some pictures were not available while practicing. Some questions were not in-line that was creating difficulty during reading. On some screens, the pronunciation was missing 	<ol style="list-style-type: none"> Necessary pictures will be added to the missing places. The alignment will be made after making corrections in the code of the game. The pronunciation issue will sort out by reviewing the code.
Assessment and Reward	<ol style="list-style-type: none"> After solving the exercises, the correct and wrong attempt was missing, which could help a user's progress. Reward with appropriate remarks was also missing, which could passionate the user for solving the exercises efficiently. 	<ol style="list-style-type: none"> Correct and wrong attempts were not available to evaluate a topic. Stars were missing in some exercises that could create the interest of the user to learn efficiently. 	<ol style="list-style-type: none"> A screen of correct and wrong attempts will be added after solving all the questions. Stars will be rewarded with an appropriate comment after solving an exercise.
Effectiveness	<ol style="list-style-type: none"> This game-based language learning application helped to learn the language. This could help to achieve the learning outcomes effectively. 	<ol style="list-style-type: none"> The game was very easy, interesting, and helpful for learning the English language. 	-
Learnability	<ol style="list-style-type: none"> The material provided for learning was easy to understand and logical. The text and pictorial representation of topics made learning easy. 	<ol style="list-style-type: none"> The content was very easy and understandable. Pictures in the game were helpful to understand the topic clearly and easily. 	-
Efficiency	<ol style="list-style-type: none"> The color scheme used in the game is not following a standard, and it looks less attractive. The keypad was not functional to solve some exercises in the medium and advanced levels. 	<ol style="list-style-type: none"> The color scheme of some screens is different from each other. On some screens, there was a problem while solving questions. 	<ol style="list-style-type: none"> The color scheme for the game will follow a standard to be the same in all interfaces. The problem will be fixed after reviewing the code.
Satisfaction	<ol style="list-style-type: none"> Instant feedback after solving the exercises developed the interest to use the game more and more. Due to standalone, it is easy to use anytime at home on parents' mobile with interest. 	<ol style="list-style-type: none"> The quick response for solving the exercise helped to see the progress and passion for using the game for a long time. This game is easy to use at home with the help of parents and with interest. 	-
Cultural Context	The cultural context is very important for developing a language learning game and focusing on graphic symbols related to gender, age, sex, and religion. More cultural context pictures will engage the students for language learning with interest.	The game has cultural context, including icons, symbols, and images that helped to use it without any hesitation.	Few more pictures could be added where required to represent the culture.

V. CONCLUSION AND FUTURE WORK

This study aimed to evaluate the usability of LLSG, a language learning serious game comprising eight modules developed for learning English as a secondary language. Each module was enriched with learning content, pronunciation of words & sentences, and evaluation. To this end, two prominent methods, namely, heuristic evaluation and the think-aloud methods, were used while engaging different stakeholders, including language experts, students, teachers, and the game developers. As far as the heuristic evaluation is concerned, the researcher proposed heuristics, used to assess LLSG. At the same time, the think-aloud method was based on thorough discussion sessions held by the stakeholders.

The evaluation demonstrated that most of the domains were ranked above average and received positive scores, whereas two domains of the questionnaire were rated below average. The findings through both methods were very appreciative for LLSG. Teachers and students felt satisfied and accepted the effectiveness of game-based teaching and learning methods for language learning. Similarly, the findings from the think-aloud method were encouraging for LLSG, and feedback provided by the evaluators required slight changes to enhance game application according to the expectations and needs of the users. These minor concerns were about the look and feel, including the color scheme, font size, labels, and buttons. The teachers' remarks were primarily based on the subject material, and the improvement of gaming functionality was more significant. Apart from this, the primary assessment was covered in this game, where right and wrong attempts were recorded, but the detailed assessment might be recorded to see each student's progress level.

Moreover, this game was a standalone application that worked only on a tablet and recorded results in the local database. LLSG might be moved to the network model to increase its scope and connect it with a centralized database to store each student's question bank and grades for each assessment activity. In future work, the enhancements of the game-based learning may be carried out, and the network model may also be adopted from the current practice.

ACKNOWLEDGMENT

This research was funded by Universiti Kebangsaan Malaysia under the grant number: FRGS/1/2019/ICT01/UKM/01/1. The authors would like to thank the school education department (Sheikhupura) to provide special permissions for experimenting in the school.

REFERENCES

- [1] Malas, R. I.; Hamtini, T. A Gamified E-Learning Design Model to Promote and Improve Learning. *Int. Rev. Comput. Softw. (IRECOS)* 2016, 11 (1), 8.
- [2] Ishaq, K.; Zin, N. A. Mat; Rosdi, F.; Jehanghir, M.; Ishaq, S.; Abid, A. Mobile-Assisted and Gamification-Based Language Learning: A Systematic Literature Review. *PeerJ Comput. Sci.* 2021, 7 (e496), e496.
- [3] Abidin, S. R. Z.; Fadzilah, S.; Sahari, N. Heuristic Evaluation of Serious Game Application for Slow-Reading Students. *Int. J. Adv. Comput. Sci. Appl.* 2019, 10 (7). <https://doi.org/10.14569/ijacsa.2019.0100764>.
- [4] Ahmad, A.; Zeshan, F.; Khan, M. S.; Marriam, R.; Ali, A.; Samreen, A. The Impact of Gamification on Learning Outcomes of Computer Science Majors. *ACM trans. comput. educ.* 2020, 20 (2), 1–25.
- [5] Ishaq, K.; Rosdi, F.; Azan, N.; Abid, A. Usability and Design Issues of Mobile Assisted Language Learning Application. *Int. J. Adv. Comput. Sci. Appl.* 2020, 11 (6). <https://doi.org/10.14569/ijacsa.2020.0110611>.
- [6] Ishaq, K.; Azan, N.; Rosdi, F.; Abid, A.; Ali, Q. Usefulness of Mobile Assisted Language Learning in Primary Education. *Int. J. Adv. Comput. Sci. Appl.* 2020, 11 (1). <https://doi.org/10.14569/ijacsa.2020.0110148>.
- [7] Nielsen, J.; Landauer, T. K. A Mathematical Model of the Finding of Usability Problems. In *Proceedings of the SIGCHI conference on Human factors in computing systems - CHI '93*; ACM Press: New York, New York, USA, 1993.
- [8] Barata, G.; Gama, S.; Fonseca, M. J.; Gonçalves, D. Improving Student Creativity with Gamification and Virtual Worlds. In *Proceedings of the First International Conference on Gameful Design, Research, and Applications*; ACM: New York, NY, USA, 2013.
- [9] Ishaq, K.; Azan, N.; Rosdi, F.; Abid, A.; Ali, Q. Usability of Mobile Assisted Language Learning App. *Int. J. Adv. Comput. Sci. Appl.* 2020, 11 (1). <https://doi.org/10.14569/ijacsa.2020.0110145>.
- [10] Elaish, M. M.; Ghani, N. A.; Shuib, L.; Al-Haiqi, A. Development of a Mobile Game Application to Boost Students' Motivation in Learning English Vocabulary. *IEEE Access* 2019, 7, 13326–13337.
- [11] Sahrir, M. S., & Alias, N. A. A study on Malaysian language learners' perception towards learning Arabic via online games. *GEMA Online Journal of Language Studies* 2011, 11(3), 129-145.
- [12] Ashraf, H.; Motlagh, F. G.; Salami, M. The Impact of Online Games on Learning English Vocabulary by Iranian (Low-Intermediate) EFL Learners. *Procedia Soc. Behav. Sci.* 2014, 98, 286–291.
- [13] Ibrahim, A. Advantages of using language games in teaching English as a foreign language in Sudan basic schools. *American Scientific Research Journal for Engineering, Technology, and Sciences (ASRJETS)*, 2017, 37(1), 140-150.
- [14] Wong, L. H. Analysis of Students' After-School Mobile-Assisted Artifact Creation Processes in a Seamless Language Learning Environment. *J. Educ. Technol. Soc.* 2013, 16(2), 198-211.
- [15] Chen, X. Evaluating language-learning mobile apps for second-language learners. *Journal of Educational Technology Development and Exchange (JETDE)*. 2016, 9(2), 3.
- [16] Wang, Z., & Han, F. Developing English language learners' oral production with a digital game-based mobile application. *PLoS ONE*. 2021, 16(1), 1–11. <https://doi.org/10.1371/journal.pone.0232671>.
- [17] Hwang, W. Y., Ma, Z. H., Shadiev, R., Shih, T. K., & Chen, S. Y. Facilitating listening and speaking with game-based learning activities in situational context. In *Emerging issues in smart learning*. Springer, Berlin, Heidelberg. 2015, 193-200.
- [18] Meyer, B. Learning English through serious games—reflections on teacher and learner performance. In *Transactions on edutainment iii*. Springer, Berlin, Heidelberg. 2009, 82-92.
- [19] Cervi-Wilson, T., & Brick, B. *ImparApp: Italian language learning with MIT's TaleBlazer mobile app. Innovative language teaching and learning at university: integrating informal learning into formal language education*. 2018, 49.
- [20] Rocchetti, M., Salomoni, P., Loiseau, M., Masperi, M., Zampa, V., Ceccherelli, A., Cervini, C., & Valva, A. On the design of a word game to enhance Italian language learning. *2016 International Conference on Computing, Networking and Communications, ICNC*. 2016, 2–6. <https://doi.org/10.1109/ICCNC.2016.7440546>.
- [21] Vasileiadou, I., & Makrina, Z. Using Online Computer Games in the ELT Classroom: A Case Study. *English Language Teaching*. 2017, 10(12), 134-150.
- [22] Lee, K., Kweon, S. O., Lee, S., Noh, H., Lee, J., Lee, J., ... & Lee, G. G. Effects of language learning game on Korean elementary school students. In *Speech and Language Technology in Education*. 2011.
- [23] Supuran, A. The opportunity of introducing serious games in teaching English for specific purposes. A study case on playing "simplycycle" serious game. *Journal of Teaching English for Specific and Academic Purposes*. 2017, 5(3), 459-466.
- [24] Casañ-Pitarch, R. An approach to digital game-based learning: Video-games principles and applications in foreign language learning. *Journal of Language Teaching and Research (Online)*. 2018, 9(6), 1147-1159.

- [25] Rachels, J. R., & Rockinson-Szapkiw, A. J. The effects of a mobile gamification app on elementary students' Spanish achievement and self-efficacy. *Computer Assisted Language Learning*. 2018, 31(1–2), 72–89.
- [26] Ishaq, K., Zin, N. A. M., Rosdi, F., Abid, A., & Farooq, U. Effectiveness of literacy & numeracy drive (LND): A students' perspective. In 2019 International Conference on Innovative Computing (ICIC). IEEE. 2019, 1–10.
- [27] Ishaq, K., Zin, N. A. M., Rosdi, F., Abid, A., & Ali, Q. Usefulness of mobile assisted language learning in primary education. *International Journal of Advanced Computer Science and Applications*. 2020e, 11(1), 384–395. <https://doi.org/10.14569/ijacsa.2020.0110148>.
- [28] Ishaq, K., Rosdi, F., Zin, N. A. M., & Abid, A. Requirements elicitation for game-based language learning application (Unpublished). In 2021 International Conference on Innovative Computing (ICIC). IEEE. 2021, 1–10.
- [29] O'Neil, H. F., Wainess, R., & Baker, E. L. Classification of learning outcomes: Evidence from the computer games literature. *Curriculum Journal*. 2005, 16(4), 455–474.
- [30] Nielsen, J. Usability engineering. Morgan Kaufmann. 1994a.
- [31] Nielsen, J. Designing websites to maximize press relations: guidelines from usability studies with journalists. Silicon Valley, CA: Nielsen Norman Group. 2003.
- [32] Adebisin, T. F., De Villiers, M. R., & Ssemugabi, S. Usability testing of e-learning. Proceedings of the 2009 Annual Conference of the Southern African Computer Lecturers' Association. 2009, 4, 1–1.
- [33] Albu, M., Atack, L., & Srivastava, I. Simulation and gaming to promote health education: Results of a usability test. *Health Education Journal*. 2015, 74(2), 244–254.
- [34] Isleyen, F., Gulkesen, K. H., Cinemre, B., Samur, M. K., Zayim, N., & Sen Kaya, S. Evaluation of the Usability of a Serious Game Aiming to Teach Facial Expressions to Schizophrenic Patients. *Studies in Health Technology and Informatics*. 2014, 205, 662–666.
- [35] Lim, C., Song, H. D., & Lee, Y. Improving the usability of the user interface for a digital textbook platform for elementary-school students. *Educational Technology Research and Development*. 2012, 60(1), 159–173.
- [36] Roscoe, R. D., Allen, L. K., Weston, J. L., Crossley, S. A., & McNamara, D. S. The writing pal intelligent tutoring system: Usability testing and development. *Computers and Composition*. 2014, 34, 39–59.
- [37] Virvou, M., & Katsionis, G. On the usability and likeability of virtual reality games for education: The case of VR-ENGAGE. *Computers and Education*. 2008, 50(1), 154–178.
- [38] Nielsen, J., & Molich, R. Heuristic evaluation of user interfaces. Conference on Human Factors in Computing Systems – Proceedings. 1990, 249–256.
- [39] Prensky, M. Digital Game-based Learning Prensky. *Games2train*. 2003, 1(1), 1–4.
- [40] Brangier, E., & Marache-Francisco, C. Measure of the Lived and Functional Effects of Gamification: An Experimental Study in a Professional Context. In *Advances in Intelligent Systems and Computing*. Springer International Publishing. 2020, 955.
- [41] Osipovskaya, E., & Miakotnikova, S. Using Gamification in Teaching Public Relations Students. In *Advances in Intelligent Systems and Computing*. Springer International Publishing. 2020, 916.
- [42] Tundjungsari, V. Mobile Learning Design Using Gamification for Teaching and Learning in Algorithms and Programming Language. *Advances in Intelligent Systems and Computing*. 2020, 916, 650–661.
- [43] Mayer, R. E. The promise of multimedia learning: using the same instructional design methods across different media. *Learning and Instruction*. 2003, 13(2), 125–139.
- [44] Garris, R., Ahlers, R., & Driskell, J. E. Games, motivation, and learning: A research and practice model. *Simulation and Gaming*. 2002, 33(4), 441–467.
- [45] Mayer, R., & Johnson, C. Adding instructional features that promote learning in a game-like environment. *Journal of Educational Computing Research*. 2010, 42(3), 241–265.
- [46] Couceiro, R. M., Papastergiou, M., Kordaki, M., & Veloso, A. I. Design and evaluation of a computer game for the learning of Information and Communication Technologies (ICT) concepts by physical education and sport science students. *Education and Information Technologies*. 2013, 18(3), 531–554.
- [47] Gee, J. P. What video games have to teach us about learning and literacy. *Computers in Entertainment*. 2003, 1(1), 20–20.
- [48] Giannakos, M. N. Enjoy and learn with educational games: Examining factors affecting learning performance. *Computers and education*. 2013, 68(246016), 429–439.
- [49] Klisch, Y., Miller, L. M., Wang, S., & Epstein, J. The Impact of a Science Education Game on Students' Learning and Perception of Inhalants as Body Pollutants. *Journal of Science Education and Technology*. 2012, 21(2), 295–303.
- [50] Steinkuehler, C., Squire, K., & Barab, S. A. Games, learning, and society: learning and meaning in the digital age. Cambridge University Press. 2012.
- [51] Domínguez, A., Saenz-De-Navarrete, J., De-Marcos, L., Fernández-Sanz, L., Pagés, C., & Martínez-Herráiz, J. J. Gamifying learning experiences: Practical implications and outcomes. *Computers and Education*. 2013, 63, 380–392.
- [52] Abidin, S. R. Z., Noor, S. F. M., & Ashaari, N. S. Low-fidelity prototype design for serious game for slow-reading students. *International Journal of Advanced Computer Science and Applications*. 2019, 10(3), 270–276.
- [53] Acquah, E. O., & Katz, H. T. Digital game-based L2 learning outcomes for primary through high-school students: A systematic literature review. *Computers and Education*. 2020, 143, 103667.
- [54] Hamari, J., Shernoff, D. J., Rowe, E., Coller, B., Asbell-Clarke, J., & Edwards, T. Challenging games help students learn: An empirical study on engagement, flow and immersion in game-based learning. *Computers in Human Behavior*. 2016, 54, 170–179.
- [55] Vee Senap, N. M., & Ibrahim, R. (2019). A review of heuristics evaluation component for mobile educational games. *Procedia Computer Science*. 2019, 161, 1028–1035.
- [56] Zhonggen, Y. (2019). A Meta-Analysis of Use of Serious Games in Education over a Decade. *International Journal of Computer Games Technology*. 2019, 2019(3).
- [57] Suo, Y. M., Suo, Y. J., & Zalika, A. Implementing Quizizz as game based learning in the Arabic classroom. *European Journal of Social Science Education and Research*. 2018, 12(1), 208–212.
- [58] Elthahir, M. E., Alsalhi, N. R., Al-Qatawneh, S., AlQudah, H. A., & Jaradat, M. The impact of game-based learning (GBL) on students' motivation, engagement and academic performance on an Arabic language grammar course in higher education. *Education and Information Technologies*. 2021.
- [59] Tsai, Y. L., & Tsai, C. C. Digital game-based second-language vocabulary learning and conditions of research designs: A meta-analysis study. *Computers & Education*. 2018, 125, 345–357.
- [60] Peterson, M. The use of massively multiplayer online role-playing games in CALL: An analysis of research. *Computer Assisted Language Learning*. 2016, 29(7), 1181–1194.
- [61] Hung, H. T., Yang, J. C., Hwang, G. J., Chu, H. C., & Wang, C. C. A scoping review of research on digital game-based language learning. *Computers & Education*. 2018, 126, 89–104.
- [62] Ho, J. Gamifying the flipped classroom: how to motivate Chinese ESL learners?. *Innovation in Language Learning and Teaching*. 2020, 14(5), 421–435.
- [63] Mifsud, C. L., Vella, R., & Camilleri, L. Attitudes towards and effects of the use of video games in classroom learning with specific reference to literacy attainment. *Research in Education*. 2013, 90(1), 32–52.
- [64] Nielsen, J., & Loranger, H. Prioritizing web usability. Pearson Education. 2006.
- [65] ISO. Ergonomic requirements for office work with visual display terminals (VDTs)-Part II Guidance on usability. ISO/IEC 9241-11. 1998.
- [66] ISO. ISO/IEC 25010. 2011.

- [67] Preece, J., Benyon, D., & University, O. A guide to usability: Human factors in computing. Addison-Wesley Longman Publishing Co., Inc. 1993.
- [68] Davis, F. D. Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly: Management Information Systems*. 1989, 13(3), 319–339.
- [69] Nielsen, J., Clemmensen, T., & Yssing, C. Getting access to what goes on in people's heads? *Proceedings of the Second Nordic Conference on Human-Computer Interaction - NordiCHI*, 101. 2002.
- [70] Cotton, D., & Gresty, K. Reflecting on the think-aloud method for evaluating e-learning. *British Journal of Educational Technology*. 2006, 37(1), 45–54.
- [71] Brown-Johnson, C. G., Berrean, B., & Cataldo, J. K. Development and usability evaluation of the mHealth Tool for Lung Cancer (mHealth TLC): A virtual world health game for lung cancer patients. *Patient Education and Counseling*. 2015, 98(4), 506–511.
- [72] Chon, Y. V. The electronic dictionary for writing: A solution or a problem. *International Journal of Lexicography*. 2009, 22(1), 23–54.
- [73] Currie, S. L., Mcgrath, P. J., & Day, V. Development and usability of an online CBT program for symptoms of moderate depression, anxiety, and stress in post-secondary students. *Computers in Human Behavior*. 2010, 26(6), 1419–1426.
- [74] Granić, A., & Čukušić, M. Usability testing and expert inspections complemented by educational evaluation: A case study of an e-learning platform. *Educational Technology and Society*. 2011, 14(2), 107–123.
- [75] Hamel, M. J. Testing aspects of the usability of an online learner dictionary prototype: A product- and process-oriented study. *Computer Assisted Language Learning*. 2012, 25(4), 339–365.
- [76] Nielsen, J. Heuristic Evaluation: How-To: Article by Jakob Nielsen. Nielsen Norman Group. <https://www.nngroup.com/articles/how-to-conduct-a-heuristic-evaluation>. 1994b.
- [77] Federoff, M. A. Heuristics and usability guidelines for the creation and evaluation of fun in video games (Doctoral dissertation, Indiana University). 2002.
- [78] Hermawati, S., & Lawson, G. Establishing usability heuristics for heuristics evaluation in a specific domain: Is there a consensus? *Applied Ergonomics*. 2016, 56, 34–51.
- [79] Omar, H. M., & Jaafar, A. Heuristics evaluation in computer games. *Proceedings - 2010 International Conference on Information Retrieval and Knowledge Management: Exploring the Invisible World, CAMP'10*. 2010, 188–193.
- [80] Paavilainen, J. (2010). Critical review on video game evaluation heuristics. *Proceedings of the International Academic Conference on the Future of Game Design and Technology*, 56–65. <http://dl.acm.org/citation.cfm?id=1920787%5Cnhttp://portal.acm.org/citation.cfm?doid=1920778.1920787>.
- [81] Korhonen, H., & Koivisto, E. M. I. Playability heuristics for mobile multi-player games. *Proceedings of the 2nd International Conference on Digital Interactive Media in Entertainment and Arts – DIMEA*. 2007, 28.
- [82] Desurvire, H., & Wiberg, C. Game usability heuristics (PLAY) for evaluating and designing better games: The next iteration. *International Conference on Online Communities and Social Computing, 5621 LNCS*. 2009, 557–566.
- [83] Law, E. L. C., & Sun, X. Evaluating user experience of adaptive digital educational games with Activity Theory. *International Journal of Human-Computer Studies*. 2012, 70(7), 478–497.
- [84] Lin, H. K., Hsieh, M., Wang, C., Sie, Z., & Chang, S. Establishment and Usability Evaluation of an Interactive Ar. *Turkish Online Journal of Educational Technology*. 2011, 10(4), 181–187.
- [85] Xenos, M., & Velli, V. A serious game for introducing software engineering ethics to university students. *International Conference on Interactive Collaborative Learning*. 2019, 579–588.
- [86] da Silva, G. C., da Silva, L. P. F., Jofilsan, N. C., Correia, W. F. M., Gomes, A. S., & Campos Filho, A. S. Satisfaction analysis for using educational serious games for teaching wound treatment. In *International Conference on Applied Human Factors and Ergonomics*, Springer, Cham. 2018, 673-682.
- [87] Barnum, C., Bevan, N., Cockton, G., Nielsen, J., Spool, J., & Wixon, D. The “magic number 5”: Is it enough for web testing? *Conference on Human Factors in Computing Systems – Proceedings*. 2003, 5, 698–699.
- [88] Nielsen, J. Enhancing the explanatory power of usability heuristics. *Conference on Human Factors in Computing Systems – Proceedings*. 1994c, 152–158.
- [89] Denzin, N. K. Introduction: Entering the field of qualitative research. *Handbook of qualitative research*. 1994.
- [90] Preece, J. A guide to usability: human factors in computing. Wokingham, England/Reading MA: Addison-Wesley. 1998.
- [91] Lincoln, Y. S., & Guba, E. G. *Naturalistic inquiry*. Newbury Park, CA: Sage. 1985.
- [92] Patton, M. Q. *Qualitative research and evaluation methods*. Thousand Oaks, CA: Sage. 2002.
- [93] Ishaq, K., Azan, N., Rosdi, F., Abid, A., & Ijaz, M. The Impact of ICT on Students' Academic Performance in Public Private Sector Universities of Pakistan. *International Journal of Innovative Technology and Exploring Engineering*. 2020d, 9(3), 1117–1121.
- [94] Ishaq, K., Rosdi, F., Zin, N. A. M. & Abid, A. 2021b. Heuristic and Think aloud method to evaluate the Low-Fidelity prototype of Game-Based Language Learning Application. *4th International Conference on Innovative Computing, ICIC 2021*. (Accepted).
- [95] Ishaq, K., Rosdi, F., Zin, N. A. M. & Abid, A. 2021c. Requirements Elicitation for Game-based Language Learning Application. *4th International Conference on Innovative Computing, ICIC 2021*. (Accepted).

APPENDIX

Appendix A. Heuristics for LLSG		
Constructs		ITEMS
Interface (I)	LHI1	Aesthetic and minimalist design
	LHI2	Maximize consistency and matches standards
	LHI3	Color, text, and space follow the principles of screen design.
	LHI4	Text, color, and font follow the readability principles.
	LHI5	The quality of text, images, and sound elements is acceptable.
	LHI6	The use of multimedia elements support meaningfully the text provided.
	LHI7	The integration of presentation means is well-coordinated.
	LHI8	The game speaks with words phrases and concepts.
	LHI9	The game helps me to navigate from one screen to another easily.
	LHI10	Pronunciation helps to understand the concept easily.
	LHI11	Consistent errors take back to learning screen.
	LHI12	Provide support (Hint) during assessment
Game Play (GP)	LHGP1	The control keys in game follow standard conventions.
	LHGP2	The game provides score after completion of stage.
	LHGP3	The game rewarded player after completion of stage.
	LHGP4	The game is interesting and engaging.
	LHGP5	The game is enjoyable to replay.
Game Mechanics (GM)	LHGM1	The game should behave in consistent, exciting and challenging way to players' action.
	LHGM2	The game controller actions have consistently mapped and learnable responses.
Content (C)	LHC1	The game has reliable and proven content with correct flow.
	LHC2	The game has clear goal, structure and learning objectives of content.
	LHC3	The content of game has main topic and subtopics.
	LHC4	Navigation is easy and accurate.
	LHC5	Supporting materials are sufficient and relevant (exercises).
	LHC6	Materials are interesting and engaging me.
	LHC7	The content helps to improve vocabulary.
	LHC8	The content helps to improve English comprehension.
Feedback (F)	LHF1	The game provides instant feedback on the progress.
	LHF2	The game notify me on the mistakes.
	LHF3	The game provide information on success or failure after completion of the stage.
Language Learning (LL)	LHLL1	The game helps to improve language learning.
	LHLL2	The game confident me after learning language.
	LHLL3	The game helps me to enhance my vocabulary.
	LHLL4	The game helps me to learn English comprehension easily.
	LHLL5	The game helps me to enhance English comprehension.
	LHLL6	The information is understandable conveyed to the users of game.
Cultural Context (CC)	LHCC1	The game should speak the language of the user with words, phrases and concepts.
	LHCC2	The game objects should be related to culture such as images, colors and familiar objects in order.
	LHCC3	The game should provide emergency exit to leave the state.
	LHCC4	The game should not the user think of similar actions, situations, or word mean the same.
	LHCC5	The game should minimize the memory burden with objects, actions and visible options.
	LHCC6	The game should provide interface without distracter elements.
	LHCC7	The game should provide the equal access to new user and expert.
	LHCC8	The error message in game should indicate to solve the problem.
	LHCC9	The game should provide help to user with less documentation.
	LHCC10	The game should provide diverse access to its provided options.
	LHCC11	The game should uses graphic symbols related to gender, age, sex, and religion where they have greater significance.

Towards Measuring User Experience based on Software Requirements

Issa Atoum¹, Jameel Almalki², Saeed Masoud Alshahrani³, Waleed Al Shehri⁴

The World Islamic Sciences and Education University, Amman, Jordan¹

Department of Computer Science, College of Computer in Al-Leith, Umm Al-Qura University, Makkah, Saudi Arabia^{2,4}

Department of Computer Science, College of Computing and Information Technology, Shaqra University, Shaqra, Saudi Arabia³

Abstract—User Experience (UX) provides insights into the users' product perceptions while using or intending to use an application. Software products are known for complexity and changeability, starting from requirements engineering until the product operation. Users often evaluate software UX based on a prototype; however, UX is semantically embedded in the software requirements, a crucial indicator for project success. The problem of current UX evaluation methods is their dependence on the actual involvement of users or experts, a time-consuming process. First, this paper builds a benchmark dataset of UX based on textual software requirements crowdsourcing several UX experts. Second, the paper develops a machine learning model to measure UX based on the dataset. This research describes the dataset characteristics and reports its statistical internal consistency and reliability. Results indicate a high Cronbach Alpha and a low root mean square error of the dataset. We conclude that the new benchmark dataset could be used to estimate UX instantly without the need for subjective UX evaluation. The dataset will serve as a foundation of UX features for machine learning models.

Keywords—User experience; benchmark dataset; requirements engineering; UX evaluation; software engineering

I. INTRODUCTION

The User Experience (UX) is a term used to indicate personnel perceptions and resulting emotions from systems or services [1]. Some of the concepts related to UX are included in the definition of Quality in Use (QinU); the user perceptions could result from a system or software's hedonic and pragmatic qualities. Very often, software UX is related to nonfunctional requirements and usability. Therefore, UX is a broader concept that includes usability, user satisfaction, emotions, and perceptions during the interaction [2]. On the other hand, the UI is considered a mechanism of functionality, usability, reliability, and satisfaction [3]. Consequently, usability is influenced by two orthogonal aspects, GUI and UX. However, the focus of this paper is evaluating the UX even if no UI is already built. Therefore, post evaluations of UX after product release (e.g., [4]) are not considered in this study.

The UX evaluation depends on components or factors of UX models. Some of the most commonly cited factors are proposed by Morville [5], known as the honeycomb model. The honeycomb model is based on balancing context, content, and users. Morville's honeycomb consists of seven factors: useful, usable, desirable, findable, accessible, credible, and

valuable. However, Morville's model is generic to any product and is not focusing on software products. Recently, questionnaire-based approaches [6][7], heuristics models [8] [9], and hybrid models [13] were proposed for UX modeling and evaluation.

One of the frameworks that lay a foundation on software requirements and UX requirements is the UX-aware framework of Kashfi *et al.* [10]. The UX-aware framework shows that UX requirements are embedded quality requirements that describe the end user's satisfaction or pleasure of using the software. However, UX is generally evaluated based on a prototype (or a release); therefore, productive UX evaluation models could be used early during the requirements development [11]. Regrettably, the unavailability of measurement metrics or a benchmark dataset breaks the early evaluation. The automation of UX measurement is widely disregarded due to its complexity. In this era, an agent was proposed to automate UX testing for specific predefined tasks of objects finding scenarios in a game application [11].

Machine learning has been extensively adopted in many domains to predict and estimate target variables; however, a useful machine learning model depends on robust and reliable datasets. To the best of our knowledge, there are no existing datasets specialized for UX based on software requirements.

Therefore, the research gap is related to the unavailability of automated UX evaluation methods, which will result in that UX evaluators spending extensive efforts. Therefore, the UX evaluators are regretted using manual UX evaluation, including conducting surveys. Worst of all the evaluators must use an existing prototype to evaluate the UX (using existing evaluation methods). As a result, requirements engineers are not fully aware of any early UX software requirements before getting any prototype. Lacking large datasets of software requirements are still a major challenge for proper cost-effective and rapid application development [12]. Moreover, the elimination of UX-compliant requirements results in UX neglect in the final product [13] or poor resource planning [14]. Therefore, the automation of UX evaluation lacks datasets and proper evaluation models.

The main objective of this paper is to build a dataset that could be used for UX evaluation using machine learning techniques solely relying on textual requirements before an actual software gets developed. We employed four UX experts

to annotate user requirements to a widely accepted scale¹, the User Experience Questionnaire (UEQ) [15][16][17]. The proposed benchmark dataset is a PROMISE-based dataset[18], one of the non-commercial requirements datasets. The research uses the latest expanded PROMISE dataset[19], part of the Open Science Tera-PROMISE repository upgraded earlier [18].

The contributions of this study are critical to software requirements engineering and user acceptance success. The prepared benchmark dataset eases the UX evaluation using machine learning models instead of traditional approaches such as questionnaires or heuristic models. This study is also important for software developers to track the software quality over the software life cycle. Therefore, the overall advantage of using an automated UX system is important for both software consumers and developers. Thereby, saving time and efforts of software developers and providing early feedback to software consumers. The main research question that addresses the UX measurement is as follows:

How UX evaluation could be automated at the early stages of requirements engineering using machine learning?

The paper structure is as follows. Section 2 discusses related works. Then, the methodology of building the benchmark dataset is illustrated in Section 3. Next, Section 4 describes the benchmark dataset reliability and provides preliminary results of machine learning methods. After that, we show the implications of the proposed dataset and its limitations in Section 5. Finally, we conclude the paper in Section 6.

II. RELATED WORK

The UX has been evaluated in several models. Morville [5], one of the leaders in UX, proposed the honeycomb model, which consists of seven factors: useful, usable, desirable, findable, accessible, credible, and valuable. A system is considered usable if its needs are delivered in a simple way considering the user learning curve. If the system fulfills the user's needs it is considered useful. However, a system is considered desirable based on its design and attractiveness. If further information is needed about the system it should be findable, easy to navigate. The system should be accessible even to a user with disabilities. Therefore, an application is considered credible if it is trustworthy. Integrating all of these factors provides a valuable system. However, Morville's model is generic to any product and is not focusing on software products.

Generally, UX evaluation models could be classified into three categories: questionnaire-based approaches, heuristics models, and hybrid frameworks. Questionnaire-based models [6], [7], [15], [20] are known for their simplicity in evaluation and aggregation. In such methods, the users are responsible for the system evaluation with a few questions based on their perceived use of products. For example, the benchmark of the User Experience Questionnaire (UEQ) [15] uses several question items to evaluate the UX. Each item of the UEQ consists of a pair of terms with opposite meanings (e.g., 'not

understandable' vs. 'understandable', 'efficient' vs. 'inefficient') on a 7-point Likert scale that each ranges from -3 to +3. With UEQ, several users would evaluate a system prototype to calculate key performance indicators (KPIs) for each software application under study (e.g., [6]). Such KPIs are based on UEQ scores and simple average and summation statistics. Recently a questionnaire survey was developed to measure usability, usefulness, and satisfaction of a chatbot UX [21]. However, the approach of [19] was customized for conversational agents.

On the other hand, heuristics models depend on rules or checklist items prepared and evaluated by experts in the specific service domain. In this category, Yeratziotis and Zaphiris [9] proposed a set of rules (heuristics) to support human-computer interaction experts to evaluate website accessibility. Similarly, online travel agency applications' UX has been evaluated formally with 8 stages [2]; however, this model [2] is application-dependent.

UX has been evaluated in the context of students' applications. The UX has been seen from the angle of usefulness and effectiveness of students teaching systems [22] [23]. For example, Krouska *et al.* [23] proposed a set of rules for students' misconception of HTML to understand the user (student) experience while using an e-learning system. Based on the student experience with the system the proposed model—based on the repair theory—was able to suggest a student learner path. Although heuristic models enable experts to key in needed knowledge to help in UX evaluation, they are generally applied to certain application domains where evaluation checklists exist.

Hybrid models combine the previous methods to measure the UX such as measuring the physiological aspects of users during software usage [24]. The multimodal deep learning model UX framework of Hussain *et al.* [24] depends on sentiment analysis, user feedback, and visual analysis of user action using sensors that detect user's objects on the screen. Koonsanit and Nishiuchi [25] proposed a framework to measure software UX based on facial expression recognition and machine learning; however, their focus is on product sentiment analysis rather than measurement of UX from software requirements [26]. A similar model was proposed by Li and Liu [27] to analyze user eye-movement tracking along with user testing methods to suggest actions for a better user experience. Furthermore, a UX framework for business intelligence (BI) systems interfaces was proposed by Eriksson and Ferwerda [28] to support users' desires and data evaluation. The evaluation of their framework utilizes several KPIs: utility, usability, visual attractiveness, and hedonic quality that covers the whole system development lifecycle. Jang and Han [29] proposed a framework for UX understanding in blockchain services. The UX is defined based on the literature in UX generality and blockchain technological aspects. More specific UX frameworks were proposed for educational games. Leong *et al.* [21] considered the game flow, player context, usability, and learnability along with psychometrically to build an educational UX measurement model.

¹Google Scholar shows 1,301 citations for UEQ paper (2008): 11/2021.

The literature shows that the gap is the current methods are time-consuming and subjective. UX measurement depends on persons with different expertise level questionnaires and product trustworthiness which are widely subjective [30]. To our knowledge, this could be the first paper that heights the importance of requirements UX evaluation before an application gets developed based on machine learning models.

III. METHODOLOGY

The proposed methodology is based on textual software requirements that are considered the initial source of software UX [31], [32]. The source dataset for software requirements is the expanded PROMISE dataset [19], as described in TABLE I.

UEQ metrics are the foundation of the benchmark dataset because it is a widely used UX evaluation method for software products[6]. Specifically, we employed the short UEQ (UEQ-S) model that has eight items [6]. The core UEQ primary constructs are as illustrated in TABLE II [6].

In addition, these constructs are represented using eight class labels in a score ranging from 1 (minimum) to 7 (maximum) for each class label, as shown in TABLE III. For example, a requirement item with a score of 5 for 'label 1' is considered supportive, while an item of score 1 is considered obstructive. The neutral value is (3). Note that the same requirement item could have eight scores simultaneously.

The annotation scheme methodology is depicted in Fig. 1. We selected four experts of UX who have more than five years of experience in UX design. First, they were interviewed online to know the robustness of their work. Then, we explain to them the objectives of the work and the UEQ measurement scales (Step 1). After the explanation, we draw a random 100 requirements (approximately 10% of the dataset) from the PROMISE dataset with different applications (Step 2). The experts studied the complete set of requirements for each application. Next, they were allowed to discuss how to classify requirements to the eight UX scales. After that, they were left to do the annotation alone (Step 3). During the data reconciliation process (Step 4), we again choose another random 50 annotated requirements (not the previous ones), and experts were allowed to discuss discrepancies (if any). It was found that all 50 pairwise scores were acceptable having an absolute error value of 1 to 2. Finally, we got four Excel sheets for the exact requirements classified into eight labels, each with a scale in the range 1-7.

TABLE I. ATTRIBUTES OF EXPANDED PROMISE DATASET [19]*

Attribute	Description	Total
Project-ID	The project IDs range from 1 to 49. Projects are generic domains such as shopping and universities.	49
Requirement-Text	Project textual requirements at the analysis stage of analysis and design.	969
Class	Functional or non-functional. Requirements where nonfunctional requirements are a set of 13 subcategories.	13 (F(1), NF(12))

*Functional (F), and Nonfunctional (NF) requirements are part of this dataset.

TABLE II. CORE COMPONENTS OF THE UEQ SCALES (ALSO DESCRIBED IN AL-HUNAIYYAN ET AL. [37])

Construct	Meaning
Attractiveness	The product should be pleasurable, user-friendly, and enjoyable
Efficiency	Perform tasks with the product in a fast manner and pragmatically
Perspicuity	The product plain to the understanding primarily because of clarity, and easiness to learn
Dependability	The product services that can be trusted within time and meets users' expectations
Stimulation	Using the product encourages its use due to being exciting and motivating
Novelty	The product should be pioneering, inspired, and creatively designed

TABLE III. UEQ-S LABELS[6]

Label ID	Quality Category	Negative Word	Positive Word
Label 1	Pragmatic Quality	obstructive	supportive
Label 2	Pragmatic Quality	complicated	easy
Label 3	Pragmatic Quality	inefficient	efficient
Label 4	Pragmatic Quality	confusing	clear
Label 5	Hedonic Quality	boring	exciting
Label 6	Hedonic Quality	not interesting	interesting
Label 7	Hedonic Quality	conventional	inventive
Label 8	Hedonic Quality	usual	leading-edge

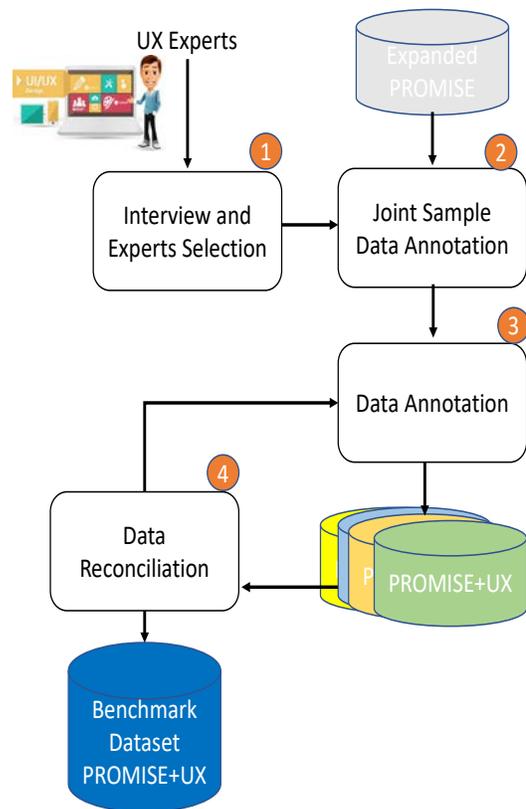


Fig. 1. Proposed Annotation Scheme Methodology.

TABLE V. ROOT MEAN SQUARE ERRORS BETWEEN EXPERTS

	Exp1	Exp2	Exp3	Exp4	Av3*	Av4*
Exp1	0.00	2.90	4.68	4.38	0.80	1.03
Exp2	2.90	0.00	5.52	5.35	0.97	2.06
Exp3	4.68	5.52	0.00	3.01	0.77	1.06
Exp4	4.38	5.35	3.01	0.00	2.83	1.34

* av3: average(3) is calculated by finding the average scores for the first three experts and then calculating the RMSE between each expert and that score. Similarly, av4 (average 4) is calculated by averaging scores for the four experts and then finding the RMSE between the expert and the average score

B. UX Evaluation

Given the dataset, the machine learning developer could tackle the problem as a multilabel or multi-regression problem. If the four annotations are averaged, then it could be seen as a multi-regression problem. However, if the resultant annotations were rounded to the original UX-scale(1-7), one might consider the problem a classification problem.

One approach to validating the benchmark dataset’s output is experimenting with the dataset with different machine learning models. We have done a simple experiment on the first expert dataset using support vector machine (SVM), eXtreme Gradient Boosting (XGBoost), Decision Trees, and Bagging Classifier (KNN). We tackle machine learning problems as multilabel (8 labels) and multiclass (7 classes) regression problems. Nevertheless, predicted label-class values were rounded to the nearest label scale (1 to 7), making the comparison meaningful over precision, recall, and F1-score. First, stop words, and special characters were removed from the requirement text column, generating a sequence of words using the Tensorflow Tokenizer. Next, the default implementation of SVM and Decision Trees were used from the sklearn library and the latest python API for XGBoost.

The results are shown in TABLE VI. The results show that the XGB algorithm provides a reasonably acceptable F1-score (0.864), indicating that the benchmark dataset is helpful and applicable in UX predictive models. Decision trees were next performing machine learning model with an F1-score of 0.861. However, the SVM with one versus rest voting and the KNN Bagging (decreasing variance) was not performing well. Results could be due to the nature of SVM that would not work well with the multilabel problem, while the decision trees were giving an acceptable performance as it could build deep trees based on dataset instance and the 8 label values.

TABLE VI. RESULTS OF CLASSIFICATION METHODS

Method	Recall	Precision	F1-score
SVM	0.662	0.680	0.658
XGBoost	0.864	0.863	0.864
Decision Trees	0.861	0.861	0.861
Bagging(KNN)	0.747	0.746	0.746

In this experiment, the XGBoost classifier using the multiclass log loss function was a better choice for this dataset. Fig. 4 shows the ROC for the XGBoost model. The results show that class labels have a high area under the curve

(except for label 3) where each score represents the average score of all eight labels. In other words, each average is calculated two times: the first time, averaging the prediction performance over a single label over the 7 class values (1 to 7), and then another average over the eight labels.

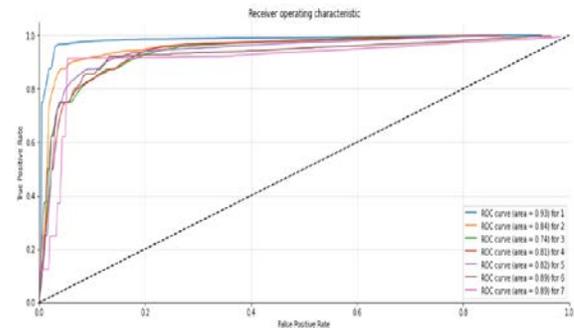


Fig. 4. ROC for XGBoost Model.

V. IMPLICATIONS AND LIMITATIONS

The new benchmark dataset allows the software engineers to predict the UX software value early in software development, and it allows the software engineers to generate UX-complaint software requirements. Moreover, the benchmark dataset extends the applicability of machine learning methods to measure a product UX instantly. The major advantage of the proposed machine learning models versus questionnaire-based approaches is automation, where UX could be evaluated on the fly at any point in time during software development. The UX evaluation could be used as a driving force for requirements analysis and validation [12]. Our study is consistent with the literature review conducted by Almeyda et al. [39] that showed that integrating the user experience and agile techniques are essential for requirements analysis.

The current dataset might have these limitations. It was assumed that all applications are similar in terms of UX features classification. Further research could enhance the dataset to support a customized dataset for each application. Moreover, the dataset is considered a small dataset; therefore, some deep learning models might not be a good choice.

VI. CONCLUSION

This paper annotated a dataset for UX based on textual requirements. The benchmark dataset helps software engineers predict the UX of an application before building a prototype or before releasing the software. Furthermore, the dataset could help software engineers generate UX-complaint requirements and as per the customer requirements. The dataset was tested with RMSE and some machine learning models. The results showed a low RMSE value between experts and a high F1-score for the XGBoost classifier. As a result, the dataset is considered the first of its kind to automate the UX evaluation. The dataset will be further expanded with new requirements, and the number of UX experts will be increased in the future. Moreover, the current contribution of this paper allows the research community to tackle requirements engineering issues using the current dataset by integrating the UX evaluation with the requirements engineering process.

REFERENCES

- [1] A. G. Mirnig, A. Meschtscherjakov, D. Wurhofer, T. Meneweger, and M. Tscheligi, "A formal analysis of the ISO 9241-210 definition of user experience," in Proceedings of the 33rd annual ACM conference extended abstracts on human factors in computing systems, 2015, pp. 437–450.
- [2] D. Quinones and C. Rusu, "Applying a methodology to develop user eXperience heuristics," *Computer Standards and Interfaces*, vol. 66, no. January, p. 103345, 2019, doi: 10.1016/j.csi.2019.04.004.
- [3] J. Nielsen, "The definition of user experience (UX). Nielsen Norman Group." Obtenido de <https://www.nngroup.com/articles/definition-user-experience>, 2018.
- [4] Q. Zhang, "Mobile Internet Product Usage Scenarios and User Experience Design," in International Conference on Cognitive based Information Processing and Applications (CIPA 2021), 2022, pp. 857–865.
- [5] P. Morville, "User experience design," Ann Arbor: Semantic Studios LLC, vol. 6, no. 2, 2004.
- [6] A. Hinderks, M. Schrepp, F. J. D. Mayo, M. J. Escalona, and J. Thomaschewski, "Developing a UX KPI based on the user experience questionnaire," *Computer Standards & Interfaces*, vol. 65, pp. 38–44, 2019.
- [7] K. Ohashi et al., "Focusing Requirements Elicitation by Using a UX Measurement Method," in IEEE 26th International Requirements Engineering Conference (RE), 2018, pp. 347–357.
- [8] J. Nielsen, "How to conduct a heuristic evaluation," Nielsen Norman Group, vol. 1, pp. 1–8, 1995.
- [9] A. Yeratziotis and P. Zaphiris, "A Heuristic Evaluation for Deaf Web User Experience (HE4DWUX)," *International Journal of Human-Computer Interaction*, vol. 34, no. 3, pp. 195–217, 2018, doi: 10.1080/10447318.2017.1339940.
- [10] P. Kashfi, R. Feldt, A. Nilsson, and R. B. Svensson, "A conceptual ux-aware model of requirements," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9856 LNCS, pp. 234–245, 2016, doi: 10.1007/978-3-319-44902-9_15.
- [11] P. M. Fernandes, M. Lopes, and R. Prada, "Agents for automated user experience testing," Proceedings - 2021 IEEE 14th International Conference on Software Testing, Verification and Validation Workshops, ICSTW 2021, pp. 247–253, 2021, doi: 10.1109/ICSTW52544.2021.00049.
- [12] I. Atoum et al., "Challenges of Software Requirements Quality Assurance and Validation: A Systematic Literature Review," *IEEE Access*, vol. 9, pp. 1–22, 2021, doi: 10.1109/ACCESS.2021.3117989.
- [13] C. Ardito, P. Buono, D. Caivano, M. F. Costabile, and R. Lanzilotti, "Investigating and promoting UX practice in industry: An experimental study," *International Journal of Human Computer Studies*, vol. 72, no. 6, pp. 542–551, Jun. 2014, doi: 10.1016/j.ijhcs.2013.10.004.
- [14] J. Choma, L. A. M. Zaina, and D. Beraldo, "UserX story: Incorporating UX aspects into user stories elaboration," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9731, pp. 131–140, 2016, doi: 10.1007/978-3-319-39510-4_13.
- [15] M. Schrepp, A. Hinderks, and J. Thomaschewski, "Construction of a Benchmark for the User Experience Questionnaire (UEQ)," *IJIMAI*, vol. 4, no. 4, pp. 40–44, 2017.
- [16] B. Laugwitz, T. Held, and M. Schrepp, "Construction and evaluation of a user experience questionnaire," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2008, vol. 5298 LNCS, pp. 63–76, doi: 10.1007/978-3-540-89350-9_6.
- [17] M. Schrepp, A. Hinderks, and J. Thomaschewski, "Applying the user experience questionnaire (UEQ) in different evaluation scenarios," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2014, vol. 8517 LNCS, no. PART 1, pp. 383–392, doi: 10.1007/978-3-319-07668-3_37.
- [18] J. Cleland-Huang, S. Mazrouee, H. Liguio, and D. Port, "nfr." Zenodo, Mar. 2007, doi: 10.5281/zenodo.268542.
- [19] M. Lima, V. Valle, E. Costa, F. Lira, and B. Gadelha, "Software engineering repositories: Expanding the PROMISE database," *ACM International Conference Proceeding Series*, pp. 427–436, 2019, doi: 10.1145/3350768.3350776.
- [20] D. Biduski, E. A. Bellei, J. P. M. Rodriguez, L. A. M. Zaina, and A. C. B. De Marchi, "Assessing long-term user experience on a mobile health application through an in-app embedded conversation-based questionnaire," *Computers in Human Behavior*, vol. 104, 2020, doi: 10.1016/j.chb.2019.106169.
- [21] P. H. Leong, O. S. Goh, Y. J. Kumar, Y. H. Sam, and C. W. Fong, "The Evaluation of User Experience Testing for Retrieval-based Model and Deep Learning Conversational Agent," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 4, pp. 216–221, 2021, doi: 10.14569/IJACSA.2021.0120429.
- [22] K. Chrysafiadi and M. Virvou, "Evaluating the user experience of a fuzzy-based Intelligent Tutoring System," in 2021 12th International Conference on Information, Intelligence, Systems Applications (IISA), 2021, pp. 1–7, doi: 10.1109/IISA52424.2021.9555516.
- [23] A. Krouska, C. Troussas, and C. Sgouropoulou, "A Cognitive Diagnostic Module Based on the Repair Theory for a Personalized User Experience in E-Learning Software," *Computers*, vol. 10, no. 11, 2021, doi: 10.3390/computers10110140.
- [24] J. Hussain et al., "A multimodal deep log-based user experience (UX) platform for UX evaluation," *Sensors (Switzerland)*, vol. 18, no. 5, 2018, doi: 10.3390/s18051622.
- [25] K. Koonsanit and N. Nishiuchi, "Classification of user satisfaction using facial expression recognition and machine learning," *IEEE Region 10 Annual International Conference, Proceedings/TENCON*, vol. 2020-Novem, pp. 561–566, 2020, doi: 10.1109/TENCON50793.2020.9293912.
- [26] C. I. Nwakanma, M. S. Hossain, J.-M. Lee, and D.-S. Kim, "Towards Machine Learning Based Analysis of Quality of User Experience (QoUE)," *International Journal of Machine Learning and Computing*, vol. 10, no. 6, pp. 752–758, 2020, doi: 10.18178/ijmlc.2020.10.6.1001.
- [27] Y. Li and C. Liu, "User Experience Research and Analysis Based on Usability Testing Methods," in *Lecture Notes in Electrical Engineering*, 2021, vol. 754 LNEE, pp. 263–267, doi: 10.1007/978-981-16-0503-1_39.
- [28] M. Eriksson and B. Ferwerda, "Towards a User Experience Framework for Business Intelligence," *Journal of Computer Information Systems*, vol. 61, no. 5, pp. 428–437, 2021, doi: 10.1080/08874417.2019.1693936.
- [29] H. Jang and S. H. Han, "User experience framework for understanding user experience in blockchain services," *International Journal of Human-Computer Studies*, vol. 158, p. 102733, 2022, doi: <https://doi.org/10.1016/j.ijhcs.2021.102733>.
- [30] A. Casare, T. Basso, and R. Moraes, "User Experience and Trustworthiness Measurement: Challenges in the Context of e-Commerce Applications," in *Proceedings of the Future Technologies Conference (FTC) 2021, Volume 1*, 2022, pp. 173–192.
- [31] I. Atoum, "A Scalable Operational Framework for Requirements Validation Using Semantic and Functional Models," *ACM International Conference Proceeding Series*, pp. 1–6, 2019, doi: 10.1145/3305160.3305166.
- [32] I. Atoum, "Requirements Elicitation Approach for Cyber Security Systems," *i-manager's Journal on Software Engineering*, vol. 10, no. 3, pp. 1–5, 2016, doi: doi.org/10.26634/jse.10.3.4898.
- [33] J. D. Brown, "The Cronbach alpha reliability estimate," *JALT Testing & Evaluation SIG Newsletter*, vol. 6, no. 1, 2002.
- [34] R. Falotico and P. Quatto, "Fleiss' kappa statistic without paradoxes," *Quality & Quantity*, vol. 49, no. 2, pp. 463–470, 2015, doi: 10.1007/s11135-014-0003-1.
- [35] D. G. Bonett and T. A. Wright, "Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning," *Journal of organizational behavior*, vol. 36, no. 1, pp. 3–15, 2015.
- [36] T. Chai and R. R. Draxler, "Root mean square error (RMSE) or mean absolute error (MAE)?--Arguments against avoiding RMSE in the literature," *Geoscientific model development*, vol. 7, no. 3, pp. 1247–1250, 2014.

- [37] A. Al-Hunaiyyan, R. Alhajri, B. Alghannam, and A. Al-Shaher, "Student Information System: Investigating User Experience (UX)," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 2, pp. 80–87, 2021, doi: 10.14569/IJACSA.2021.0120210.
- [38] I. Atoum and M. R. Ayyagari, "Effective semantic text similarity metric using normalized root mean squared square error," *Journal of Theoretical and Applied Information Technology*, vol. 97, no. 12, pp. 3436–3447, 2019.
- [39] S. Almeyda, C. Zapata Del Rfo, and D. Cohn, "Integration of User Experience and Agile Techniques for Requirements Analysis: A Systematic Review," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2021, vol. 12779 LNCS, pp. 187–203, doi: 10.1007/978-3-030-78221-4_13.

Machine Learning Driven Feature Sensitive Progressive Sampling Model for BigData Analytics

Nandita Bangera, Dr.Kayarvizhy N
BMS College of Engineering
Bengaluru, India

Abstract—BigData requires processing a huge data volume, which is an undeniable challenge for academia-industries. The classical sampling techniques are limited when addressing data-imbalance, large data-heterogeneity, multi-dimensionality etc. To alleviate it, in this paper a novel machine learning driven feature sensitive progressive sampling (ML-FSPS) that in conjunction with an improved feature selection and classification environment achieves more than 95.7% of accuracy, even with 10-14% of the original data size. The proposed ML-FSPS model was applied for IoT-device classification problem that possesses exceedingly high data-imbalance, multi-dimensionality and heterogeneity issues. Functionally, the FSPS-driven analytics model at first performed active period segmentation followed by multi-dimensional (descriptive) statistical feature extraction and Wilcoxon Rank Sum Test based feature selection. Subsequently, it executed K-Means clustering over a gigantically huge feature instances (16,00,000,000 network traces) Here, K-means algorithm clustered each feature samples into five distinct clusters. With initial sample size of 10%, FSPS model selected same amount of data elements (0.5-5% iteratively) from each cluster for each feature to perform multi-class classification using homogenous ensemble learning (HEL) model. Here HEL encompassed AdaBoost, Random Forest and Extended Tree ensemble algorithms as base classifiers. The simulation results affirmed that the proposed model achieves accuracy of almost 99% even with 10-16% of sample size.

Keywords—Feature sensitive progressive sampling; BigData analytics; machine learning; ensemble learning; rank sum test; IoT-device classification

I. INTRODUCTION

The demand for low cost infrastructure in all the business domains has opened up a new horizon for industries to provide decentralized computing solution. Majority of this applications require processing significantly large volume of data to identify patterns and trends to make decisions.[1-3].

To cope up with the demands of the decentralized, data-driven decision support systems, BigData analytics has emerged as one of the most sought technologies [4]. However, BigData which is often characterized in terms of “Volume”, “Variety”, “Velocity”, and “Veracity” (say, 4V’s) requires computing the gigantically large data to yield decision centric data support [5]. Contrarily the inherent and undeniably unavoidable issues of “Data Heterogeneity”, “Unstructured Data” “Multi-dimensionality”, and “Unbalanced Data” make most of the existing Big Data analytics methods confined. Majority of the BigData analytics models apply the different machine learning methods [3] to learn over the

gigantically large data to perform tasks such as clustering, regression, or classification. However, the efficacy of these methods primarily depends on how effectively they can learn over the large voluminous data in minimum possible time [1-4].

To achieve it, in the last few years different efforts have been made, where the focus is made on improving the process of pre-processing, feature extraction, feature selection, and then classification. However, data being central of these efforts requires a (BigData) computing model to retain “sufficiently small” amount of data to perform analytics without undergoing exhaustive computation and time-exhaustion [2][4][5]. To minimize data load and related computing exhaustion in BigData analytics, authors have found sampling [6] as one of the viable approach. Sampling can not only reduce computing exhaustion but can also retain the minimal data with uncompromising performance [7] Also in the last few years industries have started using or mining a fraction of sample rather than the entire data-warehouse [8]. It improves the scalability as well as timely decision support towards real-time applications [8]. However, the predominant challenge in developing sampling-based approaches originates from the undeniable fact that the occurrence or the frequency of a data element (say, itemset) in a sample might have the different frequency or severity across the complete data set, signifying data imbalance [9]. Under such condition, the classical random sampling approaches might undergo inaccurate performance.

Therefore, alleviating such issue requires identifying optimal size of sample which could provide higher accuracy with minimum possible sample or data load [10]. To cope up with aforesaid demands, recently an approach called progressive sampling has attracted global academia-industries because of its ability to employ minimum data while achieving expected performance [11][12]. The progressive sampling method at first employs minimum data size to perform classification and continues increasing the data volume till it reaches expected level of performance.

However, most of the existing progressive sampling approaches consider random sample selection approach. Random feature selection over exceedingly high data heterogeneity and unbalanced data condition might often results inaccurate performance. It can be because of insufficient or insignificant feature learning. Therefore, a robust computing environment with better pre-processing, feature sensitive feature selection and classification can be a potential analytics solution.

In this paper a futuristic and robust feature-sensitive progressive sampling (FSPS) driven BigData analytics model is proposed. Realizing at-hand analytics problems such as data heterogeneity and unbalanced nature the proposed model inculcates highly efficient pre-processing, feature extraction and selection mechanism, followed by FSPS and heterogeneous ensemble learning model for classification.

II. RELATED WORK

This section highlights some of the important literatures central to progressive sampling in BigData analytics.

Mahafzah et al. [17] proposed a parameterized sampling algorithm for data mining. Authors applied three conditions including the transaction frequency, transaction length and transaction frequency-length to perform sample selection in association rule-based data mining. However, being a multi-phased sampling approach its efficacy over the real-time application remained limited. To alleviate time-complexity in multi-phased sampling, Jia et al. [18] developed an adaptive sampling method that exploited association rule amongst the data elements to select sample size. To improve the performance, authors applied multi-resolution analysis with Shannon sampling theory. Chuang et al. [19] proposed sampling error estimation (SEE) based progressive sampling concept. Here, the key purpose of applying SSE was to estimate the suitable sample size for association rule-based mining. Though, SSE helped achieving sample size without performing association amongst the data elements; however, its efficacy remains suspicious over the realistic large-scale data with higher features and dimensionality. Li et al. [20] applied central limit theorem to estimate the sample size over the large datasets. Unlike other approaches depending on Chernoff bounds, they found their proposed model pragmatic in sync with the association rules mining tasks. Lin [21] examined the associations' lattices on V with a sample V' (a Small chunk or subset). It revealed that merely a very specific kinds of samples possess the "same" association rules with the complete original data and conveys the same meaning. Though, authors intended to exploit homogenous features to retain sample; however, its efficacy due to iterative homogeneity estimation over real-time data traffic becomes suspicious [22]. To resolve this problem, authors in [22] performed association rule mining along with frequent itemset mining to estimate the sample size. Interestingly, this approach selected the sample whose size was independent of both the item-frequency as well as transaction counts. Zhao et al. [23] on the other hand applied hybrid theoretical bound model for frequent itemset estimation, which was later used for sample selection. Moreover, authors applied additive error bound along with the multiplicative error bound to perform sample selection. Exelaxis et al. [24] proposed a two-phase sampling-based algorithm, FAST (Finding Associations from Sampled Transactions) for large-scale data mining. In this process, at first an initial sample was selected, which was then processed for support estimation for each selected item in the data to estimate the suitable set of samples. Once selecting the sample authors performed outlier detection by selecting the representative set of items. However, its computational exhaustion can't be denied.

Parthasarathy [25] applied the concept of equivalence with association rule mining to perform progressive sampling [25]. A similar work was done by Thakur et al. [26], who applied association rule approach to estimate the reduced sample size for data mining purpose. Though, unlike [25], authors [26] applied Apriori algorithm to estimate the frequent itemset, and thus exploiting the mid-point itemset it identified the support level across the other data elements. In case the support level of the midpoint itemset is higher in comparison to the user-specific support, that it was selected as a part of sample and its size was increased progressively. Santos et al. [27] applied retrospective sampling over different phases to perform progressive sampling. Similarly, Bosch et al. [28] developed a wrapped progressive sampling concept for large data analysis. Their proposed progressive sampling method employed complete data as input and presented elements in the form of feature vector and labelled each element in one of the known output labels. Thus, it intended to optimise data set by estimating the possible combination of parameter setting by exploiting all possible combinations during training. Realizing data sensitivity in real-time applications Portet et al. [29] developed a multi-phased or multi-period sample selection concept, where authors found that their proposed approach could attain the same performance even with one-third of the original data size. Similar to the work in [26], authors [30] performed itemset partitioning, rather than midpoint itemset estimation. Xeng et al. [31] proposed Bayesian optimization based automatic sample selection method using machine learning. Authors [31] applied machine learning to estimate the hyper-parameters values to estimate the sample size. In fact, it served as a machine learning driven Bayesian optimization for feature selection to estimate sample size. Recently, ElRafey et al. [32] applied machine learning-based progressive sampling approach in which the batch model uncertainty sampling was performed (using semi-supervised machine learning algorithm). Here, the semi-supervised machine learning helped selecting the most significant data points to the sample to perform further learning or classification. However, it failed addressing the key problem of data imbalance and heterogeneity, which is common in BigData analytics.

III. RESEARCH OBJECTIVE

A large number of BigData analytics environment has the major problem of class imbalance which can lead to incorrect predictions and analysis. On the other hand, input data or real-time stream from multiple channels often undergoes heterogeneity with diverse data elements with different or non-uniform significance (towards prediction or decision making). In such cases, merely applying random sampling can't yield optimal performance. This is because a data in sample is not guaranteed to have uniform distribution or frequency across the complete dataset. Similarly, a data element with higher frequency outside the sample is not mandatory to have the same frequency inside the sample. Therefore, in device classification problem, merely applying the random sample would create data imbalance. Also sampling methods employing random sample selection might fail in delivering optimal feature learning and classification (because of data imbalance probability).

Selecting significant feature set from a huge dataset and progressively sampling the dataset can achieve desired accuracy level and can also reduce the response time factor considering above facts as motivation for the research objective a futuristic, new and robust feature sensitive progressive sampling driven BigData analytics model is developed for IoT-device classification. This proposed model aims to reduce the time required for the analytics and also maintaining the desired level of accuracy.

IV. PROPOSED SYSTEM MODEL

A. System Model

The overall proposed BigData analytics model as shown above in Fig. 1 encompasses the following processes:

1. Network Traffic Sensitive Active Period Segmentation

- 1) Multi-dimensional Descriptive Statistical Feature Extraction
- 2) Wilcoxon Rank Sum Test based Feature Selection
- 3) K-Means Driven Feature Sensitive Progressive Sampling
- 4) HEL-assisted Multi-class Classification.

The detailed discussion of these key functions is given in the subsequent sections.

B. Network Traffic behaviour Assessment and Data Acquisition

In this research, considering the typical cases of data imbalance, multi-dimensionality, data heterogeneity and large-scale data instances, the overall proposed BigData analytics model was designed for IoT-device classification.

Typically, in IoT-ecosystems there can be a large number of independently operating devices connected through a wireless network. Once connected to the wireless-network, the IoT-devices starts generating network traffic called network traces which can of both incoming as well as out coming nature, depending on the type, role, configuration and target-services within the network. IoT-devices within the network perform routine communication with peers and the network gateway or servers. Thus, the communication between the device results network traces or traffic. Though, the different IoT-devices employ varied protocols; however, a majority of such device still use TCP/IP protocols. The overall

communication is based on network traffic in which data is generated successively over a time interval comprising the devices, their behavior, operating patterns, etc. Such non-linear network traffic patterns can be analyzed by means of the sophisticated tools such as Wireshark or TCP Dump that at first obtains the traffic packets and analyses the key details (say, traffic behavior or features). Moreover, the tools like packet analyzer operating onto the router can help seeing the incoming and outgoing network traffic, and can generate the traffic records. Here, each record comprises the information within the packet (from the MAC to the application layer of the open system interconnection). Though, in sync with realistic condition, where because of the security protocols such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and the privacy protection policies of governments, merely the packet header can be employed to perform device classification. However, the key accessible information such as Source ID, Destination ID, Protocol Used, MAC address, Packet size, Transmission Period etc. can be applied to perform more accurate and reliable device classification. These features characterizing device behavior over a definite period have been targeted in this research for device classification [14-16]. In reference to above depicted IoT-network condition, for a large device driven network the corresponding traffic flow can be characterized as per (1).

$$S = \{D^1, D^2, D^3, D^4, D^5, \dots, D^j\} \tag{1}$$

In (1), D^j represents the traffic or the information recorder for the J -th packet. Here, every packet D^j comprises the traffic information and updates as (2).

$$D^j = \{t^j, TLength^j, Protocol^j, eth.Src^j, eth.Dest^j\} \tag{2}$$

In (2), the parameter t^j states the approximate period when the packet is transmitted or received. The other parameter $TLength^j$ states the transmission length, while $eth.Src^j$ and $eth.Dest^j$ represent the source and the destination MAC ID of the devices. The parameter $Others^j$ states the other traffic feature recoded in the j -th packet. Noticeably, the above discussed network traffic packets are recoded in the form time-series order, such as, $t^1 < t^2 < \dots < t^j < \dots$. Let a network comprising N devices representing $d_1, d_2, d_3, \dots, d_n, \dots (1 \leq n \leq N)$, the corresponding traffic can be presented as per (3).

$$s = \{D_{d_1}^1, D_{d_2}^1, D_{d_3}^1, D_{d_1}^2, D_{d_2}^2, \dots, D_{d_n}^1, \dots\} \tag{3}$$

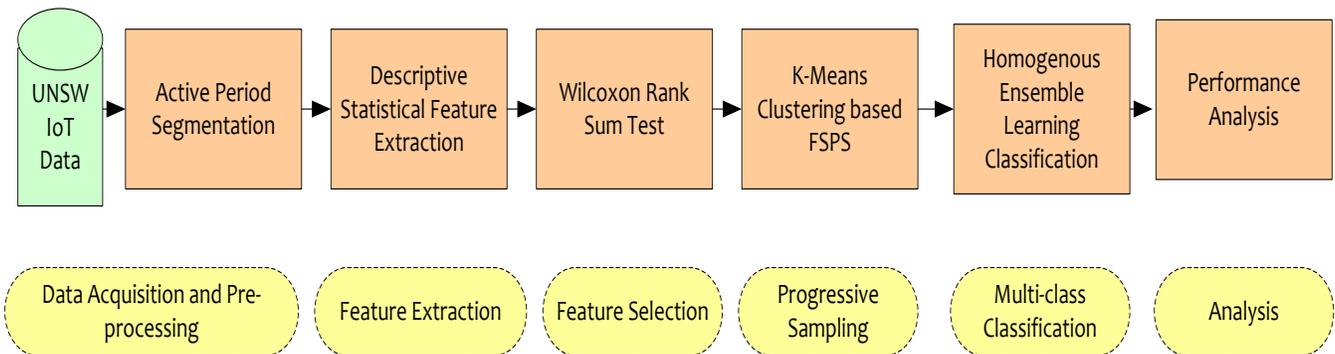


Fig. 1. Proposed ML-FSPS Driven BigData Analytics.

In (3) $D_{d_n}^i$ states the i -th packet of the IOT-device d_n . Now, towards data pre-processing task, it is needed to extract specific traffic traces or sequences for each IoT-device. In fact, each device type can be classified based on its feature such as MAC address in D or similar, on the basis of the traffic direction. Thus, the device-sensitive packet(s) can be distinguished as per (4).

$$S_{d_n} = \{D_{d_n}^1, D_{d_n}^2, D_{d_n}^3, \dots\} \quad (4)$$

Observing above discussion, it can be easily inferred that the numerous chunks of information can be logged from the communication traces including Device ID, source and destination ID, timestamp, packet length, protocol etc. Additionally, out of these features other supplementary features too can be derived [34]. Since, a typical IoT network can have a large number of devices having non-linear transmission patterns, identifying active period for each is vital. In other words, in real-time applications, the traffic intensity for the different devices can be different. For instance, a normal CCTV camera can generate almost 140 packets per minutes, on the contrary a motion sensor can generate more than 1900 packets per minute. On the other hand, a CCTV camera can generate the packets 24×7 , while a smoke sensor can have significantly lower transmission. It indicates that there are the differences in the active period and their traffic intensity amongst the devices across IoT-ecosystem. The use of average traffic over the observation period can force the model to undergo data-imbalance and hence a machine learning model can show inferior performance. Considering this fact, an active period segmentation is performed.

To achieve active period segmentation, the traffic flow across the defined time-period is segmented into multiple sub-traffics, where only active network traces are considered for the further computation. Though, traffic flow can also be segmented at the interval of time T using time-stamp information. For instance, the network traffic flow from the device d_1 can be segmented after T period, iteratively, as given in (5).

$$S_{d_1} = \{Sub_{d_1}^{0-T}, Sub_{d_1}^{T-2T}, Sub_{d_1}^{2T-3T}, \dots, Sub_{d_1}^{tT-(t+1)T}, \dots\} \quad (5)$$

In (5), $Sub_{d_1}^{tT-(t+1)T}$ states the all-traffic traces of the device d_1 during tT to $(t+1)T$ time period. Mathematically, it can be presented as per (6).

$$Sub_{d_1}^{tT-(t+1)T} = \{D_{d_n}^t, D_{d_n}^{t+1}, D_{d_n}^{t+2}, \dots, D_{d_n}^{t+m}, \dots\} \quad (6)$$

In this paper, MATLAB unique function was applied to segment the network traffic over the time-series information.

C. Multi-dimensional Descriptive Statistical Feature Extraction

In the proposed work, a standard benchmark data named UNSW IoT-traffic traces [13] was considered. Noticeably, the data comprised the network traffic of 24/7 time-period for 20 days. A total of 1,60,000,000 traces were there as the original data. Unlike, classical methods where the same network traffic is used for prediction or classification, 10-different features for each network trace for each device was obtained. To

perform descriptive feature extraction, at first the network traffic over defined time period $Sub_{d_1}^{tT-(t+1)T}$ was split into two broad types; control packets and the use packets. Here, user packet encompassed user-data and device-to-server or gateway communication packets. In this work, a packet was classified for its device to have the protocol either TCP, UDP, HTTP, DNS, ARP, or others. Similarly, on the basis of the direction of packet the traffic can be classified as either transmitted packets or the received packets. Noticeably, features for the different traces characterizing the Device ID, MAC ID, Protocol used, Size of the Data communicated etc were obtained. A specific traffic pattern for example packet size, transmission period or the timestamp etc. can have certain dynamism over the operating periods. Considering this fact a multi-dimensional descriptive (statistical) assessment such as Maximum, Minimum Median, Mean, Variance, Upper-Quartile, Lower-Quartile, Kurtosis, Skewness was performed.

In this manner, a total of ten features including Device Source ID (Packet ID), Source ID, Destination ID, source and destination MAC protocol, IP protocols for both source and destination, packet size, transmission period, etc. Thus, extracting above stated features, a humongous volume of features was obtained. Before proceeding for the sample selection the feature selection algorithm was executed. Here, the WRST algorithm was applied, which is briefed as follows.

D. Wilcoxon Rank Sum Test based Feature Selection

The WRST method was used to process the retrieved features in the suggested study. The WRST method is notable for being a sort of non-parametric test with independent samples. This method evaluates the relationship between variables (in this case, network traffic features) and their likelihood of affecting a given device type. WRST was used to estimate the association between network or trace features and their relative inclination towards a given device type in the suggested work. Different extracted attributes were treated as independent variables, whereas device type probability was treated as a dependent variable. This method calculated a p-value for each feature variable based on its importance in device prediction or classification. As a result, each feature factor was classified as significant or unimportant based on its p-value. WRST was applied to each feature element, yielding a collection of characteristics (say, a feature vector) that can be speculated to be the sole important features influencing device type categorization. After obtaining the feature vector the FSPS model was used to select the suitable samples. The proposed FSPS model is described in depth in the next section.

E. K-Means Driven Feature Sensitive Progressive Sampling

The key objective of progressive sampling is to retain the minimum possible nu samples while achieving the expected performance (i.e., accuracy, AUC, etc.). Unfortunately, in majority of the classical progressive sampling methods such as [10], the additional samples are selected randomly, and hence don't consider data imbalance or non-linear nature of the features. Such approaches can greatly be limited due to high inaccuracy. Such random sample selection based progressive sampling methods might select the network traces containing

merely CCTV, or only motion sensor. On the contrary, minimum or possibly negligible frequency of fire sensor traces might skew the learning model towards majority class (i.e., the device(s) with higher packets or its frequency). To alleviate such problems, selecting feature-sensitive samples can be vital. In sync with the proposed IoT-device classification problem, where there is non-linearity in network traces of traffic from each device, random sampling based progressive sampling concept can't be suitable. Considering this fact, in the proposed model, the entire network traces for each feature over the complete operating period (i.e., 24 hours × 20 days) was clustered. In other words, over a total of 16,000,000 network traces or packets characterizing the different features were clustered using K-Mean algorithm. K-Mean algorithm over the aforesaid packets to cluster entire traces into five distinct clusters (for each feature) was applied. Once clustering the network traces over the aforesaid operating period (24 hours × 20 days) the proposed progressive sampling method selected data from each cluster for each feature. The overall process is illustrated in Fig. 2. As depicted in Fig. 2, the proposed FSPS model at first considers 10% of the data (or the selected features) as initial sample, and executes progressive sampling that updates the sample by 0.5-5%, iteratively, till it achieves the expected performance. The sample update takes place as per the model derived in (6).

$$S_i = S_0 + \Delta S_\theta \quad (6)$$

Here, S_i represents the updated sample or data size, while S_0 states the initial sample size, which was selected as 10% in this work. The other parameter ΔS_θ represents the progressive addition value, which is selected in between 0.5% to 5%. Here, the value of ΔS_θ is appended iteratively to S_0 , till it results the expected performance (here, accuracy). Noticeably, unlike random selection-based sampling approaches [10], in the proposed FSPS method, samples from each cluster, pertaining to the different features (Fig. 2) was selected. This as a result helped retaining maximum feature diversity to train the model and hence provide better accuracy. Moreover, since the equal samples were taken from each cluster (i.e., K1 to K5

for each feature, as depicted in Fig. 2) to update the data, it tried to avoid data skewness or over-fitting.

F. HEL-assisted Multi-class Classification

A progressive sampling-based analytics model can only be effective if it maintains optimal performance in terms of both sample selection, as well as classification performance. Considering this fact, in this paper, unlike standalone classifiers such as SVM, ANN, decision tree, k-NN etc., a homogenous ensemble learning (HEL) environment was developed. As the name indicates multiple base classifiers of the same category was employed. More specifically, in the proposed HEL model, three different and well-known ensemble classifiers named AdaBoost, Random Forest and Extended Tree classifier, were applied as the base classifiers. Thus, executing these three base-classifiers independently, each device was classified and labelled. The labels obtained by each classifier was applied to estimate the maximum voting ensemble (MVE), and hence with the higher (here, minimum two out of three labels) labels, the MVE model predicted an IoT-device for a specific category. Here, the only motive was to exploit higher consensus for final prediction so as to increase reliability as well as accuracy of the analytics solution.

In the proposed multi-class device classification problem, the following algorithmic paradigm was followed:

- 1) Let $S = \{1, \dots, N\}$, $C = \{1, \dots, C\}$.

S –Set of traffic instances.

N-Number of traces.

C-Labels for each device.

- 2) $x = \{x_i, \dots, x_n\} \in \mathbb{R}^{N \times D}$ -Input dimensionality.

- 3) $y = \{y_i, \dots, y_n\} \in C$ set of labels for N traces.

- 4) let $\{X, Y\} = \{(x_i, y_i), \dots, (x_n, y_n)\}$ be the training set, comprising n samples.

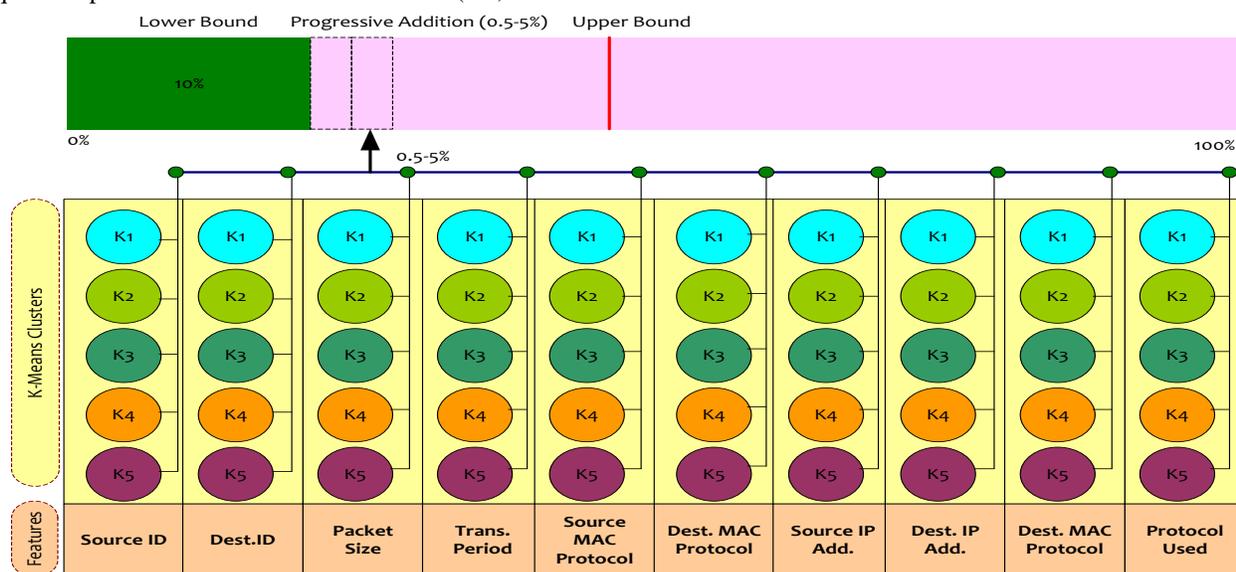


Fig. 2. Proposed Feature Sensitive Progressive Sampling (FSPS) Model.

The motive is to assign label $y_i \in C$ to each network trace $i \in S$ on the basis of the vector x and provide a network trace to the class label y_i . Unlike classical standalone classifier-based learning, three distinct ensemble learning models as the base classifiers was applied. These algorithms are:

- 1) Random Forest.
- 2) AdaBoost.
- 3) Extra Tree Ensemble Classifier.

Noticeably, all these algorithms represent an ensemble learning approach, and thus their use as the base classifier in MVE gives rise to the Homogenous Ensemble Learning (HEL) ability. A snippet of these base classifiers is given as follows.

G. Random Forest Algorithm

The RF algorithm is an ensemble machine learning method that uses numerous tree-structured classifiers. At each input, each tree in the composing tree-structures casts a unit vote (say, an individual vote to establish consensus) for the most likely or popular class. If the number of cases in the training dataset is N , a sample of N cases is randomly chosen from the original data. This sample is also used as a training set for building a tree. If there are M input variables, a number $m < M$ is supplied so that m variables are randomly chosen from the M at each node, and the best split on these m is used to divide the node. During the growth of the forest, the value of m is kept constant. In comparison to the other machine learning models such as SVM, J48, ANN, C5.0, k-NN, etc., RF algorithm requires fewer parameter estimation during processing that makes it more computationally-efficient. In RF algorithm, a collection of distinct tree structured classifier can be defined as (7).

$$\{h(x, \theta_k), k = 1, 2, \dots, i \dots\} \quad (7)$$

In (7), h states the RF classifier, while $\{\theta_k\}$ refers the random vector distributed identical and each tree possesses a vote for the most probable class at certain input variable x . The nature and dimensionality of θ relies on its use in the tree construction. In RF algorithm the most vital part is the forest of decision trees.. It applies a bootstrapped subset of training samples to train each tree across the constructed forest, which enables almost 70% of the training data usages, while the remaining dataset is stated to be the out-of-bag (OOB) samples, which are typically applied to perform inner cross-validation to assess the classification performance.

In this process during the classification process, the input sample x is classified by going through each tree till a leaf-node is obtained. Here, the classification result (say, the decision function h) is assigned to each leaf node. Thus, the final class label y is estimated by selecting the class with the major votes. Mathematically,

$$y = \text{argm}_{1,2, \dots, C} \max_{c \in \{ \}} \sum_{t: h_t(x)=c} 1 \quad (8)$$

H. AdaBoost

AdaBoost represents an adaptive boosting concept, also referred as a commonplace learning paradigm having the ability to improve the characterization potentiality, iteratively. In initialization the prerequisite tests are doled-out to a similar

weight to retrieve some weak learners with some preparation emphases. After each cycle it estimates the error rate of the weak classifier and thus the weight of the accurately classified sample is expanded that reduces the weights of the inaccurately grouped samples. Finally, the weak learner becomes a strong learner to complete the classification. The details of the algorithm applied in this work are given in [33].

I. Extra Tree Classifier

The Extra-Trees classifier constitutes a cluster of unpruned decision trees as per the classical top-down approach. Unlike Random Forest algorithm, it involves randomization of both attribute as well as cut-point selection while splitting a node of a tree. Though, it can also create complete randomized trees possessing structures independent of the output values of the training sample. Primarily, it is distinguishing itself from other tree-based ensemble methods due to two key factors. These are, it splits nodes by selecting cut-points completely at random, and employs the complete training sample (unlike Random Forest which applies bootstrap replica) to enable tree growth. Subsequently, the classified outputs or the predictions of all the trees are combined together to provide final prediction output, by applying MVE method. Summarily, the key concept behind the Extra Tree Classifier is that the complete randomization of the cut-point and attribute altogether with ensemble averaging reduces the variance better in comparison to the weaker randomization approaches used in other methods. Moreover, the use of the original training samples rather than the bootstrap replicas too decreases the likelihood of bias and hence achieved more accurate and efficient classification outputs. Thus, applying above stated classifiers as the base classifiers a MVE ensemble decision was performed where the consensus value was applied to perform device classification. To be noted, since the data considered in this study comprised a total of 26 devices pertaining to six different device categories, the proposed classification model performed multi-class classification. Hence, with the higher number of labels per traffic traces, it labelled the device for the specific category. The simulation results and related inferences are discussed in the subsequent sections.

V. RESULTS AND DISCUSSIONS

Considering the high pace increase in Big Data analytics and its time-efficient computing demands have motivated us to design an optimistically designed computing environment which could achieve expected performance while reducing computational overheads and time-exhaustion. Though to achieve it, the foundation of overall contribution was built onto the improved progressive sampling concept; however, to support efficient computation efforts were made for better pre-processing, feature extraction and selection, and classification as well. Realizing the fact that the use of progressive sampling can help retaining minimum sample volume while achieving higher accuracy, this research employed it as sample selection method. However, recalling the undeniable fact that the typical Big Data analytics models undergo exceedingly high data imbalance, heterogeneity and multi-dimensional features, the random selection based progressive sampling methods can't yield accurate performance. Moreover, the likelihood of

over-fitting and skewed performance can't be ignored. Considering all this facts a feature sensitive progressive sampling (FSPS) model was developed which comprised feature extraction and selection followed by FSPS sampling and homogenous ensemble learning to perform classification.

To assess efficacy of the proposed BigData analytics model, a highly complex and undeniably suitable data pertaining to the IoT-device classification was taken into consideration. A snippet of the considered data is given in the subsequent section. The overall performance analysis was done in terms of classification accuracy, F-Measure and Area Under Curve (AUC). To develop the overall proposed model, MATLAB2020a and Python 3.7 were taken into consideration. Here, MATLAB helped extracting the descriptive statistical features, while rest of the computing algorithms were developed using Anaconda supported Python 3.7 platform. The proposed model was simulated over Microsoft Windows armored with 8 GB RAM and 2.8 GHz processor. The details of the proposed model solution are given in the subsequent section. Before discussing the simulation outputs, a snippet of the data considered and feature distribution is given as follows:

A. Dataset

A benchmark data provided by the University of New South Wales (UNSW), Sydney, Australia [34] was considered. The database was obtained from an IoT-ecosystem created within the university with a total of 26 devices deployed randomly across the university. The network traffic traces were obtained for 20 days (23 Sep. 2016 to 12 Oct. 2016) over 24/7 operating period. Statistically, the collected data contained a total of 1,60,00,000 network traces or traffic instances carrying packets. The packets captured were parsed to the IP header and was composed to derive other features so as to further perform device category classification or identification. Noticeably, the considered data comprised 26 devices of six different categories. The device and their categories are presented in Table I.

TABLE I. DEVICE CATEGORY

Device Categories with description	No.of Devices	Label/Class
Smart Plugs	5	1
IP Camera	5	2
Motion Sensors	5	3
Temperature Sensor	5	4
Electronics	4	5
Others	22	6

The different devices and their corresponding categories and related labels are given in Table I.

A confusion matrix was obtained in the form of true positive (TP), true negative (TN), false positive (FP) and false negative (FN) to measure the overall performance. Considering data imbalance nature, the classification accuracy, F-Measure and Recall was considered as the key performance parameters. The statistical definition of these performance parameters is given in Table II.

TABLE II. PERFORMANCE PARAMETERS

Parameter	Mathematical Expression	Definition
Accuracy	$\frac{(TN + TP)}{(TN + FN + FP + TP)}$	It is a measure of predicted devices from the overall devices
F-Score	$\frac{2 \cdot (Recall \cdot Precision)}{(Recall + Precision)}$	It is harmonic mean of recall and precision numeric values
AUC	-----	It represents the area under curve performance.

The overall performance characterization is made in two phases; intra-model assessment and the inter-model assessment. Here, intra-model assessment discusses the performance of the proposed model with the currently proposed configuration, while the inter-model assessment discusses the relative performance between the proposed FSPS based BigData analytics and other existing algorithms. The outcome of the comparison is elaborated as below.

B. Intra-Model Assessment

In this assessment processes, whether the inclusion of FSPS helps achieving better performance with lower data size was examined. Moreover, the performance with the different sample sizes was also assessed. Additionally, realizing the data unbalanced nature, and a complex multi-class classification problem the accuracy, F-score and AUC with the different base-classifiers was examined. Also, the performance patterns by the proposed model when the sample size is varied were examined. To assess whether the proposed FSPS model helps achieving better performance with minimum data size, the model was tested with 10% data size and subsequently increased sample rate with 0.5%. For the sake of easy presentation and understandability, the results were obtained for 10%, 12%, 14% and 16% of the sample or data size. The accuracy F-score and AUC obtained are given in Table III. Noticeably, here, for classification (over the FSPS samples) the proposed HEL ensemble learning model comprising three base classifiers, Random Tree, AdaBoost and Extra or Extended Tree classifiers were applied.

TABLE III. PERFORMANCE WITH THE DIFFERENT SAMPLE SIZES

Data Size (%)	Accuracy (%)	F-Measure	AUC
10	95.7	0.97	0.99
12	96.4	0.98	0.99
14	97.9	0.98	1.0
16	98.9	0.99	1.0

TABLE IV. PERFORMANCE COMPARISON WITH THE FSPS DRIVEN STANDALONE CLASSIFIERS

Classifier	Accuracy (%)	F-Measure	AUC
Random Forest	97.9	0.98	0.99
AdaBoost	93.6	0.94	0.93
Extended Tree	98.6	0.99	0.99
HEL Ensemble	98.9	0.99	1.0

The key purpose of above assessment (Table IV) was to examine whether the use of FSPS sampling can help a standalone classifier achieving better performance. The results (Table IV) depicts that amongst the different base-classifiers Extended Tree algorithm has exhibited the superior performance with the (multi-class classification) accuracy of 98.6%, F-Measure and AUC of 0.99 and 0.99, respectively. On the other hand, Random Forest algorithm exhibited the accuracy of 97.9%, F-Measure of 0.98 and AUC of 0.99. Unlike Random Forest and Extended Tree algorithm, AdaBoost exhibited inferior with the accuracy of 93.6%, F-Measure of 0.94 and AUC of 0.93. Amongst the three base classifiers AdaBoost algorithm performed inferior; however, recalling the fact that the performance obtained is with merely 16% of the data size, it can be stated as a satisfactory solution.

Noticeably, the proposed IoT-device classification problem was a multi-class classification problem, where the proposed model was supposed to classify each device (here, a total of 26 devices connected to the network and operating autonomously). Though the total number of traces were almost 1,60,000,000, where each trace represents one packet belonging to a specific device of a particular category (Table I). Considering this fact, where the proposed model classified devices into six different categories (it represents the devices of Class 1.0, Class 2.0, Class 3.0, Class 4.0, Class 5.0 and Class 6.0), within micro-average as well as macro-average (between the class and within the class performance, respectively) performance was examined. The ROC performance for each category of the devices after classification was tested. The results obtained by the proposed FSPS-driven HEL ensemble classifier is given in Fig. 3.

Observing the result (Fig. 3), it can be observed that the proposed model has obtained the AUC near 0.98 for the complete classes, while the AUC observed for each class (macro-average ROC) is also 0.98. For multi-class classification as well, the average AUC obtained is 0.98.

Typically, in progressive sampling based BigData analytics, in addition to the accuracy performance, time-efficiency too remains the key motive to meet VELOCITY demands. In this reference, relative time-efficiency in between the original data (ORIG) and the FSPS based selected data (PSAM) was compared. The results obtained are given in Fig. 4 and Fig. 5 As depicted in Fig. 4, the proposed progressive sampling-based model (PSAM) performs significantly lower computation time (in seconds) in comparison to the original data-based analytics. Undeniably, such efficacy could be contributed due to significantly reduced data size (almost 86%). It indicates the robustness of the proposed model towards real-time BigData analytics, even under multi-class classification demands.

C. Inter-Model Assessment

In this section, the performance by the proposed model is compared with the other approaches. However, the survey indicates a few such as the work by ElRafey et al. [32] who developed a hybrid active learning based progressive sampling method. More specifically, authors developed a Progressive Batch Model Uncertainty Sampling (PBMUS) model to increase sample size proactively to cope up with

(performance) demands. Authors simulated their model with the different datasets, including synthetic data as well as the real-time data. They applied Decision Tree C5.0 algorithm for classification. Authors examined their performance in terms of the classification accuracy and AUC considering 50% of the data size, while the increment boundary was decided as 1%.

Venkatpathy et al. [30] too examined the efficacy of progressive sampling methods with real-time data. Though, the data considered in [30] were smaller in size and diversity as is expected from the Big Data analytics, to assess relative performance, we have considered it as a reference work, as well. Authors [30] had applied Apriori information to estimate the most frequent itemsets and resulting mid-point itemset for association rule-based mining. Authors have examined their performance with the datasets like Mushroom, Chess, Connect, Retail data, Traffic accident data, and synthetic data. To perform relative comparison, the average performance by [30].was calculated. Summarily, the performance comparison of both models and the proposed model is tabulated in Table V.

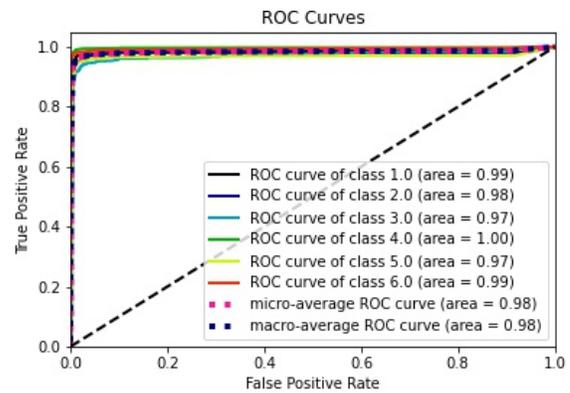


Fig. 3. ROC Performance by the Proposed FSPS-driven HEL Ensemble Model.

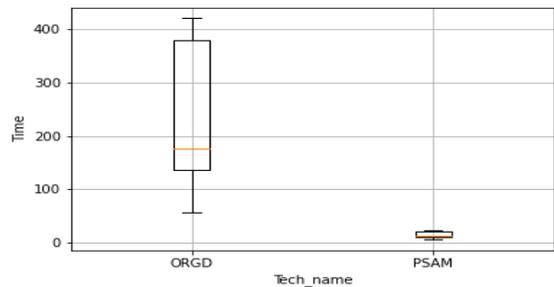


Fig. 4. Time Performance Analysis.

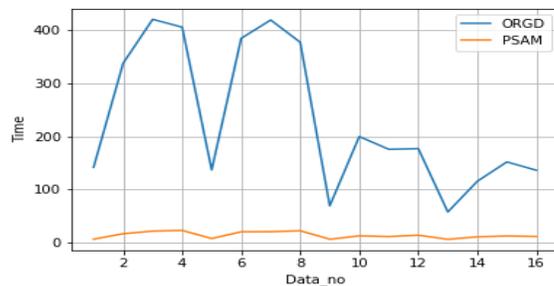


Fig. 5. Time Comparison of Original Data and Progressive Sampled Data.

TABLE V. INTER-MODEL COMPARISON PERFORMANCE OF PROGRESSIVE SAMPLING METHOD

Technique	Accuracy (%)	AUC
[30]	78.0	-
[32]	79.9	79.2
Proposed	98.9	1.0

The above results affirm that the proposed FSPS model achieves significantly better performance than the other state-of-art (progressive sampling) approaches.

Recalling the problem of IoT-device classification, the performance of the proposed model with other state-of-art methods such as [34] was examined. Bai et al. [34] applied the same dataset of UNSW to perform device classification. The authors merely applied the LSTM-CNN as classifier to perform classification over average features. The highest classification accuracy obtained by authors [34] could be merely 74.8%, which is significantly lower than the proposed model. To be noted, authors [34] had applied the complete data size (almost 2.7 GB) to perform classification. On the contrary, in the proposed model FSPS enabled applying merely 10%-16% of the original data to perform classification. Authors in [34] stated that their proposed LSTM-CNN based model could achieve the accuracy of near 99% with 75% of the data size, while with 25% of the training data they could achieve the maximum of 88.2%. However, these performances were merely for the two-class classification. For the multi-class classification, which is expected from the IoT-device classification problem (Table I), the average performance over five repeated simulation was 74.8%, which is significantly lower than the proposed model. Noticeably, in [34] authors also examined the different machine learning classifiers for their respective efficacy for device classification, and hence have compared the performance of the proposed model with the existing approaches [34].

TABLE VI. INTER-MODEL PERFORMANCE COMPARISON FOR IoT- DEVICE CLASSIFICATION

Reference	Technique	Accuracy (%)
Existing work	Support Vector Machine	58.5
	Random Forest	30.1
	KNN	27.6
	Decision Tree	46.4
	AdaBoost	48.5
	LDA	49.4
	QDA	52.4
	Multilayer perceptron	52.1
	Convolutional Neural Network (CNN)	56.3
	Long- and Short-Term Memory (LSTM)	65.4
LSTM-CNN	74.8	
Proposed work	Random Forest	97.9
	AdaBoost	93.6
	Extended Tree	98.6
	HEL Ensemble	98.9

The results depicted in Table VI shows that in comparison to the existing IoT-device classification systems, the proposed (FSPS-driven HEL ensemble learning) model exhibits superior even at significantly lower sample or data size.

VI. CONCLUSION

This paper primarily focused on developing a feature sensitive progressive sampling (FSPS) approach which could retain optimal performance even with minimal data size. Moreover, the key emphasis was to inculcate FSPS while addressing the key problem of data imbalance, multi-dimensionality and data heterogeneity in BigData analytics. Recalling the fact that in BigData analytics merely sampling can't guarantee the optimality of the performance and hence improving both data as well as computing environment is must, this research improved each functional component of the analytics solution. Unlike random (sample) selection based progressive sampling methods, which can't address the problem of data-imbalance, the proposed model employed machine learning driven FSPS to retain maximum possible feature diversity to perform better learning and hence classification performance.. The simulation results exhibited accuracy of 98.9%, F-score of 0.99 and AUC of more than one, affirming robustness of the proposed model towards lightweight, time-efficient and reliable BigData analytics solution. In future the focus can be made on further reducing data imbalance likelihood by applying certain re-sampling concepts. In addition, in future other machine learning models can also be assessed to have better performance for a generalized solution.

REFERENCES

- [1] O. Duda et al., "Data Processing in IoT for Smart City Systems," 2019 10th IEEE International Conference on Intelligent Data Acquisition and Advanced Computing Systems: Technology and Applications (IDAACS), Metz, France, 2019, pp. 96-99.
- [2] Thibaud Chardonens, "Big Data analytics on high velocity streams: specific use cases with Storm", Software Engineering Group, Department of Informatics, University of Fribourg, Switzerland, 2013.
- [3] H. Chiroma et al., "Progress on Artificial Neural Networks for Big Data Analytics: A Survey," in IEEE Access, vol. 7, pp. 70535-70551, 2019.
- [4] R. A. Alshawish, S. A. M. Alfagih and M. S. Musbah, "Big data applications in smart cities," 2016 International Conference on Engineering & MIS (ICEMIS), Agadir, 2016, pp. 1-7.
- [5] P. Bellini, F. Bugli, P. Nesi, G. Pantaleo, M. Paolucci and I. Zaza, "Data Flow Management and Visual Analytic for Big Data Smart City/IOT," 2019 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and SmartCityInnovation (SmartWorld/SCALCOM/UIC/ATC/CBDCom/IOP/SCI),Leicester, United Kingdom, 2019, pp. 1529-1536.
- [6] Cochran W.G., Sampling Techniques, 3rd edition, John Wiley and Sons, New York, 1977.
- [7] Parthasarathy S., Efficient Progressive Sampling for Association Rules, In: Ohsuga S. (Ed.), Proceedings of the IEEE International Conference on Data Mining (9-12 December 2002, Maebashi City, Japan), IEEE Computer Society, 2002, 354-361.
- [8] Chen B., Haas P., Scheuermann P., New Two-Phase Sampling Based Algorithm for Discovering Association Rules, In: Zaki M.J. (Ed.), Proceedings of the eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (23-26 July, 2002, Alberta, Canada), ACM, 2002, 462-468.
- [9] Zaki M.J., Parthasarathy S., Li W., Ogihara, M., Evaluation of Sampling for Data Mining of Association Rules, Proceedings of the 7th

- International workshop on Research Issues in Data Engineering (7-8 April 1997, Birmingham, UK), IEEE Computer Society, 1997, 42-50.
- [10] N. Bangera, and N. Kayarvizhy, "A Progressive Sampling based Approach to Reduce Sampling Time", 2019 4th International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT-2019), MAY, pp. 74-78.
- [11] Chuang K.T., Chen M.S., Yang W.C., Progressive Sampling for Association Rules Based on Sampling Error Estimation, LECT NOTES COMPUT SC, 2005, 3518, 505-515.
- [12] Estrada A., Morales E.F., NSC: A New Progressive Sampling Algorithm, Proceedings of the Workshop: Machine Learning for Scientific Data Analysis (Iberamia) (22-26 November, 2004, Iberamia), 2004, 335-344
- [13] A. Hsu, J. Tronty, D. Raymondy, G. Wang, A. Butt, "Automatic IoT Device Classification using Traffic Behavioral Characteristics", IEEE Conference, 2019, pp. 1—7.
- [14] M. Miettinen, S. Marchal, I. Hafeez, N. Asokan, A.-R. Sadeghi, and S. Tarkoma, "Iot sentinel: Automated device-type identification for security enforcement in iot," in Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on. IEEE, 2017, pp. 2177–2184.
- [15] A. Sivanathan, D. Sherratt, H. H. Gharakheili, A. Radford, C. Wijenayake, A. Vishwanath, and V. Sivaraman, "Characterizing and classifying iot traffic in smart cities and campuses," in Computer Communications Workshops (INFOCOM WKSHPS), 2017 IEEE Conf.on. IEEE, 2017, pp. 559–564.
- [16] Y. Meidan, M. Bohadana, A. Shabtai, M. Ochoa, N. O. Tippenhauer, J. D. Guarnizo, and Y. Elovici, "Detection of unauthorized IoT devices using machine learning techniques," CoRR, vol. abs/1709.04647, 2017. [Online]. Available: <http://arxiv.org/abs/1709.04647>.
- [17] Mahafzah B.A., Al-Badameh A.F., Zakaria M.Z., A new sampling technique for association rule mining, J INF SCI, 2009, 35, 358-376.
- [18] Jia C.Y., Gao X.P., Multi-scaling sampling: an adaptive sampling method for discovering approximate association rules, J COMPUT SCI TECHNOL, 2005, 20, 309-318.
- [19] Chuang K.T., Chen M.S., YangW.C., Progressive Sampling for Association Rules Based on Sampling Error Estimation, LECT NOTES COMPUT SC, 2005, 3518, 505-515.
- [20] Li Y., Gopalan R.P., Effective Sampling for Mining Association Rules, LECT NOTES COMPUT SC, 2005, 3339, 391-401.
- [21] Lin T.Y., Sampling in Association Rule Mining, In: Dasarthy B. (Ed.), Data Mining and Knowledge Discovery: Theory, Tools, and Technology VI, Proceedings of SPIE (Orlando, FL, USA), SPIE, 2004, 161-167.
- [22] Chakaravarthy V.T., Pandit V., Sabharwal Y., Analysis of sampling techniques for association rule mining, In: Fagin R. (Ed.), Proceedings of the 12th International Conference on Database Theory (23-25 March 2009, St. Petersburg, Russia), ACM Press, 2009, 276-283.
- [23] Zhao Y., Zhang C., Zhang S., Efficient frequent itemsets mining by sampling, In: Li Y. (Ed.), Proceedings of the fourth International Conference on Active Media Technology (7-9 June, 2006, Amsterdam, The Netherlands), IOS Press, 2006, 112-117.
- [24] Chen B., Haas P., Scheuermann P., New Two-Phase Sampling Based Algorithm for Discovering Association Rules, In: Zaki M.J. (Ed.), Proceedings of the eighth ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (23-26 July, 2002, Alberta, Canada), ACM, 2002, 462-468.
- [25] S.Parthasarathy, "Efficient progressive sampling for association rules", IEEE International Conference on Data Mining, 2002.
- [26] S. S. Thakur, Shalini Zanzote Ninori, "An Improved Progressive Sampling based Approach for Association Rule Mining International Journal of Computer Applications" (0975 –8887), Volume 165 – No.7, May 2017.
- [27] P.A. De los Santos, R.J. Burke, J.M. Tien, "Progressive random sampling: A multiperiod estimation technique with applications IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews)", Volume: 30, Issue: 4, Nov 2000.
- [28] Antal van den Bosch, "Wrapped Progressive Sampling for optimizing Learning Algorithm Parameters, Netherlands Organisation for Scientific Research".
- [29] François Portet, Feng Gao, Jim Hunter and René Quiniou, "Reduction of Large Training Set by Guided Progressive Sampling: Application to Neonatal Intensive Care Data".
- [30] Venkatapathy Umarani Muthusamy Punithavalli- Analysis of the progressive sampling-based approach using real life datasets <https://link.springer.com/journal/13537>.
- [31] Zeng X, Luo G, "Progressive sampling Based Bayesian optimization for Efficient and Automatic Machine Learning Model Selection", Springer 2017.
- [32] Amr ElRafey and Janusz Wojtusiak, "A Hybrid Active Learning and Progressive Sampling Algorithm, International Journal of Machine Learning and Computing", Vol. 8, No. 5, October 2018.
- [33] Q. Li, W. Li, J. Wang and M. Cheng, "A SQL Injection Detection Method Based on Adaptive Deep Forest," IEEE Access, vol. 7, pp. 145385-94, 2019.
- [34] L. Bai, L. Yao, S. alil, S. Kanhere, X. Wang, and Z. Yang, "Automatic Device Classification from Network Traffic Streams of Internet of Things", 2018, IEEE 43rd conference on Local Computer Nrtworks (LCN), 2018, pp. 1-9.

Thermal-aware Dynamic Weighted Adaptive Routing Algorithm for 3D Network-on-Chip

Muhammad Kaleem^{1*}, Ismail Fauzi Bin Isnin²

School of Computing, Faculty of Engineering

Universiti Teknologi Malaysia, Johor Bahru, Malaysia^{1,2}

Department of CS & IT, University of Sargodha, Sargodha, Pakistan¹

Abstract—3D Network-on-Chip NoC based systems have severe thermal problems due to the stacking of dies and disproportionate cooling efficiency of different layers. While adaptive routing can help with thermal issues, current routing algorithms are either thermally imbalanced or suffer from traffic congestion. In this work a novel thermal aware dynamic weighted adaptive routing algorithm has been proposed that takes traffic and temperature information into account and prevents packets being routed across congested and thermally aggravated areas. Dynamic weighted model will consider parameters related to congestion and thermal issues and provide a balanced suitable approach according to the current scenario at each node. The efficiency of the proposed algorithm is analyzed and evaluated with state-of-the-art thermal-aware routing algorithms using a simulation environment. Results obtained from the simulation shows that the proposed algorithm has performed better in terms of global average delay with 17-33 percent improvement and better thermal profiling under various synthetic traffic conditions.

Keywords—Routing algorithms; thermal-aware; dynamic weighted model; 3D Network-on-Chip

I. INTRODUCTION

3D-IC (Three Dimensional Integrated Circuit) is capable of providing small interconnections resulting in reducing delays due to die stacking. 3D NoC based chip multiprocessors (CMP) are estimated to have higher performance with less data transmission connection cost and power consumption [1]. Conventional NoC architectures consist of processing element (PE), network interface and router in every tile. Routers provide communication mechanisms for communication among tiles along communication paths. During high traffic situations, packets have to reside in the router's buffers waiting for its turn, causing congestion in the network. Routers are a source of thermal hotspot due to high switching activity and congestion resulting in higher power density [2]. Power density of the router area is higher than power density in intellectual property IP [3]. It is also the fact, higher power consumption of the chip elements results in deteriorating heat. Routers are responsible for providing communication between IPs at the cost of high heat dissipation.

Cooling mechanisms also known as heat sinks usually exist on only one side of the chip in multi-layer 3D NoC. Hence, layers further away from the heat sink have higher possibility of the thermal hotspots [4]. Due to these thermal hotspot difficulties and aggravation of failure mechanism puts

an extra strain on cooling cost of the chip and reliability reduction in 3D NoC. It is essential for designers to maintain performance of the system while reducing thermal hotspots [5]. To balance temperature distribution, various methods of thermal-aware application mapping [6] [7], floor-plan optimization [8] and thermal-aware routing [9] [10] [11] were proposed. Thermal-aware routing algorithms are classified in temporal and spatial routing algorithms. Temporal DTM (Dynamic Thermal Management) can dynamically adjust frequencies, voltages or clock cycles to reduce on-chip temperatures[12]. Usually a fully throttling scheme such as clock gating is applied to control the temperature of the thermal aggressive nodes. Hence, the temporal DTM results in reducing overall system performance but it can regulate system temperatures within short cooling time. Spatial routing algorithms are reducing thermal hotspots by diffusing traffic away from the heated regions [13]. Spatial DTM can manage thermal situations without reducing the speed of the node in terms of frequencies, voltages and clock cycles, hence, a tiny impact on the performance of the system.

Due to the lack of heat sink among the layers and poor traffic distribution, tackling the heat dissipation problem in 3D NoC is difficult. Since the center of the top layer in 3D NoC is more susceptible to thermal problems. One of the effective solutions is to divert traffic away from the center of the network or to the layers closer to the heat sink. Detoured traffic results in cooler routes yet increasing the path length. Heavy intermediate traffic results in more delays, causing congestion and induces thermal issues. Due to diverse thermal conductance between the intra layer and inter layer of the 3D NoC, the relationship between temperature and traffic behavior among NoC nodes is divergent. It is difficult to solve thermal issues without considering traffic conditions in the network. Heavy traffic can cause congestion in the network with low outflows, leads to packets stuck at router buffers waiting for its turn, dissipating heat and causing thermal difficulties. Hence, design goal of this work is to blend temperature and traffic information along with other routing parameters during the thermal control period in order to make better routing decisions. Highlights of the contribution in this work are listed below.

1) Proposed a novel thermal-aware dynamic weighted routing (TADWR) technique for dynamic distribution of traffic and heat in the 3D NoC. This technique allows packets to adaptively select their next neighbour by dynamically adjusting weights of the cost model.

*Corresponding Author.

2) TADWR works on a dynamic weight management mechanism designed to regulate new weights among the parameters to work according to network situation and need of time.

3) Extensive simulation is performed and compared the results with state-of-the-art techniques under various synthetic traffic scenarios.

The rest of the paper is organized as follows. In Section II related work to thermal-aware routing algorithms has been discussed along with its limitations. In Section III detailed methodology of the proposed routing algorithm has been presented. In Section IV results of simulations have been presented and compared with other existing routing techniques. Finally, this work has been concluded in Section V.

II. LITERATURE REVIEW

Thermal-aware routing algorithms have gained attention among researchers all over the world due to high switching activity in routers. Traffic congestion, hotspot formations, and packet delays can be reduced by using an efficient and effective routing algorithm. Hence, thermal-aware routing has gained considerable attention among researchers in recent years. In order to reduce on-chip temperature, the routing strategies outlined in [14] aim to route packets through a layer closer to the heat sink. Thermal-aware Selective Detour (TSD) and Thermal-aware MILP-based Detour (TMD) are the two techniques presented. This routing technique is non-adaptive detour-based application-specific routing for 3D mesh NoC. Authors examine the impact of various detour decisions on the chip's steady-state and transient-state temperature profiles, as well as the network's average packet latency. However, being non-adaptive it is hard to maintain performance at higher packet injection rates with critical applications.

Fast multi objective thermal-aware adaptive routing algorithm (FMoTAR) is introduced in [15] to optimize the thermal profile of 3D NoC. FMoTAR uses a bidirectional search to easily locate the shortest path. With a higher packet injection rate in FMoTAR, maintaining efficiency with sensitive applications is a challenge. The Q-learning mechanism [16] is used to create a proactive thermal management strategy for 3-D NoCs using a feedback-based technique. An agent learns its own behavior in an immersive environment during system activity. The reward values of the agent behavior are stored and updated in a table called Q-table in Q-learning. The average temperature of routers is assigned to packet traversing in the header of each ordinary packet (a packet that passes data between nodes). The routers' Q-table stores and updates these values. As a result, no learning packets are needed to spread thermal information across the chip. Incoming packets are routed to cooler routes based on their Q-table values, and they are detoured from high-temperature areas. However, it can be observed that Q-learning based routing is focusing on average temperatures which will be always less than the actual temperature of the router hence deprived decisions will be made during routing.

QTTAR [17] is a Q-learning-based adaptive 3D routing algorithm that improves overall node utilization by balancing

inter-layer traffic distribution and offering a more precise congestion analysis to prevent RTM-related performance degradations. By balancing the distribution of overheated regions in a layer, QTTAR reduces differences in inter-layer cooling performance. By learning dynamically evolving networks, QTTAR detects regional congestion and thermal hotspots. QTTAR produces an effective route and a routing decision based on the Q-table. It uses a Q function-based routable direction selection technique to achieve routable path diversity. According to 3D symmetrical buffered clock tree for thermal variation synthesis [18] initially, sinks with similar power consumption for selecting closest to median cost of the neighbor in a 3D abstract tree topology. Second, the layer assignment of the internal node is calculated for uniform TSV distribution. Finally, after completing the thermal profile centered on the grid, the buffer, wire and exact position of TSV insertion are completed. However, at low-power 3D abstract trees and clock tree synthesis needs to be further investigated.

To balance the thermal distribution and meet the efficiency requirements, an energy- and buffer-aware fully adaptive routing algorithm is proposed [19]. To balance the flow of thermal energy and reduce network congestion, a network state feature model is built that takes into account both historical and current network states. Fully adaptive routing indicates improvement in thermal distribution without performance degradation to lower the temperature and meet the performance specifications of high priority packets. A collaborative thermal-aware adaptive routing (CTTAR) scheme [4] to synchronize network traffic and thermal information is presented. Since unnecessary packet switching causes hotspots, the CTTAR first employs dynamic buffer change, which can restrict the routing resource around overheated regions to slow the rate of temperature increase based on expected thermal details. Since the routers in the overheat area switch less packets, the dynamic buffer change will reduce heat production and diffusion. CTTAR converts overheated areas into congested areas. However, it is not suitable for complicated hotspot distribution. GTDAR [20] is a game theory-based thermal delay-aware adaptive routing system that transfers long-term thermal information into short-term traffic information, allowing it to orchestrate traffic and thermal information more effectively and reduce the temperature problem into a traffic problem. The traffic load distribution in GTDAR's network is unbalanced.

In ATAR [21] packet is traversed in the network on the bases of its weighted cost model calculation. Highest weightage is given to temperature and decreasing weightage to the subsequent factors i.e. path length, neighbor queue length and its workload. Cost is calculated to find the potential best neighbor for forwarding the packet. At the source end, all best neighbors until destinations are computed to make a path list. Path list contains all the neighbors that will be used to deliver the packet. ATAR has taken all decisions at an individual node level. ATAR is lacking its view of congested and thermally active regions. If a particular neighbor has the least cost but if it is part of a congested or thermally hostile region. ATAR has little or no ability to identify congested regions due to an inflexible cost model. If such nodes are selected for

traversing packets, this leads to enhance congested areas hence higher heat dissipation and higher thermal issues. Centre of the network is naturally prone to become congested. Sending more packets to the congesting or throttling region can be fatal.

There are multiple paths between source and destination. If a routing algorithm dynamically adjusts its cost model according to intermediate nodes current conditions then we can adaptively adjust and choose better paths to reach its destination. It is observed from literature; apart from thermal-aware selection of algorithms, it is also necessary to include various other factors such as neighboring node temperatures, shortest path length, detection of congestion situation, and next router queue length.

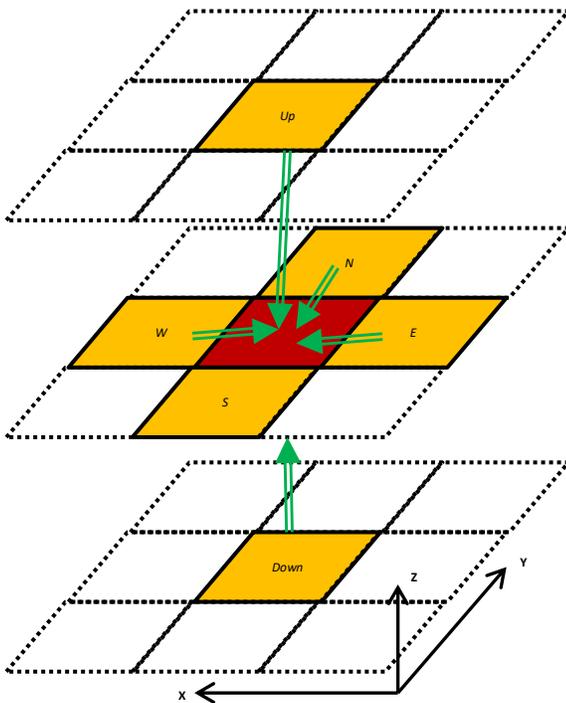


Fig. 1. Central node Neighbors of 3D NoC.

III. METHODOLOGY

Nodes in NoC get heated up due to high power usage. Even a smallest of unwanted operations can play its role in increasing the temperature and that could lead to a disaster. Therefore, uncontrolled and excessive movement in the network should be avoided. Consider if the router is already busy in sending upstream packets to the desired output ports. New arriving packet has to wait for its turn in the packet queue at the input buffers. These excessive packets stall in the input buffers accelerate the heating process. In Fig. 1, it can be observed that if the central node of the network is experiencing heavy congestion then very quickly output buffers of neighboring nodes also start to observe congestion. Which means the congestion region will extend itself if it is not handled in time. As congestion is the primary cause of thermal aggravation and throttling. Congestion cannot only occur in the center of the network but it can occur anywhere within the chip. Therefore, packets cannot be allowed to just

detour away from the center of the network to get thermal stability. Dynamic mechanism is required to handle and adjust according to the need and requirement of the situation within a chip.

In this work a technique that can consider temperature, congestion and most importantly allow packets to adaptively select their next neighbor by dynamically adjusting weights of the cost model is proposed. Dynamically adjusting the cost model means, when NoC is thermally stable with no congestion proposed algorithm should consider shortest path on priority and allow packets to choose best possible paths with least workload to reach the destination. As soon as congestion starts occurring, the dynamic model should take actions adjusting it to choose paths with less congestion in reaching destination. Similarly, when thermal issue arises then priority will be given to the thermal issue to bypass the thermally active regions. In case of multiple issues, arising at the same time proposed dynamic weighted model will consider all parameters and provide a balanced approach suitable for the situation and need.

A. Dynamic Weight Adjustment Model

In this work, following parameters are considered as given below:

1) Path Length is denoted by L, it is the number of hops a packet takes to reach its destination from source. Consider (x_1, y_1, z_1) is the source and (x_2, y_2, z_2) is its destination so path length will be calculated from the equation 1 below.

$$L = m|x_1 - x_2| + n|y_1 - y_2| + o|z_1 - z_2| \quad (1)$$

According to equation (1) m is the number of rows in x dimension n is the number of columns in y dimension and o is the number of layers in z dimensions.

2) Candidate node temperature is denoted by T and it is the current temperature of the immediate candidate node next is succession.

3) Candidate node throughput is denoted by W and it is the current throughput of the immediate candidate node next is sequence.

4) Candidate node Q length denoted by Q and it is the current Q length of the intermediate node next under consideration.

This work is using the cost model presented in ATAR [21] equation (2). Where T is temperature, L is path length, Q is next router queue length and W is node throughput. T is responsible for temperature influence, L is responsible to cover path length till destination, Q is responsible for determining congestion in next buffer and W is responsible to reflect load on the link.

$$\text{cost} = a_1 \cdot T + a_2 \cdot L + a_3 \cdot Q + a_4 \cdot W \quad (2)$$

Initially equal weights are assigned to i.e. $a_1 = a_2 = a_3 = a_4$ where a_1, a_2, a_3, a_4 are respective weights of [T, L, Q, W] whereas $\sum_1^j a_j = 1$ and $a_j \neq 0$, such that $j \in \{1, 2, 3, 4\}$. As traffic load increases and more and more packets start traversing to reach their destination, packets start occupying

buffers hence Q length will start to vary. Routers with the smallest Q length will be given priority as a next hop for the packet. Therefore, it will keep assigning new weights to the highest values of Q length. Similarly, with the passage of time throughput of the node will also reduce as traffic and congestion is increased. So, highest new weights will be assigned to nodes with highest throughput in order to choose the next hop node with highest throughput. As the traffic conditions are worsening especially under higher packet injection rates the congestion occurs and node temperature will begin to rise. If a node temperature exceeds its previous temperature then it will be known as new peak value and new weight will be calculated and assigned to the new peak value in a node. If a node experiences a temperature less than the new peak value a weight will be assigned accordingly.

As all the parameters have their own intended weights. Technique cannot simply grant all parameters to use their intended weights and violate $\sum_1^j a_j = 1$ condition. Hence, weight management mechanism is required to regulate new intended weights among the parameters. For new weight formation first calculate the weight difference β_i given in equation (3). β_i is a difference between previous weight and new intended weight for any parameter.

$$\beta_i = \text{Previous_weight}_i - \text{Intended_weight}_i \quad (3)$$

Where $i = \{1, 2, \dots, C\}$ and C is the number of all parameters under consideration. After calculating the difference between previous weights and new weights of all parameters, a weight bucket (WB) is formed. WB is a sum of all weight differences in all parameters equation (4).

$$\text{WB} = \sum_{i=1}^c \beta_i \quad (4)$$

Where $i = \{1, 2, \dots, C\}$ and C is the number of all parameters under consideration. After calculating the weight bucket, weight fraction is calculated. Weight fraction WF is the equal share for all the parameters weight in the consideration equation (5).

$$\text{WF} = \frac{\sum_{i=1}^c \beta_i}{c} \quad (5)$$

Where $i = \{1, 2, \dots, C\}$ and C is the number of all parameters under consideration. In the next step, weight fraction is added to the intended weight of the particular parameter and a new weight α_i is formed in equation (6) for calculation of the cost model given in equation (1).

$$\alpha_i = \text{Intended_weight}_i + \text{WF} \quad (6)$$

It can be observed that each node in the network will have its own weights and preferences according to the current state and condition of a particular node. Now if the routing algorithm has more than one possible neighbor to traverse, a better decision could be made according to the scenario a node is currently experiencing.

Algorithm 1 TADWR

Input: Source node, destination node, node temperature, workload, path length and queue length
Output: path
1: **function** TADWR(s_node , d_node, route_data)
2: **if** s_node= d_node then
3: directions \leftarrow direction_local
4: **else**
5: **set** i_node \leftarrow s_node
6: **while** i_node \neq d_node do
7: **set** dir \leftarrow getAvailableDirections(i_node)
8: **for** k \in dir do
9: **set** e \leftarrow i_node
10: Intended_weight₁ \leftarrow getTempIntendedWeight(i_node,dir)
11: Intended_weight₂ \leftarrow getPathlength(i_node, d_node)
12: Intended_weight₃ \leftarrow getqueueLength(i_node, dir)
13: Intended_weight₄ \leftarrow getWorkload(i_node,dir)
14: $\beta_i = \text{Previous_weight}_i - \text{Intended_weight}_i$
15: $\text{WB} = \sum_{i=1}^c \beta_i$
16: $\text{WF} = \frac{\sum_{i=1}^c \beta_i}{C}$
17: $\alpha_i = \text{Intended_weight}_i + \text{WF}$
18: **set** cost \leftarrow $\alpha_1.e.T + \alpha_2.e.L + \alpha_3.e.Q + \alpha_4.e.W$
19: **if** V[s_node][i_node] + cost < V[s_node][e.next] then
20: **set** V[s_node][e.next] \leftarrow cost
21: **end for**
22: **set** i_node \leftarrow mincostNode(V, s_node, directions)
23: **set** directions \leftarrow direction_mincostnode(s_node, i_node)
24: **end while**
25: **end else**
26: **return** directions

B. Thermal-Aware Dynamic Weighted Routing (TADWR)

Pseudo code for TADWR is presented in Algorithm 1. Algorithm takes arguments such as source node, destination node and route data (node parameters i.e. L, T, Q, W). Source node is denoted by s_node represents the node from which the packet has been initiated. Destination node is denoted by d_node, representing the node at which the packet will be terminated. In the beginning, the algorithm will check location of source node and destination node. If it is addressing itself, it will be terminated by returning direction Local in line 2-3. Checking for all possible directions available for the node in line 7-8. Get parameter T, L, Q, W values from i_node. Find the intended weight for the intermediate candidate node all parameters line 10-13. Calculate change in weight (either weight loss or gain) in all parameters with respect to previous weights line 14. Calculate sum of all the weight changes and assigned to weight bucket WB line 15. Calculate weight fraction WF according to number of criteria and to be added in respective intended weights line 16-17. The weighted cost sum is then calculated. In lines 19-20 the cost matrix is updated, if the calculated cost is less than the current cost. Now the minimum cost node will become the new i_node (intermediate node) and the minimum cost nodes direction is pushed in directions. In order to reduce the delay caused by the loop in the algorithm, parallel architecture is used to reduce the computation delay.

IV. SIMULATION RESULTS AND DISCUSSION

TADWR routing algorithm has been simulated in Access Noxim [22]. Access Noxim simulator is a cycle accurate simulator integrated with HotSpot [23] and Noxim [24]. Noxim is designed by using the System C library. SystemC is an open-source hardware description language designed in C++. Noxim is portable and can run on any SystemC based infrastructure. NoC parameters can be defined and set using a command based interface, e.g. user can set number of nodes in the network, traffic distribution system, buffer capacity, network size and dimensions, packet sizes, routing algorithm, traffic distribution time, packet injection rate, etc. Noxim can evaluate capability of NoC in terms of delay, throughput and power consumption. Noxim also possesses a transaction level mode where detailed analysis of even a single transaction can be made. HotSpot is responsible for providing architectural level thermal models. Overall Access Noxim is capable of providing thermal model, power model and network model of 3D network-on-chip.

A. Simulation Setup

To evaluate the performance of the proposed routing algorithm, 8 x 8 x 4 3D NoC is considered. Parameters used in the simulation are listed in Table I. Different synthetic traffics are simulated to test the ability of TADWR as compared to its counterparts. TADWR is compared with state-of-the-art ATAR and fully adaptive routing algorithms. Each simulation is carried out for 200,000 cycles with different PIR (packet injection rate). PIR is varying from 0.02 to 0.22 with the interval of 0.02 (flits/cycle/node). A 0.02 PIR means each node sends 0.02 flits every clock cycle. The instance at which a packet is injected depends on the distribution of the time interval.

TABLE I. SIMULATION PARAMETERS

Parameters	Value
Network Dimension	8 x 8 x 4
Simulation Time (Cycles)	200,000
Warm-up Time (Cycles)	10,000
Buffer Size (Flits)	16
Packet size (Flits)	2-10
Packet injection rate (flits/cycle/node)	0.02-0.22
Packet injection interval	0.02
Traffic Pattern	Random, Shuffle, Hotspot, Bit-Reversal

B. Performance Evaluation

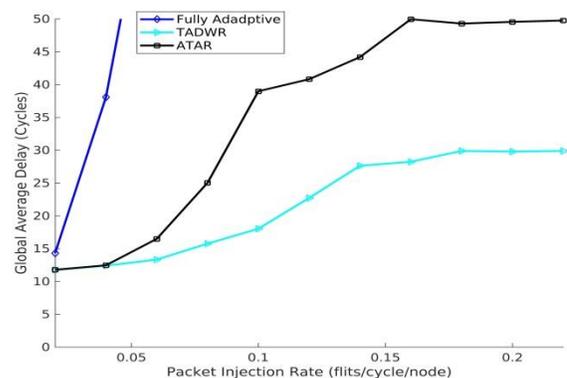
The traffic patterns applied in this section are bit-reversal, random, shuffle and hotspot traffic. Global average delay (cycle) chart is presented for each simulation. ATAR uses fixed weighted cost model and TADWR uses dynamic weighted cost model whereas, fully adaptive does not use any cost model criteria for routing. The global average delay diagram of fully adaptive, ATAR and TADWR under bit-reversal traffic is presented in Fig. 2(a). It can be observed that for the injection rate between 0.02 to 0.10 with the interval of 0.02 both ATAR and TADWR have similar results but as

injection rate increases it has begun to show diverse behaviors. Examining the graph reveals that the after 0.10 global average delay of TADWR with dynamic weight assignment has sustained as compared to ATAR, which has a fixed weighted cost model. As far as fully adaptive routing is concerned, it can be observed that it has rocketed up at PIR 0.10 due to unawareness of traffic congestion situation.

The global average delay diagram of fully adaptive, ATAR and TADWR under random traffic is presented in Fig. 2(b). It can be observed that for injection rate between 0.02 to 0.10 with the interval of 0.02 both ATAR and TADWR have similar results but as injection rate starts to grow the difference start to get more apparent. Analyzing the graph, it is obvious that after 0.10 global average delay of TADWR with dynamic weight assignment has sustained as compared to ATAR, which has a fixed weighted cost model. As far as fully adaptive routing is concerned, fully adaptive has sharply shot at PIR 0.10 due to unawareness of traffic congestion situation.

The global average delay diagram of fully adaptive, ATAR and TADWR under shuffle traffic is presented in Fig. 2(c). It can be observed that for injection rate between 0.02 to 0.10 with the interval of 0.02 both ATAR and TADWR have similar results but as injection rate starts to increase greater than PIR 0.10 the difference between ATAR and TADWR become clear. Analyzing the graph, it is obvious that after 0.10 global average delay of TADWR with dynamic weight assignment is better than ATAR, which has a fixed weighted cost model. As far as fully adaptive routing is concerned, it can be seen that fully adaptive has skied sharply around PIR 0.12 due to unawareness of traffic congestion situation.

The global average delay diagram of fully adaptive ATAR and TADWR under hotspot traffic with 20 percent is presented in Fig. 2(d). It can be observed that for injection rate between 0.02 to 0.10 with the interval of 0.02 both ATAR and TADWR have identical results but as injection rate increases change in behavior is obvious. Examining the graph tells that the after 0.10 global average delay of TADWR with dynamic weight assignment has sustained as compared to ATAR which has a fixed weighted cost model even in highly demanding traffic conditions. As far as fully adaptive routing is concerned, it can be observed that it has started to rise fairly early due to unawareness of traffic congestion situation and unable to cope with stressed traffic such as hotspot.



(a)

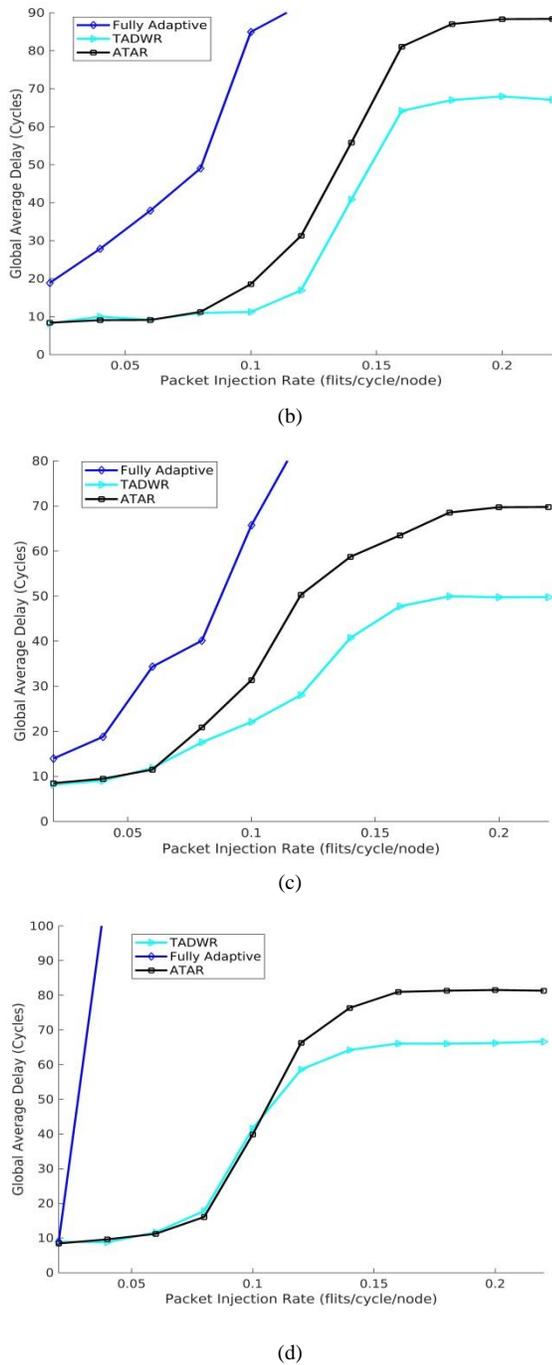


Fig. 2. Comparison of Global Average Delay under Various Traffic Patterns (a) Bit-reversal Traffic (b) Random Traffic (c) Shuffle (d) Hotspot Traffic.

C. Thermal Performance

Simulations are conducted for steady state temperatures. The thermal results are shown in the Fig. 3 for random traffic pattern with packet injection rate (PIR) of 0.02 (flits/cycle/node). The thermal image shows the drop in peak temperatures of the on-chip network of TADWR as compared to ATAR is around 6 K and massive 20K with respect to fully adaptive routing during extensive simulations and results comparison.

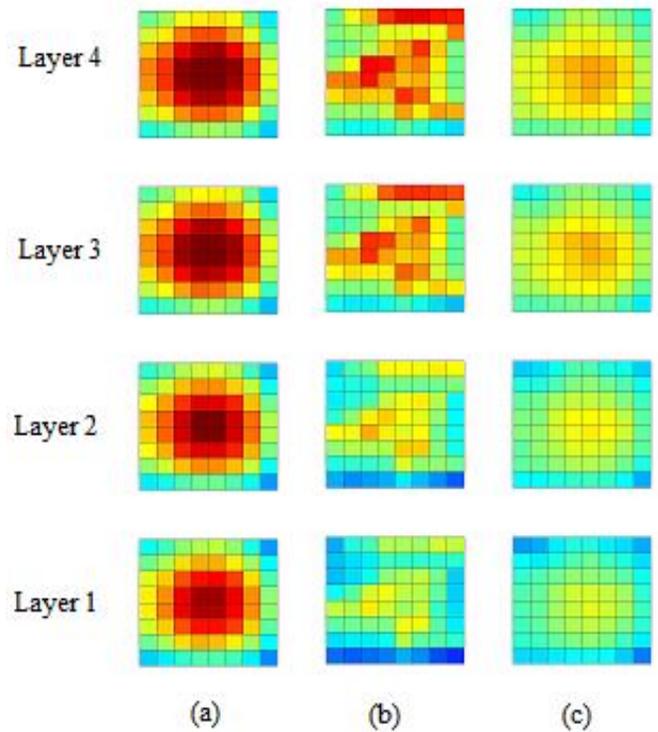


Fig. 3. Thermal Profile Comparison under Random traffic (a) Fully Adaptive Routing (b) ATAR (c) TADWR.

This indicates that TADWR achieves better thermal optimization with respect to other routing algorithms considered in this study. The simulations at each PIR have been repeated for a number of times to guarantee the accuracy of results. Fully adaptive shown in Fig. 3(a) has the highest thermal profile; this is due to the fact that fully adaptive routing does not consider thermal parameters during the routing process. In the case of ATAR, temperature imbalance occurs due to longer routes. Consequently, increases in congestion in the network leads to high thermal profile in the 3D NoC shown in Fig. 3(b). TADWR provides a better thermal profile than other routing algorithms. Thermal profile for TADWR at PIR 0.02 is illustrated in Fig. 3(c). On higher PIR, the peak temperature of the top layer is increased up to 8 K at PIR 0.10 and 10 K at PIR 0.22 with respect to thermal profile of TADWR at PIR 0.02.

V. CONCLUSION

This work proposes a thermal-aware dynamic weighted routing TADWR. TADWR can consider temperature, congestion and most importantly allow packets to adaptively select their next neighbor by dynamically adjusting weights of the cost model. Weight management mechanism is designed to regulate new intended weights among the parameters to work according to network situation and need of time. In contrast to previous work, proposed approach achieves better and balanced thermal distribution, improved network efficiency, and less hotspot in a chip. TADWR performs extremely better when in heavy packet injection rates in terms of global average delay having 17-33 percent improvement under different synthetic traffic scenarios. Thermal profiling

of TADWR is also clearly better than other routing algorithms. This work is limited to fully-connected 3D mesh topology. It can be further extended to become fault-aware in future.

ACKNOWLEDGMENT

The research is supported by Ministry of Higher Education Malaysia (MOHE) and conducted in collaboration with Research Management Center (RMC) at the Universiti Teknologi Malaysia (UTM) under Fundamental Research Grant Scheme with grant number: R.J130000.7851.5F029. The authors appreciate greatly for the support.

REFERENCES

- [1] E. Fusella and A. Cilardo, "Lattice-Based Turn Model for Adaptive Routing," *IEEE Trans. Parallel Distrib. Syst.*, no. 1, p. 1, 2018.
- [2] C.-H. Chao, K.-C. Chen, T.-C. Yin, S.-Y. Lin, and A.-Y. A. Wu, "Transport-layer-assisted routing for runtime thermal management of 3D NoC systems," *ACM Trans. Embed. Comput. Syst.*, vol. 13, no. 1, p. 11, 2013.
- [3] E. Taheri, M. Isakov, A. Patooghy, and M. A. Kinsky, "Addressing a New Class of Reliability Threats in," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. PP, no. c, p. 1, 2019.
- [4] L. Shen, N. Wu, G. Yan, and F. Ge, "Collaborative thermal-and traffic-aware adaptive routing scheme for 3D Network-on-Chip systems," *IEICE Electron. Express*, pp. 18–20200425, 2021.
- [5] D. Lee, S. Das, and P. P. Pande, "Analyzing power-thermal-performance trade-offs in a high-performance 3D NoC architecture," *Integration*, vol. 65, pp. 282–292, 2019.
- [6] M. Abdollahi, Y. Firouzabadi, F. Dehghani, and S. Mohammadi, "THAMON: Thermal-aware High-performance Application Mapping onto Opto-electrical network-on-chip," *J. Syst. Archit.*, p. 102315, 2021.
- [7] W. Liu et al., "Thermal-aware Task Mapping on Dynamically Reconfigurable Network-on-Chip based Multiprocessor System-on-Chip," *IEEE Trans. Comput.*, 2018.
- [8] S. Balakrishnan and R. Venkatesan, "Splay Tree Hybridized Multicriteria ant Colony and Bregman Divergencive Firefly Optimized Vlsi Floorplanning," 2021.
- [9] K. N. Dang, A. Ben Ahmed, A. Ben Abdallah, and X.-T. Tran, "HotCluster: A thermal-aware defect recovery method for Through-Silicon-Vias Towards Reliable 3-D ICs systems," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, 2021.
- [10] Z. Shirmohammadi, M. Mahmoudi, and M. Rostamzhad, "Int-TAR: An Intelligent Thermal-Aware Routing Algorithm for 3D NoC," *J. Electr. Comput. Eng. Innov.*, 2021.
- [11] S. S. Kumar, A. Zjajo, and R. van Leuken, "Immediate Neighborhood Temperature Adaptive Routing for Dynamically Throttled 3-D Networks-on-Chip," *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 64, no. 7, pp. 782–786, 2017.
- [12] D. Lee, S. Das, J. R. Doppa, P. P. Pande, and K. Chakrabarty, "Performance and Thermal Tradeoffs for Energy-Efficient Monolithic 3D Network-on-Chip," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 23, no. 5, p. 60, 2018.
- [13] N. Rohbani, Z. Shirmohammadi, M. Zare, and S.-G. Miremadi, "LAXY: A Location-Based Aging-Resilient Xy-Yx Routing Algorithm for Network on Chip," *IEEE Trans. Comput. Des. Integr. Circuits Syst.*, vol. 36, no. 10, pp. 1725–1738, 2017.
- [14] P. Mukherjee, N. Chatterjee, and S. Chattopadhyay, "Thermal-aware detour routing in 3D NoCs," *J. Parallel Distrib. Comput.*, 2020.
- [15] A. Majumdar, R. K. Dash, J. L. Risco-Martín, and A. K. Turuk, "FMoTAR: a fast multi-objective thermal aware routing algorithm for three-dimensional network-on-chips," in *Proceedings of the 50th Computer Simulation Conference*, 2018, p. 12.
- [16] N. Shahabinejad and H. Beitollahi, "Q-Thermal: A Q-Learning-Based Thermal-Aware Routing Algorithm for 3-D Network On-Chips," *IEEE Trans. Components, Packag. Manuf. Technol.*, vol. 10, no. 9, pp. 1482–1490, 2020.
- [17] S. C. Lee and T. H. Han, "Q-Function-Based Traffic-and Thermal-Aware Adaptive Routing for 3D Network-on-Chip," *Electronics*, vol. 9, no. 3, p. 392, 2020.
- [18] D. K. Oh, M. J. Choi, and J. H. Kim, "Thermal-aware 3D Symmetrical Buffered Clock Tree Synthesis," *ACM Trans. Des. Autom. Electron. Syst.*, vol. 24, no. 3, p. 28, 2019.
- [19] J. Wang, H. Gu, Y. Yang, and K. Wang, "An energy-and buffer-aware fully adaptive routing algorithm for Network-on-Chip," *Microelectronics J.*, vol. 44, no. 2, pp. 137–144, 2013.
- [20] K.-C. Chen, "Game-based thermal-delay-aware adaptive routing (gtdar) for temperature-aware 3d network-on-chip systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 29, no. 9, 2018.
- [21] R. Dash, A. Majumdar, V. Pangracious, A. K. Turuk, and J. L. Risco-Martín, "ATAR: An Adaptive Thermal-Aware Routing Algorithm for 3-D Network-on-Chip Systems," *IEEE Trans. Components, Packag. Manuf. Technol.*, no. 99, pp. 1–8, 2018.
- [22] K.-Y. Jheng, C.-H. Chao, H.-Y. Wang, and A.-Y. Wu, "Traffic-thermal mutual-coupling co-simulation platform for three-dimensional network-on-chip," in *Proceedings of 2010 International Symposium on VLSI Design, Automation and Test*, 2010, pp. 135–138.
- [23] W. Huang, S. Ghosh, S. Velusamy, K. Sankaranarayanan, K. Skadron, and M. R. Stan, "HotSpot: A compact thermal modeling methodology for early-stage VLSI design," *IEEE Trans. very large scale Integr. Syst.*, vol. 14, no. 5, pp. 501–513, 2006.
- [24] V. Catania, A. Mineo, S. Monteleone, M. Palesi, and D. Patti, "Noxim: An open, extensible and cycle-accurate network on chip simulator," in *2015 IEEE 26th international conference on application-specific systems, architectures and processors (ASAP)*, 2015, pp. 162–163.

A New Back-off Algorithm with Priority Scheduling for MQTT Protocol and IoT Protocols

Marwa O Al Enany¹, Hany M. Harb²

Department of Systems and Computers
Faculty of Engineering, Al-Azhar University
Cairo, Egypt

Gamal Attiya³

Department of Computer Science and Engineering
Faculty of Engineering, Menoufia University
Menouf, Egypt

Abstract—The Internet of Things (IoT) protocols have encountered great challenges as the growth of technology has led to many limitations of the performance of the IoT protocols. Message Queuing Telemetry Transport protocol (MQTT) is one of the most dominant protocols in most fields of smart applications, so it has been chosen in this research to be a use case for implementing and evaluating a new proposed Back-off algorithm that is designed to eliminate suspicious and fake messages by calculating an initial frequent rate for each publisher connected to the MQTT broker. The proposed Back-off algorithm was designed to mitigate the traffic load of the uplink traffic by applying an exponential delay factor to suspicious publishers. Another priority scheduling algorithm was proposed to classify publishers as high priority or low priority depending on the new calculated frequent rate. The two algorithms were implemented on the Mosquitto broker and evaluated using a simulation environment by measuring specified performance metrics. The simulated results proved that the Back-off algorithm eliminated network load and introduced an acceptable range of CPU and RAM consumption. The results also concluded that the priority classification algorithm managed to reduce the latency of high-priority publishers.

Keywords—Back-off algorithm; priority scheduling; MQTT protocol; average transmission frequency rate; IoT protocols

I. INTRODUCTION

Binding the whole world became an easy mission by using new technologies with the aid of the internet. One of the most important and modern technologies that conquer all the fields of human life is the IoT (Internet of Things) in which any group of devices can be connected and communicate together without the need for any interference or intervention of humans. Accessing and controlling remote applications and remote information has become easier and faster because of IoT. IoT extended the capabilities of the internet to cut across ordinary computers by allowing smart devices or actuators to send and receive information remotely from different environments and networks.

The most important fields of human life that depend nowadays on IoT are Healthcare and wearable devices [1], where treatment and patient follow-up became easier for the medical board and for patients themselves without the need of the presence of doctors and patients in the same place, smart agriculture [2] depends on IoT as monitoring soil and factors affecting agriculture crops can help in increasing the quantity and quality of final products, smart homes[3] and smart cars

where the dream of an automated life became true and modern houses are equipped with sensors which react with human to facilitate our life and help elderly [4] like door authentication scheme sensors [5], temperature sensors to adjust air conditioner [6] automatically, car sensors that allow car parking automatically [7] with only flipping a switch and other sensors that can be managed remotely with smartphones.

Due to the diversity of IoT applications in different fields of life, various types of IoT protocols are employed depending on the required function of the protocol. These protocols can gather data from sensing nodes or send data and manage communication between sensing nodes and the processing nodes depending on the function required from the protocol at every point in the network, a suitable protocol was employed [8].

One of the most widespread protocols is the Message Queuing Telemetry Transport protocol (MQTT) which is a small and lightweight messaging protocol suitable for resource-constrained and machine to machine (M2M) networks and relies on the TCP/IP protocol with a publish/subscribe model. The main function of the MQTT protocol is to gather data from sensing nodes, which are called publishers, and send them to a central intermediate device called a broker, which in turn sends this data to the required destination, which is called a subscriber.

MQTT [9] is primarily used for low bandwidth and high latency networks as it has a small fixed header of 2 bytes and depending on the publish/subscribe model which guarantees flexibility and simplicity of communication [10], it also used in loosely coupled networks as publisher and subscribers are not connected and they do not need to be available at the same time. On the contrary, publishers and subscribers do not know the availability or identification of each other. MQTT is considered to be a many-to-many protocol as many subscribers and publishers can be connected to the broker at the same time. UTF-8 string topics like mynewhouse/myroom1/temperature are used for message addressing in a hierarchal structure form that can use single-level wildcards by using + character or multilevel wildcards by using # character besides using SSL/TLS for security.

Publisher or subscriber can select one of three quality of service (QoS) levels defined in MQTT protocol depending on the employed system and network condition [11] so, message delivery assurance is performed depending on the selected level

of QoS. For QoS 0, the message is delivered at the best effort at most once without any message acknowledgment or reception assurance, so it is called "fire and forget". QoS 1 ensures message receiving at least one time. The sender keeps the message stored at its side until the reception of acknowledgment of the message from the receiver. Thus, if an acknowledgment was not received at a certain predefined time, the sender would send the same message again until receiving acknowledgment thus message could be sent several times to the receiver. QoS 2 uses 4-way handshaking for sending a message, so it is called "exactly once" because this level ensures the message receiving only one time without any duplication.

The main central device that is responsible for receiving and sending messages from publishers to subscribers is called the MQTT broker. The broker is responsible for message organization and distribution of messages among publishers and subscribers. It can handle thousands of connections simultaneously. It accepts messages from publishers then manages filters and distributes messages to the appropriate subscribers depending on the associated topics identified by subscribers. Many organizations have developed and implemented different brokers for the MQTT protocol that vary in features and programming language but all of them are made to operate with the MQTT protocol and to meet its specifications. The most famous brokers are Mosquitto which is an open-source written in C as a part of Eclipse Foundation and applicable for low powered devices because of being a very lightweight broker, RabbitMQ which is written in Erlang mainly to support AMQP protocol and MQTT protocol but it lacks some features of MQTT like QoS 2, HiveMQ is another famous MQTT broker written in Java with high and efficient performance and 100% compliance with MQTT protocol, and VerneMQ which is written in Erlang/OTP as a distributed MQTT message broker.

MQTT is implemented in different widespread applications such as Health care monitoring devices and sensors that rely on IoT technology [12], social media like Instagram, a Facebook messenger [13], energy monitoring in industrial applications [14], surveillance [15], smart farming and soil states monitoring [16], android application and smart homes[17].

II. MQTT CHALLENGES

Despite having many advantages, such as its lightweight, simplicity of implementation, deploying it in most of the life applications, and consuming lower power than other available protocols, MQTT has many open issues and faces some challenges that may affect its performance in critical applications. Some security issues that need to be solved to enhance the performance of MQTT as mentioned in [18], data transit attacks, scalable key management, and the overload resulting from TLS are the major security problems that some new researchers are concerned with.

In [19], some security issues were discussed and some mechanisms were presented that can help to enhance data encryption, authentication, and confidentiality between clients and brokers. It also proposed a Value-to-HMAC that can be used to ensure message disclosure only by its specified client. High latency and high bandwidth consumption for constrained applications may be considered as a critical open issue of

MQTT. As it relies on the TCP protocol, latency and bandwidth consumption are considered to be high because of the exchanged acknowledgments and using the triple handshake of TCP and QoS as mentioned in [20].

When comparing MQTT with Constrained Application Protocol (COAP), in the case of losses, the COAP protocol shows fewer delays than MQTT because of the TCP handshaking over heading that leads to more delays as results obtained in [21].

Another study to measure the performance of MQTT [22] was done using an NB-IoT system that provided simulation results that showed using TCP has a negative impact on the performance of the MQTT protocol when compared to the COAP protocol that uses UDP as a lightweight and cheap reliability confirmation process. This leads to the fact of adding TCP for reliability leads to less service availability than using UDP, especially when deployed with MQTT it affects the overall delay.

Most IoT applications and protocols are exposed to malicious hacking where a hacker can abuse a client or any IoT device to send fake messages only to keep the network busy and degrade the performance of the connected devices. Besides that, any sensor can be exposed to uncontrolled external factors that can affect the performance of the sensor itself, like sending the same message several times or accelerating the response and sending rate of a sensor. All that mentioned problems affect the communicating protocol and misbehave its performance, leading to more limitations that affect its performance.

MQTT-SN [23] is a new modified version of MQTT that mainly developed to operate with sensor networks was proposed to overcome the previously mentioned problem of TCP overhead work over UDP instead of TCP.

This paper contributes to proposing a new algorithm to help overcome some of the presented problems and limitations of IoT protocols, especially MQTT protocol that affects the communication delay of the overall traffic of the network. By proposing a new Back-off algorithm that organizes the communication between the broker and publishers to prevent overloading and, hence, broker failure due to unnecessary or fake messages. Besides proposing a second algorithm that can coordinate the publishing of messages between publishers depending on specified priority parameters that help critical messages to be delivered in time and reducing the latency of these messages.

III. RELATED WORK

Because of the huge growth in the number of IoT devices and applications, the number of messages generated from IoT devices and sensors has increased. This increase leads to great congestion and packet loss in some cases, resulting in a great increase in latency, besides requiring high processing power and a high amount of consumed bandwidth. So, the whole world tends to solve these limitations by introducing new layers of computing like edge, fog, and cloud computing [24], where, cloud computing offers renting only the required amount of resources where gathered data that needs further processing can be transmitted to this layer. Transmitting data to this layer is suitable for data that needs high processing. However, it can

affect sensitive data, especially real time data, and increase its latency.

The need for intermediate processing layer leads to the fog layer where it refers to moving computers with sufficient storage and processing capabilities near to the sources of data for further processing without the need of transferring data to the cloud layer that will reduce the latency caused by transferring data to the cloud layer. So, it decreased the amount of data needed to be transferred to the cloud layer.

Due to the processing of data near to data sources, responsiveness and throughput of applications will be increased as processing data in this layer will be faster than processing it in the cloud layer. The need for edge computing will be raised as this layer will allow processing of data to be transferred near to the edge of the network, which suits the most sensitive and real time data, such as data generated from healthcare devices and sensors. Because of this advancement, not all IoT application layer protocols can operate in these modern processing layers [25]. Only special protocols have the capability of transferring data between these layers. One of them is the MQTT protocol, which can operate on constrained devices and even with cloud processing servers because of its simplicity and flexibility. To cope with these new layers of processing, it has become critical to modify MQTT and add new features to its broker.

One of these MQTT enhancements was [26], where the authors proposed a new model for MQTT edge and fog communication. That model was called the multi-tier edge computing model, in which a broker was added in the fog layer besides the primary broker in the cloud layer, where users could communicate directly with the fog layer broker rather than communicate with the cloud broker. That led to reducing the overall latency. The simulation environment was created to test the proposed model as three levels of devices were created, which are IoT devices, fog instances with the introduced intermediate broker, and cloud components with the primary broker. The simulation results were compared with the original MQTT IoT-based broker and proved that the overall latency was decreased and performance outperformed the original model.

MQTT has many new features, and modern research is concerned with enhancement of this protocol not only to upgrade its performance in IoT but also to serve the edge and fog layers. [27] Proposed a novel authentication mechanism for ensuring data privacy and integrity where the authors presented security threats to the IoT layer and MQTT attacks. When a broker is installed on all edge hubs to use the MQTT protocol in edge computing, the authority's complexity grows, and the challenge of dealing with a large number of brokers develops. Generally, IoT devices transmit a certain message to maintain availability with the broker, and this operation might generate a bottleneck due to several brokers installed on the edge hub. As a result, a system is required to supervise brokers installed on all edge hubs and to exchange data between many edge systems without further affiliation with brokers by using cryptography calculations of RSA and AES to encrypt the payload in order to make the correspondence more secure.

Another new feature of MQTT was presented in [28], where integration between blockchain and IoT systems has been done and deployed in the edge layer to obtain the advantages of blockchain decentralization in securing the IoT systems using the MQTT protocol, which in turn will increase the overall performance and security of the MQTT protocol. To control the transmission of data, the authors utilized the MQTT protocol and a central edge server as a broker. The IoT network will send and receive data via a secure link provided by blockchain.

In the field of machine learning, the MQTT protocol has attracted a great deal of attention. Some research has been concerned with attacking MQTT to overcome its security limitations by using a random forest algorithm for detecting attacks, as in [29], and other research has been concerned with generating new datasets like [30] that can help models in training to detect more attacks on the MQTT protocol.

All of the mentioned new research and new features of MQTT were concerned with security and decreasing latency, with an overall increase in the performance of the MQTT protocol. This research, on the other hand, is concerned with reducing a network's overall traffic in the event of congestion, which can result in significant packet loss. The concept of the Back-off algorithm was introduced to the MQTT broker to decrease suspicious traffic and a new mechanism of assigning priority was proposed to filter and categorize received messages.

A. Back-off Algorithm in IoT

Exponential Back-off is a prominent algorithm mainly used in networks to efficiently separate the repeated retransmission of messages or data by a random delay time depending on the slot time to eliminate network congestion. This algorithm is the organizer of retransmitted packets in the CSMA/CD after a collision is detected as it identifies the waiting interval for collisional stations after collision depending on the number of collisions and the slot time. Each collide station picks a random integer that can be presented by k from the contention window to wait a period = $k * \text{slot time}$. If the collision occurs in for the same packet, the contention window will be doubled. For example, if the first collision occurs, a contention window will be between 0, 1 and each station choose a random integer of it and the probability of collision will be decreased to 50%. If a collision occurs again the contention window will be doubled and become {0, 1, 2, 3} and each station will choose a random integer then the probability of collision will be decreased to 25% and so on. The contention window is doubled for each collision and the waiting time increases exponentially.

Due to the great revolution in communication systems, wireless systems need new solutions that can control congestion and delay of messages. One of these new solutions was proposed in [31] as a new algorithm that is based on the concepts of the Back-off algorithm to help in improving the MAC-layer performance by queuing the packets based on their delay. This algorithm was evaluated in a dynamic wireless sensor network where the network consists of several mobile nodes by defining a new parameter called delay timer used for reducing the number of dropped packets. Based on this parameter, packets are queued and served with a minimum

delay timer first with a reduction in energy processing and a high delivery ratio of packets.

The Back-off algorithm also has a vital role in Wireless Body Area Networks, where [32] proposed a channel switching procedure by a rescheduling algorithm based on optimal Back-off time. By identifying the neighboring list, current channels can be switched to one of its neighboring lists in the case of performance degradation.

B. Priority Scheduling in IoT

Scheduling messages based on certain criteria is a severe issue in assigning tasks to CPUs, hence the IoT extended that concept to schedule tasks and received messages in a variety of IoT applications. Some applications use the ordinary contending priority algorithms such as First Come First Served, Round Robin or Shortest Job First or any of other primary scheduling algorithms. Other applications imposed a modified scheme of scheduling based on the procedure applied to that application or technology.

In the transportation field [33], an application was designed to overcome the problem of traffic congestion using the IoT environment by proposing a traffic monitoring system that in turn controls the passing of vehicles depending on an assigned level of priority to each lane where high priority passing vehicles lane is assigned to the lanes with high traffic.

Smart homes have gained great attention for achieving priority scheduling among their huge number of deployed sensors and applications. The author in [34] introduced a new technique for evaluating contextual priorities that is concerned with non-functional requirements based on the end user's preferences, and context awareness. According to the current context, a context-aware system can adapt itself with the aid of a developed web platform that asks users to classify their preferences then users validate the assigned priority scheduling. As a result, users were satisfied with the tested scenarios that coped with their choice of contextual factors.

For healthcare, [35] has classified received data from healthcare sensors into two categories as emerging data that has a higher priority level or vital data that has a lower priority level to save the battery life of wearable devices as much as possible. An efficient routing protocol based on these two categories of priority classification was proposed to deliver high-priority data with direct communication. In contrast, low priority data will be delivered using multi-hop communication.

Priority scheduling is one of the big open issues of the MQTT protocol because it does not have any priority algorithm of its common brokers. The author in [36] proposed a priority algorithm in which messages were classified into three categories. Based on the category, messages were classified into three queues as normal or critical or urgent queues inside the broker itself. Messages in the urgent queue have the highest priority to be served first, which causes the latency of these messages to become smaller and the message loss rate is decreased. However, this algorithm was concerned only with the latency and the loss rate of urgent messages and ignored the latency of the overall network and the consumed memory assigned to each queue.

As mentioned before, MQTT has no priority algorithms for message scheduling. Even the proposed [36] algorithm is concerned only with the urgent messages, not the overall performance of the protocol. Besides, the priority level was assigned by the client itself that allows any message to be urgent without any constraints or predetermined specifications.

IV. INTEGRATED BACK-OFF WITH PRIORITY SCHEDULING ALGORITHM

A. Proposed Back-off Algorithm

The proposed exponential Back-off algorithm aims to reduce network congestion by slowing down the transmission rate of suspicious devices. For each client connected to the broker, the broker will record the arrival time of the first message then repeat that for the next N messages. The time interval length between every two consecutive messages will be calculated to obtain an average frequent rate for each client. After a chosen N messages, the broker will have a saved average of the publishing frequent rate for each client. When the publisher asks the broker to send a new message, the broker compares the current publishing frequent rate with the initial average frequent rate of that publisher. If the current rate is higher than the initial rate, then that publisher may have a problem or be under attack. So the broker activates an exponential Back-off algorithm to hold on receiving from that client until a specified waiting time depending on a calculated delay factor based on the current frequent rate of that publisher. The exponential delay continues with a publisher whenever the current publishing rate became until the publisher reaches its original frequent publishing rate. That delay will reduce communication between these publishers and reduce network overload. Fig. 1 shows the flow chart of the proposed Back-off algorithm steps.

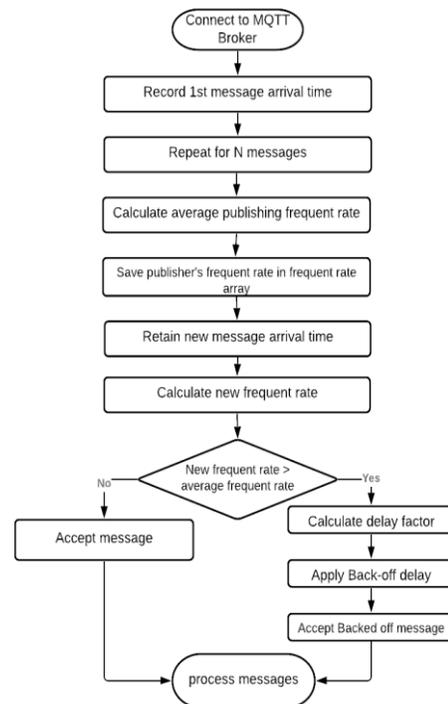


Fig. 1. Flowchart of Proposed Back-off Algorithm Steps.

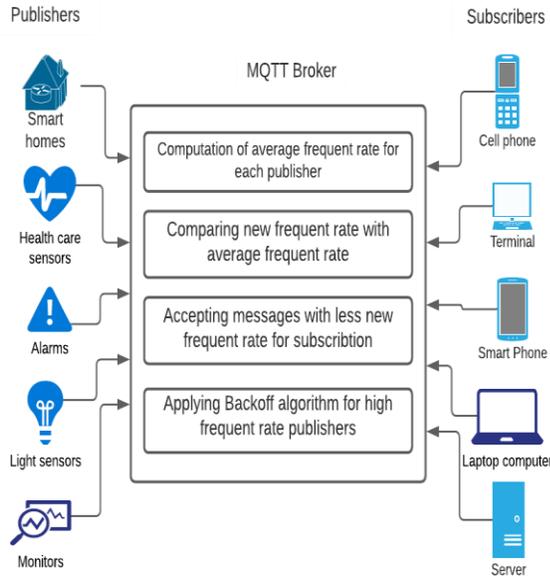


Fig. 2. The Proposed MQTT Back-off based Broker Structure.

The proposed Back-off algorithm can be deployed into the Mosquitto broker for the MQTT protocol to test the performance of the network under the new Back-off algorithm. The Mosquitto broker, the most common broker for the MQTT protocol was chosen because of its simplicity and its lightweight as it is written in C language. Fig. 2 shows the proposed MQTT Back-off based broker structure as it is modified according to the proposed Back-off algorithm. The detailed steps of the proposed Back-off algorithm were presented sequentially in Algorithm1 under the name of enhanced Back-off algorithm as it differs from the original CSMA/CD Back-off algorithm in the deployed layer, function, and execution.

Algorithm1: Proposed Back-off algorithm.

INPUT: Messages received from publisher $M_1, M_2, M_3, \dots, M_K$, Number of messages selected for calculating average frequent rate N .

OUTPUT: Delay factor D_f , Average frequent rate FR_{avg} , New frequent rate FR_{new}

```

00 For each publisher  $P_j$ 
01 For  $M_{i=1}$  to  $M_{i=N}$ 
02 Save  $T_{Mi}$ 
03 Calculate Time interval  $I_{(Mi, Mi+1)} = T_{M(i+1)} - T_{Mi}$ 
04 End for
05  $FR_{avg} = 1 / [ \sum_{i=1}^N I_{(Mi, Mi+1)} / (N-1) ]$ 
06 Save  $FR_{avg}$  in Array  $FR_{P_j} [ ]$ 
07 End for
08 For each new message  $i = N + 1$  to  $i = k$ 
09  $FR_{new} = (1 / I_{(Mi, Mi+1)})$ 
10 If  $FR_{new} > FR_{avg}$ 
11 Calculate  $D_f$  for the current message  $M_i$ 
12 Set waiting time for  $M_i = D_f$ 
13 Accept Backed off message for subscribing
14 Else
15 Accept message for subscribing
16 process accepted messages
17 End If
18 Return  $D_f, FR_{avg}, FR_{new}$ 

```

B. Back-off Delay Factor Calculations

The Back-off delay factor depends on the current frequent rate as it is an exponential function of the current frequent rate where DF represents the Back-off delay factor. Whenever the current frequent rate increases, DF for this publisher will increase until the publishing rate degrades to the original frequent rate. Hence, the Back-off delay factor reaches its threshold or its maximum value then terminates the Back-off algorithm and begins again if the new frequent rate exceeds the average frequent rate.

Suppose a publisher P sends a number of messages K and M represents a sequence of published messages $[M_1, M_2, M_3, \dots, M_K]$. Each message arrives at Time T where T_{Mi} is the arrival time saved for message M_i . For the first N messages, an interval of time I between every two consecutive messages was calculated in seconds to obtain the average frequent rate FR_{avg} of publisher P where I can be calculated from (1).

$$I_{M_i, (M_{i+1})} = T_{M(i+1)} - T_{M_i} \tag{1}$$

Let $N = 4$, where the number of messages selected by the user to calculate the average frequent rate for each publisher. Then three intervals of time I_1, I_2, I_3, I_4 will be calculated to get the average frequent rate in messages per one second from (2).

$$FR_{avg} = 1 / ((\sum_{i=1}^N I_{M_i, (M_{i+1})}) / (N - 1)) \tag{2}$$

After calculating the average frequent rate, new messages from P will be received. To calculate its current frequent rate, let FR_{new} is the new current rate that can be calculated from (3) where $I_{M_N, (M_{N+1})} = T_{(M(i=N+1))} - T_{(M(i=N))}$ that represents the new time interval between the new message M_{N+1} and the previous message M_N .

$$FR_{new} = (1 / I_{M_N, (M_{N+1})}) \tag{3}$$

After calculating FR_{new} for the new message, it will be compared with FR_{avg} . If FR_{new} exceeds FR_{avg} then a delay factor D_f can be calculated as an exponential function of FR_{new} in (4) will be added to that publisher's message.

$$D_f = e^{(FR_{new})} \tag{4}$$

For example, if publisher P sends 5 messages per 30 seconds at a regular rate, by using the mentioned equations FR_{avg} will be 0.16 messages per second. If the publisher continued with the same rate or less than that rate, the Back-off algorithm will be inactive. If $FR_{new} > FR_{avg}$, the Back-off delay factor will be calculated and applied to the message in turn.

Table I shows the effect of changing frequent rate on the delay factor with different increased frequent rates for the same publisher until reaching the maximum value of delay. Fig. 3 shows the exponential increase of delay factor based on the new calculated frequent rate until reaching the maximum allowed delay value.

C. Proposed Priority Scheduling Algorithm

Previously mentioned that MQTT protocol has no methodology for priority scheduling messages as any message received will be forward directly irrespective of its priority level. So, if 2 messages arrived at the same time which one will

be processed first, this decision never exists in the MQTT broker as there is no priority scheduling.

Based on the calculated average frequent rate recorded previously in the broker of the MQTT protocol, K number of publishers can be classified into levels based on the average frequent rate as the higher frequent rate is assigned the lower priority level donated by PRL as mentioned in (5) and the lower frequent rate is assigned a higher priority level donated by PRH as mentioned in (6) where $P_{i \text{ FRavg}}$ is the average frequent rate for publisher P_j .

$$PRL = \text{MIN} \{P_{1 \text{ FRavg}}, P_{2 \text{ FRavg}}, P_{3 \text{ FRavg}}, \dots, P_{K \text{ FRavg}}\} \quad (5)$$

$$PRH = \text{MAX} \{P_{1 \text{ FRavg}}, P_{2 \text{ FRavg}}, P_{3 \text{ FRavg}}, \dots, P_{K \text{ FRavg}}\} \quad (6)$$

For example, a sensor that sends one message every 24 hours has a higher priority than a sensor that sends a message every one second. As in the case of congestion, the first sensor's data may be lost and cannot be retrieved or resent unless the next 24 hours be over. Depending on the factor of original publishing frequent rate, the arrived messages are arranged in a queue for processing based on the assigned priority level.

This algorithm can be implemented with the Back-off algorithm to organize the overall network communication, where a network administrator can control the activation of this algorithm depending on the nature of connected devices, as the main goal of this algorithm is to assign priority to the connected devices from the broker's side, not from the client's side, where any hacker cannot assign himself a high priority.

TABLE I. DELAY FACTOR VARIATION ACCORDING TO INCREASING IN NEW FREQUENT RATE

Number of messages per seconds	$I_{M_i, (M_{i+1})}$	FR_{new}	D_f
10 messages/30 seconds	$I_1 = 3$ seconds	0.3	1.3 seconds
20 messages/30 seconds	$I_2 = 1.5$ seconds	0.6	1.82 seconds
30 messages/30 seconds	$I_3 = 1$ seconds	1	2.7 seconds
40 messages/30 seconds	$I_4 = 0.75$ seconds	1.3	3.66 seconds
50 messages/30 seconds	$I_5 = 0.6$ seconds	1.6	4.95 seconds
60 messages/30 seconds	$I_6 = 0.5$ seconds	2	7.38 seconds

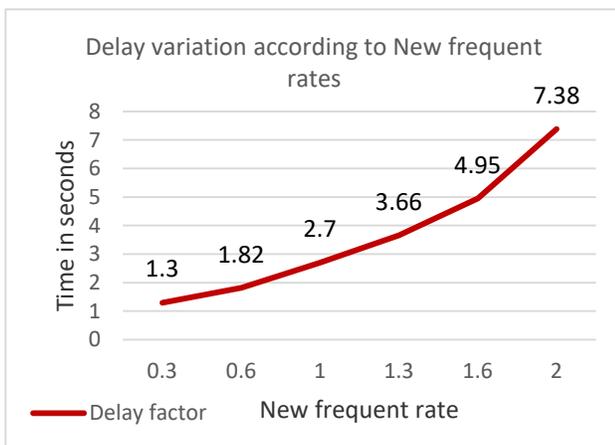


Fig. 3. The Exponential Growth of Delay Factor According to Increased New Frequent Rate.

Algorithm2: Priority scheduling algorithm based on frequent rate

INPUT: Average frequent rate Array for publishers $\{P_1, P_2, P_3 \dots P_x\}$ $FR_{P_j} []$

OUTPUT: priority level of publishers PR_{P_j}

```

00 Recall  $FR_{P_j} [ ]$  from Back-off algorithm
01 For each publisher  $p_j$ 
02 Get Max of  $FR_{P_j} [ ]$ 
03 Get Min of  $FR_{P_j} [ ]$ 
04 If  $P_j \text{ FR}_{avg} > \text{Max of all items of Array } FR_{P_j} [ ]$ 
05 Set priority level of  $P_j = PR_L$ 
06 Set location of  $P_j \text{ FR}_{avg} = \text{last item of Array } FR_{P_j} [ ]$ 
07 Else if  $P_j \text{ FR}_{avg} < \text{Min of all items of Array } FR_{P_j} [ ]$ 
08 Set  $PR_{P_j} = PR_H$ 
09 Set location of  $P_j \text{ FR}_{avg} = \text{1st item of Array } FR_{P_j} [ ]$ 
10 Else
11 Sort Array  $FR_{P_j} [ ]$ 
12 Set  $PR_{P_j} = \text{location of } P_j \text{ FR}_{avg} \text{ in Array } FR_{P_j} [ ]$ 
13 End if
14 Increment of  $j$ 
15 Return  $PR_{P_j}$ 

```

V. EVALUATION AND RESULTS

The open source Mosquitto version 1.6.12 broker was chosen for evaluation and implementation of the new proposed algorithm as it offers free, simple, and open-source libraries written in C language that helped in modifying the broker source to deploy the new algorithm in it. The Mosquitto Broker was implemented on windows 10 pro, Intel® core™ i7 machine with 16 GB RAM and 64-bit operating system. With the aid of open-source libraries supported by the Eclipse Paho project, the publishers and subscribers were implemented on the same machine.

Simulation experiments were done on a variable number of publishers and subscribers in each experiment. Starting from only 2 publishers reaching 100 publishers, the performance metrics were measured for each experiment respectively. The Wireshark which is a network tracer program was used to capture network traffic and consumed bandwidth. Consumed CPU and RAM were measured and captured on the same workstation using the jconsole application.

A. Network Traffic Load

The most important metric to be traced and measured was the network traffic, especially from the publisher's side, which is uplink traffic, because it is the main issue that this paper is concerned with to eliminate suspicious and undesired traffic from the publisher side that affects the performance of the MQTT broker. Fig. 4 illustrates the uplink traffic for discrete experiments using individual 2, 5, 10, 20, 30, 50, 100 publishers. Each experiment was traced for 10 minutes resulting in the number of bytes transferred in this specified period. For the Back-off MQTT broker, publishers were set up to publish the first 4 messages regularly at constant frequent rates then random intervals of time between messages were inserted to create suspicious publishers and force the Back-off algorithm to

be activated. Compared with the original MQTT broker, the occupied traffic was decreased in the Back-off broker by filtering out the fast rate messages from suspicious publishers. As shown in Fig. 4 for the original MQTT broker, whenever the number of publishers becomes larger the load on the broker becomes heavier and the network becomes exposed to congestion. In contrast with Back-off MQTT, the network is not exposed to congestion and still can serve a larger number of publishers than the original MQTT broker.

According to Fig. 4, as the load becomes heavier on the broker due to the increasing number of connected publishers, the Back-off broker can manage traffic and accept a higher number of publishers. However, the original MQTT broker suffers from congestion and a high load of unwanted messages that raise the network traffic. Taking 30 publishers as a use case experiment for evaluating the new algorithm, the MQTT broker consumed 29400 bytes in 10 minutes, whereas Back-off MQTT consumed 24700 bytes in 10 minutes.

B. CPU Load

The second metric to be measured is the used CPU during four whole minutes. It is expected that the processing power for

calculating the Back-off algorithm will be increased because of the sophisticated calculation of temporal frequent rate for each new message. However, the simulation results in Fig. 4 show that a slight increase in processing power can be equal to less than 0.75 % percent, which emphasizes that the Back-off broker can be implemented in IoT applications and resource-constrained devices. Fig. 5 shows that the maximum consumed processing power for the original MQTT broker was 2.53% whereas the Back-off MQTT broker consumed 3.53% where the difference is less than 1% that IoT devices can handle.

C. Consumed RAM

The third metric to be measured is the consumed RAM for the Back-off MQTT broker and the original MQTT broker. Fig. 6 compares the consumed RAM for 30 connected publishers in both cases with a table that shows the exact value of RAM consumption. The figure shows that the consumed RAM is approximately equal in both cases despite using the calculations of delay factors and saving the arrival time of N messages to calculate and save frequent rates. This proves that the Back-off broker utilizes small RAM like the original broker and can be applied to IoT devices easily.

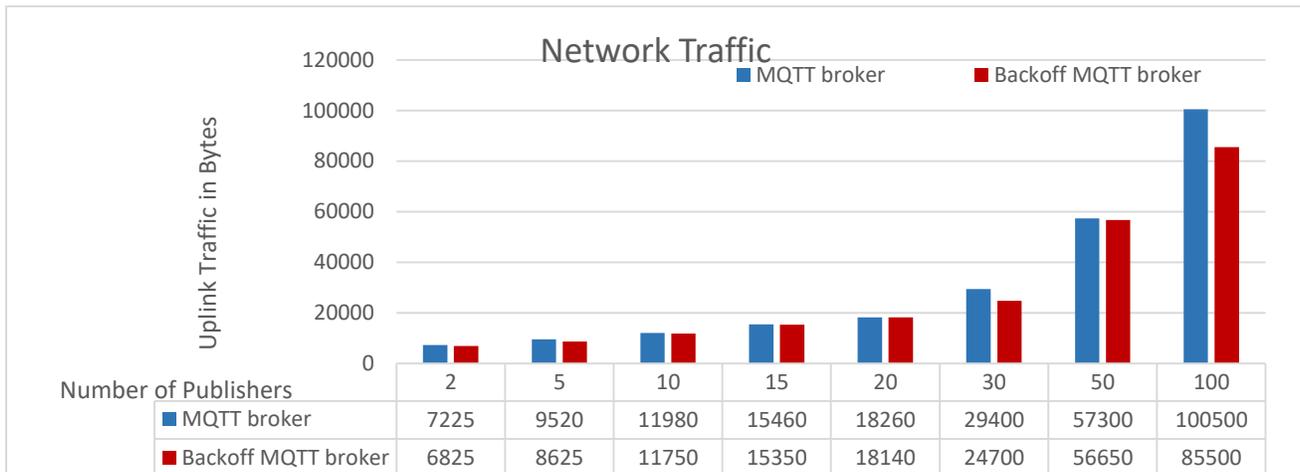


Fig. 4. Uplink Traffic for MQTT broker and Back-off MQTT Broker.

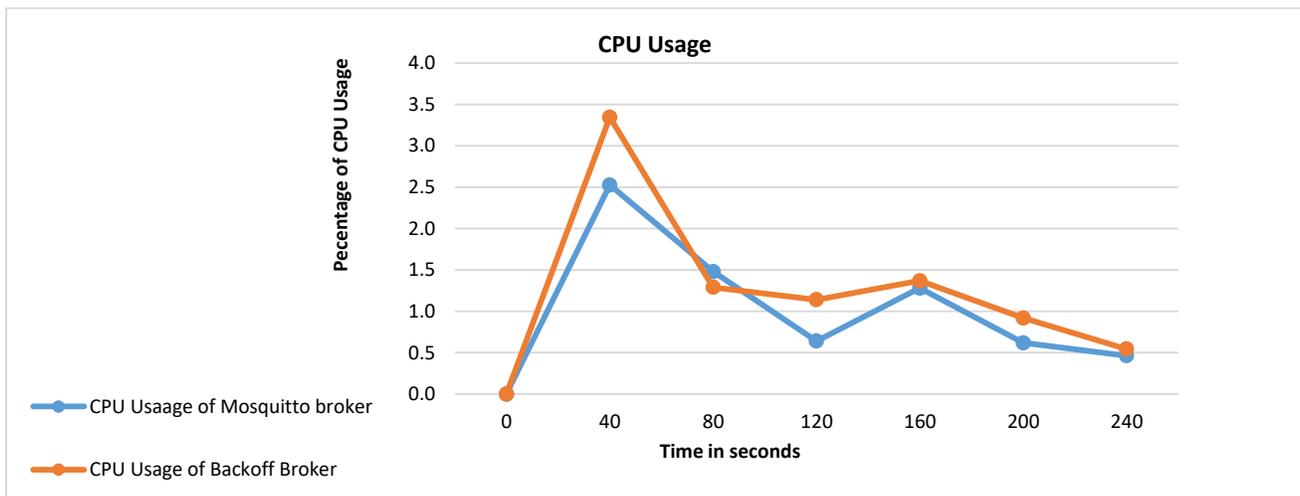


Fig. 5. CPU Consumption for MQTT Broker and Back-off based Broker.

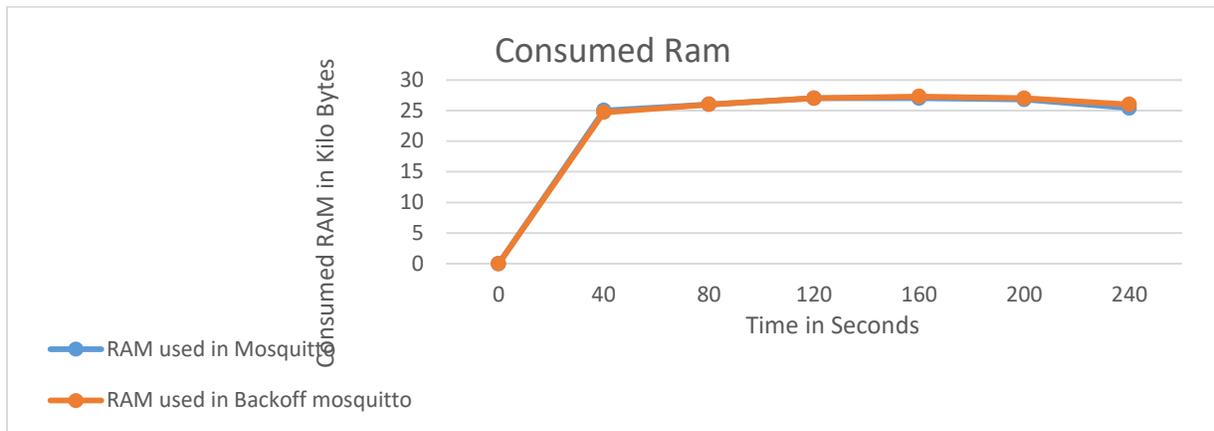


Fig. 6. RAM Consumption for MQTT Broker and Back-off Broker.



Fig. 7. The Latency Variation for High Priority Publisher in MQTT Broker and Back-off Broker.

D. Latency

The latency was the most important metric to evaluate the proposed priority scheduling mechanism as the high-priority publishers should have fewer latency measurements. The experiment was done to measure the latency of messages for one publisher with a high priority level in the MQTT broker and was repeated for the Back-off MQTT broker. Fig. 7 shows that the same publisher was exposed to less latency in Back-off Mosquitto with priority scheduling than the latency measured by the original MQTT broker. As shown, the maximum latency that was recorded for the Back-off broker was equal to the minimum latency recorded by the original broker. As a result, high-priority publishers can publish with less latency than other low-priority publishers, as they have the priority of publishing their message immediately.

VI. CONCLUSION

This research paper proposed a new Back-off algorithm that was designed to eliminate the effect of network and traffic congestion in IoT protocols. The problem was driven by suspicious clients or clients with undetected errors that affect the performance of the network. The MQTT protocol was chosen to be tested and evaluated under the new Back-off

algorithm. Some performance metrics such as uplink traffic showed better traffic performance and less congestion than the original broker. Also, the CPU and RAM consumption were measured to record approximate results as the original broker that proved the ability to deploy that algorithm in resource-constrained devices. Another algorithm for priority scheduling was designed specially to cope with the new Back-off algorithm and the MQTT broker as it does not possess any priority scheduling algorithms. The experimental results recorded less latency for the high-priority publisher in the Back-off broker than the original broker.

Generally, the proposed Back-off and priority scheduling algorithms showed an acceptable result for RAM and CPU consumption with a minimum traffic load that leads to the ability to be employed in constrained resource devices.

VII. FUTURE WORK

The MQTT protocol was chosen to be a use case for evaluating the new algorithm because of its simplicity and its prevalence. However, the new proposed algorithm can be employed in another IoT protocol to increase its performance. AMQP has a similar structure to the MQTT protocol and it relies on distributing messages in queues that can help in

deploying the priority based on frequent rate algorithm for this protocol easily. Besides AMQP, the COAP protocol was designed for resource-constrained devices that can afford the implementation of the new proposed algorithm with higher performance metrics.

REFERENCES

- [1] Arefin, ASM Shamsul, KM Talha Nahiyani, and Mamun Rabbani. "The basics of healthcare IoT: Data acquisition, medical devices, instrumentations and measurements." *A Handbook of Internet of Things in Biomedical and Cyber Physical System*. Springer, Cham, 2020. 1-37.
- [2] Farooq, Muhammad Shoaib, et al. "Role of IoT technology in agriculture: A systematic literature review." *Electronics* 9.2 (2020): 319.
- [3] Zaidan, A. A., and B. B. Zaidan. "A review on intelligent process for smart home applications based on IoT: coherent taxonomy, motivation, open challenges, and recommendations." *Artificial Intelligence Review* 53.1 (2020): 141-165.
- [4] Sokullu, Radosveta, Mustafa Alper Akkaş, and Eren Demir. "IoT supported smart home for the elderly." *Internet of Things* 11 (2020): 100239.
- [5] Kumar, Pankaj, and Lokesh Chouhan. "A secure authentication scheme for IoT application in smart home." *Peer-To-Peer Networking And Applications* 14.1 (2021): 420-438.
- [6] Ramschie, Ali AS, Johan F. Makal, and Veny V. Ponggawa. "Implementation of the IoT Concept in Air Conditioning Control System Base on Android." *International Journal of Computer Applications* 975: 8887.
- [7] Sarangi, Manisha, et al. "IoT aware automatic smart parking system for smart city." *Cognitive Informatics and Soft Computing*. Springer, Singapore, 2020. 469-481.
- [8] Pandya, Hetal B., and Tushar A. Champaneria. "Notice of Removal: Internet of things: Survey and case studies." 2015 international conference on electrical, electronics, signals, communication and optimization (EESCO). IEEE, 2015.
- [9] Standard, O. A. S. I. S. "MQTT version 3.1. 1." URL <http://docs.oasis-open.org/mqtt/mqtt/v3.1.1/> (2014).
- [10] Soni, Dipa, and Ashwin Makwana. "A survey on mqtt: a protocol of internet of things (iot)." *International Conference On Telecommunication, Power Analysis And Computing Techniques (ICTPACT-2017)*. Vol. 20. 2017.
- [11] Archana, E., et al. "A formal modeling approach for QOS in MQTT protocol." *Data Communication and Networks*. Springer, Singapore, 2020. 39-57.
- [12] Kadhim, Kadhim Takleef, et al. "Monitor human vital signs based on IoT technology using MQTT protocol." *AIP Conference Proceedings*. Vol. 2290. No. 1. AIP Publishing LLC, 2020.
- [13] Detti, Andrea, Ludovico Funari, and Nicola Blefari-Melazzi. "Sub-linear scalability of mqtt clusters in topic-based publish-subscribe applications." *IEEE Transactions on Network and Service Management* 17.3 (2020): 1954-1968.
- [14] Ramelan, A., et al. "IoT Based Building Energy Monitoring and Controlling System Using LoRa Modulation and MQTT Protocol." *IOP Conference Series: Materials Science and Engineering*. Vol. 1096. No. 1. IOP Publishing, 2021.
- [15] Norrdine, Abdelmoumen, et al. "MQTT-Based Surveillance System of IoT Using UWB Real Time Location System." 2020 International Conferences on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData) and IEEE Congress on Cybermatics (Cybermatics). IEEE, 2020.
- [16] Mandal, Santanu, Imran Ali, and Sujoy Saha. "IoT in Agriculture: Smart Farming Using MQTT Protocol Through Cost-Effective Heterogeneous Sensors." *Proceedings of International Conference on Frontiers in Computing and Systems*. Springer, Singapore, 2021.
- [17] Eleyan, Amna, and Joshua Fallon. "IoT-based Home Automation Using Android Application." 2020 International Symposium on Networks, Computers and Communications (ISNCC). IEEE, 2020.
- [18] Frustaci, Mario, et al. "Evaluating critical security issues of the IoT world: Present and future challenges." *IEEE Internet of things journal* 5.4 (2017): 2483-2495.
- [19] Dinculeană, Dan, and Xiaochun Cheng. "Vulnerabilities and limitations of MQTT protocol used between IoT devices." *Applied Sciences* 9.5 (2019): 848.
- [20] Hamdani, Samer, and Hassan Sbeyti. "A Comparative study of CoAP and MQTT communication protocols." 2019 7th International Symposium on Digital Forensics and Security (ISDFS). IEEE, 2019.
- [21] Prabhu Kumar, P. C., and G. Geetha. "Web - cloud architecture levels and optimized MQTT and COAP protocol suites for web of things." *Concurrency and Computation: Practice and Experience* 31.12 (2019): e4867.
- [22] Larmo, Anna, Antti Ratilainen, and Juha Saarinen. "Impact of coap and mqtt on nb-iot system performance." *Sensors* 19.1 (2019): 7.
- [23] Stanford-Clark, Andy, and Hong Linh Truong. "Mqtt for sensor networks (mqtt-sn) protocol specification." *International business machines (IBM) Corporation version 1.2* (2013).
- [24] Bierzynski, Kay, Antonio Escobar, and Matthias Eberl. "Cloud, fog and edge: Cooperation for the future?." 2017 Second International Conference on Fog and Mobile Edge Computing (FMEC). IEEE, 2017.
- [25] Dizdarević, Jasenka, et al. "A survey of communication protocols for internet of things and related challenges of fog and cloud computing integration." *ACM Computing Surveys (CSUR)* 51.6 (2019): 1-29.
- [26] Veeramanikandan, M., and Suresh Sankaranarayanan. "Publish/subscribe based multi-tier edge computational model in Internet of Things for latency reduction." *Journal of parallel and distributed computing* 127 (2019): 18-27.
- [27] Pandya, Sharnil, et al. "A Novel Multicast Secure MQTT Messaging Protocol Framework for IoT-Related Issues." *Proceedings of Second International Conference on Computing, Communications, and Cyber-Security*. Springer, Singapore, 2021.
- [28] Abdullah, Maha A., and Omar H. Alhazmi. "A Triumvirate Approach of Blockchain MQTT and Edge Computing Toward Efficient and Secure IoT." *Proceedings of International Conference on Communication and Computational Technologies*. Springer, Singapore, 2021.
- [29] Chunduri, Naga Venkata Hrushikesh, and Ashok Kumar Mohan. "A Forensic Analysis on the Availability of MQTT Network Traffic." *International Symposium on Security in Computing and Communication*. Springer, Singapore, 2020.
- [30] Vaccari, Ivan, et al. "MQTTset, a new dataset for machine learning techniques on MQTT." *Sensors* 20.22 (2020): 6578.
- [31] Babu, Palamakula Ramesh, et al. "An enhanced virtual backoff algorithm for wireless sensor networks." *International Journal of Wireless and Mobile Computing* 13.3 (2017): 179-187.
- [32] Xie, Zhijun, et al. "An Optimal Backoff Time-Based Internetwork Interference Mitigation Method in Wireless Body Area Network." *Journal of Sensors* 2020 (2020).
- [33] Nagmode, Varsha Sahadev, and S. M. Rajbhoj. "An IoT platform for vehicle traffic monitoring system and controlling system based on priority." 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA). IEEE, 2017.
- [34] Serral, Estefanía, et al. "Contextual requirements prioritization and its application to smart homes." *European conference on ambient intelligence*. Springer, Cham, 2017.
- [35] Bahattab, Abdullah Ali, Abdelbasset Trad, and Habib Youssef. "PEERP: An Priority-Based Energy-Efficient Routing Protocol for Reliable Data Transmission in Healthcare using the IoT." *Procedia Computer Science* 175 (2020): 373-378.
- [36] Kim, Yong-Seong, et al. "Message queue telemetry transport broker with priority support for emergency events in Internet of Things." *Sensors and Materials* 30.8 (2018): 1715-1721.

Examining User Experience of Moodle e-Learning System

Layla Hasan

School of Computing, Faculty of Engineering
Universiti Teknologi Malaysia, Johor, Malaysia

Abstract—This research investigates the user experience (UX) of the Moodle e-learning system employed at one university in Malaysia from students' perspectives. Comprehensive user experience (UX) criteria were suggested, which was adopted from two reliable criteria, to evaluate the user experience (UX) of the e-learning system. The suggested comprehensive user experience (UX) criteria consist of 8 categories and 29 corresponding sub-categories; these can be used to evaluate teaching and learning, usability, and hedonic aspects of an e-learning system. Semi-structured interviews and questionnaires were employed based on the suggested user experience (UX) criteria to collect qualitative and quantitative data regarding users' experience (UX) of the tested e-learning system. The results showed that the e-learning system had positive user experience (UX) in general from the students' perspectives. The results also showed that the students were satisfied with most of the metrics related to teaching and learning, usability and hedonic. However, the students identified some challenges they faced while interacting with the e-learning system which could be improved in order to improve their user experience (UX) and gain more benefits from a good user experience (UX) e-learning system.

Keywords—User Experience (UX); e-learning system; Moodle; usability; learning management system

I. INTRODUCTION

The importance of e-learning is well recognized globally due to the continuous advancement in information technology and the rise of Internet adoption worldwide. The COVID-19 pandemic has increased the importance of e-learning as it has facilitated education in proceeding worldwide during the lockdown [1]. e-Learning is defined as: "Education that uses computerized communication systems as an environment for communication, exchange of information and interaction between students and instructors" [2]. The e-learning market is growing rapidly worldwide; it is expected that it will reach \$336.98 billion by 2026 [3].

e-Learning is conducted based on learning management systems which are related to software systems that support the management of educational courses, either in the traditional face-to-face classroom courses or in blended or distance education [4, 5]. The use of learning management systems improves the quality of teaching, facilitates access to educational materials, and supports synchronous and asynchronous interactions between staff and students [6].

Learning management systems can be categorized in terms of their fees into: commercial software systems which have high license fees (such as Blackboard), or free, open-source

software systems (such as Moodle) [7]. Moodle is one of the most common learning management systems that is employed worldwide in academic institutions due to its robustness, security and affordability [8]. The Moodle e-learning system provides various functions and tools that lecturers can employ to enrich and support the learning experience. These include: uploading instructional materials; displaying marks and feedback; conducting online quizzes and tests; supporting communications using messages; supporting group chats and online meetings; uploading advertisements and news; and sending alerts to students as a reminder to submit materials [9].

As the employment of e-learning management systems increases globally, and since most students depend on them in their learning processes, it is important to ensure that these systems are accepted, understood and used properly by the students. One of the ways to increase the acceptance and usage of these systems is to ensure that they are free from user experience (UX) and usability problems [6]. The success of e-learning is highly dependent on the users' experience and perceptions towards such systems [10].

The user experience (UX) can be defined as: "A person's perceptions and responses resulting from the use and/or anticipated use of a product, system or service. It includes all the user's emotions, beliefs, preferences, perceptions, physical and psychological responses, behaviours and accomplishments that occur before, during and after use" [11]. However, usability is defined as related to "the extent to which a system, product or service can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [12]. Alternatively, Maslov *et al.* [10] provided a definition of the UX of e-learning system as: "inherently a fuzzy, multi-faceted, context-dependent and dynamic concept covering all aspects how end-users experience, behave, perceive, feel and think about an e-learning system and how they reflect on the use, anticipation of the use and use it in order to attain hedonic and/or functional value of e-learning".

It is agreed that usability can be used to evaluate aspects of user experience [11]. According to Bevan [13], usability employs quantitative methods to evaluate the use of an interface objectively and pragmatically with the goal of optimizing users' performance. The UX, however, is more subjective and hedonic and has the goal of optimizing users' satisfaction by achieving both pragmatic and hedonic goals [13]. Hassenzahl *et al.* [14] also describes the two types of aspect which the UX considers. These are related to:

pragmatic aspects (e.g., traditional usability features); and hedonic aspects (e.g., emotional responses).

UX and usability are critical quality factors in e-learning systems and the learning process [15]. A good UX e-learning system means that the system is usable, pleasurable, satisfactory, and attractive to the learners [14, 16]. It is important to ensure that the e-learning system provides positive UX to the learners as UX affects users' acceptance, understanding, efficiency and satisfaction while using the system [6]. This will therefore facilitate and enrich the learning process.

The Moodle e-learning system is used and customized by its local experts for each academic institution based on the institution's local context due to a general lack of UX and usability experts. This often results in an instance of Moodle which has usability and UX problems [6]. The literature showed that there are many research studies which have evaluated the usability of Moodle learning management systems employed in various academic institutions and the results of these studies have shown several usability problems [for example, 7, 17-21]. However, user experience (UX) is still a novel research area; there is lack of a specific UX technique or UX criteria that could be used to evaluate the UX of e-learning systems and there is also a lack of research which investigates the user experience (UX) of Moodle e-learning system from the perspectives of students [6].

The aim of this research is to examine the user experience (UX) of the Moodle e-learning system at the University of Technology Malaysia (UTM) from the perspectives of students. In order to examine the UX, comprehensive criteria were developed based on two reliable criteria [5, 22]. The results of this research uncover the current UX of the Moodle e-learning system used by the University of Technology Malaysia from the perspectives of the students and presents both the current challenges and suggested improvements to the e-learning system. The proposed approach (suggested criteria) employed in this research can be used to: evaluate comprehensively the user experience (UX) of an e-learning system, and increase the acceptance, satisfaction, efficiency and usage of e-learning systems from students' perspectives. Also, the results of this research could contribute towards increasing research and awareness on user experience (UX) of e-learning systems.

This research is divided into six sections. Section 2 presents earlier research which has evaluated the UX of e-learning systems. The methodology is presented in Section 3. Section 4 presents the results while Section 5 presents the discussion. Finally, in Section 6, the conclusion is presented.

II. LITERATURE REVIEW

Researchers indicated that the concept of UX is subjective and holistic and therefore there are no specific UX metrics to evaluate UX of e-learning systems [6, 15, 23, 24]. Some researchers have suggested models including UX metrics to evaluate UX for e-learning systems, while others have used existing proposed metrics to evaluate such systems. For example, Topolewski *et al.* [22] proposed a UX model which describes user experience in terms of 21 properties related to

five categories that influence users' intention to use e-learning. The model was tested empirically by designing a survey which consisted of the identified UX properties. The survey was given to students who used a specific mobile application (Jaxber app) to evaluate their UX experience with this e-learning system. The results proved the reliability and validity of the proposed model; some properties were deleted so that the model finally consisted of 18 UX properties which can be used to evaluate the UX of e-learning systems.

Maslov *et al.* [10] also explored user experience of the Moodle learning management system from the perspectives of students at one university using semi-structured interviews and a survey, which was designed based on the UX model of Topolewski *et al.* [22]. The results showed that Moodle was perceived as a useful and productive platform for learning because it provided all relevant information, such as course information and course materials, in the same place. It also supported the sending of assignments and managing the percentage of the course's completion. The results showed also that most of the students considered Moodle as an easy-to-use platform. However, for other students, Moodle was perceived as a hard platform to navigate and use but one which became easier to use over time and experience. Furthermore, the results indicated that Moodle was meaningful and engaging, although this depended on the teacher, the course content and how simply it was structured. The challenges the students faced on Moodle during their interactions with it included: slow loading of documents in a browser window; lack of support for group work; it was not entertaining or novel, and the interface was not attractive; technical issues existed (for example, server downtime, website inaccessibility, login issues); courses were sometimes badly structured; weak communication; lack of customization of the front page; and the lack of a mobile application.

Alternatively, Mtebe [6] identified the factors that influenced the UX of Moodle e-learning systems implemented in two universities in Tanzania using a questionnaire consisting of Nielsen heuristics which focused on usability; didactic metrics, which focused on teaching and learning; and hedonic metrics, consisting of three criteria (stimulation, identification, and evocation) adopted from three resources [5, 25, 26]. Focus groups were then used for further discussions with the students. The results showed that the e-learning systems of both universities had a large number of usability and UX problems. Examples of usability problems included: lack of help and documentation features; and inconsistency in colors and layouts (the organization of instructional materials differed from one course to another). The results also showed also that the e-learning systems had several UX problems related to instructor skills and usage although these were not associated directly with the UX of the system being used. These included: the systems had outdated instructional materials while some courses did not have sufficient materials of this type; many instructors were unable to use the e-learning system effectively and therefore ended up using only very few features of the systems. Finally, the results showed that the adoption and use of e-learning systems evoked, for students, positive feelings and memories of their learning activities; the students also perceived the use of the e-learning

systems communicated advantageous identities to other students and their instructors. However, the students were neutral as to whether the use of e-learning systems was interesting or had exciting functionalities, content, presentation and interaction style.

Furthermore, Nakamura et al. [16] used two UX evaluation techniques (UEQ and IEAM) to evaluate the Edmodo learning management system from the perspective of 34 students at the Federal University of Amazonas. The results from the UX evaluation of Edmodo showed that, despite the fact that students faced some difficulties during the use of the Edmodo, its UX was perceived as positive. The students found the e-learning system easy to use, useful and attractive. Examples of the challenges faced by the students included: too much time spent searching for the learning materials and a lack of understanding regarding how to perform the matching quiz correctly. The results also showed that the e-learning system did not motivate them. Adding more interesting features was suggested to increase students' engagement with learning. However, around 41% of the students reported that they were not able to fully evaluate their UX using the techniques (UEQ and IEAM), indicating a need for improvement.

III. METHODOLOGY

Earlier research indicated that no specific UX evaluation technique has been developed to evaluate the UX of e-learning. Therefore, this research suggested UX evaluation criteria adopted from two reliable criteria: instructional or didactic criteria, which focus on teaching and learning (adopted from Mtebe and Kissak [5]); and UX criteria, which focus on both usability and hedonic metrics (adopted from Topolewski et al., [22]). Research proved the reliability of the UX criteria which were developed by Topolewski et al. [22] as a technique which can be used to evaluate the UX of e-learning systems [10, 22]. However, these UX criteria focus on hedonic metrics and do not include specific metrics to evaluate the quality of the teaching and learning experience using e-learning systems. For this, the instructional or didactic criteria developed by Mtebe and Kissaka [5] were used to complement the UX criteria developed by Topolewski et al. [22] to evaluate comprehensively the UX of the e-learning system in terms of teaching and learning, usability and hedonic metrics. The suggested UX criteria consist of 8 categories and 29 corresponding sub-categories. Table I shows the categories and sub-categories of the suggested UX criteria while Appendix I presents the categories, sub-categories and the descriptions of the suggested UX criteria. Table II shows a comparison between the suggested UX criteria employed in this research with the other similar UX criteria employed by earlier research.

In order to evaluate the user experience (UX) of the UTM university from the students' perspectives using the suggested criteria, qualitative and quantitative methods were considered. For qualitative data, semi-structured interviews were conducted based of the suggested UX criteria categories and sub-categories as researchers suggest the use of interviews as one of the most common methods to evaluate the UX of learning management systems [15]. For quantitative data, a questionnaire consisting of two parts was developed. Part one

consisted of demographic information while part two consisted of 29 questions, one question for each of the UX sub-categories. The online questionnaire was sent to the students of the School of Computing at the UTM University via Email, WhatsApp and Telegram applications. The students were asked to answer the questions of the questionnaire to reflect their experience toward the Moodle e-learning system. The aim of the research, its benefits and the instructions to fill-out the questionnaire were explained in the first page of the questionnaire. Regarding the second part of the questionnaire, the students were asked to rate their agreement on each of the 29 statements using a seven-point Likert scale.

After this, the semi-structured interviews were conducted as a follow-up process to clarify the issues raised in the questionnaire and to identify students' UX problems qualitatively regarding their UX of the Moodle e-learning system. Advertisements to call for participants were sent to the students of the School of Computing at the UTM University via email, WhatsApp and Telegram applications. In each interview session, the students were asked to reflect their experience with Moodle e-learning system in terms of the identified UX categories and their corresponding sub-categories. Also, the students were asked to provide additional challenges they face while interacting with the current e-learning system. Furthermore, the students were asked to provide suggested improvements to the Moodle e-learning system to improve the learning process. An honorarium of RM30 was given to each student who participated in the interview sessions.

TABLE I. CATEGORIES AND SUB-CATEGORIES OF THE SUGGESTED UX CRITERIA ADAPTED FROM MTEBE AND KISSAK [5] AND TOPOLEWSKI ET AL. [22]

UX Category	UX Sub-category
Teaching and Learning	Instructional materials; collaborative learning; learner control; feedback and assessment; accessibility; motivation to learn
Economical	Entertaining; pleasantness; productivity; usefulness
Technological	Novelty; efficiency; reliability; user-friendliness
Emotional	Attractiveness; enjoyment; fulfilment
Cognitive	Comprehensiveness; engagement; meaningfulness
Interpersonal	Communicativeness; confidence
Emphatical	Attentiveness; helpfulness; respectfulness; responsiveness
Intention to Use	Convincingness; willingness; recommend

TABLE II. A COMPARISON BETWEEN THE SUGGESTED USER EXPERIENCE (UX) CRITERIA WITH THE OTHER SIMILAR CRITERIA

User Experience (UX) Criteria	User Experience (UX) Metrics		
	Instructional or didactic metrics	Usability metrics	Hedonic metrics
UX criteria suggested by Topolewski <i>et al.</i> [22]	✘	✓ [22]	✓ [22]
UX criteria suggested by Mtebe [6]	✓ [5]	✓ [25]	✓ [26]
UX criteria suggested by this research	✓ [5]	✓ [22]	✓ [22]

The qualitative data were analyzed based on the categories and sub-categories of the suggested UX criteria. The analysis of the qualitative data obtained from the interview sessions resulted in explaining the current UX of the students regarding their use of the Moodle e-learning system, and identified the challenges they faced while interacting with it. These are presented in the Results Section. Descriptive analysis was used for Part 1 of the questionnaire to describe the characteristics of the students; this is presented in the Results Section. Likert scores were calculated for each statement in Part 2 to describe students' responses to the 29 statements. For the purpose of the analysis, a Likert score of 1-3 was regarded as a negative response, 5-7 as a positive response and 4 as a neutral one. The Likert scores for the statements are presented in the Results Section.

IV. RESULTS

This section presents the results obtained from the analysis of the questionnaires and semi-structured interviews which describe the students' experience with the Moodle e-learning system used at the UTM University. A total of 120 students from the UTM University, School of Computing responded to the questionnaire and a total of 20 students were interviewed in 20 interview sessions. Most of the students who participated in the questionnaire were male (83%). Regarding the years of study, the students were in their first (15%), second (36%), third (33%) and fourth (16%) years. The majority (81%) had one to three years' experience with Moodle, and the majority (83%) used Moodle daily. The majority of the students (91%) used a laptop and a desktop to access Moodle. Regarding the interview sessions, most of the students who participated were male (80%). The majority of them (80%) were in the second year of study and had one to three years' experience with Moodle. The average time for the interviews was 35 minutes.

The following presents the students' experience with the e-learning system in terms of the identified eight UX categories and their corresponding 29 sub-categories obtained from the analysis of quantitative and qualitative data. The Likert scores for the UX categories and their related sub-categories are presented in Table III.

A. Teaching and Learning

- **Instructional materials:** All the students in the interviews stated that the course materials presented on the Moodle e-learning system were current and relevant to them; they supported them in the learning process, which explained the positive Likert score for this sub-category. However, the students suggested some improvements regarding the instructional materials which included:
 - Presenting course outlines for the courses before registration.
 - Providing access to courses and their materials from the previous semester.
 - Presenting exam questions/papers from the previous semester. The students stated that “we need to rely on the seniors or lecturers to get past

exam papers because this is not provided on the system”.

- Providing course materials during the exam period; the students indicated that most of the lecturers hide them early.
- **Collaborative learning:** The Likert scores showed that the students were dissatisfied with the e-learning system regarding its lack of support for collaborative learning. The reasons behind this lack of satisfaction were explained in the interviews and the complaints related to: lack of permission to create groups for assignments when most of them needed this because of their group-based assignments; and lack of support for group submissions when most of the assignments were actually group-based.

TABLE III. LIKERT SCORES FOR THE UX SUB-CATEGORIES

UX Category	UX Sub-Category	Likert Scores
Teaching and Learning	Instructional materials	5.1
	Collaborative learning	3.6
	Learner control	4.2
	Feedback and assessment	3.5
	Accessibility	5.3
	Motivation to learn	5.5
Economical	Entertaining	3.2
	Pleasantness	3.5
	Productivity	5.2
	Usefulness	5.7
Technological	Novelty	3.4
	Efficiency	5.2
	Reliability	5.3
	User-friendliness	5.1
Emotional	Attractiveness	4.5
	Enjoyment	4.2
	Fulfilment	5.1
Cognitive	Comprehensiveness	5.3
	Engagement	4.6
	Meaningfulness	5.5
Interpersonal	Communicativeness	3.7
	Confidence	4.3
Emphatical	Attentiveness	5.3
	Helpfulness	4.3
	Respectfulness	5.4
	Responsiveness	5.6
Intention to Use	Convincingness	5.5
	Willingness	5.2
	Recommend	5.4

- **Learner control:** This related to Moodle's support for organizing the e-learning materials into clear and logical units. The Likert scores for this sub-category showed that the students gave a neutral response. The students in the interviews explained the reasons behind this which related to the fact that lecturers could change the layout or the structure of the course page based on their preferences: for example, by weeks in ascending order; by weeks but in descending order, or in the middle of the page. The students stated that when lecturers chose to present the materials of their course by weeks in ascending order, the new material was displayed at the bottom of the page which required the student to scroll down to access it. One student said: "It is not easy to access the new materials when the page is too long." Another student said: "I get tired of keep scrolling down all the time to access the latest materials." Other students stated that some other lecturers would add the new materials to the middle of the page and this confused them a lot.
- **Feedback and assessment:** The Likert scores showed that the students were dissatisfied with the lack of immediate feedback on their assessments. This was explained by the students in the interviews as they indicated that there was a lack of feedback or comments on the submitted assignments, online quizzes and tests from the lecturers since most of the lecturers did not allow the marks to be viewed. The students stated, "We would suggest making a separate section for displaying our marks." The students also indicated that the system does not support students for sending their feedback.
- **Accessibility:** The students were satisfied with the fact that the e-learning system is accessible anytime and anywhere through various devices, such as laptops and desktops. This is reflected in the Likert score for this sub-category. However, in the interviews, the students identified some issues related to the mobile application. These related to it not being user friendly; there was also a lack of support for most of the used functions. For this, the students indicated that they preferred to use their laptop or desktop to access Moodle.
- **Motivation to learn:** The students stated that the Moodle e-learning system motivated them to learn since it supported quick submission of assignments. It also had the ability for assignments to be resubmitted before the due date; the viewing and grading of assignments, if the lecturer chose to present them, was enabled; online quizzes and tests could be conducted easily and students could be informed of their quizzes' and/or tests' marks instantly (if the lecturer allowed the marks to be viewed). This was in accordance with the positive Likert score related to this sub-category.
- **Pleasantness:** The students in the interviews stated that the current e-learning system was not pleasant to use; they have to use it as part of the learning process. This is in accordance with the negative Likert score related to this sub-category.
- **Productivity:** The Likert score related to this sub-category indicated that the Moodle e-learning system helped the students to be more productive. The students in the interview explained the reasons behind this which related to the fact Moodle presents all the instructional materials in one place which is easy to access and easy to use. Also, it supports the easy submission of assignments; also, quizzes and tests can be conducted easily and knowledge of the grades achieved is prompt if lecturers are using the grading system.
- **Usefulness:** The students perceived the Moodle e-learning system to be useful. It allows them to carry out their typical tasks, such as downloading materials and submitting assignments, with ease. This is in accordance with the positive Likert score related to this sub-category. However, the students indicated that the usefulness could be improved if Moodle could:
 - Be used to support communication with their lecturers instead of using other applications such as Telegram or WhatsApp;
 - Support online video meetings so that the students do not have to use other applications to meet their lecturers.

C. Technologica

- **Novelty:** The students stated that they did not consider the Moodle e-learning system as novel or new to them. This was reflected in the negative Likert score for this sub-category.
- **Efficiency:** The students considered the e-learning system to be efficient, allowing them to be efficient while learning; this is reflected in the positive Likert score for this sub-category. However, most of the students indicated that the efficiency of the e-learning system is based on how the lecturers use it in terms of the functions they provide for their students. They cited examples such as: the layout they chose for the course page; the communication methods they used to communicate with their students; the relevant use of the advertisement section to announce news; and the announcement of gradings for assignments and quizzes. The students suggested adding an internal search function to the current e-learning system to improve its efficiency.
- **Reliability:** The Likert score showed that the students perceived the Moodle e-learning system as reliable. The students in the interviews also indicated that the e-learning system is, in general, reliable. However, there were some issues which affected its reliability: for example, it was unable to handle high volumes of traffic during exams and assignment deadlines, which

B. Economical

- **Entertaining:** The students in the interviews indicated that the Moodle e-learning system did not entertain them. This is in accordance with the negative Likert score related to this sub-category.

resulted in the system breaking down. Also, the students indicated that sometimes there were login errors. Furthermore, the system did not display an appropriate error message when uploading a large file which exceeded the permitted size; instead, the system stopped responding.

- **User-friendliness:** The students indicated that the e-learning system was easy to use in terms of: it was easy to login, to navigate, to submit assignments, to access lecture materials, to download documents and files, and to go through online quizzes and tests. This is in accordance with the positive Likert score related to this sub-category. Furthermore, most of the students were satisfied with the interface design of the system which included: the interface was not cluttered, information was clearly displayed, and the fonts and colours were appropriate and clear to read. However, the students indicated that the system is not easy for computer illiterates, such as first-year students. The students also identified the following issues which related to the user-friendliness of the Moodle e-learning system:
 - Lack of color customization: the students could not change the colour of the Moodle pages.
 - Inappropriate design of the "Mark As Done" button which is used to keep track of the progress of each task. The students indicated that its size is too big which affects the length of the page.
 - Inappropriate color for the "Mark As Done" button. The students indicated that this button should be either green or red to attract the attention of the students.

D. Emotional

- **Attractiveness:** The Likert score related to this sub-category was neutral; the students in the interview indicated that they did not find the Moodle e-learning system attractive. They stated that the Moodle interface is poor and still needs several improvements in certain aspects.
- **Enjoyment:** The students stated that Moodle e-learning system is not enjoyable. The Likert score for this sub-category was neutral.
- **Fulfillment:** The positive Likert score related to this sub-category indicated that the students perceived the Moodle e-learning system as a fulfilling one. The students in the interview indicated that the e-learning system allowed them to achieve appropriately the required learning tasks, including downloading the required materials, submitting assignments and going through online tests and/or quizzes. However, the students mentioned some issues related to this sub-category which needed to be improved:
 - The permitted file size to be uploaded was small;
 - It took time to upload large files.

E. Cognitive

- **Comprehensiveness:** The students indicated that the current e-learning system is comprehensive since the instructional materials which were provided for most of the courses were sufficient and helpful; this is in accordance with the positive Likert score related to this sub-category. However, the students stated that the comprehensiveness of the e-learning system is mainly based on individual lecturers in terms of the content they added to the system and the functions they used to support the learning process.
- **Engagement:** The Likert score related to this sub-category was neutral and the students in the interviews indicated that Moodle did not allow them to engage in their tasks.
- **Meaningfulness:** The students indicated that the current e-learning system was meaningful and supported the learning process; this is in accordance with the positive Likert score related to this sub-category. However, the students stressed that the meaningfulness of the Moodle e-learning system was based on the functions and options lecturers used to manage their courses.

F. Interpersonal

- **Communicativeness:** The negative Likert score related to this sub-category indicates the students' dissatisfaction with the current communication support provided by Moodle. The students in the interviews stated that there is lack of communication options between students and lecturers offered by the system. Therefore, the students and lecturers used other communication channels, such as Telegram, to communicate with each other. The students indicated that they preferred to use Moodle to support their communication with their lecturers instead of using other applications.
- **Confidence:** The students indicated that the current Moodle e-learning system did not allow them to trust others; the Likert score for this sub-category was neutral.

G. Emphatical

- **Attentiveness:** The students indicated that the e-learning system allowed them to be attentive. For example, the students were satisfied with the availability of the constant reminder for the submission of assignments before the deadline. However, the students suggested improvements to the current e-learning system in terms of:
 - The system should support sending a notification to their email when a lecturer uploads new assignments or new materials, or makes any update to the course.
 - The Announcement forum should be used properly to notify them of any announcement, such as a public holiday or other important dates.

- **Helpfulness:** The students indicated that the current Moodle e-learning system did not allow them to help others because of the lack of supporting communications among students. The Likert score related to this sub-category was neutral.
- **Respectfulness:** The students believed that the current e-learning system allowed them to be respectful to their lecturers' deadlines for submitting assignments since it provided them with reminders to submit the assignment before the deadline. This is in accordance with the positive Likert score related to this sub-category.
- **Responsiveness:** The positive Likert score related to this sub-category showed that the students perceived the Moodle e-learning system to be responsive. The students in the interviews stated that, in general, the e-learning system allowed them to be responsive despite the fact that this is mainly based on the lecturers' choice of features they use in Moodle and the content they add to it. Specifically, the students stated that the e-learning system supported them to be responsive in terms of:
 - Submitting assignments before the deadline because of the constant reminders sent by the system to their emails;
 - Responding or taking action regarding the announcements for specific events (in the courses where lecturer used it);
 - Improving their performance since the system gives them their marks immediately after online tests and quizzes (in the courses where the lecturer activates this functionality);
 - Improving their knowledge when lecturers added additional motivating content for some courses.

H. Intention to Use

- **Convincingness:** Most of the students stated that they were convinced to continue using the Moodle e-learning system as it included all the functions they needed. However, they suggested that the Moodle e-learning system would offer more benefits if lecturers were able to use most of the available functions the system provided. The Likert score related to this sub-category was positive which stressed the fact that students were convinced of the use of the e-learning system.
- **Willingness:** The positive Likert score related to this sub-category indicates that the students were willing to re-use the Moodle e-learning system. The students in the interviews indicated that they were willing to re-use Moodle until they graduated from the university as it supported their needs.
- **Recommend:** The students stated that they could recommend using the Moodle e-learning system in other universities but they suggested that it would be more beneficial if most of the functions provided by

Moodle were used by the lecturers and students to support the learning process. The positive Likert score related to this sub-category stressed students' recommendation to use the Moodle e-learning system in other universities.

V. DISCUSSION

This research addressed the gap identified in the literature regarding the lack of a specific UX technique or UX criteria that could be used to evaluate the UX of e-learning systems and the lack of research which investigated User Experience (UX) of e-learning systems. This research suggested evaluation criteria to evaluate the UX of e-learning systems; these were adopted from two reliable methods [5, 22]. The suggested criteria included instructional or didactic metrics, and usability and hedonic metrics; thus, these can be used to evaluate comprehensively the UX of an e-learning system. Based on the suggested criteria, this research investigated the UX of the Moodle e-learning system employed at the University of Technology Malaysia (UTM) from the perspectives of students.

The results showed that the students in general had a positive User Experience (UX) of the Moodle e-learning system. However, they identified several issues which affected their experience when interacting with system. It is worth mentioning that most of the issues that were identified were based on the lecturers' use of Moodle's functions. These findings are in accordance with the findings of earlier research which also showed that the e-learning systems had several UX problems related to instructors' skills and usage, and the course content and structure managed by the instructors [6, 10].

Specifically, and with regard to the instructional, usability and hedonic metrics, the results showed that the students were satisfied with the quality of the instructional materials presented on the e-learning system in terms of them being current, relevant and supportive to the students' learning. These results opposed those obtained from earlier research which showed that the students were dissatisfied with the presence of outdated instructional materials or the unavailability of instructional materials [6].

The results also showed that the students were satisfied with the accessibility of the Moodle e-learning system; they also considered the system to be a good motivator for them to learn since it supported most of the functions they needed. However, the students also identified some issues which could be improved regarding the instructional metrics. These included: a lack of availability of previous semester exam papers; lack of support for collaborative learning; unclear organization of the course page; lack of feedback on the assignments, quizzes and tests from the lecturers; and the unusable mobile application. There were similarities between these results and the results of earlier research in terms of the identification of inconsistent layout or structure of the instructional materials which differed from one course to another based on the lecturers' preference; a lack of support for group work; server break downs; lack of customization; and the lack of an effective mobile application [6, 10].

Regarding the usability metrics, the results showed that the students were satisfied with the usability of the Moodle e-learning system on both laptop and desktop devices; this is in accordance with the results obtained from Maslov *et al.*'s research [10]. However, the students identified some minor issues or usability problems on Moodle's interface which could be improved. The students also indicated that the usability of the Moodle e-learning system was based on the level of experience of the person using it; thus, the more the students used the system, the more usable it became. These results are also similar to the results obtained from earlier research which found that Moodle for some students was a hard platform to use but one which became easier over time and experience [10, 21].

Regarding the hedonic metrics, the results showed that the students were satisfied with their experience while using the Moodle e-learning system; specifically, they indicated that they perceived Moodle as productive, useful, efficient, reliable, fulfilling, comprehensive and meaningful. They noted that it supported students to be attentive, respectful and responsible to others. The results also showed that the students were convinced of the use of the Moodle e-learning system. They were willing to re-use it and would recommend other universities to use it because of its benefits in supporting the learning process. These results are similar to those found in other research studies regarding the positive feelings and memories that Moodle provides to students [6]. However, the students indicated that the Moodle e-learning system is not entertaining, pleasant or novel, and it did not support communications with their lecturers. These results are similar to those of Maslov *et al.*'s study [10]. Also, the students were neutral regarding the attractiveness, enjoyment, engagement, confidence and help of the Moodle e-learning system. These results are also in accordance with earlier research results which showed that students were neutral regarding interesting or exciting functionalities offered by Moodle [6].

The results of this research suggest that each university or academic institution which employs an e-learning system should provide a comprehensive course for their staff to explain the wide-ranging functionalities supported by the e-learning system in order to improve their skills and knowledge regarding these functionalities. This will then help lecturers to use the e-learning system more effectively by employing most of the functionalities to support the learning process, thus improving the students' experience while using the e-learning system.

The results of this research can be used to improve the user experience (UX) at the case study university (UTM) and can also be used in general to improve the user experience of Moodle e-learning systems by considering the challenges the students face when interacting with such a system.

VI. CONCLUSIONS

This research examined the user experience (UX) of the Moodle e-learning system employed at the University of Technology Malaysia (UTM) from students' perspectives using comprehensive user experience (UX) criteria adopted from two criteria. The adopted UX criteria consist of teaching and learning, usability and hedonic metrics; these related to 8

categories and 29 corresponding sub-categories. Two methods were employed to investigate the UX of the e-learning system: semi-structured interviews and questionnaires. These were employed based on the UX criteria. A total of 20 students participated in the interviews and a total of 120 students responded to the questionnaires. The results showed that the students were satisfied with the e-learning system and they had positive user experiences while interacting with it through their learning. However, several issues relating to aspects of the UX criteria were identified by the students; these need to be considered in order to improve the UX of the e-learning system.

This research contributes to the literature regarding the suggested UX criteria which were adopted to investigate user experience (UX) of an e-learning system; it also contributes to the literature regarding the results which identified several challenges to the Moodle e-learning system which affected the experience of users (UX). However, there are some research limitations related to this study. The first relates to the fact that the study used only students to evaluate the user experience (UX) of the e-learning system. Other users, including lecturers, were not considered. The second limitation relates to the fact that the reliability of the suggested user experience (UX) criteria has not yet been tested.

Future research can be conducted to evaluate the user experience (UX) of Moodle e-learning system used by the University of Technology Malaysia (UTM) from lecturers' perspectives. Also, further research can be conducted to test and validate the reliability of the suggested user experience (UX) criteria employed in this research.

REFERENCES

- [1] H. E. D. Amandi, and W. R. M. S. Shanika, "The student perspective on usability of learning management system at university of Sri Jayewardenepura," 18th FMSC Research Sessions, 2021.
- [2] S. Bermejo, "Cooperative electronic learning in virtual laboratories through forums," IEEE Transactions on Education, vol. 48, no. 1, pp. 140-149, 2005.
- [3] Syngene Research, Global e-learning market analysis 2019, 2019. <https://www.researchandmarkets.com/reports/4769385/global-e-learning-market-analysis-2019>.
- [4] M. Simonson, "Course management systems", Quarterly Review of Distance Education, vol. 8, no. 1, vii-ix, 2007.
- [5] J.S. Mtebe, and M.M. Kissaka, "Heuristics for evaluating usability of learning management systems in Africa", in Cunningham, P. and Cunningham, M. (Eds), IST – Africa 2015, Conference Proceedings, Lilongwe, pp. 1-13, 2015.
- [6] S. J. Mtebe, "Examining user experience of eLearning systems implemented in two universities in Tanzania", Interactive Technology and Smart Education, vol. 17, no. 1, , pp. 39-55, 2020.
- [7] L. Hasan, "The usefulness and usability of Moodle LMS as employed by Zarqa University in Jordan ", Journal of Information Systems and Technology Management (JISTEM), vol. 16, 2019.
- [8] D. Ivanc, R. Vasiu, and M. Onita, "Usability evaluation of a LMS mobile web interface", in the Proceedings of the 18th International Conference, ICIST 2012, Kaunas, Lithuania, September 13-14, 2012, pp. 348-361, 2012.
- [9] Moodle, <<https://moodle.org/>>, [accessed 01.08.2021].
- [10] I. Maslov, S. Nikou, and P. Hansen, "Exploring user experience of learning management system", The International Journal of Information and Learning Technology, vol. 38, no. 4, pp. 344-363, 2021.
- [11] ISO 9241-210:2010, "Ergonomics of human-system interaction – part 210: human-centred design for interactive systems", 2010.

[12] ISO 9241-11, "International standard first edition. ergonomic requirements for office work with visual display terminals (vdots), Part11: guidance on usability", 1998.

[13] N. Bevan, "Classifying and selecting UX and usability measures", International Workshop on Meaningful Measures: Valid Useful UX Measurement, vol. 11, pp. 13-18, 2008.

[14] M. Hassenzahl, and N. Tractinsky, "UX-a research agenda", Behaviour and Information Technology, vol. 25, no. 2, pp. 91-97, 2006.

[15] W. T. Nakamura, E. H. T. de Oliveira, and T. Conte, "Usability and user experience evaluation of learning management systems – a systematic mapping study", In Proceedings of the 19th International Conference on Enterprise Information Systems (ICEIS 2017), pp. 97-108, 2017.

[16] W. Nakamura, L. Marques, L. Rivero, E. Oliveira, and T. Conte, "Are generic ux evaluation techniques enough? a study on the ux evaluation of the edmodo learning management system", Brazilian Symposium on Computers in Education (SBIE), vol. 28, no. 1, pp. 1007-1016, 2017.

[17] I. Santoso, and I. Efendy, "Usability study of Moodle LMS in statistics Indonesia learning center - case study," International Conference on Science Education and Technology, Journal of Physics: Conference Series, IOP Publishing vol. 1511, 2020.

[18] M. E. Eltahir, S. Al-Qatawneh, N. Al-Ramahi, and N. Alsalmi, "The perspective of students and faculty members on the efficiency and usability of e-learning courses at Ajman University: A case study," Journal of Technology and Science Education, vol. 9, no. 3, pp. 388-403, 2019.

[19] N. Harrati, I. Bouchrika, A. Tari, and A. Ladjailia, "Exploring user satisfaction for e-learning systems via usage-based metrics and system usability scale analysis," Computers in Human Behavior, vol. 61, pp. 463-47, 2016.

[20] J. Melton, "The LMS Moodle: a usability evaluation," Languages Issue, vol. 11/12, no. 1, pp. 1-24, 2006.

[21] I. Senol, H. Gecili, and P. Durdu, "Usability evaluation of a Moodle based learning management system," in the Proceedings of EdMedia 201, Tampere, Finland, June 23-26, 2014.

[22] M. Topolewski, H. Lehtosaari, P. Krawczyk, M. Pallot, I. Maslov, and J. Huotari, "Validating a UX model through a formative approach: an empirical study", 2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC), IEEE, pp. 1-7, 2019.

[23] V. Roto, H. Rantavuori, and V.V.M. Kaisa, "Evaluating user experience of early product concepts", International Conference on Designing Pleasurable Products and Interfaces, pp. 1-10, 2009.

[24] L. Shi, "Defining and evaluating learner experience for social adaptive E-Learning", The 4th Imperial College Computing Student Workshop (ICCSW 2014), pp. 25-26, 2014.

[25] J. Nielsen, "Heuristic evaluation", in N. Jakob, and R.L. Mack (Eds), Usability Inspection Methods, John Wiley and Sons, New York, NY, 1994.

[26] M. Hassenzahl, "The thing and I: Understanding the relationship between user and Product", in M. Blythe, C. Overbeeke, A. Monk, and P.S.N. Wright (Eds), Funology: From Usability to Enjoyment, Kluwer Academic Publishers, Norwell, MA, pp. 31-42, 2005.

APPENDIX I. CATEGORIES, SUB-CATEGORIES AND DESCRIPTION OF THE SUGGESTED UX CRITERIA ADAPTED FROM MTEBE AND KISSAK [5] AND TOPOLEWSKI ET AL. [22]

UX Category	UX Sub-category	Description
Teaching and Learning	Instructional materials	Degree to which Moodle consists of relevant learning materials (such as whether they are accurate, current).
	Collaborative learning	Degree to which Moodle has facilities and activities that encourage inter- and intra-group activities such as group projects, group debates, discussions, collaborative problem solving and presentations.

	Learner control	Degree to which Moodle supports breaking the instructional materials down into clear, logical and meaningful units from the point of view of learners.
	Feedback and assessment	Degree to which Moodle has tools to enable learners to assess their learning achievements and receive sufficient and immediate feedback. It should also have tools that enable instructors to assess, record and track learners' reports.
	Accessibility	Degree to which Moodle is easily be accessed through various devices such as with small and wide screens (e.g., PDA, laptops) as well as different platforms and browsers.
	Motivation to learn	Degree to which Moodle motivates learners to learn through various mechanisms including providing grades, physical rewards and other incentives.
Economical	Entertaining	Degree to which Moodle entertains users.
	Pleasantness	Degree to which Moodle is pleasant to use.
	Productivity	Degree to which Moodle helps users to be more productive.
	Usefulness	Degree to which Moodle allows users to carry out tasks.
Technological	Novelty	Degree to which Moodle is new to the user.
	Efficiency	Degree to which Moodle allows users to be efficient.
	Reliability	Degree to which Moodle is reliable.
	User-Friendliness	Degree to which Moodle is easy-to-use and sufficiently intuitive.
Emotional	Attractiveness	Degree to which Moodle is visually attractive.
	Enjoyment	Degree to which Moodle is enjoyable.
	Fulfillment	Degree to which Moodle allows users to achieve a task properly.
Cognitive	Comprehensiveness	Degree to which Moodle allows users to understand others.
	Engagement	Degree to which Moodle allows users to engage with their task.
	Meaningfulness	Degree to which Moodle allows users to provide meaningful results.
Interpersonal	Communicativeness	Degree to which Moodle allows users to communicate to others.
	Confidence	Degree to which Moodle allows users to trust others.
Emphatical	Attentiveness	Degree to which Moodle allows users to be attentive to others.
	Helpfulness	Degree to which Moodle allows users to help others.
	Respectfulness	Degree to which Moodle allows users to be respectful of others.
	Responsiveness	Degree to which Moodle allows users to be responsive to others.
Intention to Use	Convincingness	Degree to which users are convinced of using Moodle in the near future.
	Willingness	Degree to which users are willing to re-use Moodle.
	Recommend	Degree to which users are willing to recommend using Moodle in other universities.

Query Expansion based on Word Embeddings and Ontologies for Efficient Information Retrieval

Namrata Rastogi¹, Parul Verma²
Amity Institute of Information Technology
Amity University Uttar Pradesh
Lucknow, India

Pankaj Kumar³
Dept. of Computer Science
Sri Ram Swaroop College of Engineering and Management
Lucknow, India

Abstract—Information retrieval has been an ever-going process for end users to fetch relevant data at one go. The problem intensifies more with unstructured data in a semantic web environment. It is also a promising area for researchers to dive in and refine it from time to time. Expanding the user query and reformulating it is one probable solution to increase the efficiency of the information retrieval system. In this paper we propose “WeOnto”, a novel two-level query expansion algorithm that utilizes the combination of web ontologies and word embeddings for similarity calculation. In the first level, the Real estate Ontology (REO) is created using Protégé and Sparql queries are passed to retrieve probable semantic words from the given ontology for each inputted user query. The first level gave significant results and improved the information retrieval by 18%. The second level of algorithm uses word embedding enhanced with the domain knowledge that helps to retrieve similar meaningful words based on cosine similarity for the same user query. Word embeddings are implemented using Word2Vec method that follows two architectures namely CBOW or Skip Gram. Most similar semantic words are retrieved using the CBOW word embeddings method in the proposed algorithm and concatenated with the semantic keywords generated from the real estate ontology to form a powerful reformulated query that gives promising relevant results. Finally, two topmost words as per their similarity index are taken to reformulate the original user query. Experimental results depict that proposed algorithm has given distinct results and has showcased significant improvement of 93% over the initial user query.

Keywords—CBOW; Information retrieval; ontology; query reformulation; semantic web; skip gram; word embeddings; word2vec

I. INTRODUCTION

Internet is a deep ocean of information and efficient information retrieval has been a constant desire of users. Researchers have been continually working towards achieving this goal with various methodologies and algorithms being designed to give easy and quick access of information to the intended users. The main aim has been to work at the basic level and frame the user query such that the expanded query gives better results with increased precision.

Traditional IR methods were based on TF-IDF, Boolean, vector space models (VSM) or BM25 methods based on document frequency to solve the problem. But they all suffered from word mismatch issues called lexical gap problem [1] while at times the queries were not formulated correctly or were having ambiguous words that led to poor

retrieval. This leads to following problems that needs to be catered eventually:

- With ever-growing data over Internet, improving the efficiency of information retrieval system has always been an issue.
- How good a user query be formulated such that it increases the efficiency of retrieved web results.
- How to measure the effectiveness of the user query formulated that retrieves required relevant results.

Thus, the research objective is to increase the efficiency of information retrieval systems and focusing on query expansion such that the performance evaluation of reformulated user queries gives effective desired web results.

Finally, our research work focusses on the problem of information retrieval and low web results and proposes WeOnto algorithm, a novel algorithm that works on increasing the efficiency of information retrieval by incorporating the latest concept of word embeddings combined with web ontologies in a semantic web environment. The algorithm suggests a solution of reformulating the user query by expanding the user query with most similar new words, thereby giving better retrieved results.

Such expanded queries include the original query and some additional keywords that are found relevant to the given query keywords. These additional keywords are derived using the concept of Word embeddings amalgamated with ontologies both help to extract the semantics of the given query words.

Web ontologies are stored in the form of triples, i.e., subject, object and predicate having the entire meaning or relation between the subject and object explained within the triple. The word embeddings on the other hand take the word with respect to its meaning from the surrounding context and give us most similar words based on embeddings that store the relations in the form of vectors calculate cosine similarity to draw the appropriate results.

Word embeddings is method from natural language processing that has gradually found its application in information retrieval also [2]. Pre trained word embeddings are applied on the user corpus to retrieve most similar word for the query words such that the given user query be expanded to give efficient information retrieval. Word2Vec,

GloVe, FasText, Bert, Elmo are few methods that could be incorporated to do above mentioned tasks.

In this paper, Section II explains the background related work while Section III talks about method and material used and comprises of the description of the proposed algorithm, “WeOnto” used for query expansion to increase the efficiency of information retrieval. Section IV describes the result and discussion along with the analysis and result of the experiment done on user defined corpus. Section V is the conclusion.

II. RELATED WORK

Information retrieval has always been a topic of concern for researchers worldwide and many experiments and methodologies have been devised to increase its efficiency from time to time. We even have traditional IR models like Boolean model, vector space (VSM) model, probability-based models, and fuzzy set models [3]. These models enhanced the workability of IR systems but still with ever growing information over the Internet, the need to improve the efficiency continues. The keyword matching approach could not do better around problems like polysemy where semantics of the words was required instead of syntactical approach.

So, recent researchers evolved methods that focus more on semantics and the meaning of words based on the context used. For such purposes, a natural language processing feature called Word embeddings [4] for the purpose of information retrieval has come as a probable solution. Word2vec is a deep learning method under NLP that takes word embeddings with respect to the context learned from the given corpus and gives most similar words as output. Siriguleng [5] in the paper also used word2vec and LDA topic model to expand Mongolian query and improve retrieval. Even B. Wang, et.al. in their work had discussed about experimental results [6] they had in using six embedding models. They compared these models but could not find one universal method that would cater all possibilities. On the other hand, B. Mansurov and A. Mansurov [7] depicts the use of word embeddings on Uzbek language and used it to get semantic similar words. Farhan et.al also talks about taking top relevant results and calculating the average vector values using word embeddings in a deep neural network and improve the IR system to an extent [8]. Various researchers have recently understood the power of using ontologies with word embeddings and have showcased their effectiveness in their works; some of them have been put here. WE-based Arabic IR models also use wordnet and embeddings and depict comparisons of working after incorporating embeddings as in [9]. QSST, a Quranic searching tool based on word embeddings gave a high performance with an average precision of 91.95% [10]. Jin Ren *et. al.* in his paper [11] also explained about the effective results obtained on the use of predicate expression related to ontology and combining it with word embeddings. The work of Jayawardana, *et. al.* also describes the use of word embeddings on semi-supervised ontology population [12]. Lastra-Díaz *et. al.* in their work [13] stated that taking an average of two models i.e., Word embedding models and ontology measures in an experimental survey gave better results.

A. Word Embeddings

Word embeddings are unsupervised learning applications that also talk about transfer learning as it is incorporated in the given user corpus. Embeddings can be character level or word level [14]. The word level embeddings use word2vec method where the basic construct of embeddings is converting words into vectors and then mathematically apply relations on them based on the corpus being used. The vectors having similarity are closer to each other and have similar values. Their threshold value is mostly greater than 0.6. The closer it is to 1, the higher the similarity index is considered and thus two vectors or words are considered most similar.

Word2vec is a deep learning method under NLP that takes word embeddings with respect to the context learned from the given corpus and gives most similar words as output. The similarity is calculated using Cosine similarity [15] such that:

$$\text{Cos}(\theta) = \frac{\mathbf{A} \cdot \mathbf{B}}{|\mathbf{A}| |\mathbf{B}|} \quad (1)$$

The similarity value of the vectors ranges from -1 to +1. The Gensim library in Python language gives all capabilities of running this model and check the output. This model talks about different vector dimension and window size.

Word2Vec model is further divided into two architectures: Continuous Bag of Words (CBOW) and Skip-Gram (see Fig. 1) used to calculate vectors in their own way and giving different results but closely like each other.

CBOW architecture projects ‘Current Word’ based on inputted context words whereas Skip-Gram works vice versa, i.e., it takes current word as input and gives contextual word before and after the current word [15].

The window size plays an important role in capturing the context of the corpus and giving similar words as output. In Fig. 1, window size =2 where W(t) is the target word while t-2, t-1, t+1, and t+2 are the neighboring words that form the contextual window because of which the meaning is understood. The more-closer words, the better they are related to each other.

All the researchers have ultimately tried to incorporate various ways of implementing ontologies or word embeddings method to achieve efficient information retrieval.

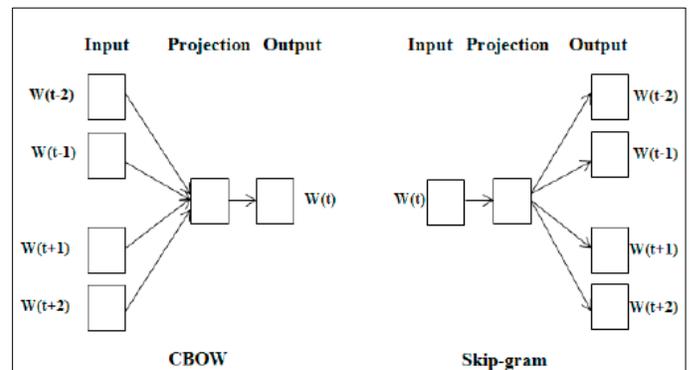


Fig. 1. Word2Vec (CBOW and Skip-Gram) Model Architecture [16].

Few of them have achieved the precision of 91% using their own methods. Our proposed algorithm “WeOnto” depicts the power of ontologies along with word embeddings that doubly work on semantics of keywords rather than pattern matching alone and show an effective information retrieval system having a 93% precision.

The user query in the proposed algorithm goes through series of steps that works on the semantics by fetching most similar words and reformulating the user query such that it improves the efficiency of information retrieved during the web search.

The next section gives a detailed description of WeOnto algorithm: a novel query optimization approach that provides users with more meaningful similar words that upon implementation improves retrieval results.

III. METHOD AND MATERIAL

With information explosion over the Internet, better information retrieval systems are always in demand. To increase its efficiency, query reformulation is one of the probable solutions.

For this purpose, we need to expand our query by preprocessing it first such that the stop words are removed and then we gather similar terms related to the major keywords left. The query after expansion will now have two set of words: i) keywords from query, ii) addition of new words.

A. Proposed Algorithm

Mathematically, let us suppose a query Q has n terms, $Q = \{t_1, t_2, t_3, \dots, t_n\}$. The reformulated query Q^+ will have two set of words: i) keywords from expanded query $Q' = \{Q - ST\}$ where ST is the list of stop words; ii) addition of new terms $T' = \{t_1', t_2, \dots, t_m'\}$. The reformulated query after expansion will look like [17]:

$$Q^+ = Q' \cup T' \quad (2)$$

$$= \{t_1, t_2, t_3, \dots, t_n, t_1', t_2, \dots, t_m'\}.$$

The question arises how to get these new terms.

“WeOnto” is the proposed algorithm that finds an answer in the form of applying a combination of Ontologies and word embeddings on the user query and reformulates it into a new query which will be more suitable in context to the domain and aims to give more relevant results with increased precision.

As per the WeOnto algorithm, there is an input user query Q in step 1 (see Fig. 2) that will be reformulated such that the expanded query Q^+ at the end of algorithm is suitable enough to retrieve more relevant web documents and has better precision.

To expand the given user query Q, the query is sent for pre-processing which includes processes like removal of stop words, lower their case and tokenization and $q[] = \{t_1, t_2, t_3, \dots, t_n\}$ is obtained. Here, $q[]$ is the query after preprocessing having list of tokens $\{t_1, t_2, t_3, \dots, t_n\}$.

Input Query: Q, Word2Vec Model: M

Output expanded Query: Q^+

Step 1: Get User input query, Q and apply Pre-Processing.
 $q[] = \text{preprocess}(Q)$ s.t. $q \in \{t_1, t_2, t_3, \dots, t_n\}$ where $t =$ tokens generated after preprocessing of Q.

Step 2A: $q[]$ passed to Real Estate Ontology (REO) to retrieve synsets. i.e., $\forall (t) \in q; \exists (s) \in \text{Ontology 'O'}$.

Step 2B: For each token ‘ t_i ’

If $t_i = s_i$ then

SW [] = add (s_i), SW is semantic words

Else

If $t_i \neq s_i$ then

SW [] = add (t_i)

End for

Step 3A: Num_tokens = len (q)

For each token, t_i ,

Sim_list [] = most similar vectors retrieved from Model ‘M’.

Step 3B:

$$\text{Threshold (th)} = \frac{\sum_{i=1}^{\text{num_tokens}} \text{sim_list}[]}{\text{num_tokens}}$$

i.e., Calculate threshold Value = Average of

Vector values retrieved for ‘ t ’.

Step 3C: For each token ‘ t_i ’

If $\text{sim_list}[] > \text{th}$ then

Act_sim_words = add (sim_list[])

End for

Step 4: For each token ‘ t_i ’

MSW[] = act_sim_words \cup SW

i.e., Combine both lists and retrieve two most suitable words from MSW[] to be used in expanded query, Q^+ .

Step 5: new words from MSW[] to initial query tokens, $q[]$ and get final expanded query,

$$Q^+ = Q + \{q[] \cup \text{MSW} []\}$$

Step 6: Retrieve documents using the new query Q^+ .

Fig. 2. “WeOnto” Proposed Algorithm.

These tokens, $t_i, i = 1 \dots n$ are sent for a Two-level process of query expansion which can be seen in the algorithm. In the first level as shown in step 2, tokens t_i are passed to real estate ontology (REO) that was created to store the legal glossary terms used in case of real estate documentation during buying and selling of real estate properties [18]. The ontology was created using the WordNet vocabulary to capture all the syntactical and semantics of the English language as well as Legal terminology used for query reformulation. Sparql queries are issued in background that fetch semantically enriched keywords or synsets for each token t_i . For every token, t_i , if its synset exists, then it gets added to the semantic words list SW[], else the token itself gets added to SW[] giving us the list of semantic words fetched from REO as seen in Fig. 3.

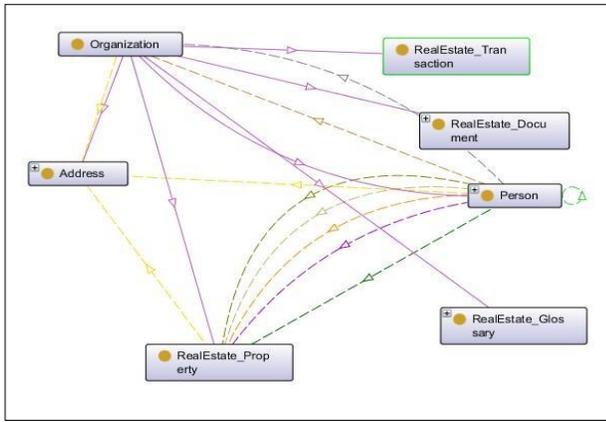


Fig. 3. Real Estate Ontology [18].

In the second level as depicted in step 3, a shallow learning NLP technique, Word2Vec model M that is using Continuous bag of words (CBOV) method to learn from the given corpus C . The corpus is made by scraping 2000 web documents related to real estate legal documentation domain. This word embedding model M has converted 1.05 million words into 12.5 thousand vectors using which most similar words would be derived for the same set of tokens, t_i .

These similar words are retrieved by calculating Cosine similarity for each pair and stored in $sim_list[]$ list.

A threshold value is calculated as per step 3B from Fig. 2 to fetch the top k most similar words by taking average of the similarity index obtained for every token. If the similarity index is higher than this calculated threshold value, then such words are put into consideration and transferred to the actual similar words list, $act_sim_words[]$.

Step 4 of WeOnto algorithm shows a union of above two lists obtained after step 2 & 3, i.e., $SW[]$ and $act_sim_words[]$ are combined on the basis of cosine similarity calculated for each pair of words and two most similar and suitable words are finally retrieved and stored to form the most suitable semantically enriched similar words, $MSW[]$.

Ontology at first level is first incorporated to find the semantically enriched words for the tokens. Then word embeddings are also applied at second level to understand the context of real estate related queries with the help of the knowledge model that has learnt from the user defined corpus.

Step 5 of proposed algorithm shows the final step of union of original tokens from user query to most suitable semantically enriched similar words as in Eq. (2), $MSW []$, i.e., $Q' = q[] \cup MSW[]$. Here, we need to remember that Q' will hold unique words only.

Hence, Q' becomes the final reformulated query that is deduced as the user query was expanded after applying the proposed algorithm where a list of semantic words retrieved from an ontology is concatenated to the list of words obtained from the word embeddings-based NLP model showing most similar words based on cosine similarity values.

The increase in the performance of information retrieval systems is calculated as defined in [19]:

$$Improvement = \frac{Reformulated\ Result - Baseline\ Result}{Baseline\ Result} \quad (3)$$

This proposed novel algorithm is again tested, and it gives promising results showing a remarkable increase in the efficiency of IR system by incorporating a methodology that uses both ontology and word embeddings from NLP.

IV. RESULTS AND DISCUSSION

A. Experiment Setup

The proposed algorithm, “WeOnto” has a two-level procedure where the first level deals with the use of real estate ontology (REO) as defined in [20]. Real estate ontology has been created for a domain of real estate related legal documentation and has a glossary of legal terminology created using Wordnet Dictionary as seen in Fig. 4. The first level uses REO to retrieve semantically enriched keywords for the given user query and improved the reformulated query by 18%. However, the second level of algorithm is designed to further improve the information retrieval system and get more relevant results.

Hence, Step 2 of the WeOnto algorithm talks about the second level of the algorithm with the generation of similar words using word embeddings of natural language processing.

Word2Vec model of word embeddings is used with the aim that it will first train the model on real estate related dataset having data from 2000 web documents that were either government based or related to legal or real estate buying and selling. The implementation is done in Python language where its Gensim library was used to train the model that contains word vectors for a vocabulary of 12,462 words trained on around 1.05 million words from the user corpus and then apply various methods from it to derive similarity values.

Various parameters were set while training the model using Gensim library in python. Some of them like vector size = 100, initial learning rate, $\alpha = 0.025$, window size = 5 which means two context words taken before and after the target word. Also, $min_count = 1$ which means that words having frequency < 1 were avoided and lastly $sg = 0$ for CBOV and 1 for skip-gram method to be used.

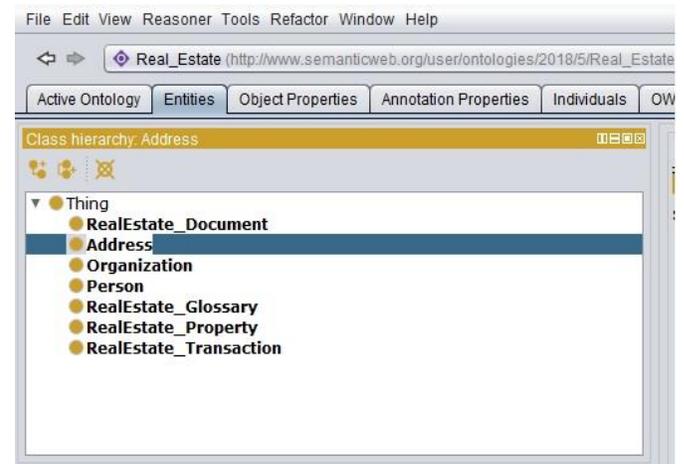


Fig. 4. Glossary Entity of Real Estate Ontology [19].

After the model has learnt and created vectors or embeddings from the corpus, the model is loaded to fetch similar words using cosine similarity (see eq. 1) for a given user query. The high cosine similarity between two words shows that the words are semantically similar and accordingly converted to vectors and are geometrically similar in the Euclidean space as well.

The ‘most_similar’ method returns the word vectors based on similarity for every token in the user query. To find the similarity between specific two words, i.e., to find similarity between user query and synsets retrieved from REO, ‘model.similarity()’ method from genism library in python is used and all values are stored in final_list.

Once the training is done, the test set includes 50 random user queries on which the entire algorithm is applied step wise. The result generated at each step is stored in Fig. 5 where every column defines a sub step of the algorithm.

Column No. 1 depicts the initial user query, Q. The query is pre-processed and converted into set of tokens, Q1 as shown in column 2 in Fig. 5 above. These tokens are passed to the real estate ontology (REO) and Synsets (named as set A) are retrieved for each token as in column 3.

The second step of algorithm talks about tokens being sent to Word2Vec model that produces most similar words (named as set B) as stored in column 4. Column 5 depicts the union of

set A and B along with cosine similarity calculated for all paired vectors.

Column 6 holds the topmost two best words that are deduced using threshold value. Threshold value is first calculated taking the average of N vectors retrieved in column 4. If the similarity is greater than the average threshold value which keeps on changing with respect to every pair of word vector, then such words are counted as the best and stored in column 5.

Hence column 5 has the topmost words that has the highest cosine similarity. Column 6 shows the best two words derived for each token that will be added to the final expanded query.

Column 7 depicts the final expanded query, Q3 that holds the tokens after pre-processing and topmost two similar contextual words retrieved after implementation of the algorithm. This Q3 query is finally tested on test bed, www.google.com to retrieve the most relevant web documents against the initial user query.

B. Result Discussion

Table I shows the number of relevant documents retrieved at three levels i.e., at the initial query Q1, then Q2 is the query transformed by applying real estate ontology (REO) only and final expanded query, Q3 that shows implementation of combination of REO and word2vec method used in word embeddings.

Col. No.	1	2	3	4	5	6	7
S.No.	Initial User Query, Q	Q1 = Tokens from Q	Synsets from Real Estate Ontology (A)	most similar from WE Model (B)	Res= A union B	Top2= Top two from Res	Reformulated Query (Q3) = [Q1 + Top2]
1	Sale deed for house	sale deed house	sale, sales agreement, deed of conveyance, title, house, home, business firm	[(‘conveyance’, 0.7810737490653992), (‘gift’, 0.7765251398086548)]	[(‘conveyance’, 0.7810737490653992), (‘gift’, 0.7765251398086548)]	conveyance gift sales deeds apartment title	sale deed house conveyance deeds apartment
2	Sale deed for a commercial property	sale deed commercial property	sale, sales agreement, deed of conveyance, title, commercial holding place	[(‘conveyance’, 0.7810737490653992), (‘gift’, 0.7765251398086548)]	[(‘conveyance’, 0.7810737490653992), (‘gift’, 0.7765251398086548)]	conveyance gift sales deeds commercial land	sale deed commercial property conveyance
3	Format for power of attorney	format power attorney	format power of attorney	[(‘template’, 0.9079666137695312), (‘standard’, 0.9062818288803101)]	[(‘template’, 0.9079666137695312), (‘standard’, 0.9062818288803101)]	template standard authorizing	format power of attorney template authorizing
4	poa for development of property by owner	POA development property owner	power of attorney development evolution holding proprietor	[(‘spa’, 0.9243891835212708), (‘gpa’, 0.8950620889663696)]	[(‘attorney’, 0.73795146)][[‘holding’, 0.41234785]][[‘proprietor’, 0.48605007]]	power of attorney venture land	POA development property owner power of
5	Property transfer deed	Property transfer deed	holding place transfer transference deed of conveyance, title	[(‘land’, 0.7449188828468323), (‘ostensible’, 0.6848605871200562)]	[(‘holding’, 0.41234785; ‘place’, 0.25646645)][[‘transference’, 0.5074328]]	land transferred deeds	Property transfer deed land transferred deeds

Fig. 5. Working of Proposed Algorithm.

TABLE I. NO. OF RELEVANT DOCUMENTS AND AVERAGE PRECISION

Query No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
No. of weblinks-Baseline query, Q1	7	7	23	8	1	10	0	15	0	1	0	6	8	2	5
No. of weblinks, Post Ontology, Q2	8	7	15	10	2	10	0	15	6	3	3	8	13	5	11
No. of weblinks- Post Word Embeddings, Q3	7	7	20	5	8	5	1	8	8	9	7	22	17	10	6
Avg. Precision for Baseline query(Q1)	0.27	0.31	0.77	0.45	0.03	0.61	0	0.83	0	0.05	0	0.36	0.79	0.21	0.35
Avg. Precision for Post Ontology Query(Q2)	0.73	0.61	0.69	0.51	0.17	0.67	0	0.72	0.39	0.44	0.17	0.38	0.55	0.54	0.44
Avg. Precision for post Word Embeddings Query(Q3)	0.8	0.82	0.98	0.86	0.78	0.82	1	0.7	0.7	0.71	0.67	0.76	0.83	0.93	0.62

Table I also depicts the average precision of each query calculated at baseline, ontology, and embeddings level.

The graph in Fig. 6 is showing the average precision of getting relevant documents for given 50 queries.

Average precision after implementing the complete algorithm gives a substantially higher precision values for post word embeddings queries, Q3 as compared to its baseline, Q1 queries (see Fig. 6).

Another metric, Precision at 10 (P@10) is also used for performance evaluation of WeOnto algorithm and information retrieval at large. Table II depicts a sample of P@10 computed for all 50 queries. P@10 gives the number of relevant documents from the top 10 retrieved documents.

Fig. 7 shows the precision at 10 (P@10) metric of 50 queries together. This metric is used for performance evaluation of information retrieval systems. Here, values of P@10 have increased considerably for every query after implementation of word embeddings as compared to the baseline queries.

The results show a major increase in the number of relevant documents retrieved and hence depicts a higher mean average precision upon implementing the proposed algorithm. Table III displays mean average precision of 0.44 for base line queries that increased to 0.85 after implementation of the second stage of WeOnto algorithm showing remarkable improvement of 93% as compared to an improvement of 18% at first level of the algorithm as per Eq. 3 in the efficiency of information retrieval system. Even precision at 10 also depicts a clear increase and states that top 10 documents retrieved are 75% more relevant as compared to initial baseline queries.

The graph in Fig. 8 depicts a significant upgrade in the values of the metrics required for performance evaluation of REIR model calculated at each level as described in the paper. It clearly shows an increase in efficiency of information retrieval using the semantically enriched ontology and word embeddings model of NLP for quick retrieval of real estate legal documents.

A trend showing usage of semantic ontology [21] for query expansion was already there. Its aggregation with word embeddings has proved to give better information retrieval results.

It is evident that WeOnto algorithm proposed in the paper includes the usage of the combination of web ontology and word embeddings as also mentioned in [22] for the purpose of query expansion has given significant results with respect to information retrieval of web documents as compared to the baseline user queries.

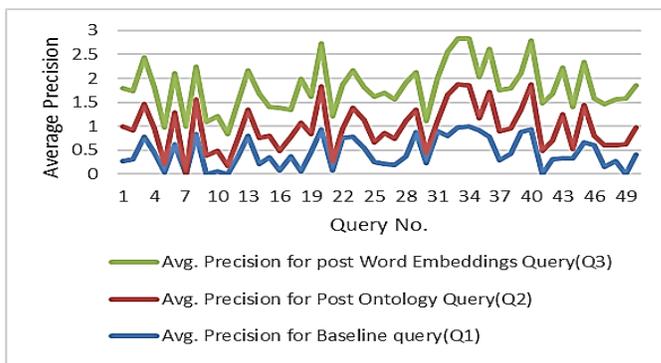


Fig. 6. Graph showing Average Precision.

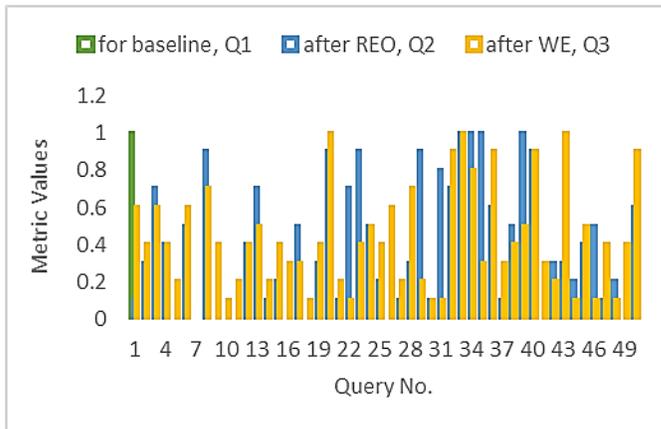


Fig. 7. P@10 of 50 Queries.

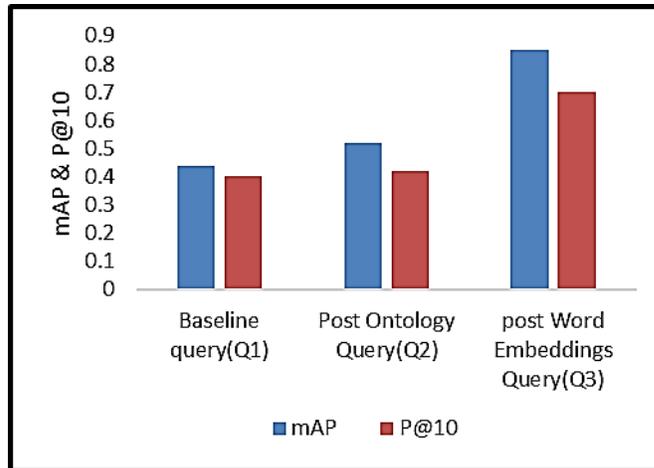


Fig. 8. Graph showing Calculated MAP & P@10.

TABLE II. SAMPLE OF P@10 METRIC FOR ALL 50 QUERIES

P@10	Query No.	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	for baseline, Q1		0.1	0.3	0.7	0.4	0	0.5	0	0.9	0	0	0	0.4	0.7	0.1	0.2	0	0.5	0	0.3
after REO, Q2		0.6	0.4	0.6	0.4	0.2	0.6	0	0.7	0.4	0.1	0.2	0.4	0.5	0.2	0.4	0.3	0.3	0.1	0.4	1
after WE, Q3		0.7	0.6	1	0.5	0.7	0.5	0.1	0.8	0.6	0.6	0.6	0.7	0.8	0.8	0.4	0.6	0.5	0.3	0.8	0.8

TABLE III. IMPROVEMENT IN MAP & P@10

Metric Used	Baseline query(Q1)	Post Ontology Query(Q2)	post Word Embeddings Query(Q3)
mAP	0.44	0.52	0.85
P@10	0.4	0.42	0.7

V. CONCLUSION

Improving the process of information retrieval for efficient retrieval of web documents with high precision has been an ever-going process. Numerous methods have been developed from time to time be it traditional Boolean models or vector state models or even probabilistic models. Each of them was more concerned with queries having keyword matching and had very little understanding of the semantics or context of the query formed.

Query expansion that includes the reformulation of the user query showing better IR results has been a promising solution. The proposed algorithm, WeOnto works on same query expansion and suggests using a two-step procedure that uses ontologies and word embeddings. The ontology gives semantically enriched keywords for the user-query tokens whereas Word2Vec model learns from the given corpus and give most similar words for the said tokens. The best keyword from the entire set is extracted to form the final reformulated query that gave remarkable results and increased precision of the web documents retrieved. In future, instead of word embeddings, sentence-based embeddings can be devised. Also, as the embeddings are shallow unsupervised NLP techniques, the learning of the model can be improved by growing the size of the corpus.

REFERENCES

[1] Q. Liu, H. Huang, J. Lut, Y. Gao and G. Zhang, "Enhanced word embedding similarity measures using fuzzy rules for query expansion", 2017 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), 2017, pp. 1-6, doi: 10.1109/FUZZ-IEEE.2017.8015482.

[2] M. Zhang, Y. Liu, H. Luan, M. Sun, T. Izuha and J. Hao, "Building Earth Mover's Distance on Bilingual Word Embeddings for Machine Translation", AAAI'16: Proceedings of the Thirtieth AAAI Conference on Artificial Intelligence, Arizona, February 2016, pp. 2870–2876.

[3] Qiu D, Jiang H and Chen S., "Fuzzy Information Retrieval Based on Continuous Bag-of-Words Model", Symmetry. 2020; 12(2):225. <https://doi.org/10.3390/sym12020225>.

[4] Phan H.T., Nguyen N.T., Musaev J., Hwang D. , "A Method for Improving Word Representation Using Synonym Information", In: Paszynski M., Kranzlmüller D., Krzhizhanovskaya V.V., Dongarra J.J., Sliot P.M. (eds) Computational Science – ICCS 2021. ICCS 2021, Lecture Notes in Computer Science, 2021, vol 12744. Springer, Cham. https://doi.org/10.1007/978-3-030-77967-2_28.

[5] Siriguleng, "Mongolian Information Retrieval Method Based on Word2vec and Topic Model," 2019 IEEE 4th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC), 2019, pp. 1217-1220, doi: 10.1109/IAEAC47372.2019.8997588.

[6] Wang, B., Wang, A., Chen, F., Wang, Y., and Kuo, C., "Evaluating word embedding models: Methods and experimental results.", APSIPA Transactions on Signal and Information Processing, 2019, 8, E19. doi:10.1017/ATSIP.2019.12.

[7] B. Mansurov and A. Mansurov, "Development of Word Embeddings for Uzbek Language", Computation and Language (cs.CL), Sep2020, <https://arxiv.org/abs/2009.14384v1>.

[8] Y. H. Farhan, S. A. M. Noah, M. Mohd and J. Atwan, "Word Embeddings-Based Pseudo Relevance Feedback Using Deep Averaging Networks for Arabic Document Retrieval", Journal of Information Science Theory and Practice, vol 9, no. 2, pp. 1-17, June 2021, DOI: 10.1633/JISTaP.2021.9.2.1.

[9] El Mahdaouy, A., El Alaoui, S.O. & Gaussier, E., "Improving Arabic information retrieval using word embedding similarities", International Journal of Speech Technology, 21, 121–136 (2018). <https://doi.org/10.1007/s10072-018-9492-y>.

[10] E. H. Mohamed and E. M. Shokry, "QSST: A Quranic Semantic Search Tool based on word embedding", Journal of King Saud University - Computer and Information Sciences, Jan 2020, <https://doi.org/10.1016/j.jksuci.2020.01.004>.

[11] J. Ren, H. Wang, and T. Liu, "Information Retrieval Based on Knowledge-Enhanced Word Embedding Through Dialog: A Case Study", International Journal of Computational Intelligence Systems, Volume 13(1), pp 275-290, 2020 <https://doi.org/10.2991/ijcis.d.2003.10.002>.

[12] V. Jayawardana et al., "Semi-supervised instance population of an ontology using word vector embedding," 2017 Seventeenth International Conference on Advances in ICT for Emerging Regions (ICTer), 2017, pp. 1-7, doi: 10.1109/ICTER.2017.8257822.

[13] J. J. L-Díaz, J. Goikoetxea, M. A. H. Taieb, A. G.-Serrano, M. B. Aouicha, and E. Agirre, "A reproducible survey on word embeddings and ontology-based methods for word similarity: Linear combinations outperform the state of the art", Engineering Applications of Artificial Intelligence, volume 85, pp 645-665, 2019, <https://doi.org/10.1016/j.engappai.2019.07.010>.

[14] Aubaid, M. Asmaa, and A. Mishra, "A Rule-Based Approach to Embedding Techniques for Text Document Classification" Applied Sciences, Vol. 10, no. 11: 4009, 2020, <https://doi.org/10.3390/app10114009>.

[15] D. Jatnika, M. A. Bijaksana, A. A. Suryani, "Word2Vec Model Analysis for Semantic Similarities in English Words", 4th International Conference on Computer Science and Computational Intelligence 2019 (ICCS2019), Procedia Computer Science, Volume 157, Pp.160-167, 12-13 September 2019.

[16] T. Mikolov, K. Chen, G. Corrado, J. Dean, "Efficient Estimation of Word Representations in Vector Space", Computation and Language (cs.CL), 2013, arXiv:1301.3781 [cs.CL].

[17] H. K. Azad and A. Deepak, "Query expansion techniques for information retrieval: A survey", Information Processing & Management, Volume 56, Issue 5, Pages 1698-1735, 2019, ISSN 0306-4573, <https://doi.org/10.1016/j.ipm.2019.05.009>.

[18] N. Rastogi, P. Verma and P. Kumar, "Evaluation of Information Retrieval Performance Metrics using Real Estate Ontology," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 102-106, 2020, doi: 10.1109/ICSSIT48917.2020.9214285.

[19] G. Besbes and H. Baazaoui-Zghal, "Fuzzy ontology-based Medical Information Retrieval," 2016 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE), pp. 178-185, 2016, doi: 10.1109/FUZZ-IEEE.2016.7737685.

[20] N. Rastogi, P. Verma, P. Kumar, "Ontological Design of Information Retrieval Model for Real Estate Documents", In: Chaudhary A., Choudhary C., Gupta M., Lal C., Badal T. (eds) Microservices in Big Data Analytics. Springer, Singapore., 2020.

[21] N. Yusuf, M. A. M. Yunus, N. Wahid, A. Mustapha, and M. N. M. Salleh, "A Survey of Query Expansion Methods to improve Relevant Search Engine Results", International Journal on Advanced Science, Engineering and Information Technology, Vol 11, No 4, pp 1353-1359, 2021, <http://dx.doi.org/10.18517/ijaseit.11.4.8868>.

[22] S. D. Kok and F. Frasinca, "Using Word Embeddings for Ontology-Driven Aspect-Based Sentiment Analysis", SAC '20: The 35th ACM/SIGAPP Symposium on Applied Computing, pp 834-842, Sep 2020, <https://doi.org/10.1145/3341105.3373848>.

A Novel Integrated Scheme for Detection and Mitigation of Route Diversion Attack in MANET

H C Ramaprasad¹

Research Scholar
Visvesvaraya Technological University
Belagavi, Karnataka, India

S.C. Lingareddy²

Professor and Head
Department of Computer Science and Engineering
SVCE, Bengaluru, Karnataka, India

Abstract—With the involvement of Mobile Adhoc Network (MANET) in many upcoming technologies and applications, there is an increasing concern about secure data transmission. Until the last decade, various solutions have evolved to circumvent this threat; however, the security issue is still a more significant threat. The problems studied during the review are usage of Complex Cryptographic Usage, Less Energy Efficient, Fewer studies towards Route Diversion Attack, and Less Emphasis towards Securing Beacon. An analytical method has been used to study these problems. This paper introduces a novel scheme that carries out dual operation viz. i) assessing the link legitimacy for detection of route diversion attack, and ii) cost-effective countermeasures for the same attack. The key findings of proposed study is token generation process when associated with link legitimacy offers more routing security from various ranges of threats. The broader implication of this finding is that proposed system when characterized by lightweight encryption operation, it is capable of excelling better balance between data transmission and security performance unlike existing security solutions in MANET.

Keywords—Mobile Adhoc network; route diversion attack; routing attack; link legitimacy; encryption

I. INTRODUCTION

Mobile Adhoc Network (MANET) offers a decentralized network of connected mobile nodes and can perform communication using any dependency towards infrastructure [1]. These mobile nodes are characterized by the formation of dynamic topology and have limited processing and storage capability. Secure routing among these mobile nodes is the better option to protect the communication in MANET. At present, there are various forms and taxonomies of secure routing protocol in MANET [2]-[4]. Each has its advantage as well as its limitations. The target of secure routing in MANET is to offer data protection from various potential threats in MANET in the complaint of security standards, i.e., non-repudiation, integrity, confidentiality, availability, authentication [5]. There are multiple types of reported attacks in MANET where the potential threats are classified into rushing attacks, fabrication attacks, impersonation attacks, and modification attacks [6]. Some of the potential attacks that target routing process in MANET are classified as i) common routing attacks -Cache poisoning attack over routing, Rushing attack, Packet replication attack, Overflow attack on routing table, and Poisoning attack on routing table, and ii) advanced attack-location disclosure attack, resource consumption attack,

flooding attack, black hole attack, sleep deprivation attack [7]. Some of the conventional solutions to mitigate such attacks are Secure Efficient Ad-hoc Distance Vector, Ariadne, Secure Routing Protocol, Authenticated Routing for Ad-hoc Network, and Secure Ad-hoc On-Demand Distance Vector Routing [8]. Out of all this existing secure routing scheme, there is also much talk about the benefits of Optimized Link State Routing (OLSR) because of its beneficial communication features viz. i) confirms minimal delay in data transmission in MANET, ii) independent of any form of centralized scheme for managing data transmission and hence more suitable in MANET, iii) highly adaptable to dynamic changes in topology in MANET, and iv) freedom from link reliability for transmitting control message [9]. Owing to this reason, the adoption of OLSR is preferred compared to its other counterpart routing methodologies in MANET [10]. However, the adoption of OLSR in secure routing in MANET has seen very few research-based approaches in recent times. Some of the challenges that OLSR encounters when integrated with conventional encryption protocols are i) increased memory as it retains all information of routes and hence highly vulnerable for any routing attacks in MANET, ii) increased overhead with an increase of mobile host due to inclusion of encryption while it uses two different message, i.e., hello packet and topology control message, iii) not applicable for time-critical application as a considerable amount of time is required for an OLSR to identify faulty links, and iv) conventionally, OLSR demands more energy to perform route discovery process and hence when integrated with encryption, it consumes more power.

Therefore, this paper offers a solution meant to introduce a secured OLSR for resisting routing attacks considering the use case of route diversion attacks in MANET. It applies a lightweight encryption model, unlike any existing secure routing scheme. The model contributes towards a novel key management scheme without using any complex encryption scheme. The idea is to balance security demands without affecting the communication performance of mobile nodes. The paper organization is as follows: Section II discusses the existing literature followed by research problem in Section III. Methodology is discussed in Section IV, system design is discussed in Section V. Result is briefed in Section VI, while Section VII highlights outcome discussion, Section VIII makes conclusive remarks while Section IX briefs about future research direction.

II. REVIEW OF LITERATURE

At present, various routing-based attacks are targeting to disrupt the communication system in MANET. It is also found that routing attack leads to incoming of multiple other forms of attacks in a decentralized environment in MANET. This section discusses all the practical approaches to mitigate such routing-based intrusion in MANET.

The recent work carried out by Cai et al. [11] have used a trust-based scheme to mitigate route disruption attacks in MANET. This scheme uses evolutionary techniques using the cognitive process of humans to resist such attacks in MANET, mainly meant for internal attackers. The existing system also emphasizes overusing authentication schemes for assessing the legitimacy of the link. The work of Tu et al. [12] has exploited the characteristic of active routing schemes towards resisting route spoofing, byzantine attack, false routing, selective forwarding attack, etc. The study outcome has witnessed a minimal increase in the packet delivery ratio. Jhaveri et al. [13] have used a pattern-based intrusion monitoring scheme over routing attacks leading to eavesdropping. The idea of this work is also to increase the security during the discovery of the routing phase. Route diversion attacks can also be in the shape of a wormhole attack in MANET. The recent work of Tahboush et al. [14] has presented a security scheme using the round trip time to reduce delay and explore the tunnel presented by wormhole attack. The study outcome is found to stop both in-band and out-band attacks by wormhole attackers by controlling the transmission range. The work of Li et al. [15] has presented a scheme capable of identifying the different variants of anomalies in MANET when exposed to a vulnerable routing scheme. The presented scheme presented an allocation and verification of the anomalies present in the dynamic environment of MANET.

The work carried out by Li et al. [16] has used reputation-based attributes to formulate the route. This technique has used a cooperative-based secure on-demand data transmission scheme to differentiate the selfish and malicious behavior of the node. The work carried out by Dhananjayan and Subbaiah [17] has used a trust-based technique to perform a better form of secure routing scheme in Adhoc networks. The uniqueness of this work is about the usage of the mobility model and energy attribute to understand an indicator for security. The work carried out by Mohindra and Gandhi [18] has presented a scheme where a clustering-based operation along with encryption is used for securing the data transmission in MANET. This technique has used a signature generation for a better authentication scheme. The presented method has used elliptical curve encryption to offer security and usage of digital signature. The work carried out by Mohammadani et al. [19] has used a unique access scheme to secure the data transmission in MANET. The unique part of this implementation is that the system uses time synchronization for all the time slots; however, it doesn't assign anything for blackhole attackers owing to the constant time slot.

Discussion about security strength of routing scheme in MANET based on the use of Internet-of-Things (IoT) is carried out by Trivedi and Khanpara [20]. Tripathy et al. [21] have developed an adaptive scheme for protecting the data

transmission scheme in MANET from various attacks. The study presents a consideration of the context-based factors for specific factors to formulate trust values of the nodes. The existing system has also utilized fuzzy logic to address both security and quality of service in MANET. Rajashanthi and Valarmathi [22] carry out the work in such direction. In this study, an on-demand routing scheme along with fuzzy logic is used along with homomorphic encryption. The study has also used a bio-inspired algorithm to obtain a better route. The work carried out by Manjula and Anand [23] has implemented a key exchanged mechanism using Diffie-Hellman. The approach has used advanced encryption standards for encrypting data.

The existing system has presented different variants of approach where routing scheme along with various use-cases are considered for assessing security. The work carried out by Pu [24] has considered securing the communication from the flying Adhoc network to secure jamming and any other form of route disruption attack. It is also claimed by various researchers where reliability is potentially linked with securing communication in MANET. One such significant study has been presented by Liu et al. [25] that considers the cost of transmission and packet delivery ratio followed by evaluation of road weight. However, no significant evidence is found to offer resistivity against attackers. The work of Anand et al. [26] has presented a model capable of identifying the malicious behavior of MANET nodes. According to this scheme, a dynamic model of distributed form is developed along with the misbehavior of mobile nodes in the network to present preventing measures. The work of Smith et al. [27] has harnessed the potential of the existing security scheme capable of secure communication among mobile nodes, access control, and authentication of mobile nodes in MANET. The work carried out by Wang et al. [28] have developed a secure trust-based routing scheme where Petri net is used along with fuzzy logic to ascertain the eligibility of the nodes using OLSR protocol. Doss et al. [29] have presented a scheme for identifying and preventing novice forms of attack in MANET. This technique makes use of a learning approach for understanding the malicious behavior of mobile nodes. Usage of the learning scheme is also observed in Sankaran et al. [30], where the selection mechanism of the neighboring mobile node is secured in MANET. The learning scheme is used for reviewing the secure routing consistency. The following section discusses all the potential limitations explored after reviewing existing schemes of secure routing in MANET.

III. RESEARCH PROBLEM

There are various mechanisms implemented to date to find out if the mobile node is a regular node and malicious node; however, there are few standard and effective research implementations towards exploring the legitimacy of the communication link. The initial implementation is more inclined to identify the precise legitimacy of link; however, the countermeasures offered are based on non-cryptographic mechanisms to ensure cost-effective modeling. Good resistivity cannot be ensured; however, delivering complex cryptographic measures is challenging to implement in WSN. The summarized version of the open end research problems found in existing studies are as follows:

- **Complex Cryptographic Usage:** There is no doubt that cryptographic algorithms offer the potential for resisting attacks in a wireless network. However, when it comes to MANET, the mobile nodes consistently drain energy along with its movement. It demands a novice cryptographic model that is lightweight and less iterative. The majority of the existing encryption mechanism uses extensive essential management operation, which requires the storage of secret keys, which are again vulnerable to various attacks in MANET.
- **Less Energy Efficient:** Existing secure routing schemes are more inclined towards data encryption and less on achieving optimal communication performance concerning data transmission. Majority of the existing techniques demands maximum resources to function in vulnerable scenario in MANET properly. Hence, there is a need for an encryption mechanism that is equally energy efficient when it comes to securing the data transmission scheme in MANET.
- **Fewer studies towards Route Diversion Attack:** Various approaches offer protection from routing-based attacks. But they are precisely not meant for route diversion attacks. To some extent, certain studies were carried out towards resisting wormhole attacks, which also bears nearly similar characteristics to route diversion attacks. However, the actual route diversion attack has received less attention as it is highly dynamic in its properties concerning the selection of the victim link. Moreover, the absence of any scheme for ascertaining link legitimacy is another reason for the lack of a standard solution towards route diversion attacks in MANET.
- **Less Emphasis towards Securing Beacon:** The complete route discovery process in MANET demands to broadcast its beacon. The attacker quickly captures such beacons, which can disclose various essential information related to application and network topology. Unfortunately, fewer OLSR based secure routers have addressed this problem in the last five years in MANET. The existing approaches don't emphasize protecting the beacons.

IV. RESEARCH METHODOLOGY

The proposed study continues our prior model SRDP [31], presenting a solution towards resisting route diversion attack. This work adds up furthermore lightweight security operations to offer more resilience. The implementation mechanism is highlighted in Fig. 1 as shown.

On top of SRDP architecture [31], the proposed system introduces a novel initialization stage where a sequential countermeasures process is carried out. The first stage of countermeasure is carried out by assessing the vulnerability in the link in MANET. In contrast, the second level of assessment is carried out considering multiple entity-based and entity-based single evaluations. The former type uses a mobile node and trusty third party while the latter uses only a mobile node

to carry out an assessment. The proposed scheme uses homomorphic encryption to encrypt the data, followed by a series of encryption processes unlike any existing approach of resisting route diversion attacks. The experiment of this logic has been performed in MATLAB environment where the algorithms are written in the form of function, which will executed offers the results discussed in result section. The main target of the proposed system is to develop an analytical model that can identify route diversion attacks and mitigate them using a cost-effective optimal solution. The following section further elaborates on design and algorithm.

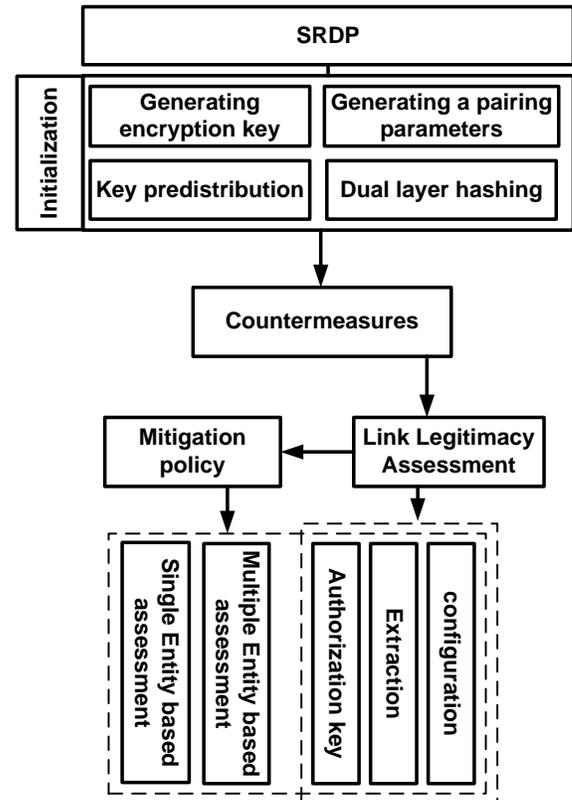


Fig. 1. Proposed Implementation Scheme.

V. SYSTEM DESIGN

This section discusses the essentials of the design aspects involved in the proposed implementation. The complete performance is classified into two stages where the first stage of implementation is wholly focused on generating the link legitimacy. In contrast, the second stage of implementation is focused on mitigating the intruder in the MANET environment. The elaborated discussion of both the implementation modules in the proposed system is as follows:

A. Algorithm for Link Legitimacy Token Generation

This algorithm is responsible for assessing the score of the vulnerability of the communication link among the mobile nodes in the dynamic environment of MANET. The idea is mainly to ensure that all the communicating links are secure enough to perform communication. The steps of the proposed algorithm are as follows:

Algorithm for Link Legitimacy Token Generation

Input: n_t (transmitting mobile nodes), Φ (core authority key)

Output: ψ (link legitimacy token)

Start

1. **For** $i=1:n_t$
 2. $S \rightarrow n_t[\Phi, \pi]$
 3. $n_t(\Phi) \rightarrow \lambda_{ID}$
 4. $n_t(B, ts, \tau) \rightarrow \psi$
 5. **For** $\psi = \text{valid}$
 6. $n_2(ID, B, \psi) \rightarrow \text{flag } \textit{accept}$
 7. **Else**
 8. $n_2(ID, B, \psi) \rightarrow \text{flag } \textit{reject}$
 9. **End**
- End**
-

This algorithm takes the input of transmitting mobile nodes n_t , core authority key Φ that after processing yields an outcome of link legitimacy token ψ . There are four sets of operations being carried out by this algorithm. The first set of actions of the algorithm is to carry out the configuration of essential actors present in the simulation study. Considering all the transmitting mobile nodes (Line-1), this algorithm lets a sink node generate a core attribute key Φ along with an attribute for private key generation π . All this information is then forwarded to the transmitting mobile node (Line-2). This completes the configuration step before the development of the communication model. The next set of actions for the proposed system is to perform an extraction of security information. In this process, the transmitting mobile node generates the authorization key τ associated with the identity ID using the core authority key Φ . This operation is related to the identity considered for the mobile transmitting mobile node (Line-3). After this operation, the proposed system feels a beacon B, timestamp ts, and an authorization key τ , the transmitting mobile node generates a link legitimacy token ψ (Line-4). The next operation step involves assessing the link legitimacy token by the receiving node n_2 , which flags the outcome of acceptance of the validated link legitimacy token (Line-6) or invalid link (Line-8).

In this part of the proposed scheme, identity concatenated with time is considered a public key where the successive interval of times is obtained by the division of time. Further, homomorphic encryption is utilized to carry out the data where a dual hash function is used, viz. i) the first hash function is used for mapping the strings in the group while ii) the second hash function is used for mapping the random inputs. The first step in the process of link verification is extracting security information associated with it. The receiver node computes the private key.

$$\lambda_{\text{receiver}} = \text{hash}(\text{ID}_{\text{receiver}} \parallel t_s) \quad (1)$$

The expression (1) highlights the private key generated by the leader node LN. The next process is the mechanism of assessing the authorization key, which is generated as follows:

$$\tau_{\text{receiver}} = \text{generator}^r \quad (2)$$

In the above expression (2), the proposed system uses a generator considering r as a natural random number. Further,

the system carries out concatenation of the broadcasted beacon along with its identity, timestamp, the security validation token of the receiver node over the ciphered data, and encrypted data. The computation of the security validation token svt of the receiver node over the ciphered data is carried out as follows:

$$svt = ct. \lambda_{\text{receiver}} + r_{\text{receiver.generator}} \quad (3)$$

In the above expression (3), the variable ct will represent ciphertext. The svt is incorporated within the data to ensure that no intruder could test the legitimacy of the link apart from the regular receiver node. The final step of this process is to assess the link legitimacy by the receiver node. For this purpose, the timestamp is evaluated concerning the current interval of time for the receiver node to find the freshness of the data received. After that, further computation is carried out by the receiver node:

$$\text{Generator}_{\text{receiver}} = A. e(\text{B-generator}_{\text{public}}) \quad (4)$$

In the above expression (4), the generator of the receiver is calculated concerning the following dependable parameters viz. i) $A = (svt, \text{generator})$, ii) $B = \text{hash}(\text{ID}_{\text{receiver}} \parallel t_{s_{\text{receiver}}})$. If the condition is found to be validated concerning legitimate link, further expression (4) is progressively computed to yield an amended version of a conditional check as follow, which is if the value of $\text{hash}(ct_{\text{receiver}} \parallel t_{s_{\text{receiver}}} \parallel \tau_{\text{current}})$ is equivalent to $\text{hash}(ct_{\text{receiver}} \parallel t_{s_{\text{receiver}}} \parallel \tau_{\text{old}})$, then the proposed system considers the link to be legitimate link and the message received from the link has higher data integrity. This message is further transmitted to another mobile node. Upon failure of this condition, all the communication with this link is aborted, and a new link is searched. From a security viewpoint, it can be seen that dependable parameters in all the mathematical expressions are entirely different. Hence, even if the message falls in intruder captivity, they will not find any link legitimacy information. Therefore, the algorithm offers a more straightforward link legitimacy assessment in MANET.

B. Algorithm for Countermeasure for Intruder

This algorithm continues the prior algorithm, which inherits its characteristics followed by mitigation strategy and targets towards mitigating the threat. The prior algorithm is about threat identification, while the second algorithm optimizes the first by incorporating mitigation measures. The steps of the proposed algorithm are as follows:

Algorithm for Countermeasure for Intruder

Input: n_t, Φ

Output: ψ_{me} / ψ_{se}

Start

1. **For** $i=1:n_t$
2. $S \rightarrow n_t[\Phi, \pi]$
3. $\text{LN}(\pi, ts) \rightarrow \psi_{me}(n_{\text{leaf}})$
4. $n_{\text{leaf}}(\lambda_{ID}, B) \rightarrow \psi_{se}$
5. **For** $\psi = \text{valid}$
6. $n_2(\text{ID}, B, \psi_{se}) \rightarrow \text{flag } \textit{accept}$
7. **Else**
8. $n_2(\text{ID}, B, \psi_{se}) \rightarrow \text{flag } \textit{reject}$
9. **End**

End

The algorithm mentioned above takes the input of transmitting mobile nodes n_i and core authority key Φ that, after processing, yields an outcome of link legitimacy token with multiple-single entity ψ_{me} / ψ_{se} . This algorithm poses a similar configuration and extraction process as discussed in the prior algorithm for legitimacy check of link. The different operation carried out by this algorithm starts from Line-3. In this case, the algorithm performs two sets of novel operations, i.e., single entity assessment se and multiple entity assessment me . Numerous entities carry out the mechanism of the generation of the authorization key. In this case, the leader node LN generates link legitimacy token ψ_{me} using the attribute for private key generator π and time stamp ts (Line-3). This link legitimacy token is then forwarded to the mobile lead nodes in its group.

On the other hand, the algorithm also performs a single entity assessment where the transmitting leaf node n_{leaf} generates a link legitimacy token based on private key $\lambda_{ID(me)}$ and beacon B (Line-4). The final validation step is carried out from Line-5 onwards, where the mobile receiver node, i.e., n_2 , flags either acceptance or rejection based on the validated link legitimacy token. It should be noted that dependable parameters for this are carried out based on identity ID, beacon B, and link legitimacy token ψ_{se} . This completes the operation of the proposed algorithm.

This algorithm mainly targets to reduce the possible overhead in the prior algorithm for identifying the degree of threat where the functionalities of distribution of security token are revised as follows: the prior algorithm assigns an attribute for private key generator with the highest number of parameters, i.e., encryption key, beacon, pairing parameters (elliptical curve, finite field), two discrete cyclic groups, bilinear map, global and local hash, generator, random integer. This algorithm uses a reduced number of parameters, i.e., encryption key, beacon, cyclic group, order of the cyclic group, random integer, random number of master key, and global hash. Similar homomorphic encryption is used in this part of the algorithm when the beacon B is transmitted to LN. In this algorithm, the receiver node obtains the private key from the core authority key Φ (randomly considered integer value) and node identity. The computation of the private key λ for receiver node uses two dependable attributes, e.g., k_1 and k_2 , where k_1 is equivalent to the randomly selected generator from the multiplicative group and k_2 is expressed mathematically as follows:

$$k_2 = \text{rand}_{\text{receiver}} + \text{hash}(k_1, \text{ID}_{\text{receiver}}).B \quad (5)$$

In the above expression (5), the first component is a random number of mobile receiver nodes. In contrast, variable B of the second component represents a random natural integer (assuming it as core attribute key) and modulus of pairing parameter. The following process is for the usage of multiple entity-based assessments. A secure validation token svt' is generated by the receiver node along with the timestamp of transmission. This information is stored for carrying out a single entity-based assessment during beacon transmission. The mathematical expression of svt' is as follows:

$$svt(me) = 1 / \text{generator}^{ts} \quad (6)$$

The above expression is used for multiple entity assessment. The proposed algorithm also carry out a single entity assessment of vulnerability where a receiver node computes the link legitimacy token based on svt obtained in prior algorithm and randomly selected integer towards the encrypted data where svt' is created as follows:

$$svt(se) = \text{generator}^{svt} \quad (7)$$

The beacon is then forwarded by the mobile receiver node, the timestamp, randomly selected generator, and svt of a single entity. The beacon carries out the following information, i.e., the identity of the receiver node, timestamp, randomly selected generator. Finally, the algorithm proceeds towards the validation operation where all the mobile nodes perform validation of the received beacon. It starts with assessing the current time stamp, then computation of generator and product of svt randomly selected generator, and a random number. The proposed system also set a condition as follows:

$$\mu_1 = svt. \mu_2. \mu_3 \quad (8)$$

In the above expression (8) for the conditional check, the variable μ_1 represents the mobile receiver node generator. In contrast, the variable μ_2 represents hashing of the random generator, and the variable μ_3 represents the random integer to the power of the hashed value of μ_2 and identity of the receiver node. A closer look at this algorithm's internal operation showcase that the proposed system introduces complex attributes for the attackers to perform intrusion. It is a complex process as the attacker will be required to decode multiple interconnected hashing operations with unknown variable definitions. The following section discusses the outcomes of the study.

VI. RESULT ANALYSIS

This section discusses the outcomes obtained from implementing the algorithms discussed in the prior section. Scripted in MATLAB, the observations were carried out considering the following simulation parameters: i) several mobile nodes 1400, ii) initialized energy is 10J, iii) Size of the message is 1000 bytes, iv) total simulation rounds is 1000. The implementation environment involves the dispersion of mobile nodes in random order over a 1000x1000 m² simulation area. The mobile nodes form a group, and each group is assigned a leader node based on higher residual resources. The leader node carries out all the communication from one group to another, while a normal mobile node itself carries out communication within a group. The proposed system claims security in MANET considering the standard OLSR protocol; the comparison is carried out concerning the OLSR protocol. Irrespective of various availability of routing protocol, the justification behind selection OLSR are as following: i) the routing process of OLSR is decentralized and theoretically claimed to offer lower delay; however, still there is an issue with maintaining routing table for all sorts of routes, which is vulnerable for attack in MANET, ii) it offers supportability of dynamic changes in MANET; however, it also witnesses higher beacon overhead and consumes more processing power. Moreover, the proposed study is implemented in order to address such issues in OLSR. To closely observe the outcome,

the proposed method is split into Prop-1 and Prop-2, exhibiting the algorithm for link legitimacy and cost-effective countermeasures. The outcome analysis concerning standard performance parameters in MANET is mainly associated with resource utilizing, delay, and packet delivery ratio.

The first performance parameter used towards investigating the effect on communication performance is resource depleted nodes. After initializing the nodes with energy, there is a decrement in power. The idea of these performance parameters is to check the availability of nodes in the proposed security scheme.

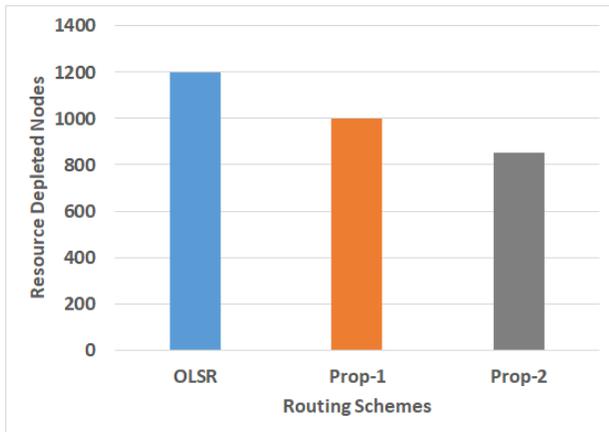


Fig. 2. Comparative Analysis of Resource Depleted Nodes.

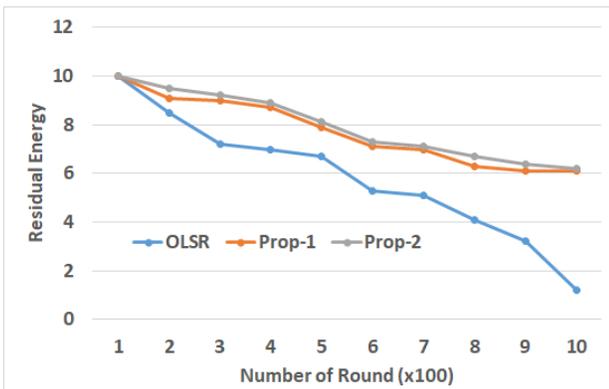


Fig. 3. Comparative Analysis of Residual Energy.

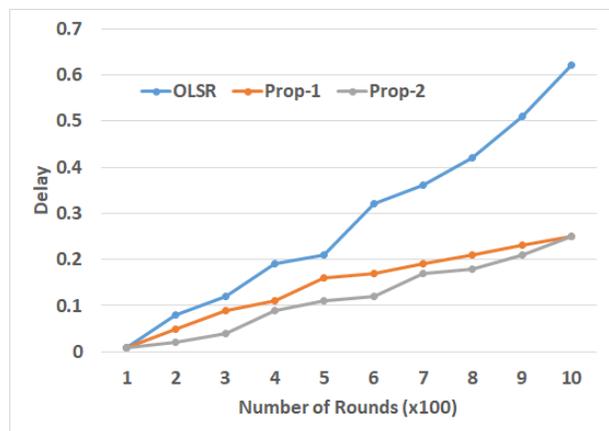


Fig. 4. Comparative Analysis of Delay.

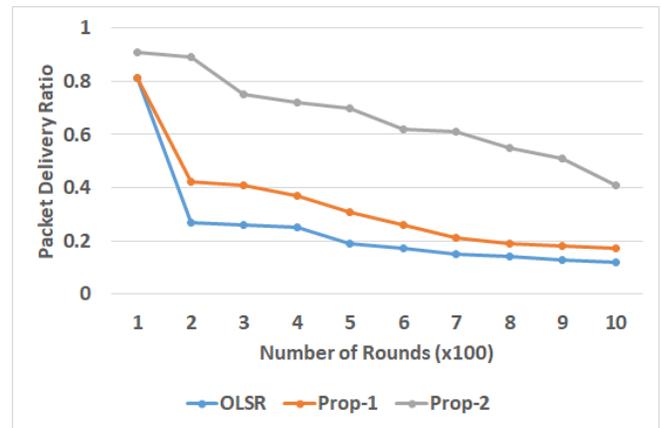


Fig. 5. Comparative Analysis of Packet Delivery Ratio.

Fig. 2 to Fig. 5 represents comparative analysis of the proposed system (with two variants) with the existing standard OLSR protocol with respect to resource being depleted, residual energy, delay, and packet delivery ratio respectively. In every case, the proposed system is witnessed to offer superior outcome in contrast to OLSR protocol.

VII. DISCUSSION

This section discusses about the outcome obtained from the proposed study briefed in prior section.

- Discussion of Resource Depleted Nodes (Fig. 2): The outcome exhibited in Fig. 2 showcases that the proposed system offers better node availability than the existing system. OLSR scheme is much occupied into formulating topology control which increases its resource dependency when the encryption scheme is applied along with OLSR. On the contrary, the Prop-1 scheme also does a similar job finding link vulnerability owing to route diversion attacks. However, this scheme uses more random numbers and generators and more minor encryption operations, leading to lesser resource consumption than OLSR. On the other hand, the extensive usage of parameters in key distribution is further controlled in Prop-2, leading to further saving of resources in contrast to Prop-1. The following associated performance study is towards residual study to validate the prior outcome of node availability.
- Discussion of Residual Energy (Fig. 3): As exhibited in Fig. 3, it can be seen that the depletion of energy for Prop-2 and Prop-1 is far better than the OLSR protocol. This ensures that with the increase of simulation rounds (where traffic load is also increased), the proposed scheme can successfully achieve better retention of energy and better node availability. The following performance parameter understudy is an end-to-end delay, a duration involved in packet transmission from transmitting to receiving mobile nodes in MANET. The outcome of the delay is shown in Fig. 4.

- Discussion of Delay (Fig. 4): The outcome in Fig. 4 exhibits that OLSR offers extensive delay compared to the proposed scheme. The prime reason is the involvement of multi-point relay and extensive cryptographic mechanism; the establishment of the route takes time in the presence of traffic load with increasing simulation rounds. Apart from this, the involvement of time for multi-point relay further adds to more delay. However, an operation carried out in Prop-1 involves conditional checks more and less encryption, which involves less duration. Further, Prop-2 offers the advantage of updating the link legitimacy token with a recent time stamp, which further authenticates the link with the presence of a route diversion attack. This causes lesser dependency on performing repeated route discovery processes in Prop-2. Apart from this, the inclusion of group-based communication also contributes towards lower delay. Finally, the proposed system assesses data forwarding performance via packet delivery ratio computed by cumulative data received at the destination and forwarded by transmitting mobile nodes.
- Discussion of Packet Delivery Ratio (Fig. 5): Fig. 5 showcases that the proposed system offers a better packet delivery ratio in comparison to OLSR. With the depletion of energy, the trend of packet delivery ratio will also degrade. The prime reason behind this outcome is that once the mobile node depletes its energy in OLSR, the number of relay nodes is significantly affected in formulating better routes. A further change of topology also involves time, and hence increasing the number of data when subjected to encryption further takes a slow performance in OLSR. However, this problem is mitigated in the proposed system by group-based communication using a leader node with forwarding aggregated data from its candidate mobile node in the proposed scheme. The difference between OLSR and Prop-1 is that – in OLSR, a single mobile node performs complete data transactions. In contrast, the proposed scheme performs aggregated data transmission via leader node, which saves time and increases the data transmission rate. However, Prop-1 has extensive usage of key management mechanism which is optimized in Prop-2 model and hence, the Prop-2 model offers further better outcomes than the Prop-1 model.
- Discussion of Security Analysis: It is to be noted that although the proposed system is designed towards resisting route diversion attacks, it still offers intrusion prevention capabilities furthermore. Owing to the usage of homomorphic encryption, the proposed method (Both Prop-1 and Prop-2) offers resistance from eavesdropping. Due to a series of dependencies towards the verification process, the proposed system doesn't allow the intruder to decrypt the ciphered beacon and data, ensuring optimal privacy and confidentiality. Apart from this, the encryption process considers identity, which will offer privacy protection for the mobile nodes in MANET. Another interesting

fact is that the proposed system communicates via the leader node, which possesses extensive information to be forwarded or received. Hence, they are more prone to attack. It should be noted that Prop-2 is mainly carried out towards protecting the leader node, while Prop-1 is carried out towards protecting the mobile node. Hence, there is no feasibility of an active attack as well.

VIII. CONCLUSION

Route diversion attack is a severe problem in the dynamic environment of MANET. Irrespective of various research works towards resisting such routing attacks; the existing scheme lacks autonomous precise monitoring and a robust prevention scheme. Hence, the proposed system offers a solution against this problem by introducing an integrated computational model that offers a scheme to confirm link legitimacy and prevent attackers in MANET. The contribution and novelty of the proposed study are as follows: i) The proposed scheme offers an asymmetric essential management technique potential enough to stop eavesdropping along with resisting routing attacks, ii) The proposed model facilitates neighborhood authentication unlike conventional secure OLSR model in MANET, iii) the proposed model uses lightweight encryption mechanism to offer low storage cost and comparatively higher network scalability, and iv) the proposed model offers a good balance between optimal security performance with efficient data transmission performance in MANET.

IX. FUTURE WORK

After reviewing the outcomes and their inference, it has been noticed that with a unique proposed research methodology without using complex form of cryptography. However, there are few questions which are further required to be analyzed viz. i) can memory used for processing secret key be optimized? ii) can any non-encryption based operation be performed on top of this model in order to offer more privacy and further more security? Working towards these questions will be a part of future plan of implementation. The future work of the proposed study is to carry out implementation of bio-inspired algorithm to address the question of memory optimization for secret key processing. Further, trust based stochastic modelling can be carried out in order to address the second question towards deploying non-encryption based approach for offering more privacy and security. Deep learning method can be also further applied in order to generate attack graph in preemptive form prior the actual attack takes place.

REFERENCES

- [1] M. Al Mojamed, "Integrating Mobile Ad Hoc Networks with the Internet Based on OLSR", *Hindawi-Wireless Communications and Mobile Computing*, Article ID 8810761, 2020.
- [2] Kalime, Srinivas & Sagar, K. "A Review: Secure Routing Protocols For Mobile Adhoc Networks (MANETs)", *Journal of Critical Reviews*, vol.7, pp.8385-8393, 2021.
- [3] H. Yang, "A Study on Improving Secure Routing Performance Using Trust Model in MANET", *Hindawi-Mobile Information Systems*, Article ID 8819587, 2020.

- [4] G. M. Borkar; A.R. Mahajan, "A review on propagation of secure data, prevention of attacks and routing in mobile ad-hoc networks", *InderScience-International Journal of Communication Networks and Distributed Systems*, vol.24, No.1, 2020.
- [5] M. S. Sheikh, J. Liang, "Security and Privacy in Vehicular Ad Hoc Network and Vehicle Cloud Computing: A Survey", *Hindawi-Wireless Communications and Mobile Computing*, Article ID 5129620, 2020.
- [6] M. Karthigha, L. Latha and K. Sriprayan, "A Comprehensive Survey of Routing Attacks in Wireless Mobile Ad hoc Networks," *International Conference on Inventive Computation Technologies*, pp. 396-402, doi: 10.1109/ICICT48043.2020.9112588, 2020.
- [7] R. Meddeb, B. Triki, F. Jemili and O. Korbaa, "A survey of attacks in mobile ad hoc networks," *International Conference on Engineering & MIS (ICEMIS)*, 2017, pp. 1-7, doi: 10.1109/ICEMIS.2017.8273007.
- [8] C. Ran, S. Yan, L. Huang & L. Zhang, "An improved AODV routing security algorithm based on blockchain technology in ad hoc network" *EURASIP Journal on Wireless Communications and Networking*, 2021.
- [9] T. K. Priyambodo, D. Wijayanto, and M. S. Gitakarma, "Performance Optimization of MANET Networks through Routing Protocol Analysis", *MDPI-Journal*, vol.10, No.2, 2021.
- [10] Y. Maret, J. -F. Wagen, M. Raza, J. Wang, N. Bessis and F. Legendre, "Preliminary results of OLSR based MANET routing algorithms: OLSRd2-Qx reinforcement learning agents and ODRb," *International Conference on Military Communication and Information Systems (ICMCIS)*, 2021, pp. 1-8, doi: 10.1109/ICMCIS52405.2021.9486409.
- [11] R. J. Cai, X. J. Li and P. H. J. Chong, "An Evolutionary Self-Cooperative Trust Scheme Against Routing Disruptions in MANETs," *IEEE Transactions on Mobile Computing*, vol. 18, no. 1, pp. 42-55, 1 Jan. 2019, doi: 10.1109/TMC.2018.2828814.
- [12] J. Tu, D. Tian and Y. Wang, "An Active-Routing Authentication Scheme in MANET," *IEEE Access*, vol. 9, pp. 34276-34286, 2021, doi: 10.1109/ACCESS.2021.3054891.
- [13] R. H. Jhaveri, N. M. Patel, Y. Zhong and A. K. Sangaiah, "Sensitivity Analysis of an Attack-Pattern Discovery Based Trusted Routing Scheme for Mobile Ad-Hoc Networks in Industrial IoT," *IEEE Access*, vol. 6, pp. 20085-20103, 2018, doi: 10.1109/ACCESS.2018.2822945.
- [14] M. Tabboush and M. Agoyi, "A Hybrid Wormhole Attack Detection in Mobile Ad-Hoc Network (MANET)," *IEEE Access*, vol. 9, pp. 11872-11883, 2021, doi: 10.1109/ACCESS.2021.3051491.
- [15] T. Li, J. Ma, Q. Pei, H. Song, Y. Shen and C. Sun, "DAPV: Diagnosing Anomalies in MANETs Routing With Provenance and Verification," *IEEE Access*, vol. 7, pp. 35302-35316, 2019, doi: 10.1109/ACCESS.2019.2903150.
- [16] Z. Li and H. Shen, "Game-Theoretic Analysis of Cooperation Incentive Strategies in Mobile Ad Hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 11, no. 8, pp. 1287-1303, Aug. 2012, doi: 10.1109/TMC.2011.151.
- [17] G. Dhananjayan & J. Subbiah, "T2AR: trust-aware ad-hoc routing protocol for MANET", *SpringerOpen*, Vol.5, Article No. 995, 2016.
- [18] A. R. Mohindra, C. Gandhi, "A Secure Cryptography Based Clustering Mechanism for Improving the Data Transmission in MANET", *Walailak Journal of Science and Technology*, Vol.18, No.6, 15 March 2021.
- [19] K. H. Mohammadani, K. A. Memon, I. Memon, I. Memom, "Preamble time-division multiple access fixed slot assignment protocol for secure mobile ad hoc networks", *International Journal of Distributed Sensor Networks*, 2020.
- [20] R. Trivedi, P. Khanpar, "Robust and Secure Routing Protocols for MANET-Based Internet of Things Systems—A Survey", *Springer-Emergence of Cyber Physical System and IoT in Smart Automation and Robotics*, pp 175-188, 2021.
- [21] B. K. Tripathy, S. K. Jena, P. Bera & S. Das , "An Adaptive Secure and Efficient Routing Protocol for Mobile Ad Hoc Networks", *Springer-Wireless Personal Communication*, vol.114, pp.1339-1370, 2020.
- [22] M. Rajashanthi & K. Valarmathi, " A Secure Trusted Multipath Routing and Optimal Fuzzy Logic for Enhancing QoS in MANETs", *Springer-Wireless Personal Communications*, vol.112, pp.75–90, 2020.
- [23] T. Manjula & B. Anand, "A secured multiplicative Diffie Hellman key exchange routing approach for mobile ad hoc network", *Springer-Journal of Ambient Intelligence and Humanized Computing*, vol.12, pp.3621–3631, 2021.
- [24] C. Pu, "Jamming-Resilient Multipath Routing Protocol for Flying Ad Hoc Networks," *IEEE Access*, vol. 6, pp. 68472-68486, 2018, doi: 10.1109/ACCESS.2018.2879758.
- [25] L. Liu, C. Chen, B. Wang, Y. Zhou and Q. Pei, "An Efficient and Reliable QoF Routing for Urban VANETs With Backbone Nodes," *IEEE Access*, vol. 7, pp. 38273-38286, 2019, doi: 10.1109/ACCESS.2019.2905869.
- [26] A. Anand, H. Aggarwal and R. Rani, "Partially distributed dynamic model for secure and reliable routing in mobile ad hoc networks," *Journal of Communications and Networks*, vol. 18, no. 6, pp. 938-947, Dec. 2016, doi: 10.1109/JCN.2016.000128.
- [27] D. Hurley-Smith, J. Wetherall and A. Adekunle, "SUPERMAN: Security Using Pre-Existing Routing for Mobile Ad hoc Networks," *IEEE Transactions on Mobile Computing*, vol. 16, no. 10, pp. 2927-2940, 1 Oct. 2017, doi: 10.1109/TMC.2017.2649527.
- [28] X. Wang, P. Zhang, Y. Du and M. Qi, "Trust Routing Protocol Based on Cloud-Based Fuzzy Petri Net and Trust Entropy for Mobile Ad hoc Network," *IEEE Access*, vol. 8, pp. 47675-47693, 2020, doi: 10.1109/ACCESS.2020.2978143.
- [29] S. Doss et al., "APD-JFAD: Accurate Prevention and Detection of Jelly Fish Attack in MANET," *IEEE Access*, vol. 6, pp. 56954-56965, 2018, doi: 10.1109/ACCESS.2018.2868544.
- [30] K. S. Sankaran, N. Vasudevan, K. R. Devabalaji, T. S. Babu, H. H. Alhelou and T. Yuvaraj, "A Recurrent Reward Based Learning Technique for Secure Neighbor Selection in Mobile AD-HOC Networks," *IEEE Access*, vol. 9, pp. 21735-21745, 2021, doi: 10.1109/ACCESS.2021.3055422.
- [31] Ramaprasad, H & Lingareddy, S., "SRDP: Secure Route Diversion Policy for Resisting Illegitimate Request in MANET", *International Journal of Engineering & Technology*, vol.7. No.290. 10.14419/ijet.v7i3.12.16044, 2018.

Multi-level Hierarchical Controller Assisted Task Scheduling and Resource Allocation in Large Cloud Infrastructures

Jyothi S, B S Shylaja

Department of Information Science & Engineering
Dr.Ambedkar Institute of Technology, Bengaluru, India

Abstract—The high-pace emergence in Cloud Computing technologies demands and alarmed academia-industries to attain Quality-of-Service (QoS) oriented solutions to ensure optimal network performance in terms of Service Level Agreement (SLA) provision as well as Energy-Efficiency. Majority of the at-hand solutions employ Virtual Machine Migration to perform dynamic resource allocation which fails in addressing the key problem of SLA-sensitive scheduling where it demands timely and reliable task-migration solution. Undeniably, VM consolidation may help achieve energy-efficiency along with dynamic resource allocation where the classical heuristic methods which are often criticized for its local minima and premature convergence doesn't guarantee the optimality of the solution, especially over large cloud infrastructures. Considering these key problems as motivation, in this paper a highly robust and improved meta-heuristic model based on Ant Colony System is developed to achieve Task Scheduling and Resource Allocation. CloudSim based simulation over different PlanetLab cloud traces exhibited superior performance by the proposed task-scheduling model in terms of negligible SLA violence, minimum downtime, minimum energy-consumption and higher number of migrations over other heuristic variants, which make it suitable towards realistic Cloud Computing purposes.

Keywords—Task-scheduling; VM-migration; improved ant colony system; SLA assurance; energy-efficient consolidation

I. INTRODUCTION

In the last few years, the high-pace rise in advanced software systems and decentralized computing environments has broadened the horizon for a state-of-art new paradigm named cloud computing. Cloud computing has emerged as a potential technology serving decentralized scalable services to the significantly large number of users for respective data and/or query driven computation and information services. Cloud computing technology can be characterized as an array of network-enabled services facilitating quality-of-service (QoS) assured scalable and personalized (computing) solutions, even at the inexpensive cost [1-3]. The potential to serve decentralized data or (computing) infrastructure, independent of the geographical boundaries makes cloud computing an inevitable need to meet contemporary or even NextGen industrial as well as personal computing demands [2]. Based on the usage of the Cloud it is understood that it has been applied as a key technology to serve civic purposes, financial sector, industries, government agencies, scientific community, diverse business houses, etc. Noticeably, to serve aforesaid

stakeholders, cloud services are classified into three key types; Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS). Irrespective of the service types, fulfilling QoS in cloud computing has always remained a challenge. To meet aforesaid service demands industry requires providing decentralized storage infrastructure, often called data centers; however, with exponential rise in computing demands with non-linear (demand or use) patterns, the at-hand solutions often undergo disrupted performance or connectivity. This as a result impacts overall QoS performance. Typically, delivering Service Level Agreement (SLA) by Cloud Service Providers ensures to provide QoS support to its customers while maintaining reliable services with higher scalability, reliability and continuity over operating periods [4, 5]. It is a challenging task to retain SLA over highly dynamic load demands and use patterns across a gigantically large user-base, located around the globe.

A cloud infrastructure mainly encompasses physical machines, also called servers, virtual machines (VMs) and allied controllers. Noticeably, hosts of the physical machines primarily acts as the component serving computing ability and memory, while VMs function as containers possessing different independent tasks. A huge cloud infrastructure may consist of multiple hosts, where each host can have multiple VMs, carrying different parallel-computing tasks. In this case, due to dynamism in resource demands by each task a VM might undergo an exceedingly large resource demand, which could not be facilitated by the currently attached physical machine or host. In such a case, a VM carrying multiple tasks is required to be migrated to the suitable host, which could provide sufficient resources to the associated task for SLA assurance and QoS provision. However, it may take significantly large traversal time or allocation scheduling related delay, impacting downtime and hence overall performance. Being an uncertain demand scenario, the tasks or allied VMs can have to traverse across the network as per at-hand overloading and under-loading scenario. Undeniably, it can increase downtime as well as QoS violation. On the other hand, cloud being an energy-exhaustive technique requires addressing energy-minimization needs and therefore simultaneous dynamic resource allocation, task scheduling and energy minimization turn out to be a complex NP-hard problem [1-5]. In sync with cloud with the heterogeneous demand types, the load pertaining to each VM might vary as per task-types and demand-density over the operating period.

Therefore, merely random host selection concepts or even the classical bin-packing models, cannot be appropriate. Such classical methods might give rise to the overloading or underloading condition, and hence can impact both SLA as well as energy-efficiency.

With this context, the research work proposes a “Multi-Level Hierarchical Controller Assisted Dynamic Task Scheduling and Resource Allocation Model for Large Cloud Infrastructures” which involves a hybrid evolutionary concept named Improved Ant Colony System (I-ACS) to achieve SLA with energy efficiency to meet cloud demands. The proposed model is developed using CloudSim platform, where simulation over PlanetLab cloud trace data revealed superiority of the proposed model over major existing approaches in terms of downtime, SLA violation, number of migrations and energy-consumption.

The further sections of the presented document are given as follows. Section II discusses the Literature Survey pertaining to SLA oriented and Energy-Efficient task-scheduling methods, Section III discusses the proposed method followed by Section IV which provides Results and Discussion. The overall research Conclusion and allied inferences are presented in Section V. References followed in this research are provided at the end of the manuscript.

II. RELATED WORK

Afzal et al. [6] focuses on Load balancing based heuristic assisted task scheduling concept under static or dynamic load conditions. However, unlike classical static resource allocation that employs a first-come-first-served method, it can't be suitable under dynamic load conditions. Pradhan et al. [7] discusses about modifying especially round robin methods, which authors applied in their research to reduce the waiting time. Mogeset al. [8] focused on energy efficiency as the key concept to perform task scheduling. To reduce energy-exhaustion, authors proposed VM consolidation concept, which was performed to shut-down underutilized hosts and by removing hotspots. However, the classical use of bin-packing based consolidation could not address latency and QoS degradation issues. In addition to the power enhancement, the work suggested to perform consolidation scheduling in such a manner that it could retain lower task response time to meet SLA demands. To achieve it, authors suggested to focus on modified bin-packing based consolidation.

Syed Arshad Ali et al. [9] implemented task scheduling using Resource aware min- min algorithm where task-scheduling was performed on the basis of the load of the servers to minimize makespan. Mosa et al. [10] on the other hand emphasized on load balancing in the cloud by distributing the workload dynamically across the cloud infrastructure with multiple nodes. Authors applied utility functions and GA heuristic model to optimize VM allocation, Energy consumption and SLA violations. Jyothi S et.al. [18] Bhaskar R et.al [19] discussed numerous key challenges in dynamic load management in heterogeneous cloud environments. Authors proposed a heterogeneity- aware dynamic application provisioning model to reduce energy consumption in cloud environments.

Doppaet al. [11] designed a self-aware framework to adjust or optimize resource and SLA. However, the use of DVFS based methods can't be suitable for a heterogeneous cloud network with dynamic load conditions. In addition to the SLA expectations, authors [12 -13] focused on resource allocation while maintaining lower computation and energy-exhaustion. Liet al. [12] designed a directed acyclic graph (DAG) model to perform priority bound task scheduling. Here, in DAG construction the nodes characterize the tasks, while the edges represent the allied messages among jobs [14-16]. Tang et al.[14] applied DAG-based workflow where tasks were prioritized based on respective sizes to perform resource allocation. Zhu et al. [17] Jyothi et al. [18] performed task scheduling on the different multiprocessing environment, which can be solved using NP-hard optimization. Considering this as motivation, dynamic task-scheduling and resource allocation is performed by applying the concepts of co-evolution system and multi-population strategy for Meta-heuristic method such as ACO is considered.

III. SYSTEM MODEL

This discussion primarily discusses the proposed model and its implementation including the multi-controller assisted overload and underload detection, VM selection and the proposed Improved Ant Colony System (I-ACS) based task scheduling.

The task scheduling or allied VM migration can be inducted as per the task-(heterogeneous) demands' and hence a controller can migrate one or multiple VMs to the suitable hosts (via consolidation) while retaining SLA performance and energy-efficiency. The proposed model introduces multi-layered controller units to dynamically monitor the VMs and allied task's demand to stochastically predict the demands and accordingly the global controller performs scheduling in advance to avoid any SLA violation, QoS-compromise or even energy-exhaustion.

The overall proposed model encompasses four key steps. They are:

Step-1 Hierarchical Multi-layered controller assisted cloud monitoring,

Step-2 Underload and Overload detection,

Step-3 Minimum Migration Time (MMT) oriented VM selection,

Step-4 Improved ACS (I-ACS) assisted S-DTS

The details of the overall proposed model are given in the subsequent sections.

Hierarchical Multi-layer Controller assisted Cloud Monitoring.

An illustration of the different controller and its respective task is given in Fig. 1.

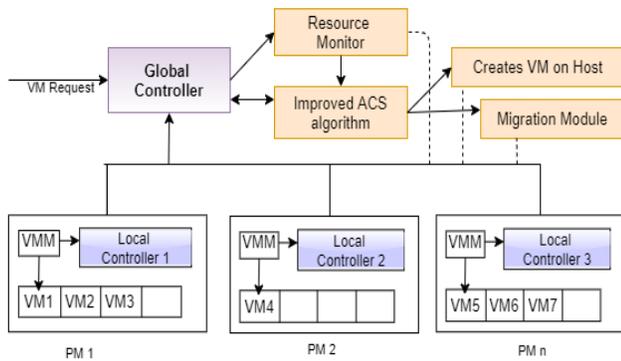


Fig. 1. Proposed Multi-controller Assisted Cloud Monitoring and Task-Scheduler.

Typically, cloud infrastructures that often accommodate a significantly large number of independent tasks operating or executed onto assigned VMs, undergo exceedingly high demand-dynamism. In other words, the different tasks connected to each VM undergo non-linear traffic demands, and therefore might require dynamic resource to continue its operation. Under such scenario, a VM encompassing single or multiple tasks might exhibit non-linear resource demand, influencing a host or physical machine to undergo under-utilization or overloading. Consequently, it might significantly impact the overall performance and SLA-reliability of the system. Considering this fact, performing demand-sensitive resource allocation or task-scheduling is must. To achieve it in the proposed method, a state-of-art new Hierarchical Multi-Layered Controller (HMLC) design is applied, which especially monitors demands or resource utilization pattern at each task connected to a VM. The proposed HMLC model encompassed a local controller and a global controller, especially designed to perform task-scheduling or dynamic resource allocation so as to preserve SLA, QoS as well as energy-efficiency. To perform task-level resource utilization assessment, local controller (LC) is applied that measures resource utilization per VM and updates the same to the global controller (GC), dynamically so as to make stochastic prediction-based task-scheduling decision in advance.

As shown in Fig. 1, the proposed local controller unit operates over each VM, accommodating multiple tasks. Here, it acts as an autonomous VMM manager that measures resource utilization dynamically and updates to the global controller so as to make dynamic task reallocation. Additionally, the proposed controller mechanism enables dynamic underload/overload detection and (proactive) avoidance. Once detecting any hotspot or any PM undergoing overload, the local controller executes VM selection mechanism (discussed in subsequent section) and selects the VM to be unloaded from the at-hand overloaded hosts. However, recalling the SLA assurance to the offloaded VM and allied tasks, the proposed model introduces a state-of-art new and robust dynamic VM scheduling model which guarantees optimal task-scheduling and allied VM migration, without affecting SLA performance. To achieve it, the proposed global controller model retrieves VM's and hosts' information proactively from the local controller and executing the proposed I-ACS concept it schedules VM placement or

migration in advance so as to retain SLA intact. Once traversing or offloading the suitable VM from a host, the local controller updates the node-parameters and updates the same to the global controller for further decision making. To achieve SLA-assurance and energy-efficiency, at first, a dynamic threshold-based underload and overload detection unit is applied. The details are given as follows.

A. Underload and Overload Detection

To cope up with the dynamic resource demands and allied scheduling tasks, the work is carried out which examines the load condition of each task and associated host that helps in identifying under-loaded and overloaded nodes in the network. To ensure SLA-sensitive and energy-efficient scheduling, once detecting a node as under-loaded either certain specific VM (including all connected tasks) or all VMs are off-loaded, which are then migrated to the other suitable hosts. This approach not only helps in optimal resource allocation, but also preserves significant energy. On the other hand, detecting a host undergoing overload, the proposed model offloads tasks or allied VM(s) and migrates them to the other suitable host, while ensuring that the migration doesn't cause overload on another host (say, target host) or impacts SLA performance.

1) *Underload detection:* The proposed model discusses a host with load lower than a predefined minimum workload condition or resource utilization is referred as an underload host. In order to preserve energy, once identifying a host with under-utilized resources, it's connected VMs or allied tasks are migrated to the other host(s) strategically. However, this scheduling or migration takes place in such a manner that it doesn't cause overload on other nodes or hosts. In sync with the concept of VM consolidation, once migrating all VMs to the other host, successfully, it shuts down the host to preserve the energy. Here the task-migration or allied resource allocation strategy schedules the migration in such a manner that neither it causes SLA violation nor energy exhaustion or any possible overload situation on the target host. To guarantee SLA provision, the source host remains active or ON, until all allied tasks and the target host(s) holds the migrated connected VMs.

2) *Adaptive threshold-sensitive host overload detection:* To detect the overloaded VM (containing independent tasks), a stochastic prediction assisted approach is applied. In this each host node performs periodic load assessment of each host which eventually assists detecting an overloaded node. Here, each host's resource (i.e., CPU or MIPS) utilization is measured to assess the host node whether it is overloaded or not. Most of the existing approaches towards task-scheduling apply a static threshold method to detect an overloaded host. Unfortunately, IaaS which often undergoes dynamic loads over the operating period and the different tasks consume different resources at the varied time-instant. Therefore, the use of the static threshold method can't be suitable for overload detection. Here, dynamic CPU utilization (cumulative CPU utilization per VM over multiple independently processing tasks) assessment method to perform overload detection is applied. More specifically, in

this method, the CPU utilization threshold value is adjusted dynamically on the basis of the changes in continuous CPU utilization. It assumes that higher fluctuation in use-pattern can be stated as the lower upper CPU utilization (threshold).

In general, the higher value of such non-linear resource utilization indicates an overloaded condition, with 100% resource utilization. To cope up with the exceedingly high dynamism in the cloud network, a hybrid concept encompassing both inter-service (task) relation along with varying information to achieve dynamic thresholding is applied. Here, a state of art new hybrid concept to exploit task level resource utilization and their cumulative impact as eventual load to perform overload detection is designed.

More specifically, interquartile range (IQR) and modified local regression methods is applied to measure dynamic CPU utilization and eventually predict adaptive threshold. Here, IQR algorithm follows a statistical dispersion approach to represent association between the first and the third quartile, as depicted in equation (1). The value of IQR is estimated to employ the equation (2) to obtain the upper-threshold of the CPU utilization.

$$IQR = Q_3 - Q_1 \quad (1)$$

$$T_u = 1 - s.IQR \quad (2)$$

With the consideration of dynamic load conditions and fluctuations in resource utilization for the same ongoing task, there can be significant effect on the upper threshold estimation (2). Any possible inaccuracy in threshold estimation might cause wrong resource allocation and allied task migration activities that as a result can affect overall SLA performance. Realizing this fact, in this research paper a state-of-art new dual-level threshold estimation model is formulated, where at first it applies IQR based T_u estimation, while in the subsequent phase it applies local linear regression (LRR) method. Noticeably, in the proposed model, LRR exhibits fitting of the (utilization) trend polynomial to the preceding k CPU utilization values, obtained as per (3) for each observation value.

$$\hat{g}(x) = a + \hat{b}x \quad (3)$$

Now, measuring the observation values, the next observation value, $\hat{g}(x_{k+1})$ is estimated. Now, to perform offloading of a host, the following condition is applied.

$$s.\hat{g}(x_{k+1}) \geq 1 \quad (4)$$

$$x_{k+1} - x_k \leq t_m$$

In above conditions (4), $s \in R^+$ signifies the maximum level of tolerance by a host. Here, the maximum time required to migrate a VM (containing one of multiple independently executing tasks) from host d be t_m . The classical local regression concepts which are often found limited under higher dynamic value changes and allied regression estimation. Additionally, it performs inferior due to the outliers introduced by leptokurtic or heavy-tailed distributions. Considering this

fact, modified the classical least square (LR) algorithm is applied by a bi-square model. Noticeably, LR improves iteratively so as to estimate the initial fitting for which the tricube weights are obtained using a Tricube Weight Function (TWF). Here, the obtained fitting parameter at x_i was applied to retain the fitted values using \hat{y}_i . In this manner, the residual value, signifying $\varepsilon_i = y_i - \hat{y}_i$ was estimated. Thus, with the estimated values of x_i and y_i , it was assigned in (5) to estimate a factor called robustness factor R_i .

$$R_i = B\left(\frac{\hat{\varepsilon}_i}{6s}\right) \quad (5)$$

Every observation value was allocated R_i . In (6), $B(\cdot)$ represents the bisquare weight function and s represents the Medium Absolute Deviation (MAD) to achieve least square fitting. Thus, obtaining $B(\cdot)$ As per (6).

$$B(\cdot) = \begin{cases} (1-u^2)^2 & \text{if } |u| < 1,0 \\ \text{Otherwise} & \end{cases} \quad (6)$$

In above derived equation (5), s was obtained as per (7).

$$s = \text{mediun}|\hat{\varepsilon}_i| \quad (7)$$

Thus, employing the above derived model (4) for the estimated trend line, the predicted possible value or instance, for any inequalities (with reference to the predicted value and the observed value), a host was identified as an overloaded host. Eventually, identifying the overloaded host, the local controller unit informs the global controller and meanwhile identifies the VMs to be migrated to the other resource-sufficient (optimal) host node. Though, in literature, researchers have randomly considered any VM to execute migrate; however, for SLA-sensitive task migration purposes, such approaches might undergo SLA-violation phase or QoS compromise, especially due to increased downtime and even complete task or transaction failure. Considering this fact, distinct unit called VM selection model is necessary. A snippet of the VM selection method applied is given as follows.

B. SLA Oriented Minimum Migration Time-based VM Selection

In order to preserve SLA, while guaranteeing minimum downtime, the minimum migration time (MMT) based VM selection method is applied. In other words, once identifying an overloaded host, only that specific VM is migrated, which takes minimum migration time. Hypothesizing the fact that higher downtime can lead higher losses, so maintaining lower downtime as favorable, MMT as a VM selection policy is considered. This approach can be suitable towards SLA preserving effort as well as reliable cloud service provision. Migration time for each task and allied VM connected to the overloaded host of PM is estimated. Thus, sorting the VMs based on their respective migration time, the VM is chosen with the minimum migration delay, at first to migrate towards the target host. Thus, applying this method, broadened the horizon for delay-resilient migration over cloud platforms. Now, once selecting the VM to be migrated, the local controller passes all allied details to the global controller, which employs a highly robust improved ACS heuristic

concept to perform VM placement of migration. Though, the proposed VM migration or allied task scheduling concept resembles a VM consolidation problem; however, considering real-time tasks characteristics, classical meta-heuristics is improved to not only alleviate local minima and convergence but also ensure timely and SLA-centric task-migration or allied resource allocation.

The following section discusses the proposed I-ACS model for task-scheduling over a large Infrastructure as a Service (IaaS) cloud platform.

C. Task-Migration Problem Definition

Consider that the set of operating physical machines or the hosts be $PM = \{pm_1, pm_2, pm_3, \dots, pm_m\}$ where, pm_i represents the specific host conditioned as $1 \leq i \leq m$. In the same manner, let the set of VMs encompassing or containing multiple autonomously operating tasks be $VM_i = \{vm_1, vm_2, vm_3, \dots, vm_{n,i}\}$, where each VM is connected to certain host. $vm_{j,i}$ be the j -th VM connected on the i -th host. The variable $x_{i,j}$ presents a binary variable signifying on host j connected by the i -th VM. Consider that $P_{r,i}$ be the resource capacity (in terms of the CPU utilization) of r on the j -th host and the resource demanded by the j -th VM be $v_{r,j}$. In this manner the total load at that host can be characterized in the form of the total load caused by all VMs and allied tasks running onto it. Let, T be the time-period or observation period. Thus, the sub-gap can be estimated by splitting T into $q - 1$ intervals $T = [(t_2 - t_1)(t_3 - t_2) \dots (t_q - t_{q-1})]$. Noticeably, the time-slot $t_k - t_{k-1}$ represents the interval k . Thus, over k , the CPU utilization is estimated at a host using (8).

$$CPU_{i,Util}(k) = \sum_{j=1}^n vm_{CPU,j} \div pm_{CPU,i} \quad (8)$$

In (8), the parameter k refers to the CPU utilization which was collected for certain period. The average CPU utilization is estimated using (9).

$$pm_{i,AvgUtil} = \sum_{t=t_k}^{t_k-n} pm_{i,Util}(t) \div (q-1) \quad (9)$$

In (9), $(q - 1)$ states the total amount of sub intervals or gap over T observation period. Let, $pm_{i,w}(k)$ be the power of i -th host over t_k span, then the power status can be obtained based on the CPU utilization value. $pm_i E^{(k)}$ which signifies the energy consumption by the i -th host from the last time interval to the current time interval and hence is estimated as per (10).

$$pm_i E^{(k)} = pm_{i,w}(k-1) + (pm_{i,w}(k-1) + (pm_{i,w}(k))(t_k - t_k - 1)) \quad (10)$$

Based on host consumption hypothesis, for any host pm_j , employing CPU utilization, $CPU_{i,Util}(k)$ the energy consumed can be obtained as per (11).

$$E(pm_j) = K_j \cdot e_j^{max} + (1 - k_j) \cdot e_j^{max} \cdot CPU_{i,Util}(k) \quad (11)$$

In (11), k_j signifies the portion of energy exhausted when the host (i.e., pm_j) is in idle state; while e_j^{max} refers the energy exhaustion of pm_j when being utilized completely. Moreover, the parameter $CPU_{i,Util}(k)$ presents the CPU utilization by pm_j over k duration. Thus, applying this mechanism, the resource utilization is estimated dynamically over each host and correspondingly the resource demand by each task or allied VM is estimated. Now, the resource consumption for all active hosts, $D_E(k)$ since the last or passed time interval to the current instant is estimated as per (12). The key dominant goal behind task migration or VM allocation problem is to obtain the set of VM-host mapping, where the proposed allocation model is supposed to place the targeted VM onto the suitable host, without impacting SLA performance or energy-exhaustion. Here, the resource allocation is performed in such manner that the proposed scheduling model attains minimal resource exhaustion $D_E(k)$, conditioned at:

$$\forall_i \sum_{j=1}^m x_{ij-1} \quad (12)$$

$$\forall_j \sum_{i=1}^n vm_{CPU,i} X_{ij} \leq pm_{CPU,j} \quad (13)$$

Thus, with the above derived motive, in this research work, a state-of-art new improved ACS heuristic model is developed for SLA-centric task-scheduling and allied VM or resource allocation strategy. The details of the planned I-ACS model is given in the following section.

D. Improved-ACS based Task Scheduling

Unlike classical heuristic models, a hybrid ACS algorithm for task scheduling or allied VM allocation is applied. The VM scheduling model proposed in this paper is based on a well-known heuristic model named ACO in which multiple agents estimate the solution-likelihood in iterative cycles. During this process, they converse ultimately by dropping the pheromone, which is a chemical substance called on respective paths they traverse. But, for research-intended task-scheduling or VM placement doesn't employ the notion of path, in the proposed model pheromone is deposited by the ants on each task (or VM) and within a pheromone matrix by the host pair. The ants retrieve VMs in each series, and starts forming local solutions by means of a probabilistic decision rule that signifies the attractiveness for an ant to select a specific VM (MMT based VM selection) as the next one to pack in its current host. In this mechanism, the higher the amount of pheromone deposition and higher information related to a VM-host pair, the probability that it will be selected for migration will also be higher. Fig. 2 presents the solution formation for a single ant. In this mechanism, the ant initiates with four VMs, calculates the probabilities for each of the VMs using the probabilistic decision rule, and begins allocating the (selected) VMs for each selected host as per the estimated probabilities. Once the host is completely occupied with the migrated task or allied VMs the proposed model identifies a new host on the basis of corresponding likelihood.

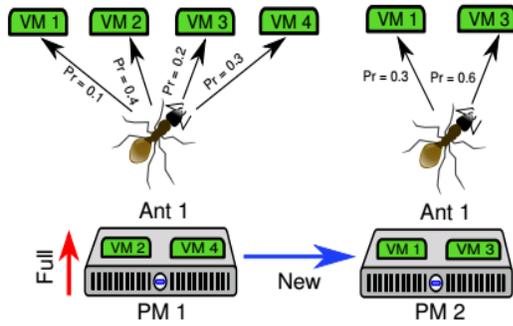


Fig. 2. ACS-assisted Task-scheduling or VM Placement.

This process continues till all tasks or VMs are assigned to the suitable hosts. During the optimal solution estimation, in each cycle or iteration, local solutions are assessed and the one demanding the minimum number of hosts is selected as the different optimal solution globally. Subsequently, it updates the pheromone matrix to estimate pheromone loss and reinforce VM-host pairs belonging to the set of the optimal or the best solution. To achieve it, ACS implements the pheromone update rule. In the proposed ACS based task-migration model, the proposed I-ACS gets triggered during VM assignment to the target host. It outputs a solution comprising VM to host (map) while maintaining no (or negligible) SLA violation or maximum host-shutdown (to achieve energy-efficiency).

In this research the emphasis has been made on optimizing classical ACO to avoid local minima, convergence and enhance solution diversity to meet dynamic cloud resource optimization. The proposed model encompasses some of the key optimizations such as multi-population strategy, co-evolution concept, dynamic pheromone update and dynamic pheromone diffusion. Such optimization measures enable the proposed model to retain optimal balance in between the convergence rate as well as solution diversity which helps perform better VM scheduling or placement decisions. Moreover, it helps perform swift computation which is effective towards large scale mega-cloud infrastructures. To achieve it, the proposed model is designed in such manner that it splits overall optimization problem into multiple sub-problems where to avoid local minima and convergence (i.e., to achieve local optima), the ant-population is split into two specific categories; Elite Population and Normal Ant-Population. This process not only increases computational efficiency (i.e., higher convergence rate) but also retains swift global-optima identification. Additionally, incorporating a dynamic pheromone update mechanism to enhance optimization ability over large network sizes. Similarly, the intent of pheromone diffusion was to make the pheromone released by ants at a certain point, which gradually affects a certain range of adjacent regions.

Realizing large scale cloud infrastructure, the concept of co-evolution (in reference to both populations based as well as diffusion based) is applied that helps interchanging local information amongst varied sub-population to achieve dynamic information sharing. Noticeably, each VM is hypothesized to be a component possessing or encompassing operating tasks, and therefore the concept of co-evolution can enable dynamic decision without imposing an SLA violation issue. Thus, the

implementation of the overall proposed model can ensure optimal energy as well as QoS oriented task scheduling across a large-scale cloud-infrastructure.

Before discussing the overall proposed improved ACS model for the intended task-scheduling or VM migration, a ACO model is given as follows.

E. Probabilistic Decision Rule

In VM allocation strategy, at first ACS defines the likelihood of an ant to select a VM v for migrating it to a specific host p using (14).

$$Pr_p^v := \frac{[\tau_{v,p}]^\alpha \times [\eta_{v,p}]^\beta}{\sum_{u \in N_p} [\tau_{v,p}]^\alpha \times [\eta_{v,p}]^\beta}, \forall v \in N_p \quad (14)$$

In (14), the parameter $\tau_{v,p}$ states the pheromone-based attractiveness to migrate or attack VM v onto the host p . Similarly, the parameter $\eta_{v,p}$ represents the VMs heuristic information. Moreover, the other variables $\alpha, \beta \geq 0$ are applied to either focus more on the pheromone or the vital heuristic information. Moreover, N_p states the total number of VMs encompassing single or multiple tasks which are suitable to be attacked or connected with the current host p . l_p states the overall utilized memory or capacity of the current host, which can be estimated as the sum of all requested resources by the connected VMs, i.e., $l_p := \sum_{v \in V} RC_v$. Here, the task scheduling or allied VM placement is accomplished by means of a parameter $\eta_{v,p}$, which is estimated as per (15).

$$\eta_{v,p} := \frac{1}{|TC_p - (T_C + RC_v)|_1} \quad (15)$$

Thus, once estimating the value of (15), a d-dimensional demand vector is created which is subsequently mapped in terms of a scalar value. Here, the L1-norm method is applied to perform mapping the VM and host so as to perform migration decisions.

F. Pheromone Trail Update

Once performing initial solution construction, the pheromone trails on all the pairs of VM-hosts are updated, which helps global solution retrieval. Classically ACS systems apply MAX-MIN Ant System (MMAS) and therefore the ant with the best solution in iteration is permitted to deposit pheromone. Thus, the pheromone update is performed as per (16).

$$\tau_{v,p} := (1 - \rho) \times \tau_{v,p} + \Delta \tau_{v,p}^{best}, \forall (v, p) \in V \times P \quad (16)$$

In (16), ρ ($0 \leq \rho \leq 1$) plays a vital role in simulating the pheromone evaporation. Noticeably, the higher value of ρ results in an increased rate of evaporation. Additionally, a few pairs of the target VM and host pair require reinforcement and therefore $\Delta \tau_{v,p}^{best}$ is defined as the best pheromone amount deposited in each iteration by that VM-host pair. In other words, $\Delta \tau_{v,p}^{best}$ states the amount of pheromone added or deposited to the edge (v, p) . In this manner, the VM-host pairs with S_{best} is reinforced that gains higher attraction.

$$\Delta \tau_{v,p}^{best} := \begin{cases} 1 & \text{if } x_{v,p} = 10 \\ f(s_{v,p}) & \text{otherwise} \end{cases} \quad (17)$$

In ACS based task-scheduling or resource allocation, VMs and host nodes are considered as input along with respective demanded resource capacity and total capacity RC_p and TC_p , respectively. Furthermore, certain parameters like $\alpha, \beta, \rho, g, \tau_{max}, nCycles, nAnts$ are initialized and the initial pheromone trails for VM (tasks)-host pairs is defined as τ_{max} . $nCycles$ represents the number of iterations. In individual iteration an ant a initiates a host set PM_p and performs solution retrieval process S_a . Thus, with these initialized parameters, ACS model performs task-migration or VM allocation to the different suitable hosts, while maintaining optimal SLA and higher energy-efficiency. A snippet of the classical ACS based task scheduling is given as follows.

```

if  $T_{v,p} < T_{min}$  then
     $T_{v,p} := T_{min}$ 
end if
end for
end for

```

return S_{best}

As depicted in the above snippet, once identifying the best host solution, the proposed global controller schedules the VM (containing task(s)) to the selected host, and this process continues till all tasks or allied VMs are assigned a suitable host to continue respective functions. In classical ACS based optimization methods, ACS algorithm exploits the positive feedback and parallel computing concept to perform optimization. However, the majority of the ACS solutions undergo local minima and convergence problems, especially due to the complexity in estimating the optimal control parameter, etc. Though, a few efforts such as co-evolution, derived on the basis of the co-evolutionary phenomenon in nature have emerged as potential alternatives to the classical optimization solutions. These approaches employ the concept of decomposition and coordination to split a complex problem into multiple small but interacting optimization sub-problems. Such sub-problems are enhanced distinctly and perform as an eventual standalone solution. Thus, the strategic implementation of multi-population strategy along with co-evolution can improve overall performance. In sync with the ACS solution, the implementation of multiple generation, co-evolution, improved pheromone update concept and pheromone diffusion can achieve relatively better performance. Additionally, such approaches can greatly help avoiding local minima and convergence issues in the ACS system.

The intended improvement in convergence rate can significantly help in avoiding local optimal value and hence more precise resource allocation can be accomplished. This approach can be well suited towards the large-scale task-scheduling and allied resource allocation problem in cloud (IaaS) infrastructure. In reference to the above stated ACS optimization requirement, the proposed model applies a multi-generation concept that splits the complete population or ants into two broad categories; elite ants and the common ants. Moreover, it introduces state-of-art new and robust pheromone update mechanism to enhance the optimization capacity of ACS to meet at-hand task scheduling and allied VM migration control. Subsequently, a novel pheromone diffusion model is applied that effectively controls the pheromone release by ants at specific points, which subsequently impacts adjacent regions to optimize solution faster.

On the other hand, the proposed co-evolution concept helps exchanging information amongst the varied sub-populations for better information sharing. These enhancement efforts intend to achieve more efficient, fast and accurate task-scheduling over cloud to meet real-world cloud demands. The detailed discussion of the above stated improvement and allied implementation towards S-DTS purpose is given in the subsequent sections.

G. Multi-Population Generation Mechanism

In the classical ACS model, as discussed in the previous section, it applies merely one kind of population (i.e., ants) to

Algorithm 1 ACS-based VM scheduling or the task scheduling

Input: Declare VMs and hosts with respective resource requirement, RC_v and TC_p

Output: Best solution S_{best}

Assign initial pheromone value for the pair of VM-host with τ_{max}

for all $q \in \{0 \dots nCycles - 1\}$ **do**

for all $a \in \{0 \dots nAnts - 1\}$ **do**

$IS := V; p := 0$

$S_a := [x_{v,p} := 0], \forall v \in \{0, \dots, m-1\}, \forall p \in \{0, \dots, n-1\}$ **while**
 $IS \neq \emptyset$ **do**

$N_p := \left\{ v \sum_{p=0}^{n-1} x_{v,p} = 0 \wedge l_p + RC_v \leq TC_p \right\}$

if $N_p \neq \emptyset$ **then**

 Select $VM_v \in 2 N_p$ as per the probability

$$Pr_p^v := \frac{[\tau_{v,p}]^\alpha \times [\eta_{v,p}]^\beta}{\sum_{u \in N_p} [\tau_{v,p}]^\alpha \times [\eta_{v,p}]^\beta}$$

$$x_{v,p} := 1$$

$$IS := IS \setminus \{v\}$$

$$lp := lp + RC_v$$

else

$$p := p + 1$$

end if

end while

end for

Estimate the solutions S_a as per the objective function and declare as S_{cycle}

if $q = 0 \vee IsBest(S_{cycle})$ **then**

 Declare iteration (cycle) as best solution with S_{best} as the best solution.

end if

Estimate τ_{min} , and T_{max} .

for all pair of VMs and hosts $(v, p) \in V \times P$ **do**

$$T_{v,p} := (1 - p) \times \tau_{v,p} + \Delta \tau_{v,p}^{best}$$

if $\tau_{v,p} > \tau_{max}$ **then**

$$T_{v,p} := T_{min}$$

end if

retrieve new solutions. In this process, these classical methods apply predefined fixed values of the ant-colony size, convergence parameter, and selection parameter to control the solution-estimation. However, under dynamic applications such as at-hand cloud computing problems, it is highly complex and challenging to estimate the suitable set of parameters to retrieve the enhanced performance with swift convergence rate. Such limitations often results in premature convergence, and hence seems inferior towards task-scheduling in cloud infrastructure. To alleviate such problems, a concept of multi-population is applied that splits the entire population of ants into two categories: elite ants and common ants. The elite ants retrieve information from the solution archive that eventually helps in generating solutions by implementing a Gaussian kernel function assisted likelihood selection model. More specifically, the proposed elite ants possess a set of distinct parameters that help them (i.e., elite ants) to enhance the convergence rate. On the contrary, the common-ants are employed to generate new solutions with relatively slower speed by means of a single Gaussian function. Noticeably, to achieve it, the common ants employ the mean value of each dimension that helps in avoiding local optima. The proposed model applies the following Gaussian function to generate common ants.

$$f_N^i(x) = \frac{1}{\sigma_{i,N} \sqrt{2\pi}} e^{-\frac{(x-\mu_{i,N})^2}{2\sigma_{i,N}^2}} \quad (18)$$

$$\mu_{i,N} = \sum_{k=1}^K S_{i,k} \quad (19)$$

$$\sigma_{i,N} = \xi_N \sum_{e=1}^K \frac{|S_{i,e} - S_i|}{K-1} \quad (20)$$

In (18), the parameter $f_N^i(x)$ represents the Gaussian function used for common ant generation in the i -th dimension. The other parameter, $\mu_{i,N}$ represents the sample value while $\sigma_{i,N}$ refers to the obtained standard deviation. The average value of the solution in the i -th dimension is given by S_i . Here, ξ_N be the constant employed to control the convergence rate of the common ants. Thus, the proposed model enables common antsto increase the search space sufficiently large which eventually helps improve the global search ability.

H. Multi-level Pheromone Update

In the majority of the classical ACS solutions, the key challenge is the pheromone update. To alleviate such limitations in the proposed ACS solution, the two different pheromone update mechanisms; the local pheromone update and the global pheromone update is applied. A snippet of the proposed multi-level pheromone update method is given as follows:

I. Local Pheromone Update

In the proposed model, before executing the optimization (say, the first iteration of the optimization), the pheromone deposition on each edge (signifying the VM-host pair) remains

the same and constant. The local pheromone model is executed on each (passed) VM-host pair's edge once any ant completes the current iteration. Similar to the classical ACS model, it updates the local pheromone using (21).

$$\tau_{x,y}^{(i)} = (1 - \rho_G) \tau_{x,y}^{(i)} + \rho_L \Delta \tau_0^{(i)} \quad (21)$$

In (21), $\rho_L \in (0,1)$ refers the local pheromone evaporation coefficient, while $1 - \rho_L$ be the pheromone residue factor. The other parameter, $\tau_0^{(i)}$ presents the initial pheromone value. For a node value as 1, $\tau_0^{(i)}$ used to be the small negative number, while the same as 0, indicates $\tau_0^{(i)} = 0$.

J. Global Pheromone Update

Once all ants complete one iteration and achieve a solution set, the passed nodes exhibit the global pheromone update. Unlike classical pheromone update model (17), the proposed model performs pheromone update as per (22).

$$\tau_{x,y}^{(i)} = (1 - \rho_G) \tau_{x,y}^{(i)} + \rho_L \Delta \tau_0^{(i)} \quad (22)$$

$$\Delta \tau_G^{(i)} = \{F_G^{(i)}, (x, j)$$

\in Global optimal Solution $F_1^{(i)}$,

\in Iterative optimal Solution 0, Otherwise $\quad (23)$

In (22-23), $\rho_G \in (0,1)$ refers the global pheromone evaporation coefficient, while $(1 - \rho_G)$ presents the residue factor, $F_G^{(i)}$ is global optimal solution and while $F_1^{(i)}$ signifies the iterative optimal solution.

K. Pheromone Diffusion

In Pheromone Diffusion process, the ants (agent) apply a single pheromone release mechanism. This approach can merely influence the subsequent ants with the passed same point; however doesn't guide the ant-search within a specific range of neighboring regions, and therefore influences the overall optimization performance. Based on the above discussed multi-layer pheromone update model, the pheromone diffusion concept to enhances the performance. The likelihood of superior solutions in the neighboring region used to be higher in comparison to the other neighboring regions. Hence, the pheromone diffusion concept can enable pheromone release by the agents at a certain point that slowly influences a specific range of the adjoining regions. On the other hand, the other ants (elite ants) intend to avoid making any search in its vicinity of the poor solution and often intend to search the solution near or in the neighborhood of the better solution. This as a result not only improves time performance but also accuracy of the selected solution in each iteration. Mathematically, the pheromone update and diffusion concept are presented as per (24-25).

$$\tau_{x,y}^{(i)} = (1 - \rho_D) \tau_{x,y}^{(i)} + \rho_L \Delta \tau_{x,y}^{(i)} \quad (24)$$

$$\Delta \tau_{x,y}^{(i)} = \left\{ \frac{1}{N+1} \times \frac{\tau_x^{(i)}}{d_r(o_x, o_y)}, d_r(o_x, o_y) < 10, \text{Otherwise} \right. \quad (25)$$

In (25), N refers the total number of estimated solutions in current iteration, while $\tau_x^{(i)}$ refers the left guiding pheromone concentration on the source object o_x . The other parameter, $d_r(o_x, o_y) = 1/(f + 1)$ represents the correlation distance in between the two maps or objects.

L. The Co-Evolution

Unlike classical evolutionary computing approaches, co-evolution is an improved concept that enables higher biological diversity, by emphasizing on certain reliance on intra-organisms (between organisms and organisms), inter-organisms (organisms and environment) during the evolution process. Functionally, it employs evolution theory to construct the competition relation or cooperation relation among two or more populations so as to enhance optimization performance by the interaction of multiple populations. It also focusses on exploiting at-hand interaction amongst the varied sub-populations, and eventually influences each other to co-evolve altogether to attain superior optimization performance. In proposed ACS solution, a co-evolution concept to realize the information interaction amongst the varied sub-population to yield better optimization performance. Thus, implementing the above stated improved ACS model dynamic task scheduling and allied resource allocation. The results obtained by carrying out simulation and its inferences are discussed in the following sections.

IV. RESULTS AND DISCUSSION

Ensuring SLA/QoS centric task migration while preserving energy-efficiency is a NP-hard problem, a state of art new Improved ACS model (I-ACS) for VM migration scheduling is applied. Unlike classical heuristic methods, including the conventional ACS or ACO, the proposed method applied multi-population with co-evolution and dynamic pheromone update capacity. This approach not only intended to improve overall scheduling efficiency but also intended to alleviate the problem of local minima and convergence. Thus, performing above stated activities achieves SLA-sensitive and energy-efficient task scheduling in large scale cloud infrastructure. The details of the simulation environment applied is given as follows.

A. Experimental Setup

To simulate the overall proposed model, CloudSim simulation environment and allied benchmark tool is considered. The overall programs were developed in Java programming language and emulation was performed over Java Eclipse platform. Noticeably, the higher scalability, ease of implementation and realistic problem realization was the foundation behind the selection of CloudSim based simulation.

In cloud configuration setup, each host is characterized in terms of corresponding utilization of memory and the performance of Central Processing Unit (CPU). The parameters are Million Instruction Per Second (MIPS), signifying the resource being used or demanded by each task and the resource available onto a host. Moreover, memory (RAM) utilization and bandwidth information of each host as well as VM, which are supposed to be monitored continuously to ensure QoS and SLA oriented task scheduling.

To consider the effectiveness of the proposed task-migration of the VM allocation model, the multiple real-time cloud-computing traces obtained from the CoMon data project, a PlanetLab simulation benchmark (cloud trace) dataset are used. The employed dataset comprised the cloud traffic and allied CPU utilization traces from 1000 plus VMs and allied autonomous tasks, where the different VMs were located at the different locations. The considered benchmark data encompassed the cloud traces over 10 randomly selected data in March and April, 2011. In the considered dataset, the CPU utilization measurement interval was fixed at five minutes. A simulation environment is considered with the system architecture consisting of two heterogeneous servers with dual-core CPUs, one HP ProLiant ML110 G5 with Intel Xeon 3040, 2 cores \times 1860 MHz processors, armored with 4GB RAM. Additionally, it encompassed HP ProLiant ML110 G5 server with Intel Xeon 3075, 2 cores \times 2660 MHz, 4 GB RAM to represent a heterogeneous cloud environment. The server's frequency is mapped onto MIPS specifications where HP ProLiant ML110 G4 server was mapped with 1860 MIPS, while for HP ProLiant ML110 G5 server mapping with 2660 MIPS. Each server was armored with 1 Gbps network bandwidth. To assess the efficacy of the proposed task migration or VM allocation (say, resource allocation) model, the performance is obtained in terms of SLA violation (often called, SLAV), SLA downtime, number of migration and energy-consumption. Before discussing the empirical outcomes, a snippet of the different SLA sensitive performance variable is given as follows:

B. The Cost of Task-Scheduling or VM Migration

Undeniably, the key intent behind the task-migration or allied VM migration is its QoS-affinity or SLA demands. Additionally, this mechanism demands the proposed scheduling model to ensure minimum SLA violation (SLAV), maximum migration with minimum downtime performance. Moreover, maintaining lower energy-consumption has always been the dominant demand from cloud infrastructures. Typically, the SLAV or downtime probability primarily rely on the key factors such as resource demand or memory expected by the different tasks operating onto the VMs, number of memory disks updated over varied execution periods, etc. Under dynamic workload scenarios, the average performance degradation caused due to the downtime is nearly 10% of the overall CPU utilization. Each VM migration introduces a certain SLAV and therefore the minimization of the migration while maintaining SLA performance can be vital. However, maintaining higher task migration without causing any SLAV can also be suitable towards real world application. It seems more realistic under resource constrained scenarios with exceedingly high dynamism. Practically, the migration period relies on the total amount of memory used by the tasks at a certain VM and the available network bandwidth. The migration period for a specific VM, say VM_j can be estimated as per (26).

$$T_{m_j} = \frac{M_j}{B_j} \quad (26)$$

In (26), the memory employed by VM_j is M_j , while the available bandwidth is given by B_j . Here, the focus is on reducing SLAV by maintaining MMT to avoid downtime. To assess performance, the overall performance degradation during the targeted task-scheduling was assessed as per (27).

$$U_{d_j} = 0.1 \cdot \int_{t_0}^{t_0+T_{m_j}} u_j(t) dt \quad (27)$$

In (27), the parameter U_{d_j} signifies the overall performance degradation during the task-migration or VM allocation from one host to another, t_0 be the initial migration (start) time, while T_{m_j} be the overall time exhausted during migration. The other parameter $u_j(t)$ is the overall CPU utilization by a node VM_j .

C. SLAV Metrics

Considering the SLA objective in cloud infrastructure, the performance of the proposed task scheduling or VM migration model in terms of the different SLAV parameters is examined. To meet QoS and SLA demands, migration model are required to be optimal in delivering minimum throughput and maximum response time. Functionally, these performance parameters change based on the application demands and allied scheduling modalities. The overall SLAV is defined as the disparity in between the demanded MIPS by the tasks or VMs ($U_{r_j}(t)$) and the actual assigned MIPS ($U_{a_j}(t)$) over the life time of VM (28).

$$SLA = \frac{\sum_{j=1}^M \int_t U_{r_j}(t) - U_{a_j}(t) dt}{\sum_{j=1}^M \int_t U_{r_j}(t) dt} \quad (28)$$

In (28), the total number of active VMs is given as M . This work considered MIPS information as well as CPU utilization. Noticeably, here the CPU utilization refers the memory demands which couldn't be assigned when demanded. In the proposed method, distinct two SLA metrics, one the duration through which the active host nodes have experienced 100% CPU utilization, called Overload Time Fraction (OTF); and the performance degradation by VMs (PDM) caused due to VMs migrations have been considered for performance analysis. Here, the value of OTF and PDM is estimated using the following equations (29-30).

$$OTF = \frac{1}{N} \sum_{i=1}^N \frac{T_{s_i}}{T_{a_i}} \quad (29)$$

$$PDM = \frac{1}{M} \sum_{j=1}^M \frac{C_{d_j}}{C_{r_j}} \quad (30)$$

In (29-30), N represents the total number of active hosts, while the number of active VMs is M . The other parameter T_{s_i} be the total time-period over which the i -th host experienced complete (i.e., 100%) resource utilization giving rise to the SLAV. Here, the total number of active hosts or

servers are T_{a_i} and C_{d_j} be the performance degradation of VM_j due to migration. In the proposed model, the overall CPU demanded by the cumulative tasks at VM_j is C_{r_j} . Since, the above stated SLAV parameters or metrics, OTF and PDM represent SLAV distinctly, and therefore combining the both metrics as a unified performance parameter named SLAV, which is defined as (31).

$$SLAV = OTF.PDM \quad (31)$$

The detailed discussion of the simulated performance outcomes in terms of the above discussed SLA performance metrics, downtime and energy is given as follows: Unlike major classical researches such as [1-5], authors have focused on assessing resource scheduling performance based on the parameters like make span, scheduling time, etc.; however, could not assess whether their approach delivers SLA or not. Unlike the performance assessment in terms of makeover or scheduling time, a real-world cloud infrastructure, especially IaaS often demands ensuring minimum or even negligible downtime, SLAV, etc. Moreover, assessing their suitability in terms of energy is equally significant. Therefore, taking into consideration of this fact, in this research the performance of the proposed system is examined in terms of the following parameters:

- No. of VM migrations,
- SLA-Violation (SLAV),
- SLA performance degradation,
- SLA Violation per active host,
- Host Shut-Down,
- Energy-Consumption.

Amongst the above stated performance metrics, 2, 3, and 4 represents robustness of the scheduling methods towards SLA assurance or QoS. On the contrary, 1 and 5 presents scalability of the proposed cloud model, while 7 indicates swiftness. Though, 1, 3 and 5 are highly dependent. Similarly, 6th performance metrics indicate the energy-efficacy by the proposed model. Noticeably, for an SLA-oriented solution a task scheduler requires maintaining a greater number of migrations while maintaining negligible SLAV, SLAV per active host, and scheduling time. On the contrary, higher number of active hosts shut down indicates energy-convergence ability by the proposed model. To compare the performance by the proposed model i.e. I-ACS model, with other recent approaches as well; though these methods examined their performance in the different terms like make-span or time over varying tasks. Noticeably, scheduling methods are considered as the foundation and performed task-migration hypothesizing that each VM carries a single operating task, and hence the task migration can be realized as a classical VM-consolidation or migration problem. Thus, with this hypothesis, three different existing approaches as mentioned in [2], [3] and [4] are implemented.

Velliangiri et al. has focused on improving heuristic model to achieve better performance and local minima and convergence avoidance. In this regard, authors [2] designed a

Hybrid Electro Search with GA (HESGA) algorithm for task-scheduling. To achieve better performance, authors applied GA to obtain local optimal solution, while Electro Search algorithm was applied to improve global optima solution. However, authors failed in addressing the dynamism of the resource demands under uncertain predefined heterogeneous (dynamic) clouds. Recalling the fact, unlike [2], where authors applied static threshold-based hotspot detection, to cope up with the exceedingly dynamic cloud environment IQR-LRR based stochastic prediction concept for overloading detection is applied, which helped making task-scheduling on time and hence preserved SLA performance. Recently, an improved effort was made in [3], where Liu et al. [3] proposed an improved GA based collaborative scheduling concept for cloud infrastructure. With the same intend as [2], or the proposed I-ACS model, authors [3] targeted on avoiding local minima and convergence problems for better scheduling.

Xiang et al. [4] recently proposed the Greedy-ACO algorithm for workflow scheduling in heterogeneous cloud environments. To be noted, there are a large number of existing method or literatures discussing heuristic based task scheduling, VM consolidation and VM migration; however, considering these three key recent methods which not only intend to perform task-scheduling, but also address the existing drawbacks of the major existing methods such as local minima and convergence.

Recalling the fact that the considered cloud traces or benchmark data was taken from PlanetLab datasets, to examine or simulate the proposed model (as well as the existing methods [2-4] over the different datasets. More precisely, the proposed model is executed with the cloud traces obtained 03 March 2011, 06 March 2011 09 March 2011, 22 March 2011, 25 March 2011, 03 April 2011, 09 April 2011, 11 April 2011, 12 April 2011 and 20 April 2011. Thus, simulating the different methods, including the proposed I-ACS model obtains performance outputs in terms of 1-6 metrics. To generalize the performance over multiple test instances or cases, the average performance is considered. The outputs obtained in terms of the different SLA metrics is given as follows:

Fig. 3 presents the number of VM migrations by the different techniques. After the observations, the overall results obtained by the proposed I-ACS model show a higher number of task migration, exhibiting robustness towards superior scalability. It is further be identified in terms of the minimum SLA violation and downtime, as depicted in Fig. 4 to Fig. 6. Noticeably, literature hypothesizes that maintaining a lower number of migrations can avoid any likelihood of SLAV; however, the proposed model has exhibited on the contrary, affirming that one can achieve superior SLA performance even with a higher number of migrations. Since, in the proposed model, each VM was considered as one autonomously operating task, scheduling a larger number of tasks shows the superior scalability by the proposed method. It affirms robustness of the proposed model towards realistic mega data center applications.

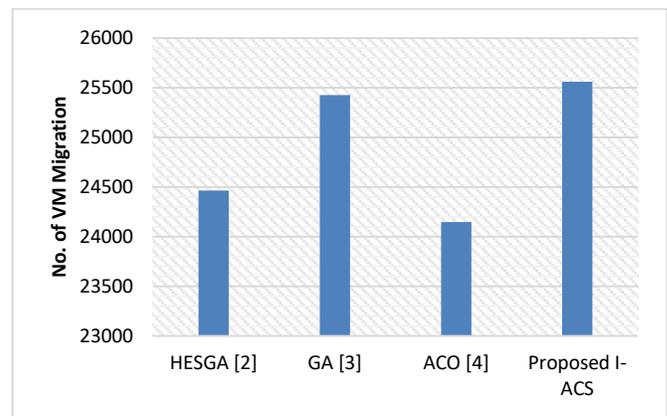


Fig. 3. Number of VM Migrations using different Techniques.

Fig. 4 presents the SLA violation, here called SLAV. The observations with overall results achieved by the proposed I-ACS model shows better than other existing approaches; however, its performance is far better than the classical ACO algorithms. This performance enhancement could be contributed because of multiple-generation, dynamic pheromone update and co-evolution concept. Statistically, I-ACS model has exhibited almost 0.03% of SLA violation, which shows its robustness. A similar performance was observed in terms of SLA performance degradation per host (Fig. 5). As depicted in Fig. 5, the proposed method performs superior over other heuristic based scheduling. To be noted, since HESGA [2] and improved GA [3] algorithms were developed similar to the proposed I-ACS concept, where the key focus was made on alleviating the at hand local minima and convergence and hence these approaches showed better performance than the classical ACO based scheduling. However, these methods [2][3], due to the lack of adaptive overloading or hotspot detection and dynamic scheduling (performed using multiple controller-based systems), were found inferior than the proposed model.

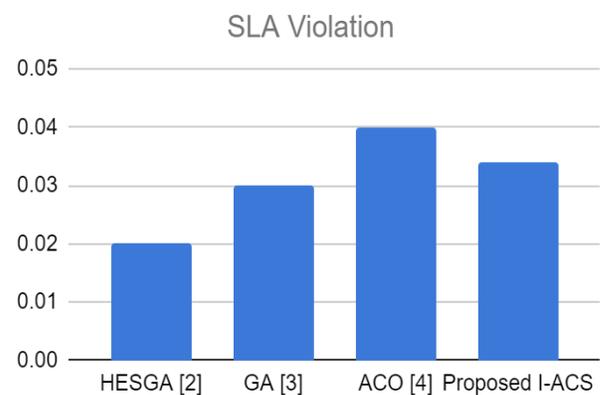


Fig. 4. SLA Violation (SLAV) Performance by the different Techniques.

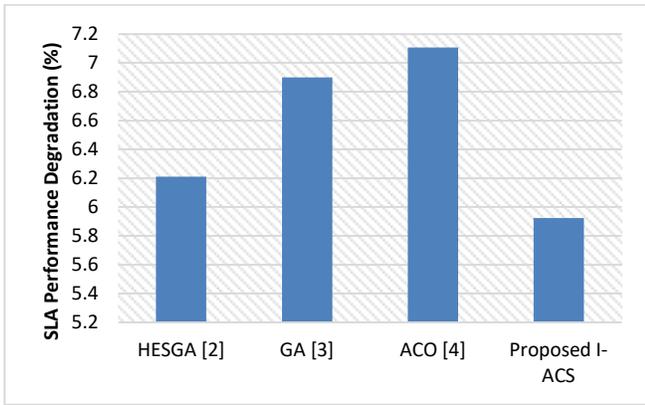


Fig. 5. SLA Performance Degradation by the different Techniques.

A similar performance was found in SLA per active host (Fig. 6). Observing overall performance, it can easily be found that the proposed multi-controller assisted I-ACS based task-scheduling model achieves better SLA performance and eventual QoS to meet major cloud computing demands. In terms of time of execution, Fig. 6 reveals that the proposed I-ACS model exhibits superior in terms of the SLA time per active host (second), signifying very small or near tolerable downtime. The comparative outcomes too reveal that the proposed model shows almost 18% lower downtime than other heuristic based approaches.

Considering about the number of hosts shut-down, Fig. 7 reveals that the proposed I-ACS based task-scheduling model exhibits a higher number of host-shut down, signifying better energy-efficiency and optimal resource utilization.

Fig. 8 can be found in affirmation, where the proposed I-ACS model has exhibited almost 8% lower energy than the classical ACO based scheduling. Noticeably, in Fig. 8, the energy consumption by GA variants is relatively higher. This could be because of the predefined number of stopping criteria (considering 200 number of generations). It could have taken more time for computation and hence higher energy exhaustion. Thus, considering the overall performance outputs, it can be stated that the proposed I-ACS based model achieves superior performance than other existing (recent) heuristic based task-scheduling systems or resource allocation (say, VM migration) methods. The overall research conclusion and its related inferences are given in the subsequent sections.

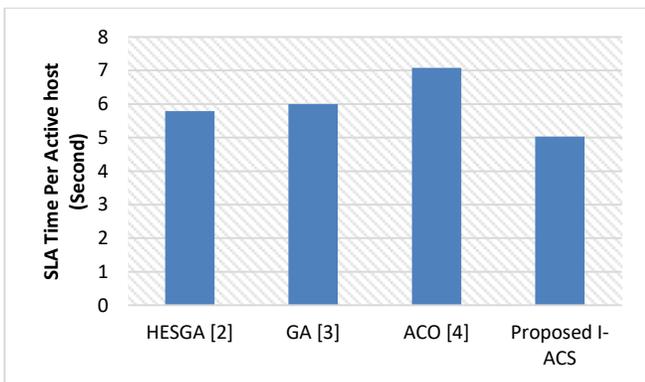


Fig. 6. SLA Time Per Active Host (sec.) by different Techniques.

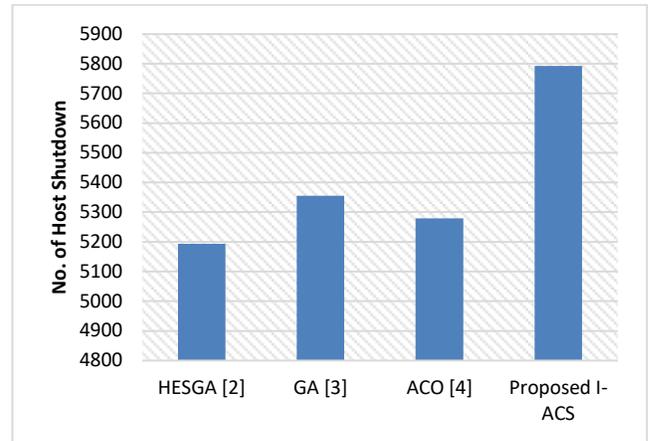


Fig. 7. No. of Host Shut-down by the different Techniques.

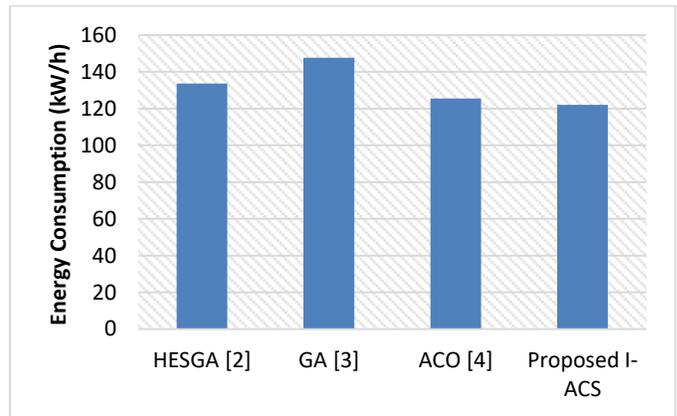


Fig. 8. Energy Consumption by the different Techniques.

V. CONCLUSION

The research work primarily focused on improving the task-scheduling and allied dynamic resource allocation to meet SLA-centric cloud services. To meet contemporary as well as future demands including QoS, SLA-agreement and energy-efficiency, the proposed work introduced multiple enhancement at the different levels of computation. The proposed model applied multi-controller strategies, where the use of local controllers enabled task-level resource utilization assessment and stochastic prediction-based overloading or underloading detection avoiding any possible downtime. The proposed local controller applied minimum migration time based VM selection strategy that greatly helped for timely task-migration scheduling. Eventually, exploiting the task and possible target host information, the proposed involves improved multi-population, adaptive or dynamic pheromone update and co-evolution-based I-ACS model which performs dynamic task-migration or allied resource scheduling. The overall proposed I-ACS model not only enabled superior task-migration but also avoided any possible local minima and convergence problem. This as a result affirmed optimality of the proposed solution exhibiting superior performance in terms of minimum SLA violation, minimum downtime, lower energy consumption and higher number of task-migration.

REFERENCES

- [1] S. Pang, W. Li, H. He, Z. Shan and X. Wang, "An EDA-GA Hybrid Algorithm for Multi-Objective Task Scheduling in Cloud Computing," in *IEEE Access*, vol. 7, pp. 146379-146389, 2019. DOI:10.1109/ACCESS.2019.2946216.
- [2] S. Velliangiri, P. Karthikeyan, V.M. Arul Xavier, D. Baswaraj, "Hybrid electro search with genetic algorithm for task scheduling in cloud computing", *Ain Shams Engineering Journal*, pp. 1-9; July 2020. DOI:10.1016/j.asej.2020.07.003.
- [3] S. Liu and N. Wang, "Collaborative Optimization Scheduling of Cloud Service Resources Based on Improved Genetic Algorithm," in *IEEE Access*, vol.8, pp.150878-150890,2020. DOI:https://doi.org/10.1155/2021/5582646.
- [4] B. Xiang, B. Zhang and L. Zhang, "Greedy-Ant: Ant Colony System-Inspired Workflow Scheduling for Heterogeneous Computing," in *IEEE Access*, vol.5, pp.11404-11412,2017. DOI: 10.1109/ACCESS.2017.2715279.
- [5] S. G. Domanal, R. M. R. Guddeti and R. Buyya, "A Hybrid Bio-Inspired Algorithm for Scheduling and Resource Management in Cloud Environment," in *IEEE Transactions on Services Computing*, vol. 13, no. 1, pp. 3-15, 1 Jan.-Feb. 2020. DOI: 10.1109/TSC.2017.2679738.
- [6] Afzal, S., Kavitha, G. Load balancing in cloud computing – A hierarchical taxonomical classification. *J Cloud Comp* 8, 22 (2019). https://doi.org/10.1186/s13677-019-0146-7.
- [7] Pradhan, P., Behera, P.K. and Ray, B.N.B., 2016. Modified round robin algorithm for resource allocation in cloud computing. *Procedia Computer Science*, 85, pp.878-890.https://doi.org/10.1016/j.procs.2016.05.278.
- [8] Moges, F., Abebe, S. Energy-aware VM placement algorithms for the OpenStack Neat consolidation framework. *J Cloud Comp* 8, 2 (2019). https://doi.org/10.1186/s13677-019-0126-y.
- [9] Syed Arshad Ali, Samiya Khan, MansafAlam, Resource-Aware Min-Min (RAMM) Algorithm for Resource Allocation in Cloud Computing Environment, *International Journal of Recent Technology and Engineering (IJRTE)* ISSN: 2277-3878, Volume-8 Issue-3, September 2019. Pp 1863-1870 DOI: https://doi.org/10.35940/ijrte.c5197.098319.
- [10] Mosa, A., Paton, N.W. Optimizing virtual machine placement for energy and SLA in clouds using utility functions. *J Cloud Comp* 5, 17 (2016). https://doi.org/10.1186/s13677-016-0067-7.
- [11] J. R. Doppa, R. G. Kim, M. Isakov, M. A. Kinsy, H. Kwon and T. Krishna, "Adaptive many core architectures for big data computing: Special session paper," 2017 Eleventh IEEE/ACM International Symposium on Networks-on-Chip (NOCS), Seoul, pp. 1-8, 21017. DOI: https://doi.org/10.1145/3130218.3130236.
- [12] 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. DOI: https://doi.org/10.1109/TSC.2015.2466545.
- [13] 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. DOI: https://doi.org/10.1016/j.jcss.2015.07.001.
- [14] 28 -30 Z. Tang, L. Qi, Z. Cheng, K. Li, S. U. Khan, and K. Li, "An energyefficient task scheduling algorithm in DVFS-enabled cloud environment," *J Grid Comput.*, vol. 14, no. 1, pp. 55–74, Mar. 2016. DOI: DOI:10.1007/s10723-015-9334-y.
- [15] G. Xie, L. Liu, L. Yang, and R. Li, "Scheduling trade-off of dynamic multiple parallel workflows on heterogeneous distributed computing systems," *Concurrency Comput.-Parctice Exp.*, vol. 29, no. 8, pp. 1–18, Jan. 2017. DOI:10.1002/cpe.3782.
- [16] G. Zeng, Y. Matsubara, H. Tomiyama, and H. Takada, "Energy Aware task migration for multiprocessor real-time systems," *Future Gen.Comput. Syst.*, vol.56, pp.220–228,Mar.2016. https://doi.org/10.1016/j.future.2015.07.008.
- [17] 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. DOI: 10.1109/TPDS.2015.2446459.
- [18] Jyothi.S, Dr.B.S.Shylaja, "Efficient Approach for Resource Provisioning to manage Workload in Cloud Environment" in *International Journal of engineering Research and Technology(IJERT)*,ISSN 2278-0181,Vol 9,Issue 06,June2020.DOI:http://dx.doi.org/10.17577/IJERTV9IS060979.
- [19] Bhaskar, Shylaja.B.S (2019)"KBR Knowledge Based Reduction Method for Virtual Machine Migration in Cloud Computing", *International Conference on Recent Trends in Advanced Computing 2019, ICRTAC-2019* published in Elsevier *Procedia Computer Science* 00 (2019) 000–000. DOI: https://doi.org/10.1016/j.procs.2020.01.026.

A Review of a Biomimicry Swimming Robot using Smart Actuator

Muhammad Shafique Ashroff Md Nor¹, Mohd Aliff^{2*}

Malaysian Institute of Industrial Technology
Universiti Kuala Lumpur
Malaysia

Nor Samsiah³

Center for Artificial Intelligence Technology (CAIT)
Faculty of Information Science and Technology
Universiti Kebangsaan Malaysia, Selangor, Malaysia

Abstract—Biomimicry-based robotic mobility is a newer subgenre of bio-inspired design and it's all about applying natural concepts to the development of real-world engineered systems. Previously, researchers used actuators such as motors, pumps, and intelligent materials or intelligent actuators to build many biomimicry robots. Due to the field's growing interest, this study will examine the performance of several biomimicry robots that have been built based on their different design, the type of material the robot utilizes, and the type of propulsion for the robot to swim while providing huge thrust. Robots must not only design such an animal, but its maneuverability and control tactics must also be tied to wildlife to provide the finest impersonation of biological life. Fish propulsion can be separated into two categories which are body and/or caudal fins (BCF) and median and/or paired fins (MPF). The old propeller system in underwater robot usually uses motor and pump. Many researchers have begun developing smart materials as drivers in recent years that can be grouped into four categories: shape memory alloy SMA, ionic polymer metal composite IPMC, lead zirconate titanate (PZT) and pneumatic soft actuator as replacement for pump or motor. Varied materials produce different result and can be applied for different propulsion modes. Future researchers working on biomimetic fish robots will be guided by the findings of this study.

Keywords—Biomimicry; fish propulsion; biological life; smart actuator

I. INTRODUCTION

Water covers 71 percent of the earth's surface, providing mankind with resources such as oil, food, and other necessities. Many engineers and biologists have worked to build new tools, machinery, and vehicles for underwater jobs like installing and maintaining cables and pipes, drilling for oil and gas on the seabed, and exploring the ocean floor for military and rescue missions. As a result, there has been a rise in demand for underwater robotics and vehicles [1]. However, today's underwater vehicles still have issues such as power conservation, mobility, limited thrust, and a design that is not ideal for usage in deep seas with high pressure. [1],[2]. However, there is always room for improvement for technologies and sciences. One of the methods is biomimetic approach which compares biological life as reference for the improvement. Biomimicry or biomimetic can be defined as a study of biological life such as animal and plant which will be implemented to science and technology.

Fish like robot that mimic biological life has gaining popularity in science and technology field. Fish exist in a wide range of shapes, sizes, and movement rates, which are influenced by several characteristics including dynamic shape and functional fins [3],[4]. Varied fish species have different advantages and drawbacks based on a variety of characteristics including shape, propulsion mechanism, and environment. All these specialties cannot be combined into a single robot system. The robot system, on the other hand, may always be improved. As a result, the goal of this work is to look at prior research on robots with fish-like characteristics to improve robot design and propulsion methods.

Current underwater vehicle can come out with result needed but more advance technology still needed since the result still limited. For example, in incident relate to Indonesia submarine crash in April 2021, underwater robot can help the exploration become faster rather than going in with another submarine for exploration and rescuing which may lead to the same incident happen. Some depth of the sea also cannot yet be explored by human due to pressure and dark surrounding. With robot this dream can be achieved with probability of success to increase, and risk can be reduced especially with robot that have underwater nature.

To create or build the best mimicry of biological life, the robot must not only act like the animal, but the shape design and control strategy also must relate to the wildlife. There are still significant challenges need to address to achieve good result. Algorithm to optimize control also needs to focus by the research community since this play's enormous potential in biomimicry robot. The choice of swimming style whether BCF or MPF and its modes are also important to choose based on the robot practical to maximize performance. BCF and MPF propulsion modes will be discuss later in another chapter.

Materials use to build the robot also must be considered since error in design can affect directly to performance of the robot. This has been proved in paper L. Neely et al. [5]. Same goes with the materials selection for actuator since this the most important part that will be used as propulsion system, and it will define whether the robot can act like subject animal or not. Lastly, dynamic modelling or the shape design of the fish needs to focus more to ensure robot not only can work on test bench but also the real underwater like deep sea or stream river.

*Corresponding Author.

Underwater robot can consider robot that perform underwater operates without pilot or in another word works automatically. The idea initially started during late nineties by the marines. However, the development of underwater robot started way long before during 1950s where Dimitri Rebikoffin created first underwater robot called POODLE which later around 1970 more technology came used to gather and transfer data [6]. This technology test keeps increasing where during 1980 to 1990 many robots were built and evaluate to perform more specific task.

Many firms attempted to design and build robots to accomplish certain duties in the year 2000, but the robots produced still had many flaws, and their ability to maneuver in water was limited. Furthermore, corporations must invest a significant amount of money to construct these robots. However, in recent years, a growing number of scientists and research organizations have begun to investigate and construct robots made of less expensive materials. This version can lower the amount of money needed to manufacture a single robot while also meeting the demand for robots that can execute jobs in the water while moving faster.

Later, several scientists and researchers began investigating how to make robots by emulating the way fish swim in water. Various challenges faced by researchers at the time were handled by replicating the style of fish swimming in water, particularly those relating to the thrust for swimming robots and the dynamic design for underwater robots. Furthermore, smart actuators have been designed to replace traditional pumps and motors, allowing robots to swim and move in the water faster while using less energy. However, much more study and development are required before underwater robots can achieve the same level of capacity as fish that can swim more flexibly and steadily. The smart actuator will be explored later in this paper to better grasp the notion or operating principle, as well as other investigations carried out by other researchers in order to create this biomimetic robot.

II. UNDERWATER ROBOT TECHNOLOGY DEMAND

Although several have been constructed, autonomous underwater robot technology is still in the experimental stage. Proper navigation and propulsion, together with the suitable means to execute a task, are the keys to the best underwater technology [7],[43],[44]. The three main characteristic that limit the development are the compactness of the robot, flexibility, and the multifunction capabilities in single robot [8],[30],[60]. In oil and gas industry alone, this technology is critical as it can improve many outcomes. There are many depths of sea beyond reach of the current technology and dangerous for human to dive. With the usage of remote technology underwater robot, the job of diving and exploration will increase the effectiveness and at the same time eliminating danger or incident that might occur.

The demand on the exploration of the underwater increases the demands of the robot technology. This exploration can cover much as sea mapping, sea monitoring and deep-water oil search. Unmanned with the advance smart sensor will help the sea exploration. Technically, underwater robot demand can be divided into four main categories which are commercial mission, oceanographic research mission, military mission, and

engineering research [9, 10],[62]. The main major factor for underwater robot grows demand is exploration of mineral since of the sea mineral is still vast with most part of it still not be explored by researcher.

Commercial mission is usually being developed by multiple industry related to deep water especially oil and gas company. This robot task covers underwater survey, inspection, and repair, welding cutting, collecting sample and object recovery at the offshore. Since oil and gas industry work with deep sea, this technology is important to them specially to reduce risk and loss. For example, people who are related to this industry do not have to go and dive deep sea to look and find the oil under the sea. By sending robot, it can find and look for the oil and at the same time can collect the sample.

Meanwhile, oceanographic research mission helps to monitor index level of health in maritime life and environment. It also helps to search and discover new species and deep-sea exploration. Scientist or marine's scientist also use demanding robot for sea exploration to increase their input such as exploration for sea mapping [29]. Technically, only less than 20% of sea has been explored and the rest remain mystery to the world and science. Explorer cannot just send submarine to explore this part of deep sea because it not only costs a lot of money but the submarine itself needs human to operate which is dangerous and life of this explorer at stake. To do this, scientist really needs smart robot to this for them.

Military also demand underwater technology to defend especially country that surrounded by sea. The military mission also includes rescue mission in deep sea incident such as when Indonesia submarine collapsed in 2021. The rescue and retrieve mission took a lot of time and military technology from various countries due to rough sea condition. military demand also related to intelligence, surveillance, inspection, underwater repair and maintenance navigation and communication. It is believed that more advance and smart technology will help this mission to work better and faster if this incident happens again in the future.

For engineering research, the current design robot will be improved, and the current design will be used as the sample. This process includes the improvement of navigation, propulsion, and control system. This will help the future design and product to work better as compared to current robot. Data from this research later will be significant for the future robot and researcher to produce better technology.

Some robots also can be use as other purpose for example sea cleaning and fisherman work related. This may not improve the quality of the job but may reduce the risk on wildlife itself. As per For Market report on 25th February 2020, global underwater robotics market demand expected reach up to 7.08 billion US Dollar by 2025. This show that underwater robot demand is big and needed by many industries.

III. FISH SWIMMING PROPULSION

Fish swimming propulsion can be divided into two categories which are body and/or caudal fins (BCF) and median and/or paired fins (MPF) [10,23,31]. Almost 85% of fish use BCF locomotion modes to swim while the rest 15%

use MPF modes [1,2,10]. BCF locomotion fish uses its body to produce propulsive force opposing its direction force to provide forward swimming movement and MPF use it median or paired fins to produce propulsive force. Swimming in BCF mode is faster than swimming in MPF mode, however MPF variants are more maneuverable than BCF modes [11]. For the movement characteristic of swimming fish, it is divided into two categories which are undulation and oscillation. Undulation is process of fish body propeller to provide waves along its propulsive structure while undulation is body part by swinging back and forth. This example can be seen from stingray (undulation) and manta ray (oscillation) [12,33]. To measure fish speed, scientist usually uses Body Length per second (BL/s), but some also still prefer centimeter per second (cm/s) or meter per second (m/s).

A. Body and/or Caudal Fins (BCF)

The modes of BCF propulsion are categorized into five groups. The modes are anguilliform, subcarangiform, carangiform, thunniform and ostraciiform [11,13,23]. BCF modes fish use undulation or oscillation throughout their body to produce thrust force. Fig. 1 shows the difference in the wavelength and the amplitude which later proportional with the thrust generated. From image, anguilliform has the highest degree of change in body change which entire body to generate thrust force compared to others. Example of this propulsion method can be seen on the eel. These modes can change the direction of the swim forward or backward by changing it body undulation. It has high maneuverability but lack in hydrodynamic which lead to more energy loss [32]. These modes have been practiced in robot lead Niu X. et al. by replicating movement to swim forward and backward like fish and succeed. Because it exploits the connection of small elements joined together to form a robot, this robot design uses a lot of servo motors compared to other designs. Other report also has been recorded to imply this method to robotic and based on their design it required up to twenty serial linked actuators as a propeller.

Subcarangiform and carangiform use half and one-third of their body to produce thrust force. Although the movement of body anguilliform is higher compared to other, subcarangiform has higher speed but must compromise in term of their abilities to turn and accelerate due to inability to bend on their body. 3D simulation test suggests that robot that wanted to apply carangiform method should have flexible tail with multiple joint and right frequency to achieve appropriate speed and thrust [14],[15],[24].

Thunniform mode uses less than 30% of its body (fins are) participate in undulation to produce thrust force and the rest of the body remain stationary. Ostraciiform meanwhile purely uses oscillatory and can be categorized into both BCF and MPF based on use to flap. These two designs are hydrodynamically less efficient due to most of their body parts remain stationary.

B. Median and/or Paired Fins (MPF)

Just like BCF, MPF propulsion also divided into five modes which are rajiform, diodontiform, amiiform, gymnotiform and balistiform. MPF mostly used by fish in term

of auxiliary propulsor and maneuvering as well as stabilization. It also provides acceptable thrust force as a locomotion at every low speed (3BL/s and below) [8]. MPF fish multiple small fins rays that are connected through flexible or soft membrane as medium to produce wave for propulsion. This due to fins capability of two-degree of freedom movement. Rajiform and diodontiform use undulation method to produce propulsive waves throughout large and flexible pectoral fins [47]. Rajiform modes can be seen mostly in manta, skates, and rays. Aminiiform also uses undulation, but usually only dorsal fins move and in many cases body axis is hold straight. Gymnotiform also same as aminiiform which body axis is held straight during swimming, but it uses long based anal fins. Balistiform can be seen mostly on balistidae family of fish. It uses both anal and dorsal fins to provide propulsive force as a locomotion. The overview of fins use in MPF propulsion can be seen in Fig. 2.

Scientists have also worked on MPF Style swimming robotic because MPF based fish has better role in linear motion, controllability table and maneuvering [16],[17]. Many from MPF design robots that include paired pectoral fin has shown good propulsive efficiency and maneuverability. A group of researchers from National University of Singapore has developed a manta robot that can swim up to 2 BL/s and can work up to 10 hours which show a significant result in biomimicry robot.

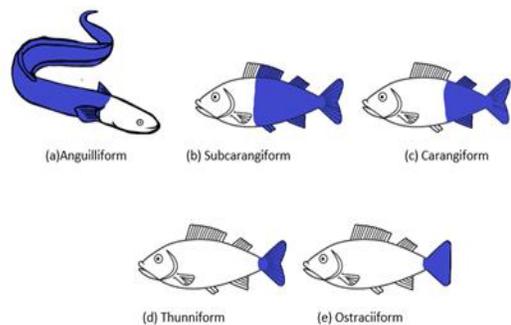


Fig. 1. Degree of Body Movement of BCF Fish. (a) Anguilliform (b) Subcarangiform (c) Carangiform (d) Thunniform (e) Ostraciiform. (Adapted and Redraw from P. Du Raisamy et al. [13]).

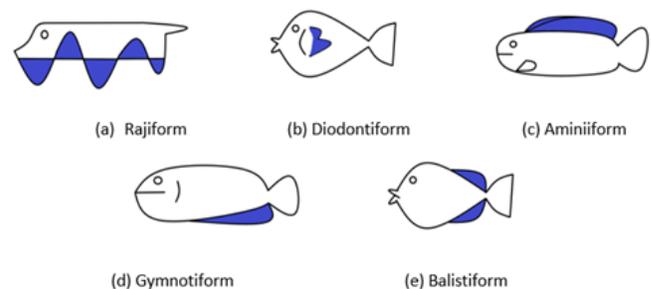


Fig. 2. Degree of Body Movement of BCF Fish. (a) Rajiform (b) Diodontiform (c) Aminiiform (d) Gymnotiform (e) Balistiform (Adapted and Redraw from P. Duraisamy et al. [13]).

IV. SMART MATERIALS IN FISH PROPULSION ROBOT

Authors To make a fish robot biomimicry body that can copy fish movement, the propeller or pump needs to be replaced. These materials are called smart actuators which can be classified into four categories which are shape memory alloy (SMA), ionic polymer metal composite IPMC, lead zirconate titanate (PZT) and pneumatic soft actuator [27]. Smart materials use continuously increasing due to capability of materials to meet the demand of the robot to become smaller and lighter in design [18].

SMA is a thermomechanical actuator due to its ability to change phase with the change of temperature of the materials. The capability of SMA to change shape by applying temperature variant make it valuable to use as smart materials [18],[45]. There are two types of SMA which are one way and two-way memory. One way memory will only be deformed or shrink when heat is applied while two-way has shape with high temperature and low temperature. At two-way, during room/low temperature, it will have one shape and at heated temperature it will have one shape. The different is one way needs to be heated first before it can back to normal temperature [13],[77]. Fig. 3 shows concept of the SMA material using SMA connected to spring [67]. Lower figure shows that during heated, the spring expanded due to steel spring shrink compared to upper figure where steel spring is in normal condition when no heat applied.

IPMC made of three-layer materials which two are metal electrodes and single layer of thin electrode membrane. These three layers are arranged like sandwich which membrane in between the electrode. When voltage applied and create electric field, cation with water molecules will move toward cathode which will create imbalance. This will create more concentration on cathode and bend toward anode [19,37]. There are many different IPMC which usually differed based on chemical structure and properties such as Nafion, Flemion and other properties. However, IPMC usually made with Nafion is widely used [40,59].

PZT applied and piezoelectric effect which is the ability of certain materials to produce or generate electric charge upon the mechanical stress. When both surface of PZT is compressed by outside pressure, it will generate electric field propositional to external pressure.

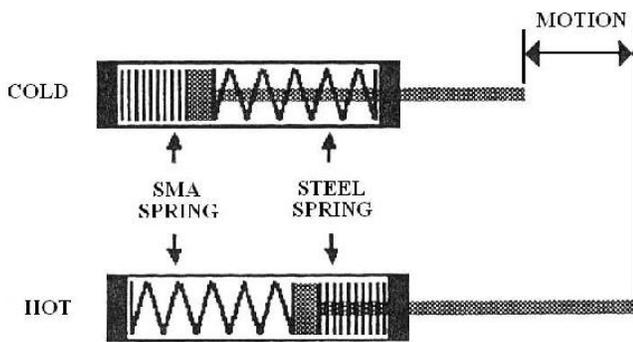


Fig. 3. SMA Actuation Sample (Adapted from Degeratu, S. et al [67]).

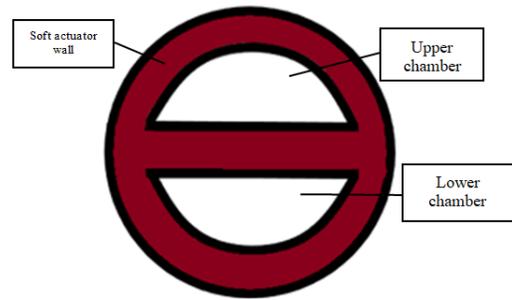


Fig. 4. Example Cross Section Design of Bending in Pneumatic Soft Actuator (Adapted and Redraw from K. Suzumori et al).

Pneumatic soft actuator is the newest technology that has been implemented to bio-mimicry robot. The working principle of pneumatic soft actuator is simple which consists of single or more chamber of rubber structure which is used with fiber or vice versa. This method is expected to be the most promising actuator in biomimicry robot due to its simple structure, high power/weight ratio, water resistance and high compliance [14]. Fig. 4 shows possible simple cross section for bending use in soft actuator. For example, when air is applied to bottom chamber, it will bend upward. By applying concept of bending up-down or front-back, it can be used for propulsion.

V. BIOMIMETIC ROBOTS

Several factors must be considered when developing a robotic fish propulsion system that incorporates intelligent materials, including the robot's dynamic shape, swimming pattern, and environment [46]. In brief, the actuator and swimming modes are listed according to the institution that developed the biomimetic underwater robot. John Finkbeiner et al. [34] design has two major components for the build which are fins and tail that use SMA. The fins are made up of five separate fins that are coupled together and respond to the fish robot's movement and direction. Fishtail fins are also used to assist robots swim more efficiently and steadily. In Fig. 5, center plate will act actuator for the SMA using which is attached to pulley that act like muscle. It uses a maneuvering system and at the same time produce flapping motion that help the robot swimming by moving the back part (tip) of body left and right. This swimming style can be seen in many fish.

SMA wires come in many sizes and produce different result. Selecting thicker wire will produce greater full force but will cause longer time for full actuation. To calculate force, drag on the robot can be calculate as Eq. (1). ρ is the water density ($997.1(\text{kg}/\text{m}^3)$), V is the model velocity, C_d is the flat plate perpendicular, and A is the surface area of the fins.

$$d = (\rho V^2 C_d A) / 2 \tag{1}$$

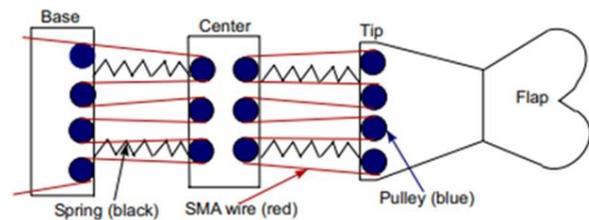


Fig. 5. Fish Tail (Adapted from J. Finkbeiner et al.).

The design of manta ray by Zhenlong Wang et al. also uses SMA as a propulsive system. Two SMAs are attached to each side of ray's fin to provide flapping motion. Fig. 6 shows the structure of fins ray's design. These fins are connected to polyvinyl chloride (PVC) sheet to make a triangle shape that mimicking manta rays. When upper side of SMA applied an electric, it will bend upward and when applied to bottom part it will bend downward. The SMA wire no change when no electric applied since no thermo change (cool) [35,36]. Zhenlong Wang also has made a design based in subcarangiform modes making half of the back side of the body to use as a propulsive system. It uses two different parts where one part is active component and another one is passive component that react based on active component (biomimetic fins using SMA) [25,26,38].

Fig. 7 shows the speed forward and turning swimming of robot by Zhenlong W. et al. Forward swimming achieve maximum frequency of 8.33 Hz with 25% duty ratio and 11.1 Hz for turning with 33.3% duty ratio. Duty ration means ratio of power on time of period over the periodic time. The longer power on time indicates the larger bending angle of the robot. The fastest swimming forward achieves at 2.1 Hz frequency with 16.7% duty ratio. Both 25% and 16.7% duty ratio of fish swimming speed decrease with the increase of frequency.

For turning radius, the result increase for both 33% and 25% duty ratio but start to decrease at certain frequency. The highest value come at 3.13Hz with 25% duty ratio. Speed of turning achieve minimum turning radius at 136mm at 3.7Hz with 33% body ratio. The lower the speed of turning means faster time. All this result achieve from testing in tank and result may different if test outside or in water with flow.

Joel J. Hubbard et al. has designed a robot that uses both MPF and BCF propulsion. The project uses both pectoral fins mainly for maneuverability such lift, dive and turning while caudal fins mainly for propulsion. The robot takes advantage of IPMC with seven different surface that react differently for propulsion and maneuverability. Maximum speed for in initial test for propulsion on platform was 2.8cm/s. The idea of using seven different surfaces for more flexibility and multiple degree of freedom can be applied for further research [20].

To test effect waveform on stingray surface velocity, J. Nowell et al. developed a stingray test platform that body mainly made of acrylic. The robot design is not aerodynamically good since it only shape of box. The mechanical drive for this robot uses servo that attach with node to produce waveform. Each side has 10 servos and nodes resulting total 20 servos and nodes. The speed of this design varies depending on frequency of the servo applied. This paper can be used as baseline to understand surface velocity of stingray for future researchers. Three factors during robot tuning that can affect the performance of fish robot are frequency, amplitude, and Mean Wave Number (MWN) [41].

Fig. 8 shows that relationship between the wave parameters and surface velocity. By changing parameters of frequency velocity and Mean Wave Number (MWN) produce different result on surface velocity of the robot. Fig. 8a shows that zero amplitude resulting zero velocity and increasing linearly with increase of amplitude. This prove that amplitude has great

impact on robot speed. Fig. 8b also shows almost same result with increase of frequency has effect on fish velocity. Meanwhile, MWN produce rocking result along the stingray as the MWN will determine how many cycles of waves along the robot fins.

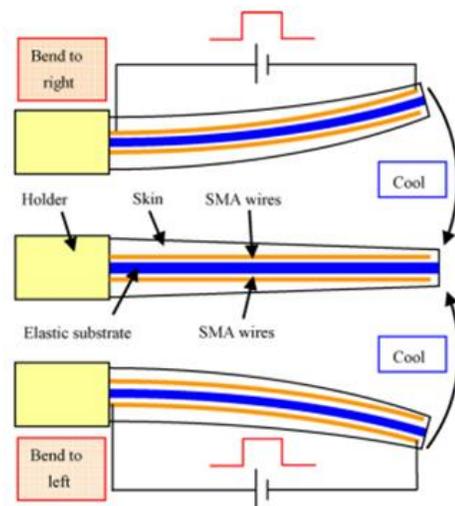


Fig. 6. Structure of Biomimetic Fin (Adapted from Z. Wang et al.).

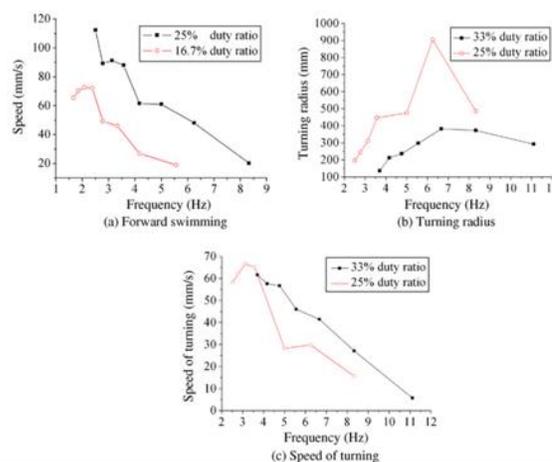


Fig. 7. The Micro-robot Fish's forward Swimming Speed, Turning Radius, and Turning Speed (Adapted from Zhenlong W. et al).

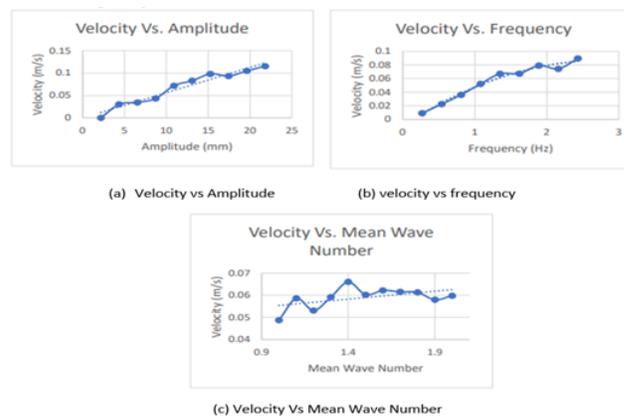


Fig. 8. Test Result. (a) Velocity vs Amplitude. (b) Velocity vs Frequency (c) Velocity Vs Mean Wave Number (Adapted from Jordan N. et al.).

The speed result compared to expected result based on mathematical result can be seen in Fig. 8. By applying 5V amplitude over different frequencies, the result was tested three times for each frequency to get average. Maximus speed was founded at frequency of 2Hz. The team assume the speed increase with the increase value of frequency as shown in Fig. 9, but the result does not match due to low actuation of frequency will make larger tail actuation and resulting large yaw angle of the robot. The assumption only work frequency below the 2Hz and start to decrease in speed when frequency is greater than 2.

Manta ray robot using IPMC, and Polydimethylsiloxane (PDMS) membrane as shown in Fig. 10 was developed by team of University of Virginia which achieved 0.055 BL/s which is slower compared to robot that uses servo motor and SMA as a propeller. However, IPMC shows advantages with lighter design and less power consumption. Later, the writer also improves the design and achieve 0.067 BL/s in speed. To increase the efficiency, writer suggested two key points for the future which are dynamic of the manta robot and second is optimal design and of the fins [21,39].

Pneumatic soft actuator developed by K. Suzumori et al. [19] uses manta ray as sample for the fish. The design uses basic two degree of freedom in bending. The manta robot size is 17cm width and 15cm in length. The pneumatic tube is part one in each side of the robot and each tube in robot connected with two sources of pneumatic tube as source resulting four pneumatic tube to control the robot. The robot reaches speed of 10cm/s. The simple robot design uses soft actuator which only rubber resulting the robot water resistance, simple structure, and light weight. The drawback here is robot must connect to pneumatic supply as power source for the fin undulation.

Design and preliminary evaluation by Lei Liu et al. conclude in their test that useful design of propulsion system with optimized phase control method can make a good MPF fish robot. The test subject reaches up to 0.8BL/s in speed which is comparable to some BCF swimming robot. The robot suggests that by changing the frequency of servo, and phase shift and deflection angle of undulation fins will directly affect the swimming performance of the robot [42].

The testing considers three variable that may affect the robot swimming performance which are change in the phase of a waveform between adjacent fins ray (φ_0), deflection angle between the fin's rays and the horizontal plane (φ_b) and frequency of the robot. Fig. 11a shows that the speed of the robot increases linearly with frequency with φ_0 and φ_b is 60° and 0° , respectively. Fig. 11b meanwhile shows that speed increase until certain degree of phase of a waveform between adjacent fins ray at max 60° and start decrease in speed when the φ_0 increase. This due to theoretically that the swept area and the generating force undulating fins increase when phase of a waveform between adjacent fins ray decrease.

Tiefeng Lie et al. on paper title fastmoving soft electronic fish uses commercial silicone elastomer to as the body part [22]. The fabrication process takes few steps as shown in Fig. 12. Since the materials use here falls under categories soft actuator, the fins will flap as the voltage applied. The thrust force generates through periodic flapping pectorals and

produce up to 135mm/s in speed for indoor and 64mm/s for outdoor.

Servo motor uses to control rod for stingray mimicry robot build group of researchers of Washington and Lee University a bit different from another robot since it uses flexible rod. This is due to aim of researchers to behave more like natural stingray skeletal structure. Same as other robot that uses servo motor, the speed of the robot depends on input parameter such as frequency to affect the swimming performance or speed. The robot can swim up to 6m in straight line before it drifts from direction. This unintended drifting causes by the imbalance internal build and wing thickness (manufacturing error).

The result of swimming speed versus flapping frequency from this robot can be seen in Fig. 13. The robot swim fastest at 1.4 Hz flapping frequency by producing 13cm/s and 11.9cm/s or 0.37 bl/s or 0.34bl/s. the slowest is at 0.7 Hz which 4cm/s and 2cm/s. interestingly, the sample fish for this robot design which is southern stingray swim with beat frequency of $1.74 \pm 0.42\text{Hz}$ which is meeting the optimal value for the robot to swim at it best.

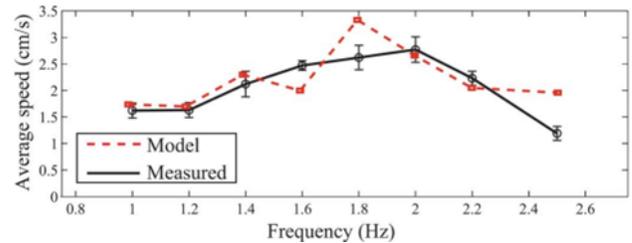


Fig. 9. When Operated by a 5-V Sinusoidal Voltage, the Experimentally Measured Swimming Speed of the Robotic System was Compared to the Model's Prediction. (Adapted from Joel J. Hubbard et al.).

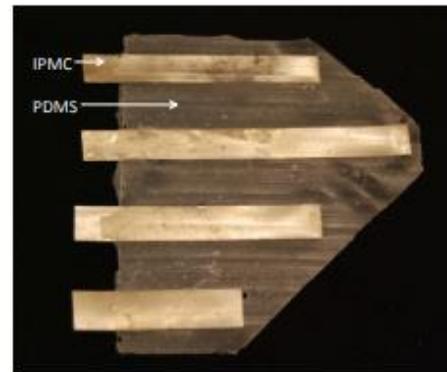


Fig. 10. IPMC/PDMS Artificial Pectoral Fins (Adapted from Z. Chen et al.).

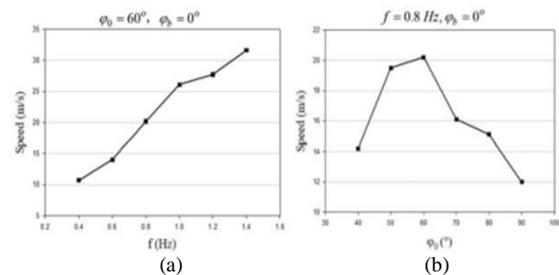


Fig. 11. Forward Motion Test (Adapted from Lei Liu et al.).

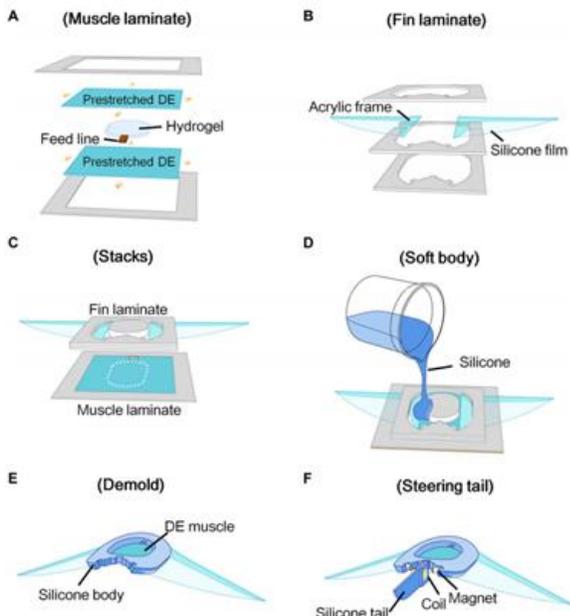


Fig. 12. Fabrication Process of Electro-ionic Fish (Adapted from T. Li et al.).

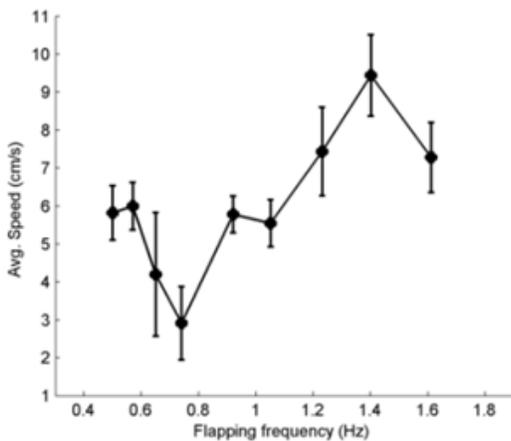


Fig. 13. Average Speed Versus Flapping Frequency (Adapted from Lincoln N. et al.).

Table 1 shows the summary and brief detail of the paper been discussed in this section. All project title, objective, project design and propulsion mechanism in this paper can be referred here.

TABLE I. SUMMARY OF PAPER DISCUSSED

Title	Objective	Design	Propulsion Mechanism
Biomimetic Fish Actuated by Shape Memory Alloy	Develop Koi's fish like robot using SMA to pectoral and caudal fin.		Shape Memory Alloy link together with spring pulley.
A micro-robot fish with embedded SMA wire	To develop and study the robot propulsion using SMA.		Shape memory alloy and power by battery.

actuated flexible biomimetic fin	The result to identify whether robot can swim and turning using this method.		
Monolithic IPMC Fins for Propulsion and Maneuvering in Bioinspired Underwater Robotic	To develop IPMC fins that can provide novel and efficient propulsion.		Monolithic platinum gold Ionic polymer-metal composite
Bio-inspired robotic manta ray powered by ionic polymer-metal composite artificial muscles	To improvise bio-inspired robotics manta ray propeller using artificial pectoral fins.		Ionic polymer-metal composite with thin membrane of poly-dimethyl siloxane (PDMS)
A Bending Pneumatic Rubber Actuator Realizing Soft-bodied Manta Swimming Robot	To introduce modern design and prototype for pneumatic rubber actuator for soft-bodied manta ray.		Pneumatic soft actuator
Analysis of the Effect Waveform Parameters have on Stingray Surface Velocity	To analyze and produce numerical model for baseline of robotic stingray		Servo motor
Design and Preliminary Evaluation of a Biomimetic Underwater Robot with Undulating Fin Propulsion	To build a prototype of underwater robot with undulation fins propulsion.		Servo motor attach with thin layer of membrane
Fast-moving soft electronic fish	To build robot using Dielectric Elastomer (DE) soft actuator.		Soft actuator
Stingray-inspired robot with simply actuated intermediate motion	To create an underwater swimming robot that have same propulsion method as <i>dasyatis americana stingray</i>		Servo motor

VI. HYBRID PROPULSION

Hybrid propulsions is a combination of two or more smart materials as a propulsive method for the robot [48,49]. Harbin Engineering University and Kagawa University develop jellyfish like robot by using SMA and IPMC. This method does produce propulsive force by bending both smart actuators to produce propulsive force by bending and shrinking [50, 51].

Guo S. et al. also develop a jellyfish like robot using hybrid method of IPMC and SMA with rubber materials as a body. With highest frequency of 0.6Hz, it produces 6mm/s speed. Fig. 14 shows the structure of the robot. Lead wires use to produce applied voltage to SMA and IPMC. This robot consists of four legs made of IPMC while SMA attach to the body to produce shrinking to mimic the jellyfish.

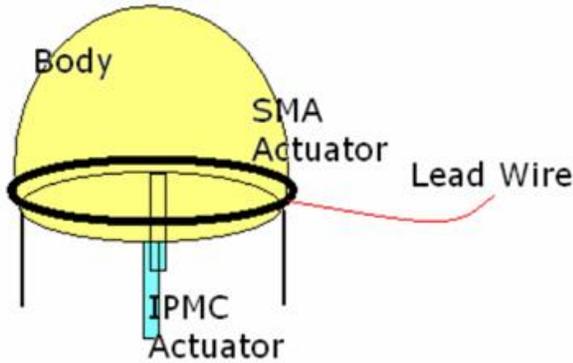


Fig. 14. Structure of the Robot. (Adapted from Guo S. et al.).

VII. MODELLING AND CONTROL OF ROBOTIC FISH

To control, maneuver and actuate the robot fish, controller is part of the important component to build. Controller system is used to change of normal existing behavior to achieve the desired wanted from the study or design [52],[57],[58]. Controller system usually connection between microcontroller as processor with sensor or transducer as an input for the process [53]. From papers that been discussed in chapter 5, none of them applied control mechanism in their robot since most of the study focus on propulsion of the smart actuator. The use of control mechanisms can improve the robot's capacity to complete tasks.

T.Salumäe et al. robot used two flow sensors located at nose of the robot to sense incoming flow to maintain balance by using Braintenberg 2b controller. Braintenberg 2b controller perform rheotaxis to maintain the orientation of the robot [64]. The conclusion from this study concludes that rheotaxis behavior can be achieve by measure flow coming to sensor as feedback.

This paper use Brainternerg 2b controller for wheeled and implement into fish robot by comparing pressure on both left and right side of the fish body [54]. The result from testing can be seen in Fig. 15. The red line is actual result which can be seen very noisy, and relation based on equation.

$$\theta = f(P_R - P_L) \quad (2)$$

f is frequency of the robot applied. P_R and P_L can describe as pressure on both right and left sensor.

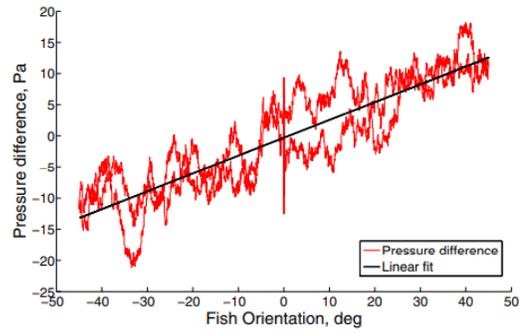


Fig. 15. Pressure difference on the Left and Right Versus the Orientation of the Robot θ .

As the aim of this project to keep angular deviation close to direction of incoming flow. Derived from equation (2), the tail angle offset ϕ_0 can be measure using control law (3) and equation (4) is added to minimize the drift in sensor reading. K_ϕ and C_d here are constant.

$$\phi_0 = [0 - (P_R - P_L)c] K_\phi \quad (3)$$

$$(P_R - P_L)c = C_d \int [0 - (P_R - P_L)]Dt + (P_R - P_L) \quad (4)$$

To control the tail beat amplitude (A), equation (5) is use. X_{sp} is desired position of the robot and X_{pv} is actual postion of the robot. K_A is chosen to be constant.

$$A = (X_{sp} - X_{pv}) K_A \quad (5)$$

Ming W. et al. use Central pattern Generator (CPG) as controller to control robotic fish. CPG can be said as all essential or basic movement that require repetitive action of specific muscle [65],[66]. Data from CPG controller is feed to Back Propagation Neural Network (BPNN) to optimize. The design use three separate servomotor joint together to react. BPNN prediction method able to provide optimize motion control for robotic fish swimming [55].

The proportional – integral – derivative (PID) controller is one of the most popular and widely used in the process industry due to its simplicity, wide applicability, and robustness. [68]. Su Si Yuan, et al. used PID controller to perform the steady swim of the fish robot by combining with Kalman filter. Kalman filtering can minimize the movement error and improve movement accuracy to get shortest time to the target based on the variable feed [61]. Fig. 16 shows PID algorithm combining with Kalman filter. According to the findings of this study, combining PID control and the Kalman filter results in faster reaction, better stability, and higher accuracy [56].

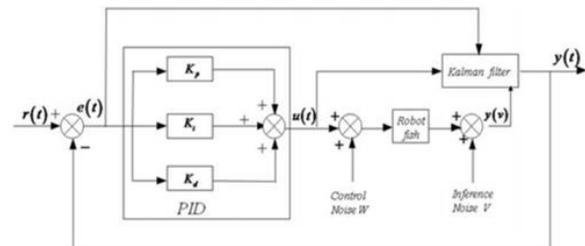


Fig. 16. PID Flowchart Algorithm (Retrieve from Su Si Yuan et al.)

Kalman filter give five basic formulas.

$$X(k|k-1) = A \times X(k-1|k-1) + B \times U(k) \quad (6)$$

$$P(k|k-1) = A \times P(k-1|k-1)A^T + Q \quad (7)$$

$$X(k|k) = X(k|k-1)Kg(k)(Z(k) - H \times X(k|k-1)) \quad (8)$$

$$Kg(k) = (P(k|k-1)H^T(H \times P(k|k-1)H^T + R)^{-1} \quad (9)$$

$$P(k|k) = (1 - Kg(k) \times H) P(k|k-1) \quad (10)$$

$X(k|k-1)$ is the prediction of last state. $X(k-1|k-1)$ is the optimal result of last state. $P(k|k-1)$ is $X(k|k-1)$ prior error, $P(k-1|k-1)$ is $X(k-1|k-1)$ posterior error. Kg is the matrix gain and R is system measurement of noise covariance matrix. Based on result achieve by the writer, PID control with Kalman filter may be look deeper to have better understanding and to implement into robot control.

VIII. CONCLUSION

The development of underwater fish robotics is one of the challenging research areas to improve underwater technology [28]. A comprehensive review on biomimetic underwater robots in this paper is reviewed based on their actuators and swimming modes. The ability of a robot to mimic wildlife can help improve the robot such propulsion and maneuverability [63]. Right propulsion materials have shown improvement in building the robot. Each material has its own advantages and disadvantage. It can be understood materials use for actuator has different result and can be applied for different propulsion mode. However, smart materials still slower compared the robot with engine or pump. As for writer, the application of soft actuator shows promising future since its newer technology. Soft actuators use simple implementation to operate. It is understandable that the designed robot must properly mimic the real fish to achieve it desires and to sustain the robot from damaging the aquatic life.

As the fish can adapt to vary environment, robot is manmade machine and lack of this ability. The robot must be equipped with smart technology to face all probable causes by taking proper measurement. As the current research shows promising result, there are still rooms for improvement for underwater robot to work better. This propulsion method with smart actuator can be considered still a testing stage where significant improvement can be made for each smart actuator. Future researcher also may come out with new propulsion alternative which may work better compared to current option. Researcher also may focus on control system and robot design to improve the fish robot itself.

For the robot design, design from the preliminary result show a good result. Depend on reference fish, the design and be both MPF and BCF swimming mode fish. The main idea to be considered during build is the reference fish since it will impact the result. Some fish can swim good in deep water and some fish only good with shallow water. Same goes the water condition with flow since most of the current study do testing in lab, aquarium, or pool. The result may different when put into sea or river or wildlife environment. For further study, it is recommended the testing is done in river or water with flow to study the result.

With the popular demand of underwater robot from various party, researcher technically should improve the current robot to meet with the demand. With the market around 7 million US dollar, it shows that the underwater robot is bigger market than what people seen. Thus, more researcher and study needed to come out with better robot to perform specific task with smart technology.

As the paper initially study to help writer on understanding about biomimetic underwater robot and smart actuator use, this paper also hope can be help for further researcher to understand in developing underwater robot and biomimetic robot.

ACKNOWLEDGMENT

The authors gratefully acknowledge to the Ministry of Higher Education (MoHE) Malaysia for financial supports given under the Fundamental Research Grant Scheme (FRGS/1/2019/TK04/UNIKL/02/11).

REFERENCES

- [1] G. Eason, Razif Muhammad, Mohd Faudzi, Ahmad Athif, Mohd Nordin, Ili Najaa Aimi, Natarajan, Elango, Yaakob, Omar. A Review on Development of Robotic Fish, (2014), Vol. 1. Pp. 12-22.
- [2] Chu, WS., Lee, KT., Song, SH., et al. Review of biomimetic underwater robots using smart actuator. Int. J. Precis. Eng. Manuf.13, (2012).
- [3] M. Aminur R B, B. Hemakumar and M. P. R Prasad. Robotic Fish Locomotion & Propulsion in Marine Environment: A Survey, 2018. 2nd International Conference on Power, Energy and Environment: Towards Smart Technology (ICEPE), pp. 1-6,
- [4] Feilich, Kara & Lauder, George. Passive mechanical models of fish caudal fins: Effects of shape and stiffness on self-propulsion. Bioinspiration & biomimetics. (2015).
- [5] Neely, Lincoln, Gaiennie, Jack, Noble, Nick, Erickson, Jon. Stingray-inspired robot with simply actuated intermediate motion, 2016.
- [6] Robert Bogue. Underwater robots: a review of technologies and applications, 2015, Industrial Robot: An International Journal, Vol. 42 Iss 3.
- [7] Yinghao Wu, Xuxiang Ta, Ruichao Xiao, Yaoguang Wei, Dong An, Daoliang Li. Survey of underwater robot positioning navigation, Applied Ocean Research, 2019, Volume 90.
- [8] Shi, L. Guo, S.; Li, M.; Mao, S.; Xiao, N.; Gao, B.; Song, Z.; Asaka, K. A Novel Soft Biomimetic Microrobot with Two Motion Attitudes. Sensors 2012, 12, 16732-16758.
- [9] Amit Shukla, Hamad Karki. Application of robotics in offshore oil and gas industry— A review Part II, Robotics and Autonomous Systems, Volume 75, Part B, 2016, Pages 508-524.
- [10] Jianhui He, Yonghua Zhang. Development and motion testing of a robotic ray. 2015. Journal of robotic, Vol. 2015.
- [11] Sfakiotakis, D. M. Lane and J. B. C. Davies. Review of fish swimming modes for aquatic locomotion.1999. IEEE Journal of Oceanic Engineering, vol. 24, no. 2, pp. 237-252.
- [12] Smits, A. Undulatory and oscillatory swimming. (2019). Journal of Fluid Mechanics, 874, P1.
- [13] Duraisamy, P., Kumar Sidharthan, R., Nagarajan Santhanakrishnan, M. Design, Modeling, and Control of Biomimetic Fish Robot: A Review. (2019). J Bionic Eng 16, 967-993.
- [14] Pichet Suebsaiprom, Chun-Liang Lin, Maneuverability modeling and trajectory tracking for fish robot, Control Engineering Practice, 2015, Volume 45, Pages 22-36, ISSN 0967-0661.
- [15] P. ValdiviaAlvarado, K. Youcef-Toumi. Performance of Machines with Flexible Bodies Designed for Biomimetic Locomotion in Liquid Environments, 2005. IEEE International Conference on Robotics and Automation, 2005, pp. 3324-3329.
- [16] S. B. Behbahani and X. Tan. Design and Modeling of Flexible Passive Rowing Joint for Robotic Fish Pectoral Fins. 2016. IEEE Transactions on Robotics, vol. 32, no. 5, pp. 1119-1132.

- [17] S. Zhang, Y. Qian, P. Liao, F. Qin and J. Yang. Design and Control of an Agile Robotic Fish with Integrative Biomimetic Mechanisms. 2016. IEEE/ASME Transactions on Mechatronics, vol. 21, no. 4, pp. 1846-1857.
- [18] Riccio, A.; Napolitano, C.; Sellitto, A.; Acanfora, V.; Zarrelli, M. Development of a Combined Micro-Macro Mechanics Analytical Approach to Design Shape Memory Alloy Spring-Based Actuators and Its Experimental Validation. *Sensors* 2021, 21, 5506.
- [19] K. Suzumori, S. Endo, T. Kanda, N. Kato and H. Suzuki. A Bending Pneumatic Rubber Actuator Realizing Soft-bodied Manta Swimming Robot. 2007. Proceedings 2007 IEEE International Conference on Robotics and Automation, 2007, pp. 4975-4980.
- [20] J. J. Hubbard, M. Fleming, V. Palmre, D. Pugal, K. J. Kim and K. K. Leang. Monolithic IPMC Fins for Propulsion and Maneuvering in Bioinspired Underwater Robotics. 2014. in *IEEE Journal of Oceanic Engineering*, vol. 39, no. 3, pp. 540-551, July 2014.
- [21] Huang, P. H., & Wang, J. A New Design of Underwater Robot Fish System Using Shape Memory Alloy. *Applied Mechanics and Materials*. (2012). Pp. 187, 260–266.
- [22] Li T, Li G, Liang Y, Cheng T, Dai J, Yang X, Liu B, Zeng Z, Huang Z, Luo Y, Xie T, Yang W. Fast-moving soft electronic fish. *Sci Adv*. 2017.
- [23] M. Sfakiotakis, D. M. Lane and J. B. C. Davies. Review of fish swimming modes for aquatic locomotion. 1999. in *IEEE Journal of Oceanic Engineering*, vol. 24, no. 2, pp. 237-252, April 1999.
- [24] Jian-Xin Xu, Qinyuan Ren, Wenchao Gao and Xue-Lei Niu. Mimicry of fish swimming patterns in a robotic fish. 2012. *IEEE International Symposium on Industrial Electronics*, 2012, pp. 1274-1279.
- [25] X. Niu, J. Xu, Q. Ren and Q. Wang. Locomotion Learning for an Anguilliform Robotic Fish Using Central Pattern Generator Approach. 2014. *IEEE Transactions on Industrial Electronics*, vol. 61, no. 9, pp. 4780-4787, Sept. 2014.
- [26] Song, Sung-Hyuk, Lee Hyeok, Lee Jonggu, & Lee, Jang-Yeob, Cho, Maenghyo, Ahn, Sung-Hoon. Design and analysis of a smart soft composite structure for various modes of actuation. (2016). *Composites Part B: Engineering*. 95.
- [27] D. Zhang, K. H. Low, H. Xie and L. Shen. *Advances and Trends of Bionic Underwater Propulsors*. 2009. WRI Global Congress on Intelligent Systems, 2009, pp. 13-19.
- [28] Curet, Oscar, Patankar, Neelesh, Lauder, George, Maciver, Malcolm. Mechanical properties of a bio-inspired robotic knifefish with an undulatory propulsor. (2011). *Bioinspiration & biomimetics*.
- [29] Hirata K. Development of experimental fish robot. *Proc. of Japan Society for Design Engineering*, Tohoku Branch.
- [30] Deepak Trivedi, Christopher D. Rahn, William M. Kier & Ian D. Walker. Soft robotics: Biological inspiration, state of the art, and future research. (2008). *Applied Bionics and Biomechanics*.
- [31] Blake, R. W. REVIEW PAPER Fish functional design and swimming performance (2004).
- [32] X. Niu, J. Xu, Q. Ren, Q. Wang. Locomotion Learning for an Anguilliform Robotic Fish Using Central Pattern Generator Approach. 2014. *IEEE Transactions on Industrial Electronics*, vol. 61, no. 9, pp. 4780-4787, Sept. 2014.
- [33] Pichet Suebsaiprom, Chun-Liang Lin, Anumat Engkaninan. Undulatory locomotion and effective propulsion for fish-inspired robot.
- [34] J. Finkbeiner, J. Ahmad, W. Santosa, G. Y. Xu and J. Xiao, "Biomimetic fish actuated by shape memory alloy," 2011 6th IEEE Conference on Industrial Electronics and Applications, 2011, pp. 2139-2144, Doi: 10.1109/ICIEA.2011.5975945.
- [35] Z. Wang, Y. Wang, J. Li and G. Hang, "A micro biomimetic manta ray robot fish actuated by SMA," 2009 IEEE International Conference on Robotics and Biomimetics (ROBIO), 2009, pp. 1809-1813, Doi: 10.1109/ROBIO.2009.5420423.
- [36] Zhenlong Wang, Guanrong Hang, Jian Li, Yangwei Wang, Kai Xiao. A micro-robot fish with embedded SMA wire actuated flexible biomimetic fin. (2008).
- [37] Xiufen Ye, Yudong Su and Shuxiang Guo, "A centimeter-scale autonomous robotic fish actuated by IPMC actuator," 2007 IEEE International Conference on Robotics and Biomimetics (ROBIO), 2007, pp. 262-267.
- [38] Zheng Chen, Tae I. Um & Hilary Bart-Smith (2012) Bio-inspired robotic manta ray powered by ionic polymer–metal composite artificial muscles, *International Journal of Smart and Nano Materials*/.
- [39] Chen, Zheng & Um, Tae & Bart-Smith, Hilary. (2011). Ionic Polymer-Metal Composite Enabled Robotic Manta Ray. *Proceedings of SPIE - The International Society for Optical Engineering*.
- [40] Hao M, Wang Y, Zhu Z, He Q, Zhu D and Luo M. A compact review of IPMC as soft actuator and sensor: current trends, challenges and potential solutions from our recent works. (2019).
- [41] Nowell, Jordan & Connor, Jack & Joordens, Matthew & Champion, Benjamin. (2018). Analysis of the Effect Waveform Parameters have on Stingray Surface Velocity.
- [42] Lei Liu et al 2020 IOP Conf. Ser.: Mater. Sci. Eng. 790 012160.
- [43] Ying He, Dao Bo Wang and Zain Anwar Ali. A review of different designs and control models of remotely operated underwater vehicle. (2020).
- [44] Marras Stefano and Porfiri Maurizio. 2012. Fish and robots swimming together: attraction towards the robot demands biomimetic locomotion. *J. R. Soc. Interface*.
- [45] Riccio, A.; Napolitano, C.; Sellitto, A.; Acanfora, V.; Zarrelli, M. Development of a Combined Micro-Macro Mechanics Analytical Approach to Design Shape Memory Alloy Spring-Based Actuators and Its Experimental Validation. *Sensors* 2021, 21, 5506.
- [46] Mohd Aliff, Ahmad Raziq Mirza, Mohd Ismail and Nor Samsiah, "Development of a Low-Cost Bio-Inspired Swimming Robot (SRob) with IoT" *International Journal of Advanced Computer Science and Applications (IJACSA)*, 12(7), 2021.
- [47] T. V. Truong, V. K. Viswanathan, V. S. Joseph and P. V. y. Alvarado, —Design and Characterization of a Fully Autonomous Under-Actuated Soft Batoid-like Robot, 2019 IEEE/RSJ International Conference on Intelligent Robots and Systems (IROS), 2019, pp. 5826-5831.
- [48] C. M. Chew, Q. Y. Lim, and K. S. Ye, —Development of propulsion mechanism for Robot Manta Ray, in *Robotics and Biomimetics (ROBIO)*, 2015 IEEE International Conference on, pp. 1918–1923.
- [49] Y. Yang, X. Ye and S. Guo, "A New Type of Jellyfish-Like Microrobot," 2007 IEEE International Conference on Integration Technology, 2007, pp. 673-678.
- [50] S. Guo, L. Shi, X. Ye and L. Li, "A New Jellyfish Type of Underwater Microrobot," 2007 International Conference on Mechatronics and Automation, 2007, pp. 509-514.
- [51] B. Tang, L. Jiang and R. Li, "Bionic Robot Jellyfish Based on Multi-Link Mechanism," 2020 International Wireless Communications and Mobile Computing (IWCMC), 2020, pp. 649-652.
- [52] Canete, J. & Galindo, Cipriano & Moral, Inmaculada. (2011). *Introduction to Control Systems*. 10.1007/978-3-642-20230-8_5.
- [53] T. Salumäe, I. Rañó, O. Akanyeti and M. Kruusmaa, "Against the flow: A Braitenberg controller for a fish robot," 2012 IEEE International Conference on Robotics and Automation, 2012, pp. 4210-4215.
- [54] Wang Ming, Yu Junzhi, TanMin and Yang Qinghai, "Back-Propagation Neural Network based predictive control for biomimetic robotic fish," 2008 27th Chinese Control Conference, 2008, pp. 430-434.
- [55] Su, Si Yuan, et al. "Robotic Fish's Movement Based on Kalman Filter and PID Control." *Applied Mechanics and Materials*, vol. 568–570, Trans Tech Publications, Ltd., June 2014, pp. 1059–1062. Crossref, Doi: 10.4028/www.scientific.net/amm.568-570.1059.
- [56] Lei Liu, et al. 2020. Design and Preliminary Evaluation of a Biomimetic Underwater Robot with Undulating Fin Propulsion. *IOP Conf. Ser.: Mater. Sci. Eng.*
- [57] Shi, Q., Ishii, H., Sugahara, Y., Takanishi, A., Huang, Q., & Fukuda, T. (2015). Design and Control of a Biomimetic Robotic Rat for Interaction with Laboratory Rats. *IEEE/ASME Transactions on Mechatronics*, 20(4), 1832–1842.
- [58] Lauder, G. V., & Santo, V. D. (2015). *Swimming Mechanics and Energetics of Elasmobranch Fishes*. *Fish Physiology Physiology of Elasmobranch Fishes: Structure and Interaction with Environment*, 219–253.

- [59] Yamakita, M., Kamamichi, N., Luo, Z. W., & Asaka, K. (2016). Robotic Application of IPMC Actuators with Redoping Capability. *Electroactive Polymers for Robotic Applications*, 199-225.
- [60] Kiebert, L., & Joordens, M. (2016). Autonomous robotic fish for a swarm environment. 2016 11th System of Systems Engineering Conference (SoSE).
- [61] Younghoo K and Hyochong B. (2019). Introduction to Kalman Filter and Its Applications. DOI 10.5772/intechopen.80600.
- [62] G. Li, Y. Deng, O. L. Osen, S. Bi, and H. Zhang, —A bio-inspired swimming robot for marine aquaculture applications: From conceptdesign to simulation, | OCEANS 2016 - Shanghai, 2016, pp. 1-7.
- [63] Shi, L., Guo, S., and Asaka, K., “A novel multifunctional underwater microrobot,” 2010 IEEE International Conference on Robotics and Biomimetics (ROBIO) pp. 873-878, 2010.
- [64] Pan, X., Li, L., Chen, S., & Xie, G. (2015). An effective tracking control for robotic fish: Implementation and application. 2015 34th Chinese Control Conference (CCC). doi:10.1109/chicc.2015.7260598.
- [65] Bucher, D., haspel, G., Golowasch, J., & Nadim, f> (2015). Central Pattern Generators. DOI 10.1002/9780470015902.a0000032.pub2.
- [66] Marder, E., and Bucher D.,. 2001. Central pattern generators and the control of rhythmic movements, *Current Biology*, [https://doi.org/10.1016/S0960-9822\(01\)00581-4](https://doi.org/10.1016/S0960-9822(01)00581-4).
- [67] Degeratu, S., Bîzdoaca, N.G., Manolea, G., Diaconu, I., Petrisor, A., & Degeratu, V. (2008). On the design of a shape memory alloy spring actuator using thermal analysis. *WSEAS TRANSACTIONS on SYSTEMS* archive, 7, 1006-1015.
- [68] Navid Razmjooyand Mehdi Ramezani. (2014). Using Quantum Gates to design a PID Controller for Nano robots. *International Research. Journal of Applied and Basic Sciences*, 8(12), 2354-2359.

Fuel Consumption Prediction Model using Machine Learning

Mohamed A. HAMED, Mohammed H.Khafagy, Rasha M.Badry
Department of Information Systems, Faculty of Computers and Information
Fayoum University, Fayoum 63514, Egypt

Abstract—In the paper, we are enhancing the accuracy of the fuel consumption prediction model with Machine Learning to minimize Fuel Consumption. This will lead to an economic improvement for the business and satisfy the domain needs. We propose a machine learning model to predict vehicle fuel consumption. The proposed model is based on the Support Vector Machine algorithm. The Fuel Consumption estimation is given as a function of Mass Air Flow, Vehicle Speed, Revolutions Per Minute, and Throttle Position Sensor features. The proposed model is applied and tested on a vehicle's On-Board Diagnostics Dataset. The observations were conducted on 18 features. Results achieved a higher accuracy with an R-Squared metric value of 0.97 than other related work using the same Support Vector Machine regression algorithm. We concluded that the Support Vector Machine has a great effect when used for fuel consumption prediction purposes. Our model can compete with other Machine Learning algorithms for the same purpose which will help manufacturers find more choices for successful Fuel Consumption Prediction models.

Keywords—Fuel consumption; machine learning; support vector machine; feature weight; feature selection; on-board diagnostic

ABBREVIATIONS

DT:	<i>Decision Tree</i>
FC:	<i>Fuel Consumption</i>
FS:	<i>Feature Selection</i>
GB:	<i>Gradient Boosting</i>
IoT:	<i>Internet of Things</i>
ML:	<i>Machine Learning</i>
MAF:	<i>Mass Air Flow</i>
MAE:	<i>Mean Absolute Error</i>
NN:	<i>Neural Networks</i>
OBD:	<i>On-Board Diagnostics</i>
RF:	<i>Random Forest</i>
RFE:	<i>Recursive Feature Elimination</i>
RMSE:	<i>Root Mean-Squared Error</i>
RBF:	<i>Radial Basis Function</i>
RPM:	<i>Revolution Per Minute</i>
SVM:	<i>Support Vector Machine</i>
ANN:	<i>Artificial Neural Network</i>
TPS:	<i>Throttle Position Sensor</i>
VS:	<i>Vehicle Speed</i>
ECU:	<i>Electronic Control Units.</i>

I. INTRODUCTION

In this study, we are trying to enhance fuel consumption (FC) prediction using machine learning algorithms. We used a Support Vector Machine algorithm to predict fuel consumption. We measure fuel consumption based on a legacy Dataset containing On-Board Diagnostics (OBD) data. The aim is to achieve a good value for the R-Squared metric using the SVM.

OBD is the protocol responsible for scanning and reading the ECU in the vehicle. OBD adapter can scan the ECU and send the FC data to a third-party device. OBD is considered a part of the Internet of Things technique. It can be connected to remote datasets to save its data for important and urgent analysis related to vehicles depending on Big Data, Deep Learning, and Machine Learning techniques. These analyses are helpful for instant diagnoses for vehicles and other types of machines which are using the same OBD protocol[1-4].

Fuel Consumption has an essential interest for individuals, businesses, and the globe. The price of fuel controls the economy of the world. Therefore, changes in the price of fuel affect the economical side for businesses.

Machine Learning is considered an application of Artificial Intelligence. Arthur Samuel said that Machine Learning: “is defined as the field of study that gives the computers the ability to learn without being explicitly programmed” [5].

One of the famous algorithms of Machine Learning is the Support Vector Machine (SVM) algorithm. SVM is an algorithm that tries to predict a specific value or a set of classes either in classification or regression form [6, 7]. It has been used in several studies related to the prediction of fuel consumption. These studies are considered to be related to our work similarly.

We used SVM to propose an ML model for fuel consumption prediction purposes. The other related research work had applied the SVM algorithm to predict FC based on a training dataset of a small size. Its results were not enough good. Its model had returned an R-Squared value equal 0.004624. It depended on the RPM_TPS-based equation only, which will be discussed later. However, in our research, we used both the RPM_TPS-based equation besides the VS_MAF-based equation. There is no other literature that discussed the same problem with the SVM algorithm depending on both RPM_TPS-based and VS_MAF-based equations. The RPM_TPS-based equation depends on RPM and TPS parameters. The VS_MAF-based equation depends on VS and

MAF parameters. These two equations are considered the most important equations that can be used to measure the fuel consumption rate when a complete FC Dataset exists. Our FC Dataset is considered a high-dimensional size dataset.

It's important to note that our proposed model and its internal experiments couldn't be observed without an FC Dataset containing the parameters which are existing in the FC equations used.

Before using SVM for the prediction of fuel consumption, Feature Weighting should be described. Feature Weighting is the ranking process of the importance of the features, as it depends on a voting approach for ranking the importance of the features in datasets [8].

Feature Weighting is followed by the Feature Selection step. Feature Selection is applied to the highly ranked features after the Feature Weighting step. Then, these highly ranked features are filtered and applied to the classifier [8].

Feature Selection can be applied to datasets using different algorithms. Random Forest and Decision Tree are the most famous algorithms used to rank the importance of the features and select the highly ranked features.

In the last decade, scholars talked about the importance of predicting the consumed fuel percentage depending on some of the sophisticated algorithms from both Data Mining (DM) and Machine Learning (ML). However, in an earlier time, scholars had discussed the prediction of fuel consumption with different algorithms, including Neural Networks (NN), Random Forest (RF), Gradient Boosting (GB), and Support Vector Machine (SVM) [9, 10].

The prediction of fuel consumption value will become more precise when predicted with sophisticated ML techniques. The discussion of fuel consumption has been a trending topic when discussed from the view of ML in the last five years.

Many research papers have been developed to discuss the most followed methods for monitoring fuel consumption in vehicles. Fuel consumption scholars have focused on different methods that should be followed to eliminate fuel consumption.

In [11], the authors had used sophisticated techniques depending on ML models to detect and measure levels of fuel consumption using Support Vector Machine (SVM) and Artificial Neural Networks (ANNs) models. They used 27 vehicles in their experiments. They discussed their multiple tries for achieving better accuracy on different types of vehicles of the same age, different segments, engine displacement, and type of transmission. Finally, they achieved accuracy with 83%.

In [12], the authors had discussed the problem of predicting fuel in fleets of vehicles depending on machine learning techniques. They had used Random Forest, Gradient Boosting, and Neural Networks as machine learning models. Random Forest Algorithm had achieved the best result between the other used algorithms. However, they depended on the Nash-Sutcliffe coefficient for measuring the predictive power for the efficiency of each model. Also, they used Bias, Mean Absolute

Error (MAE), and Root Mean-Squared Error (RMSE) as error statistics to evaluate their model's accuracy.

In [13], the authors had used a machine-learning algorithm to predict fuel consumption depending on a set of variables in a large-scale Dataset gathered by 153 drivers during a month depending on GPS and CAN (Controller Area Network) bus data, including speed of the vehicle and moved distance. They used regression methods for the machine learning methods: SVM, ANN, Linear Regression (LR), and Link Fuel Summation SVM model (LSSVM). Their study revealed that SVM had the best R-Squared value with 0.92 while ANN, LR, and LSSVM had R-Squared values of 0.86, 0.74, and 0.79. The training phase had affected the superiority of SVM over other models. However, SVM had generated the best fit results/accuracy. Also, it wasn't affected by cost functions as it provided a linear penalty to huge error rates where the ANN model minimizes the sum of squared errors.

In [14], the authors had used Boruta Algorithm (BA) and Neural Networks (NNs) algorithm to measure fuel consumption regarding a huge fleet of trucks on different road pavements. BA had shown a good result in comparison with previous studies, which used the same data. While the developed NN algorithm had achieved (R2) value of 0.88 for test data. NN appeared to be a suitable candidate for analyzing large datasets effectively and predicting the impact of roughness and macrotexture of roads on truck fuel consumption.

In [15], the authors had addressed the identification of driving style issues. They used the K-means clustering algorithm to differentiate between different types of driving styles. Driving styles are divided into three categories: normal, soft, and aggressive category. Also, they used random forest, K-nearest neighbor, support vector machine, and neural network models. Random forest overall accuracy was 95.39% while trucks are in their heavy load, and 90.74% on no-load status. The aggressive driving style achieved the largest fuel consumption and reached 10 % higher than the average driving style.

In [16], the authors had used Autonomie, which is a simulation tool, to simulate the process of fuel and vehicle power consumption. They proposed a Large-scale learning and prediction process (LSLPP) with machine learning models. LSLPP tests were successful as they could accelerate analysis processes and prediction of vehicle's fuel consumption.

In [17], the authors had used the Support Vector Machine (SVM) model as one of the ML prediction techniques with OBD-II to monitor and predict fuel consumption levels. The proposed model uses both TPS and RPM variables to measure the consumed level of fuel. Finally, their RMSE value was 2.43.

In [18], the authors had used SVM, RF, and ANN algorithms for fuel consumption prediction purposes. SVM and ANN algorithms achieved the best results. However, RF outperformed both of them. The coefficient of determination (R2) for SVM, RF, and ANN are 0.83, 0.87, and 0.85, respectively.

II. PROPOSED MODEL

The proposed model aims to predict fuel consumption using SVM. The proposed model consists of four phases: Data Preprocessing, Feature Weighting, Feature Selection, and SVM Prediction Model, as shown in Fig. 1. The proposed prediction model has been applied to FC Dataset with 8262 records. The Dataset includes 18 fields, as shown in Table I. FC Dataset was gathered by 19 drivers using an OBD scanner in vehicles, which was used for a previous dissertation for profiling automotive data in 2018 [19]. The Dataset gathered by 19 drivers had been collected depending on a vehicle model of the well-known Brazilian vehicle, A 2015 Chevrolet S10, which has a 2.5-liter flex-fuel engine by 206 hp. This Dataset is gathered in an urban road in the city of Natal (Brazil). It was gathered at a distance of 18.8 kilometers for 34 minutes for each driver [20, 21].

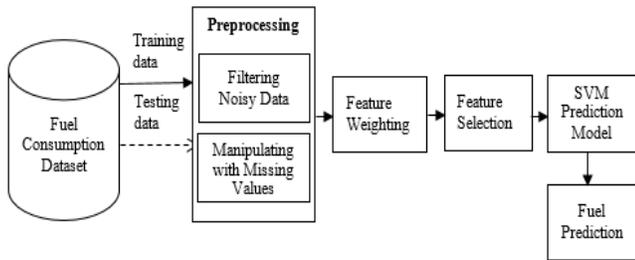


Fig. 1. Proposed Model Diagram.

TABLE I. FC DATASET FIELDS

No.	Field Name	Field Description
1	TIME	Vehicle's work period.
2	LATITUDE	Latitude of the vehicle while reading time.
3	LONGITUDE	Longitude of the vehicle while reading time.
4	ALTITUDE	The altitude of the vehicle while reading time.
5	BAROMETRIC_PRESSURE	Measuring the atmospheric pressure.
6	ENGINE_COOLANT_TEMP	Measuring the engine's temperature.
7	FUEL_LEVEL	Level of fuel in tank at the reading time.
8	ENGINE_LOAD	Measure sucked air and fuel into the engine.
9	AMBIENT_AIR_TEMP	Refer to the outside air temperature.
10	ENGINE_RPM	Refer to the frequency of rotation around a fixed axis.
11	INTAKE_MANIFOLD_PRESSURE	Refer to the negative air pressure inside the intake pipe.
12	MAF	Measure the amount of air entering the engine.
13	AIR_INTAKE_TEMP	Refer to air temperature in the engine.
14	SPEED	Speed value of the vehicle at request time.
15	Short Term Fuel Trim Bank 1	Refer to ECU signaling response according to the changes of the oxygen levels.
16	THROTTLE_POS	Identify the value of air-delivered quantity to vehicle's engine accurately.
17	TIMING_ADVANCE	Refer to the required time for the air-fuel mixture to be burned.
18	EQUIV_RATIO	Refer to the commanded air/fuel ratio of the engine.

A. Pre-processing

Data pre-processing is the first step in the proposed prediction model. Converting the data into a more desired and eligible form is essential to ensure that the Dataset is accurate and ready for further processing [22, 23]. In our proposed model, we are performing filtering noisy data and manipulating with missing values steps.

1) *Filtering noisy data:* This step is a very important step in which the noisy records in FC Dataset are removed. For example, some cells are filled with symbols and characters like the Speed field, which contains (50 km/h). Such characters and symbols affect the implementation and results of the prediction model.

2) *Manipulating with missing values:* Most of the fields in our FC Dataset had filled with data. However, our FC Dataset was high-dimensional. Hence, it was difficult to discover the missing values by hand. So, we had to automate this process using specific techniques to avoid exceptions happening while training the SVM algorithm as the missing values may cause a big issue for processing the prediction model. For example, the FC Dataset contains fields with Nan, Null, or Zero values, in which the R2 value of the regression model is affected negatively and returned exceptions in the runtime. There are several methods to handle missing values. One of these methods is the mean imputation. The imputation method estimates the missing values by replacing them with the mean for that variable [24].

B. Feature Weighting

Feature weighting is an essential step in identifying the most feature or a set of features affecting other specific features. In the proposed model, feature weighting is used to set weights for FC Dataset features to identify which feature mostly affects the fuel consumption level. We used two models for weighting features in our Dataset. These models are Random Forest (RF) and Decision Tree Algorithm.

The Random Forest Algorithm is considered a good and reliable algorithm for features ranking for small and larger datasets. This is because it can distinguish the relevant and the irrelevant attributes in the Dataset. It can handle both classification and regression problems by constructing multiple decision trees concurrently and returning equivalent forecasting for the average result of the processed decision trees. RF can handle high-dimensional datasets as it can process too many inputs and return results with high performance [25, 26].

Decision Tree Algorithm is also an important model used to identify the importance of the attributes in the Dataset in which feature selection can be used in higher and lower-dimensional classification tasks. It describes the relations between data that can be simulated by leaves in the trees. Each node has other leaf nodes under it. Each leaf node holds a specific value that represents a meaningful form for the algorithm. A tree constitutes a leaf and a node. In classification, nodes represent a group to be classified and each node subset represents a value that can be taken by the node [27, 28].

Feature weighting is applied to the whole selected features of the FC Dataset to determine the most important features that affect fuel consumption. Clarification of feature weighting phase and used methodologies and algorithms will be discussed in another following section.

Feature weighting is applied to features in equations that are used for calculating fuel consumption. Fuel consumption can be calculated via two methods, the first is based on VS and MAF features, and the second is based on RPM and TPS features.

1) *VS_MAF-based*: VS_MAF is the first method used for calculating fuel consumption, according to (1).

$$f = VS / MAF \quad (1)$$

Where f is fuel consumption value, VS is the vehicle speed parameter, which is measured in km/hour, and MAF refers to the value of Mass Air Flow in the engine, which is measured in g/s (gram per second).

Depending on (1), fuel consumption can be measured using two metrics, the first metric is Mile Per Gallon (MPG), and the second metric is Liters per 100 Km. For example, the following equation retrieves the fuel consumption values in MPG and L/100KM.

To retrieve the fuel consumption value in US MPG, based on (2), the value of Speed is divided by MAF then multiplied by $\alpha = 7.718$, which is a constant.

$$f = VS * \alpha / MAF * \beta \quad (2)$$

Further, to retrieve fuel consumption value in liters per 100 km, we multiply the fuel consumption value in US MPG by the value of the constant β [17].

2) *RPM_TPS-based*: RPM_TPS is the second method used for calculating fuel consumption, according to (3).

$$\text{Fuel}_{(\text{rpm}, \text{tps})} = p00x^2 + p10x + p01xy \quad (3)$$

Where X refers to Revolutions Per Minute (RPM), Y refers to Throttle Position Sensor (TPS), and the coefficients $p00$, $p10$, $p01$ values are 2.685, -0.1246, and 1.243, respectively.

Our feature selection experiments had been applied using the VS_MAF-based Equation and the RPM_TPS-based Equation. Generated results from our Random Forest Algorithm indicated that RPM, SPEED, and MAF have the highest effects on fuel consumption levels. Results and analysis for applying RF to FC Dataset will be provided in more detail in specific sections for the experiments, discussion, and results.

C. Feature Selection

After feature weighting, feature selection is applied to determine the most weighted features that affect the fuel consumption value after feature weighting. First, the generated weights of the FC features by the weighting models RF and DT are ranked, then a selection of the most important features is done.

D. The SVM Prediction Model

The proposed model is based on Support Vector Machine (SVM). The SVM model is a machine learning algorithm that

reads input data and represents points on a 2d space or 3d space to be drawn on X-axis and Y-axis in 2d view or X-axis, Y-axis, and Z-axis in 3d view. Then, it draws a boundary line that splits the groups and classifies the data to refer to which class the point is grouped or classified. SVM has a maximum margin line that usually divides the class of points equally called "hyperplane". The hyperplane looks for the maximum distance between each point and its nearest group or class [18]. The hyperplane is divided into two different types. The first one is the optimal hyperplane, which is the linear function with the maximum margin between vectors or multiple vectors in two groups, and the second one is called the soft margin hyperplane, which happens when two classes of the data are not linearly separable [6].

E. Experiments

In the experiment section, the details of the performed experiments are illustrated. Several experiments had been done using a historical FC Dataset. However, the proposed work for predicting fuel consumption using SVM with a regression model is considered the first experiment with this algorithm to be conducted specifically on this Dataset. The experiments are conducted using two equations. The first is based on MAF and VS features, and the second is based on RPM and TPS features.

The results of the experiments have been evaluated using the coefficient of determination metric R-Squared/R², a statistical metric that represents the variance between dependent and independent variables and evaluates the model's ability for prediction purposes [29].

After applying feature weighting and selection, we update both the VS_MAF-based equation and the RPM_TPS-based equation. These updates improve the Squared Correlation Coefficient metric R-Squared/R² value of the proposed model compared with other studies.

1) *Applying feature weighting*: Feature Weight/importance is identified via different algorithms used to select the most important features in high-dimensional datasets. RF and DT are two important algorithms used to measure features and find the correlations in FC Dataset.

Random Forest (RF) is a machine learning algorithm commonly used to evaluate the model's ability for prediction purposes.

Recursive Feature Elimination (RFE) was first used and proposed to enable the SVM model to evaluate the features/attributes importance and identify field ranking in datasets. The same methodology has been added to the RF algorithm to find the correlated features/fields in datasets with high dimensionality [30].

RF and DT algorithms are reliable enough to be considered for measuring the importance of the features in our FC Dataset. Using RF and DT for features weighting purposes during our observation leads to a better focus of the prediction purpose, after removing the unnecessary features from the experiment.

We had imported both RF and DT algorithms in Spider engine to run them using Python v.9 programming language.

Python has become an essential programming language for ML research. We used Python to print the weight results for FC Dataset features. We could draw figures using Matplotlib, which is a drawing and visualization library using Python, to differentiate the features with high and low importance values [31].

We had applied the RF-RFE algorithm on most of the features of the FC Dataset, which are 18 features. We had removed 15 features from the original FC features, which were 33 features. For example, Term Fuel Trim Bank 1, FUEL_ECONOMY, Long Term Fuel Trim Bank 2, FUEL_TYPE, FUEL_PRESSURE, Short Term Fuel Trim Bank 2, and TROUBLE_CODES had been removed because they were empty field. DTC_NUMBERS had been removed because it contained String values like 4101000761001:00410100076100, which is not meaningful. ENGINE_RUNTIME had been removed because it contained time values like 12:03:20 AM. VEHICLE_ID had been removed because it contained String values like s11. Finally, we had applied the feature selection experiment on both the VS_MAF-based equation and the RPM_TPS-based equation. We had measured the importance/weight score of all measured features in our FC Dataset. The results of feature weighting algorithms which were returned with high importance values looked to exist in the FC equations that we are already depending on during our proposed model. That means that using RF and DT for feature weighting has returned reasonable features for measuring FC Dataset weights.

a) *Feature Selection experiment applied on 18 features using (RF)*: We applied the Random Forest Algorithm for identifying the importance/weight score for the features existing in our Dataset. Table II shows the importance of our Dataset features. Fig. 2 and Fig. 3 show a representation of the feature's importance in our Dataset. It was found that the most important features that affect the fuel consumption level after applying the feature selection algorithm according to the VS_MAF-based equation are MAF and SPEED. However, when applying the RPM_TPS-based equation, it was found that RPM is the most important feature.

Fig. 2 indicates that MAF and SPEED parameters are the most important parameters in the Dataset that affect fuel consumption according to VS_MAF-based equations. While Fig. 3 indicates that ENGINE_RPM is the most important feature that affects fuel consumption between the whole features in the dataset according to the RPM_TPS-based equation.

b) *Weighted VS_MAF-based equation*: According to the VS_MAF-based equation, fuel consumption calculation is based on MAF and VS features. Depending on RF and DT algorithms, Table III, Fig. 4, and Fig. 5 represent the feature importance results for both MAF and VS features.

In Table III, and Fig. 4 the results show and indicate that both MAF and SPEED features affect fuel consumption features with a feature weight of 0.50876 for MAF and 0.49124 for SPEED using the RF algorithm. However, in Table III and Fig. 5 both the MAF and SPEED features affect

the fuel consumption feature with a feature weight of 0.50665 for MAF and 0.49335 for SPEED using the DT algorithm. This indicates that the importance value of the MAF and SPEED features doesn't hugely change when applied to the RF or DT algorithms.

Also, the previous importance values for both of the features refer to the more significant impact of the MAF feature over the SPEED feature when compared to each other according to their effect on the fuel consumption value.

After calculating feature weight for MAF and VS, the VS_MAF-based equation can be updated by adding the weight values for the equation.

So, we can multiply each feature in the equation by its importance according to Table III to become:

$$f = VS * vs_i / MAF * maf_i \tag{4}$$

Where $vs_i = 0.49124$ and $maf_i = 0.50876$ by RF algorithm.

TABLE II. WEIGHTS OF FEATURES USING RANDOM FOREST ALGORITHM

No.	Field Name	VS_MAF-Equation	RPM_TPS-Equation
1	TIME	0.00037	0.00000
2	LATITUDE	0.00046	0.00001
3	LONGITUDE	0.00046	0.00000
4	ALTITUDE	0.00038	0.00001
5	BAROMETRIC_PRESSURE	0.00018	0.00000
6	ENGINE_COOLANT_TEMP	0.00024	0.00000
7	FUEL_LEVEL	0.00028	0.00000
8	ENGINE_LOAD	0.00506	0.00001
9	AMBIENT_AIR_TEMP	0.00024	0.00000
10	ENGINE_RPM	0.00050	0.99992
11	INTAKE_MANIFOLD_PRESSURE	0.00035	0.00000
12	MAF	0.56186	0.00000
13	AIR_INTAKE_TEMP	0.00032	0.00001
14	SPEED	0.42643	0.00000
15	Short Term Fuel Trim Bank 1	0.00042	0.00000
16	THROTTLE_POS	0.00197	0.00000
17	TIMING_ADVANCE	0.00048	0.00000
18	EQUIV_RATIO	0.00000	0.00000

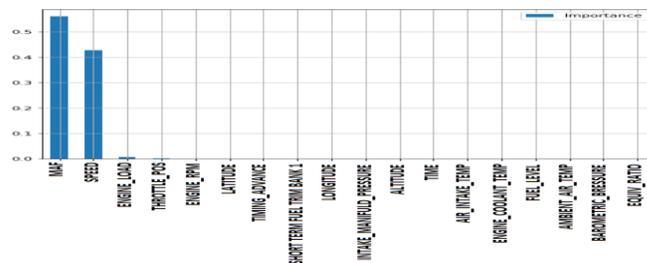


Fig. 2. Features Importance using VS_MAF-based Equation Results with Random Forest Algorithm.

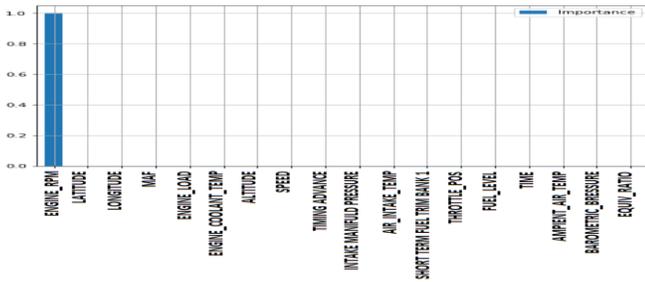


Fig. 3. Features Importance using RPM_TPS-based Equation Results with Random Forest Algorithm.

TABLE III. MAF AND VS FEATURE IMPORTANCE ACCORDING TO RF AND DT ALGORITHMS

VS_MAF-based Equation		
Algorithm	MAF Weight	VS Weight
Random Forest	0.50876	0.49124
Decision Tree	0.50665	0.49335

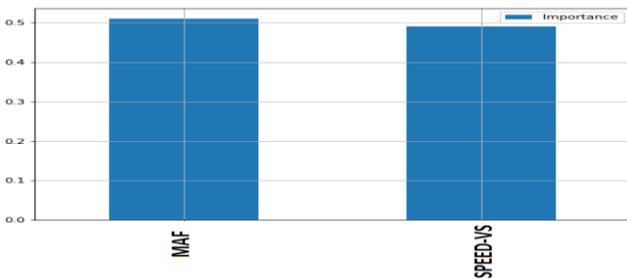


Fig. 4. MAF and VS Feature Importance using Random Forest Algorithm.

c) *Weighted RPM_TPS-based equation*: According to the RPM_TPS-based equation, fuel consumption calculation is based on RPM and TPS features. Therefore, depending on the RF and DT algorithms, Table IV and Fig. 6, and Fig. 7 include the feature importance results for both RPM and TPS features.

Table IV and Fig. 6 indicate that both RPM and TPS features affect the fuel consumption feature with a feature weight of 0.999952 for RPM and 0.000048 for TPS using the RF algorithm. However, in Table IV and Fig. 7, both the RPM and TPS features affect the fuel consumption with a feature weight of 0.999969 for RPM and 0.000031 for TPS using the DT algorithm. This indicates that the importance value of the RPM and TPS features doesn't change when applied to the RF or DT algorithms. Also, the previous importance values for both of the features refer to the massive importance of the RPM when compared with TPS importance.

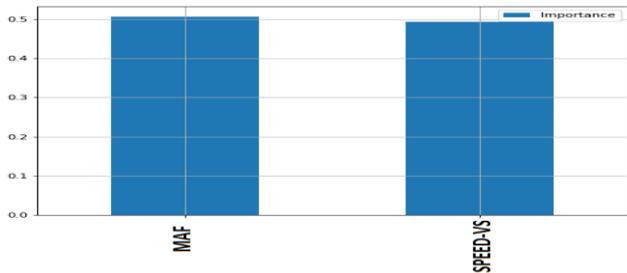


Fig. 5. MAF and VS Feature Importance using Decision Tree Algorithm.

TABLE IV. RPM AND TPS FEATURE IMPORTANCE ACCORDING TO RF AND DT ALGORITHMS

RPM_TPS-based Equation		
Algorithm	RPM Weight	TPS Weight
Random Forest	0.999952	0.000048
Decision Tree	0.999969	0.000031

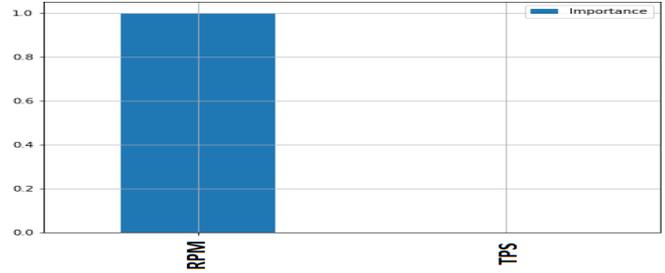


Fig. 6. RPM and TPS Features Importance using Random Forest Algorithm.

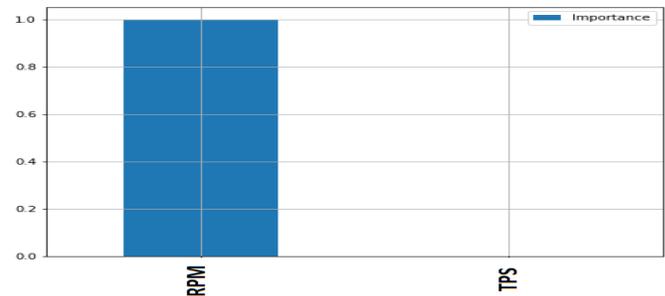


Fig. 7. RPM and TPS Features Importance using Decision Tree Algorithm.

The same as the VS_MAF-based equation, the RPM_TPS-based equation calculate fuel consumption rate using the following equation:

$$\text{Fuel}_{(rpm, tps)} = p00x^2 + p10x + p01xy \quad (5)$$

We can update the last equation via multiplying RPM and TPS by their importance values according to the generated results by the RF algorithm in Table IV to become:

$$\text{Fuel}_{(rpm, tps)} = p00x^2 * rpm_i + p10x * rpm_i + p01xy * rpm_i * tps_i \quad (6)$$

Where $rpm_i = 0.999952$ and $tps_i = 0.000048$ by RF algorithm.

2) *Applying SVM on fuel consumption equations*: The SVM model is applied using the original and the new-weighted fuel consumption equations, which calculates fuel consumption values. We had noticed the difference in the squared correlation coefficient R^2 metric value for each conducted experiment.

Table V shows a sample of the data using the VS_MAF-based experiment and the RPM_TPS-based experiment. Fig. 8 compares the actual and predicted values of fuel using the VS_MAF-based equation when implemented using the SVM model, while Fig. 9 compares the actual and predicted values of fuel using the RPM_TPS-based equation when implemented using the SVM model.

In Fig. 8, according to the VS_MAF-based experiment, it looks that some of the actual fuel consumption data are quite

similar to the predicted values, which are likely similar to the result of the R-Squared/R² value of the model that reached 0.97, which indicates that the SVM model has achieved a high accuracy depending on the VS_MAF-based equation. Also, in Fig. 9, according to the RPM_TPS-based experiment, it looks that some of the actual data are quite similar to the predicted fuel consumption values, which are likely similar to the result of the R-Squared/R² value of the model that reached 0.96, which indicates that the SVM model has achieved a high accuracy too using the result of applying the RPM_TPS-based equation.

TABLE V. VS_MAF SAMPLE DATA

Dataset – Data Frame				
Index	MAF (g/s)	SPEED (VS) (km/h)	RPM (rev/min)	TPS (%)
0	24.77	48	2124	34.9
1	30.96	60	2617	36.1
2	18.58	64	3005	32.2
3	18.38	65	3156	32.5
4	19.77	67	1798	33.3
5	9.99	65	1818	28.6

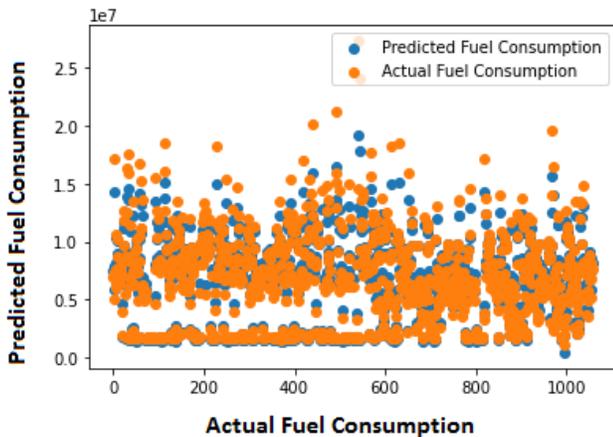


Fig. 8. Comparing the Actual to the Predicted Values of Fuel using VS_MAF-based Equation and SVM Algorithm.

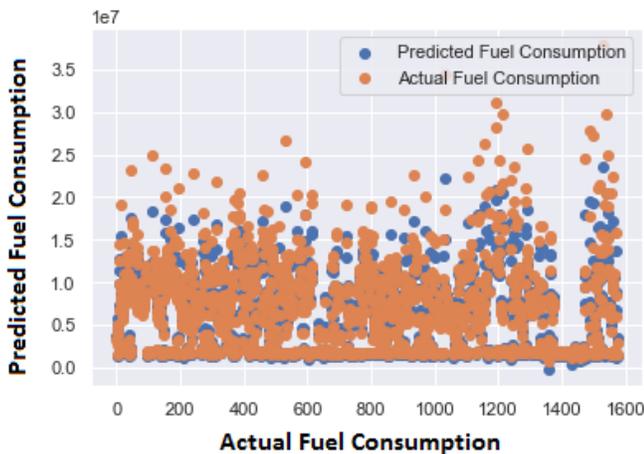


Fig. 9. Comparing the Actual to the Predicted Values of Fuel using RPM_TPS-based Equation and SVM Algorithm.

III. DISCUSSION

The performance of the proposed model is evaluated using the R-Squared/R² metric. The model is applied using two equations. The new VS_MAF-based equation depended on two variables are SPEED and MAF, while the new RPM_TPS-based equation depended on RPM and TPS variables. The squared correlation coefficient R-Squared/R² metric using the original VS_MAF-based equation and the original RPM_TPS-based equation is 0.96, according to Table VI.

We can notice that the squared correlation coefficient R-Squared/R² metric value has changed after applying the new-weighted equations for the VS_MAF-based equation. For example, the squared correlation coefficient R-Squared/R² metric using the new VS_MAF-based equation became 0.97 after applying the new-weighted equation for the original VS_MAF-based equation, according to Table VI. This is because we had depended on a Radial Basis Function (RBF) as a kernel function of the SVM model while training and testing phases of the VS_MAF-based equation. However, we had depended on a Linear function of the SVM model while the training and testing phases of the RPM_TPS-based equation, which became 0.96 after applying the new-weighted RPM_TPS-based equation.

We had achieved a superior result better than other candidates [17] who achieved lower results: R-Squared/R² = 0.004624 than our experiment using the same SVM predictor model depending on the RPM_TPS-based equation. Therefore, our goodness of fit using the R-Squared/R² metric equals 0.96 when applied their original RPM_TPS-based equation and our new-weighted RPM_TPS-based equation, according to Table VI.

Finally, the new weighted-VS_MAF-based equation had affected the R-Squared/R² metric value to be 0.97, while the new weighted-RPM_TPS-based equation had affected the R-Squared/R² metric value to be 0.96, according to Table VII.

IV. RESULTS

The value of the R-Squared/R² metric is 0.96 for the original VS_MAF-based equation and the original RPM_TPS-based equation, while the value of the R-Squared/R² metric is 0.97 while applying the New-weighted VS_MAF-based equation and 0.96 for applying the New-weighted RPM_TPS-based equation.

Table VI refers to the R-Squared/R² value of our prediction model, SVM, using the original and the new-weighted equations.

TABLE VI. R2 METRIC VALUE OF SVM MODEL WHEN APPLYING THE ORIGINAL AND THE NEW-WEIGHTED EQUATIONS FOR PREDICTION OF FUEL CONSUMPTION

FC equation	R-Squared/R ² metric value		
	Proposed model results		Related work results
	VS_MAF	RPM_TPS	RPM_TPS
Original	0.96	0.96	0.004624
New-weighted	0.97	0.96	-----

TABLE VII. R2 METRIC VALUES AFTER APPLYING THE VS_MAF AND RPM_TPS EQUATIONS USING THE SVM MODEL

FC Equation	R-Squared (R ²)
Proposed weighted VS_MAF- equation	0.97
Proposed Weighted RPM_TPS- equation	0.96

Finally, Table VII shows the final result of the squared correlation coefficient R-Squared/R² metric value using the new weighted VS_MAF-based equation and new weighted RPM_TPS-based equation, respectively.

V. CONCLUSION

This study had applied four different equations in four experiments on a historical OBD dataset for predicting fuel consumption using the SVM regression model as an ML technique. These equations were the original VS_MAF-based equation and the new weighted-based equation which depended on Speed and MAF variables. Also, these equations included the original RPM_TPS-based equation and the new weighted-based equation which depended on RPM and TPS variables.

The squared correlation coefficient R-Squared/R² metric value of the SVM model became 0.96 for both of the original equations, and (0.97, 0.96) for the new equations, VS_MAF-based equation, and RPM_TPS-based equation, respectively.

This study had achieved better results than other candidates who applied the RPM_TPS-based equation using the SVM model [17] as their R-Squared/R² equals 0.004624 while implementing their RPM_TPS-based equation.

Future research may be a try to investigate more correlated parameters in FC Dataset to create more mathematical equations for measuring FC. The more correlated parameters the more equations that calculate FC, consequently, the more experiments and observations that lead to better enhancements and more accurate FC prediction models with ML. MAF, RPM, SPEED, ENGINE_LOAD, and ENGINE_RPM may have a greater correlation that can be used to create a new mathematical equation to measure FC in our FC Dataset or we can use a larger dataset for implementing FC prediction observations. Also, the great enhancement will be to convert the proposed model to a running system integrated with Internet of Things components and devices in the vehicle and predict fuel consumption instantly with SVM in the runtime applying our proposed model.

REFERENCES

[1] A. A. M. S. Medashe Michael Oluwaseyi "Specifications and Analysis of Digitized Diagnostics of Automobiles: A Case Study of on Board Diagnostic (OBD II)," vol. 9, 1 ed: IJERT, 2020.

[2] T. A. Nikolaos Peppes, Evgenia Adamopoulou and Konstantinos Demestichas, "Driving Behaviour Analysis Using Machine and Deep Learning Methods for Continuous Streams of Vehicular Data," vol. 4704, Machine Learning Applied to Sensor Data Analysis ed: MDPI: sensors, 2021.

[3] A. K. S. Siddhanta Kumar Singh, and Anand Sharma, "OBD - II based Intelligent Vehicular Diagnostic System using IoT," ed. ISIC'21: International Semantic Intelligence Conference: Mody University of Science and Technology, Lakshmangarh, Sikar, Rajasthan, India, 2021.

[4] U. M. P. Pirapuraj, "Intelligent Vehicle Diagnostic System for Service Center using OBD-II and IoT," ed. Conference: International

Conference of Science and Technology - 2021: Faculty of Technology, South Eastern University of Sri Lanka, Oct 2021.

[5] B. Mahesh, "Machine Learning Algorithms - A Review," vol. 9, 1 ed: International Journal of Science and Research (IJSR), 2020, p. 7.

[6] C. Cortes, & Vapnik, V., "Support-vector networks. ," vol. 20, ed. Machine learning, 1995, pp. 273-297.

[7] M. P. Theodoros Evgeniou, "WORKSHOP ON SUPPORT VECTOR MA CHINES: THEORY AND APPLICATIONS," vol. 2049, ed. Conference: Advanced Course on Artificial Intelligence (ACAI 1999) :Machine Learning and Its Applications , Lecture Notes in Computer Science, 2001, pp. 249-257.

[8] M. D. d. L. N. L. da Costa, R. Barbosa, "Evaluation of feature selection methods based on artificial neural network weights," vol. 168, ed. Expert Systems with Applications (2020), 2020.

[9] A. Schoen, Byerly, A., Hendrix, B., Bagwe, R. and d. S. M., E. C., & Miled, Z. B., "A machine learning model for average fuel consumption in heavy vehicles.," vol. 68, 7 ed. IEEE Transactions on Vehicular Technology: IEEE, 2019, pp. 6343-6351.

[10] Y. Yao, Zhao, X., Liu, C., Rong, J., Zhang, Y., and Z. Dong, & Su, Y., "Vehicle fuel consumption prediction method based on driving behavior data collected from smartphones," vol. 2020, ed. Journal of Advanced Transportation, 2020.

[11] E. Moradi, & Miranda-Moreno, L., "Vehicular fuel consumption estimation using real-world measures through cascaded machine learning modeling. ," vol. 88, ed. Transportation Research Part D: Transport and Environment, 2020.

[12] S. Wickramanayake, & Bandara, H. D., "Fuel consumption prediction of fleet vehicles using machine learning: A comparative study. ," ed. In 2016 Moratuwa Engineering Research Conference (MERCOn) IEEE., 2016, pp. 90-95.

[13] W. Zeng, Miwa, T., & Morikawa, T., "Exploring trip fuel consumption by machine learning from GPS and CAN bus data. ," vol. 11, ed. Journal of the Eastern Asia Society for Transportation Studies, 2015, pp. 906-921.

[14] F. Perrotta, Parry, T., Neves, L. C., & M. Mesgarpour, "A machine learning approach for the estimation of fuel consumption related to road pavement rolling resistance for large fleets of trucks.," ed. The Sixth International Symposium on Life-Cycle Civil Engineering (IALCCE 2018), 2018.

[15] Q. Wang, Zhang, R., Wang, Y., & Lv, S., "Machine learning-based driving style identification of truck drivers in open-pit mines. ," vol. 9, 1 ed: Electronics, 2020, p. 19.

[16] J. Yao, & Moawad, A., "Vehicle energy consumption estimation using large scale simulations and machine learning methods.," vol. 101, ed. Transportation Research Part C: Emerging Technologies, 2019, pp. 276-296.

[17] T. Abukhalil, AlMahafzah, H., Alksasbeh, M., and B. A. & Alqaralleh, "Fuel consumption using OBD-II and support vector machine model.," vol. 2020, ed. Journal of Robotics, 2020, pp. 1-9.

[18] F. Perrotta, Parry, T., & Neves, L. C., "Application of machine learning for fuel consumption modelling of trucks.," ed. In 2017 IEEE International Conference on Big Data (Big Data) IEEE, 2017, pp. 3810-3815.

[19] B. a. C. A. D. Silveira, "Use of machine learning techniques to identify car usage profiles based on automotive data," ed. <https://repositorio.ufrn.br/jspui/handle/123456789/26017>: Metropole Digital Institute, Fedral University of Rio Grande do Norte, Natal, 2018.

[20] J. C. Cephas A, Anne M, Ivanovitch S., "A Machine Learning Approach Based on Automotive Engine Data Clustering for Driver Usage Profiling Classification.," ed. In Anais do XV Encontro Nacional de Inteligência Artificial e Computacional (ENIAC)At: Brazil, 2018, pp. 174-185.

[21] C. A. d. S. Barreto, "OBD-II Datasets," no. v0.3, 2018. [Online]. Available: <https://www.kaggle.com/cephasax/obdii-ds3>.

[22] U. a.-l. a. c. r.-i. l. t.-l. t.-d. n. d.-l. s. b.-s. border-box et al., "A Novel Machine Learning Data Preprocessing Method for Enhancing Classification Algorithms Performance," ed. 16th EANN workshops: Proceedings of the 16th Engineering Applications of Neural Networks Conference WORKSHOPS: Association for Computing MachineryNew YorkNYUnited States, 2015, pp. 1-5.

- [23] M. A. P. M. Md Manjurul Ahsan, Pritom Kumar Saha, Kishor Datta Gupta and Zahed Siddique, "Effect of Data Scaling Methods on Machine Learning Algorithms and Model Performance," vol. 9, ed. technologies: MDPI, 2021.
- [24] I. Pratama and A. E. Permanasari, Ardiyanto, I., & Indrayani, R., "A review of missing values handling methods on time-series data.," ed. In 2016 International Conference on Information Technology Systems and Innovation (ICITSI): IEEE, 2016, pp. 1-6.
- [25] M. B. Kursu, & Rudnicki, W. R., "The all relevant feature selection using random forest.," ed. <https://arxiv.org/abs/1106.5112>: arxiv.org, 2011.
- [26] N. M. K. S. A. Chinmay, "Optimization of the Random Forest Algorithm," ed. Advances in Data Science and Management, 2020, pp. 201-208.
- [27] K. Grabczewski, & Jankowski, N., "Feature selection with decision tree criterion.," ed. In Fifth International Conference on Hybrid Intelligent Systems (HIS'05): IEEE, 2005, p. 6.
- [28] B. T. J. a. A. M. Abdulazeez, "Classification Based on Decision Tree Algorithm for Machine Learning," vol. 2, ed. Journal of Applied Science And Technology Trends, 2021, pp. 20-28.
- [29] D. B. Figueiredo Filho and J. A. S. Júnior, & Rocha, E. C., "What is R2 all about? , " vol. 3, ed. Leviathan: Universidade de Sao Paulo, Agencia USP de Gestao da Informacao Academica (AGUIA), 2011, pp. 60-68.
- [30] B. F. Darst, Malecki, K. C., & Engelman, C. and D., "Using recursive feature elimination in random forest to account for correlated variables in high dimensional data.," vol. 19, ed. BMC Genetics (BMC GENET): BioMed Central, 2018, pp. 1-6.
- [31] Sebastian Raschka , a. Joshua Patterson , and C. Nolet, "Machine Learning in Python: Main Developments and Technology Trends in Data Science, Machine Learning, and Artificial Intelligence," ed: MDPI - Information, April, 2020.

Scalable and Reactive Multi Micro-Agents System Middleware for Massively Distributed Systems

EZZRHARI Fatima Ezzahra, EL ABID AMRANI Nouredine, YOUSSEFI Mohamed, BOUATTANE Omar
SSDIA Laboratory, ENSET, Hassan II University
Casablanca, Morocco

Abstract—IT transformation has revolutionized the business landscape and changed most of organizations business model into digital and innovation driven firms. To fully take advantage of this digitalization and the exponential growth of data, organizations need to rely on resilient, scalable, extremely connected, highly available & very performant systems. To meet this need, this paper presents a model of middleware for multi micro-agents system based on reactive programming and designed for massively distributed systems and High-Performance Computing, especially to face big data challenges. This middleware is based on multi-agents systems (MAS) which are known as a reliable solution for High Performance Computing. This proposal framework is built on abstraction and modularity principles through a multi-layered architecture. The design choices aim to ensure cooperation between heterogeneous distributed systems by decoupling the communication model and the cognitive pattern of micro agents. To ensure high scalability and to overcome networks latency, the proposal architecture uses distribution model of data & computing, that allows an adaptation of the grid size as needed. The resilience problem is addressed by adopting the same mechanism as Hazelcast middleware, thanks to his peer-to-peer architecture with no single point of failure.

Keywords—Massively distributed system; multi agent system (MAS); high performance computing; reactive programming; hazelcast

I. INTRODUCTION

Information technologies have faced breakthrough changes during the last decades: a huge acceleration of artificial intelligence, the invasion of cloud computing, an exponential growth of data with the appearance of 5G, the emergence of the big Data & IoT [1], and the birth of the blockchain.

This revolution is a real catalyst for the different fields and industries. It is the trend changing the future and requiring each organization to boost innovation, to ensure the performance and to improve the time to market so that it remains competitive and differentiated. So, companies need new information systems able to connect permanently with many objects, while executing treatments, analyzing huge quantities of data & making various decisions.

To meet these expectations, we need to establish new IT applications allowing data exploitation and enabling collective intelligence. The massive quantity of data received from all connected objects and social media need to be stored and analyzed differently with suitable strategies. Moreover, the systems need an acceleration of computing and are adopting

more and more massively distributed machines such as GPU architecture (Graphic Processing Units) [2] to perform their treatments more efficiently. Even so, the use of massively distributed machine unitary is not enough efficient to process a very large amount of data and perform the needed processing quickly, so the use of massively distributed systems [3] has become very common, with the deployment of several heterogeneous systems to allow faster data processing and more efficient data storage and analysis, it is today the real solution for High Performance Computing [4].

This solution has been approved with the development of new middlewares offering the possibility of cooperating several heterogeneous hardware and software systems: mobile devices, servers, PCs, electronic cards, embedded systems, etc. However, challenges for this type of architecture remain relevant: limitation in terms of network latency, load balancing, scalability, maintenance & fault tolerance.

To design a such complex system, we must use a paradigm capable of integrating these different constraints and providing a complete solution, promoting cooperation, interaction & scalability. This is the case of Multi-Agent Systems [5] which have proven their usefulness for this type of high complexity problem.

This article proposes a new model of multi micro-agent middleware for massively distributed systems based on reactive programming and applied to big data applications. The proposal framework is built on several abstraction levels to ensure modularity, scalability, load balancing and fault tolerance. It allows to cooperate different micro-agents that can be deployed in heterogenous IT infrastructure with different communication channels and various learning models. This middleware offers several technological implementations & interfaces for each layer and it is also open to extension by new implementations. To ensure a good performance level and to deal with fault tolerance challenge, we chose to use the mechanism of Hazelcast in term of data and computing distribution. So, the present model ensures resilience by guaranteed replication, a peer-to-peer architecture for the distribution of processing operations, and fault tolerance with the absence of Single Point Of Failure (SPOF).

We have organized the rest of this paper into six sections. The following section II is a description of the overall middleware architecture. Section III details the micro agent structure and kinematics. In the fourth section, we carried a deep dive of the data distribution model. The fifth section describes the computing distribution model of the middleware.

Section VI present some performance measurement of the proposal framework. And last section concludes with highlighting advantages and improvement areas of the present work.

II. GLOBAL ARCHITECTURE OF THE PROPOSED MIDDLEWARE

We have designed this framework to ensure a high level of abstraction and modularity [6], it is composed of several abstraction layers that are 7 APIs:

- An agent API for easy creation and deployment of micro-agents allowing different implementations and using multiple programming languages. This API defines the lifecycle of a micro-agent such as instantiation, initialization, deployment, serialization, deserialization, and destruction;
- A Communication API, that allows clear and transparent communication between micro-agents by adopting semantic messages ACL compliant;
- A cognitive API to implement & assign learning models to micro-agents with both supervised models and/or reinforcement learning models;
- A data distribution API: allowing to the middleware a balanced and transparent distribution of massive data. It uses distributed collections to dispatch data across cluster's nodes of heterogeneous computers.
- A data computing that enables a transparent distributed computing among the cluster nodes.
- A monitoring API to scan the status of the MAS.
- An API to build the cluster by defining the infrastructure to use for the distributed system.

Figure 1 illustrates the architecture and the different layers of a multi micro-agent system built by three member nodes.

A. Cluster Builder API

To create a Multi micro-Agent System using this middleware, we need first to identify the soft & hard infrastructure by launching a cluster of nodes. These infrastructures enable the distribution of data & computing for massive data applications or for computationally intensive applications.

A cluster [7] is a network of machines where each machine executes a member Instance. Each member automatically joins the others to form the cluster in a decentralized model while still having instances fully connected to each other's. The cluster's instances represent the hard core of the infrastructure allowing the nodes of the cluster to accommodate the data and the distributed computing over the micro-agents of the application.

To ensure the junction between the members of the cluster, different discovery mechanisms can be used by members to find each other, namely:

- Multicast mode: This mode uses the multicast mechanism with UDP protocol. It is useful when the cluster instances belong to the same local network.
- TCP mode: This mode requires the specification of the IP address of one of the active nodes of the cluster when a new member joins the cluster.
- Cloud Discovery: The proposal framework allows the use of cloud discovery services such as: AWS Cloud Discovery, ZooKeeper, Apache jclouds, GCP Cloud Discovery.

After establishing the junction between the members of the cluster, any communication between these members is carried out exclusively by a TCP / IP mode.

B. Monitoring API

In order to monitor the state of the cluster, we suggest starting a special instance in the cluster. Once it joins the cluster, this instance receives real-time notifications from all instances in the cluster whenever the state of an instance changes. Therefore, this instance will allow real-time monitoring of the distribution of data and computing at the cluster level.

C. Data Distribution API

To allow data distribution, this layer provides the default interfaces and implementations to represent data in standard structures and collections such as List, Map, Queue, Set, etc.

D. Computing Distribution API

This layer allows to distribute the execution of massive tasks of an application among the nodes of the cluster. It provides various interfaces & implementations allowing to submit complex jobs for distributed execution.

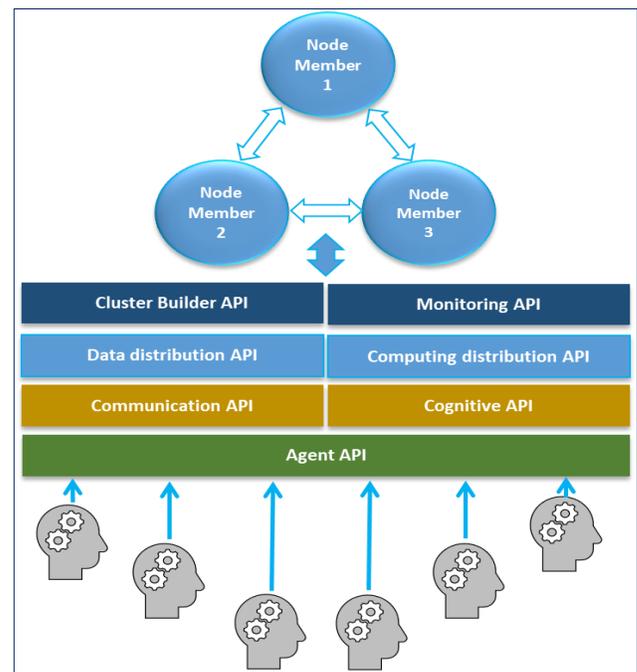


Fig. 1. Overall Architecture of the Proposal Middleware.

E. Communication API

We define at this layer the communication mechanisms between micro-agents. After each micro-agent deployment, the framework provides to this new agent a subscription to a Topic at the cluster level, then allows him to receive messages from other platform's micro-agents. This API also provides an implementation of Agent Communication Language (ACL) which allows agents to exchange semantic messages compliant to the FIPA [8] ACL standard and therefore ensuring interoperability with other MAS platforms.

F. Cognitive API

This API provides the interfaces and implementations for machine and deep learning models. It defines supervised, unsupervised and reinforcement learning models.

G. Agent API

This is the layer deploying interfaces & implementations to easily create micro agents by using and extending the functionalities offered by the other layers of the framework. This API also provides the mechanisms for managing the agent life cycle.

III. MICRO AGENT STRUCTURE AND KINEMATICS

In this section, we will have a deep dive on the Agent layer by presenting its static structure, its ecosystem, and its interactions with the other layers. We will detail the life cycle of a micro-agent by its deployment and migration processes.

A. Agent API Description

To create a micro-agent, the developer has just to extend the abstract class "Agent" and to redefine the operators that composes the agent's life cycle at its container level.

The created micro-agent inherits all operators allowing:

- Creating and configuring ACL messages;
- Sending messages to a micro-agent or to a community of agents by choosing a communication strategy by the developer. In fact, the present framework is open to extension by using any communication mechanism as by external brokers such as KAFKA, RabbitMQ or ActiveMQ based on several messaging protocols as MQTT, AMQP or STOMP. If the developer does not have a preference, the system is based by default on an internal communication system as a broker directly using the messaging functionalities offered by the middleware cluster [9].

The figure 2 focuses on the principle of micro-agent's communication of the model.

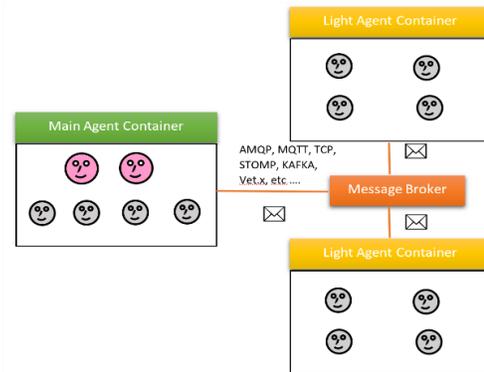


Fig. 2. Micro Agents Communication Model.

- Assign learning behavior to the micro-agent using one of the possible strategies. The framework implements 3 interfaces representing respectively:
 - supervised learning strategy with different implementations of machine and deep learning techniques based on neural networks.
 - unsupervised learning strategy with various implementations: the k-means clustering algorithm, fuzzy-cmeans, ...
 - reinforcement learning strategy with several possible implementations such as the Qlearning algorithm.

The developer is free to choose the appropriate learning strategy among these three implementations, to assign to his micro-agent according to the context of his application.

- Create and access the data collections distributed over the nodes of the cluster. We have defined interfaces and implementations based on classic distributed structures like Queue, Map, Topic.
- Submit distributed tasks for cluster-level executions. To create a distributed task, the developer must create a class that inherits from the abstract DistributedCallableTask class and then redefine the call method by implementing the code of the task to be distributed. The micro-agent can submit this distributed task to a cluster node transparently for remote execution returning the result asynchronously. Once deployed in a node, the task becomes bound to the instance, allowing it to transparently access the functionality and data distributed in the cluster.

Figure 3 illustrates the core class diagram of this API.

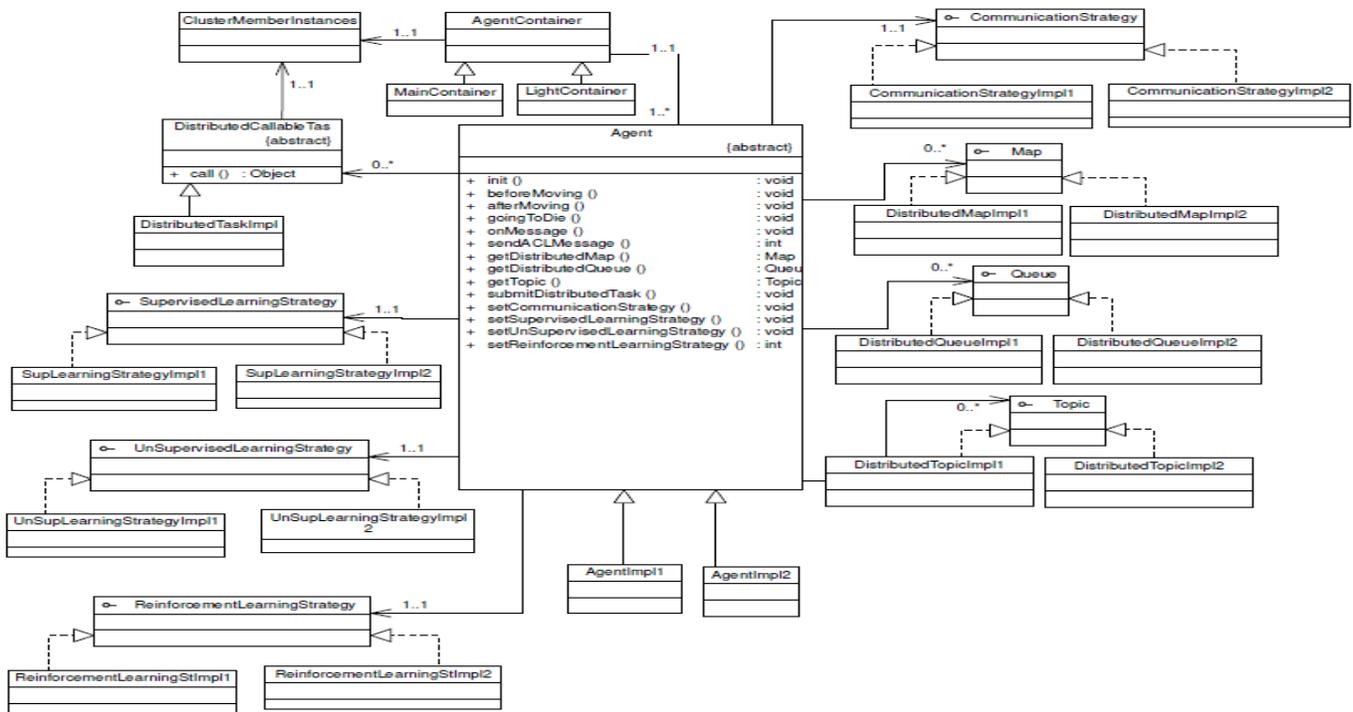


Fig. 3. Summary Class Diagram of the Agent API.

B. Agent Container

A micro-agent is systematically deployed in a container where it lives and finds the various techniques for managing its life cycle. An agent is systematically deployed in a container where it lives and finds the various techniques for managing its life cycle.

The present model is FIPA Compliant, it deploys two types of container: MainContainer which is deployed in a single instance of the MAS platform, and several LightContainers which allow the deployment of the agents of the developed MAS platform.

The MainContainer essentially deploys technical agents in accordance with the specifications of the FIPA:

- Agent Management System (AMS): used to manage the identity of agents and the communication system between agents.
- Directory Facilitator (DF) Agent: which defines the directory of yellow pages allowing agents to publish their services and discover the services offered by other agents of the MAS platform.

Once the MainContainer instance is started, the following operations are automatically performed:

- the launch of the first instance of the cluster for distributed computing.
- the deployment of AMS and DF agents that each subscribes their own mailbox as a Topic, at the level of the messaging service provided by the cluster.
- The subscription to a topic specific to the MainContainer.

Indeed, each time a container is created, the system must create a specific mailbox for this container, which is used in different agent operations, notably when a migration of an agent is requested to this container, by retrieving the code of the migrant agent in the mailbox.

- The start of the MainContainer graphical interface. This interface has a graphical component representing each agent deployed in the container to easily and visually identify the agents deployed and their location/status.

Figure 4 shows the sequence diagram illustrating the deployment of the MainContainer.

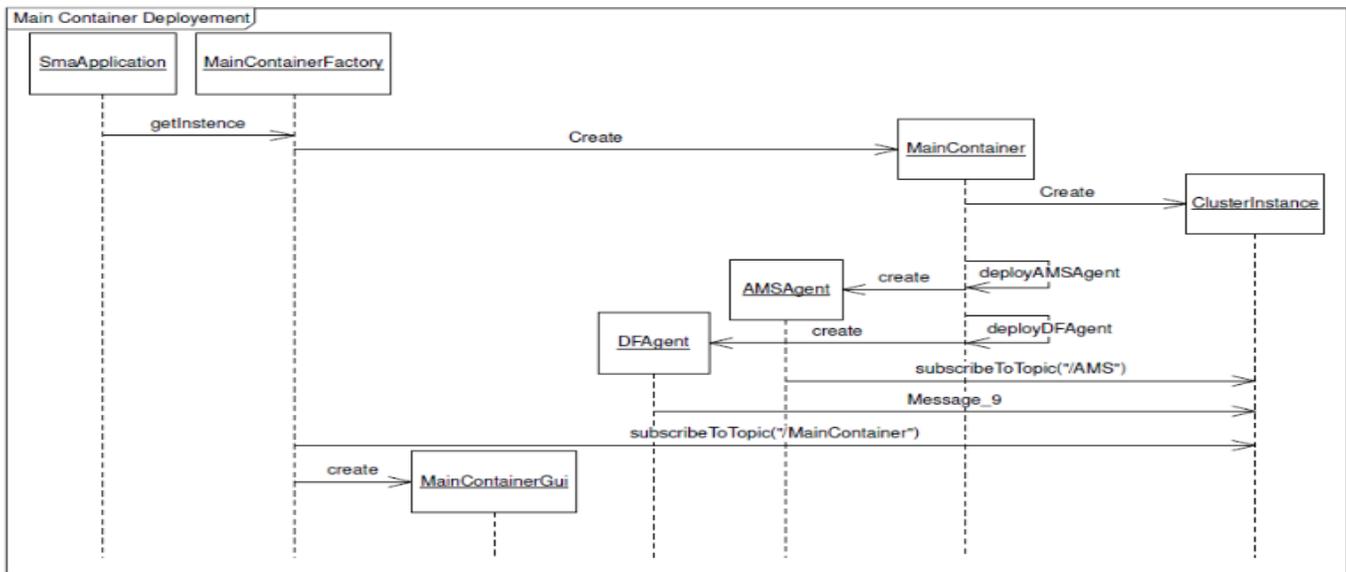


Fig. 4. Sequence Diagram for MainContainer Deployment Process.

To deploy a MainContainer with its Graphical interface, the developer must use just one code line:

```
MainContainer mainContainer=MainContainer.getInstance(true);
```

Figure 5 is a screenshot of the MainContainer graphical interface.

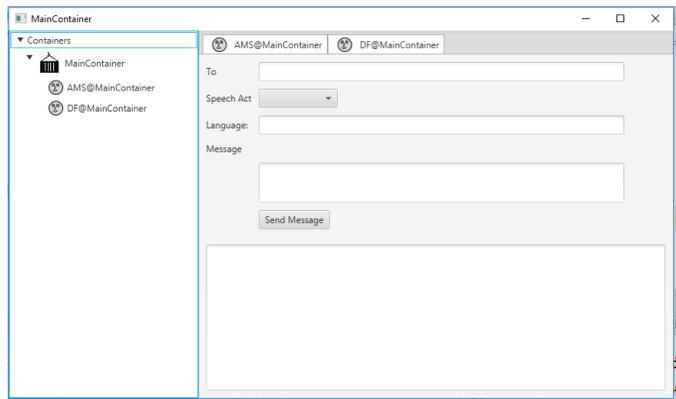


Fig. 5. Default Graphical Interface for the MainContainer.

C. Agent Deployment

The creation of an agent goes through an extension of the abstract class "Agent", then a redefinition of the various methods of the agent lifecycle management, in particular:

- `init()` method: is called by the container while its deploying just after instantiation. This method allows to the developer to initialize the agent and assign its behaviors.
- `onMessage()` method: is invoked by the container every time a message is received by the agent topic.

- `beforeMoving()`: is called just before activating the agent migration process to another container.
- `afterMoving()` method: is invoked after the agent migration process.
- `goingToDie()` method: is performed just before the agent destruction.

The listing 1 represents an example code for a java implementation of an agent. It shows the main methods of the agent lifecycle.

```

public class SampleAgent extends Agent {
    @Override
    public void init() {
    }
    @Override
    public void onMessage(ACLMessage aclMessage) {
    }
    @Override
    public void beforeMoving(String from, String to) {
    }
    @Override
    public void afterMoving(String from, String to) {
    }
    @Override
    public void goingToDie() {
    }
}
    
```

To deploy an agent, we have first to create a LightContainer where the agent will live, then deploy the agent using the `deployAgent ()` method. Figure 6 illustrates the deployment process of an agent.

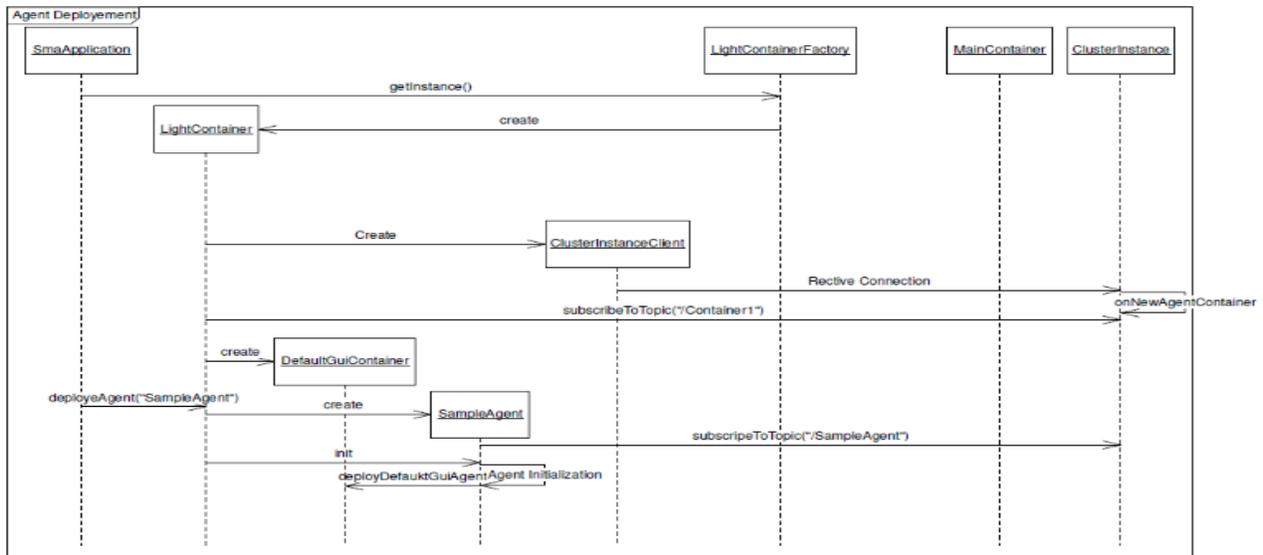


Fig. 6. Sequence Diagram for the Agent Deployment.

The deployment process begins by calling the container factory “LightContainerFactory” that creates an instance of LightContainer. This container will connect to the distributed computing cluster by Launching an instance of “ClusterInstanceClient”. This instance establishes a permanent and transparent connection to the container through its instance linked to the MainContainer. The created lightContainer subscribes to his own topic at cluster level, which constitutes a reception box for agents requesting to migrate to this container. Subsequently, if the developer wishes, a default graphical interface for this container is displayed.

Once the container is ready, the agent is deployed using the deployAgent () method - which is an instantiation of the agent class -, then the agent asks the cluster to create its own mailbox by creating its own topic. After this initialization, the agent deploys its default graphical interface inside the graphical interface of its container. these graphical interfaces are very useful to allow the developer to graphically visualize the different agents of the platform without having to develop code for this purpose; it can send messages to agents, activate the migration of an agent to another container or even display the messages received by the various agents.

These two code lines below represent the creation of a LightContainter and the deployment of an agent with default graphical interface.

```

LightContainer
lightContainer=LightContainer.getInstance("Container1",true);
lightContainer.deployNewAgent("SampleAgent",
SampleAgent.class,true);
    
```

The following screenshots show the graphical interfaces of two containers MainContainer and LightContainer (Figure 7 & figure 8).

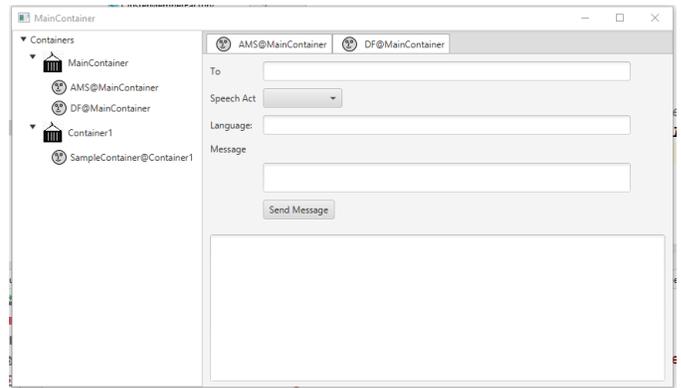


Fig. 7. MainContainer Graphical Interface.

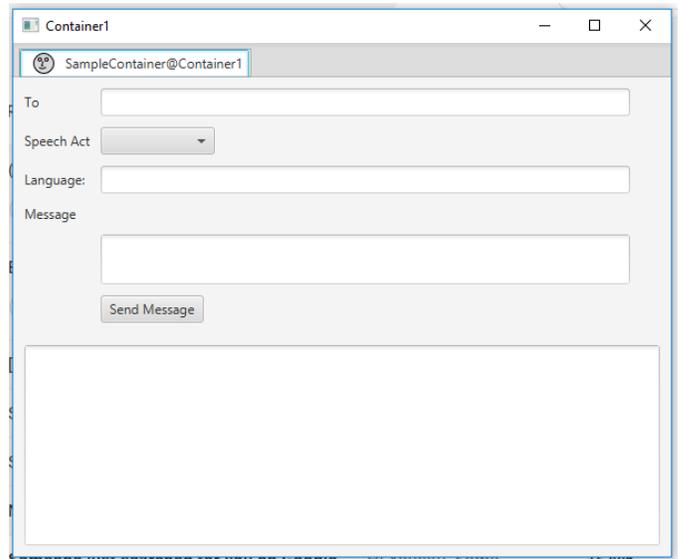


Fig. 8. LightContainer Graphical Interface.

D. Agent Migration

The agent mobility or migration is an essential asset of Multi Agents Systems, it provides the ability to agents to migrate from their initial container to other containers for many reasons: load balancing to overcome problems of overloading

resources, requirements or constraints of applications requesting agent relocation.

To migrate an agent, we must send to the agent an ACL message with the communication act is “MIGRATE” and the content is the address of the destination container. Figure 9 shows the sequence diagram of an agent migration process.

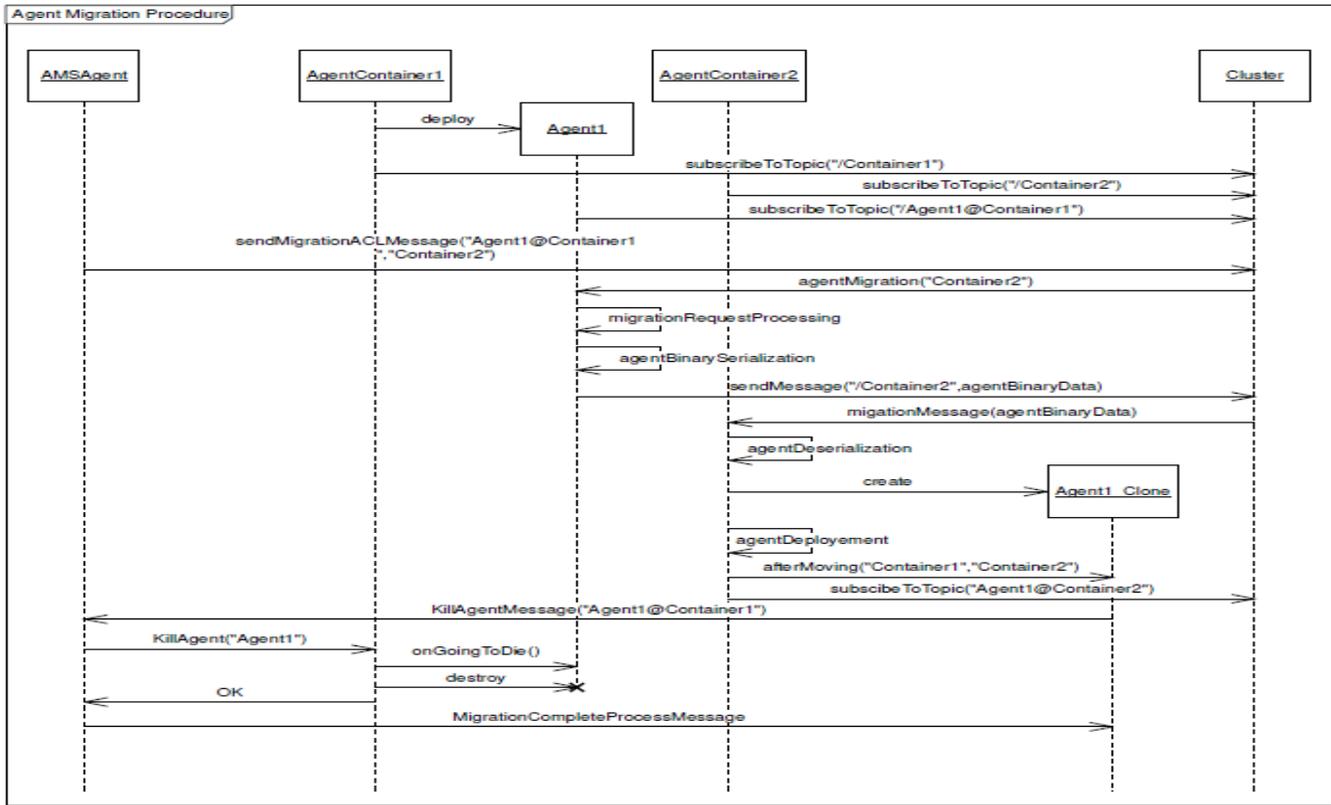


Fig. 9. Sequence Diagram of an Agent Migrating between Two Containers.

As explained previously, each container subscribes to a reception topic for migrant agents.

The sequence diagram above illustrates an agent “Agent1” initially deployed in “AgentContainer1”. This agent had its own topic “Agent1@Container1”. Once “Agent1” received from AMS agent an ACL message requesting him to migrate to “Container2”, he studies the possibility of this migration according to his state, then, if the migration is possible, he auto-serializes into a byte array. Afterwards, the agent sends his clone by message to the Container2 topic. This latter deserializes the Agent1 clone and deploy it. The agent method “afterMigration” is invoked by Container2 and a notification is sent to the AMS agent requesting him to kill the original agent. The AMS agent sends to the Container1 an ACL message with the act of KILL and the content is the Agent1 address. Container1 runs the onGoingToDie() method, kill the original agent and sends a notification to AMS agent. AMS agent updates his context and the graphical interface of the MainContainer with current localization of agents, then sends to Agent1 his new localization using the afterMoving() method.

The following figures show some screenshot of containers graphical interface before and after migration. We can see the change of location of the agent “SampleContainer” that moved from Container1 to Container2. All graphical interfaces of MainContainer, Container1 & Container2 tracked this migration (Figure 10 to figure 15).

- 1) Before migration:
 - a) MainContainer

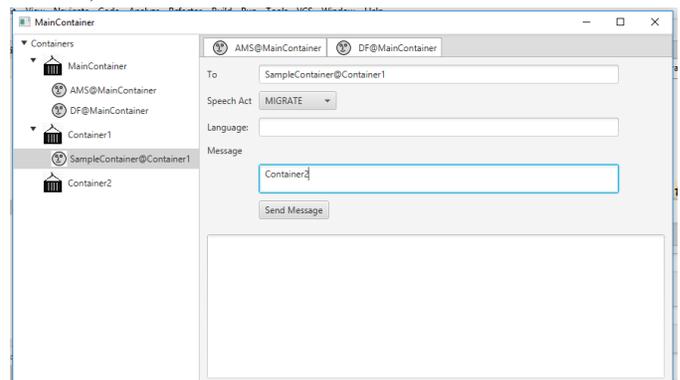


Fig. 10. MainContainer before Migration.

b) Container1

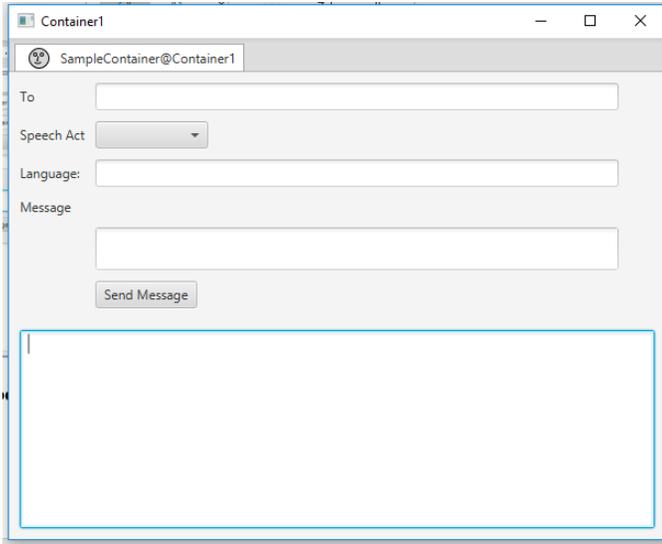


Fig. 11. Container1 before Migration.

b) Container1

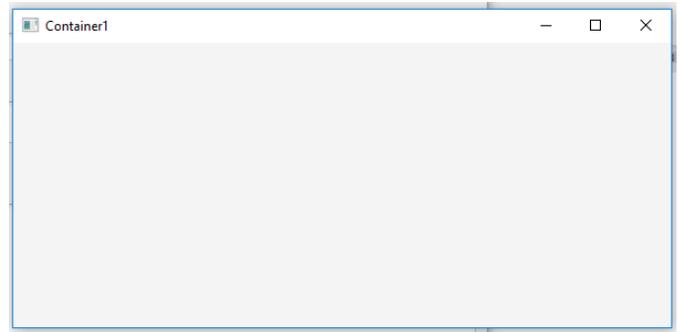


Fig. 14. Container1 after Migration.

c) Container2

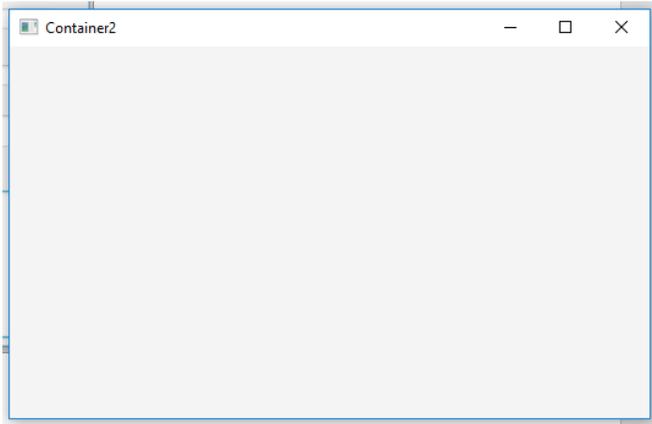


Fig. 12. Container2 before Migration.

c) Container2

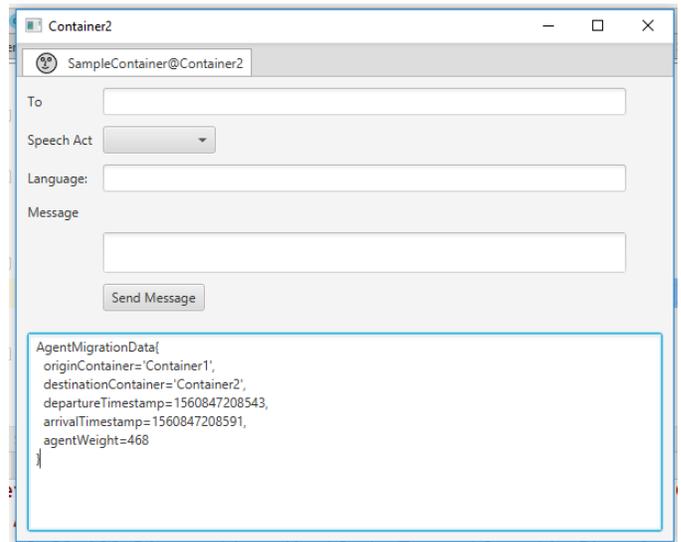


Fig. 15. Container2 after Migration.

2) After migration:
a) MainContainer

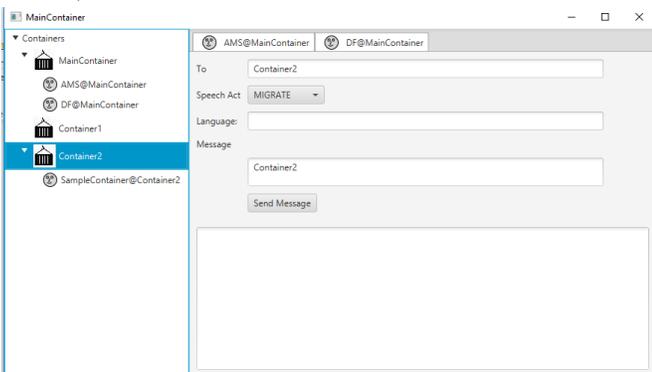


Fig. 13. MainContainer after Migration.

It is important to retrieve the migration information, including the duration of the migration and the size in bytes of the agent. to take advantage of this logging functionality, just run the `getLastMigration ()` method of the agent class. It allows us to log in:

- The original container;
- the destination container;
- the start time of migration;
- the end time of migration;
- the size of the agent.

IV. DATA DISTRIBUTION MODEL

Data distribution requires the definition of data structures as collections. For the management of these distributed collections, we chose the same mechanism used by the Hazelcast middleware [10].

A. Hazelcast

Hazelcast is an In Memory Distributed Grid (IMDG), it is a java open-source middleware allowing to create distributed memory cache.

In a Hazelcast grid, data are distributed evenly among the nodes of a group of computers to ensure:

- Scalable distributed storage (distributed memory cache).
- Scalable distributed computing.
- Replication of data on several nodes for fault tolerance.

These three Hazelcast principles reduce the load of database queries and improve the performance of distributed systems.

The following figure 16 shows the Hazelcast architecture. It consists of a cluster of nodes which host the distributed data (3 nodes in the example diagram below), a memory cache distribution layer which performs dispatching and ensures compliant addressing of the data, and various client APIs of various and varied programming languages to allow communication with other components of the system which could be heterogeneous.

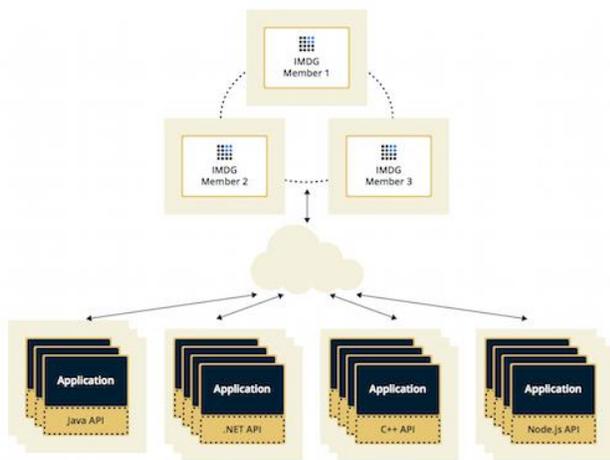


Fig. 16. Hazelcast Architecture.

B. The Distribution Model Description

The creation of a distributed collection can simply be done using one of these methods: `getMap()`, `gestQueue()`, `getTopic()` of a cluster's instance.

For example:

```
Map<String, String> data=memberInstance.getMap("myData");
```

The expression above allows to implicitly return an instance of `DistributedMapImpl`. Then, we can easily manipulate the inputs of this collection using methods "put" & "get" as follows:

```
data.put("key1","Item 1") ;
data.put("key2","Item 2") ;
data.put("key3","Item 3") ;
String value=data.get("key1");
```

A distributed collection is splitted into several partitions. A partition is a memory segment able to contain hundreds or even thousands of data inputs depending to the capacity of the system memory.

Each partition can have several backups that are distributed over the cluster nodes. One of these partitions becomes the main replica and others are secondary. The cluster member that has the main replica becomes the owner. When we need to read or write a specific data entry, we address transparently the owner of the partition containing that entry.

By default, the system proposes a number n of partitions to create. When we start the cluster with one member, it owns all n partitions. For example, if n=100, we will have:

P 1
P 2
P 3
...
P 98
P 99
P 100

Node 1

Once we launch a second member of the cluster, the partitions are distributed over the two nodes as follows:

P 1	P 51
P 2	P 52
...	...
P 50	P 100
P 51	P 1
P 52	P 2
...	...
P 100	P 50

Node 1 Node 2

The 50 first partitions remain at node 1 that is the owner, while partitions 51 to 100 are sent implicitly to node 2 which will be their owner. A backup (in red) of the 50 partitions of node 1 is created in node 2, and vice-versa.

If we start or stop other cluster members, the same distribution mechanism happens again. For example, if the cluster has 4 nodes, we will have:

P 1	P 26	P 51	P 76
P 2	P 27	P 52	P 77
...
P 25	P 50	P 75	P 100
P 76	P 1	P 26	P 51
P 77	P 2	P 27	P 52
...
P 100	P 25	P 50	P 75

Node 1 Node 2 Node 3 Node 4

Thereby, we distribute main and secondary partitions equally among cluster members. backup replicas of partitions are kept for redundancy.

For data partitioning, we use the following algorithm:

- When a cluster member starts up, a partition table is created in that member.
- This partition table records the IDs of the partitions and the cluster members to which these partitions belong. This allows each member to know where the data is.
- The oldest member of the cluster (the one that started first) periodically sends the partition table to all members. This way, every member of the cluster is informed of any change in partition ownership.
- Repartitioning is carried out each time a new member joins or leaves the cluster.

C. Advantages of this Distribution Model

This mechanism offers to us solutions to 3 main problems:

- First, spread the data over several nodes of the cluster, which overcomes the problem of storage limit of the memories of the physical units representing the nodes (scalability).
- Second, face the challenge of fault tolerance, because if a node goes down, the data is not lost (replication).
- Third, in the case of distributed computing, the execution of each node can perform the elementary task using the part of the elementary data fragments of the local node (performance).

V. DISTRIBUTED COMPUTING MODEL

A. Static Model

To create a distributed task, you would have to create a class that extends the abstract generic DistributedCallableTask

<T> class, then implement the code to be executed in the generic public T call () method.

This class implementing the two interfaces Callable <T> and Serializable is linked to the instance of the cluster that hosts this task. This allows access to data distributed in the cluster grid.

To deploy a distributed task, we define in this layer an ExecutorService with several implementations allowing this task to be submitted to an instance, a group of instances or to all instances of the cluster.

Figure 17 shows the main part of the class diagram of this API.

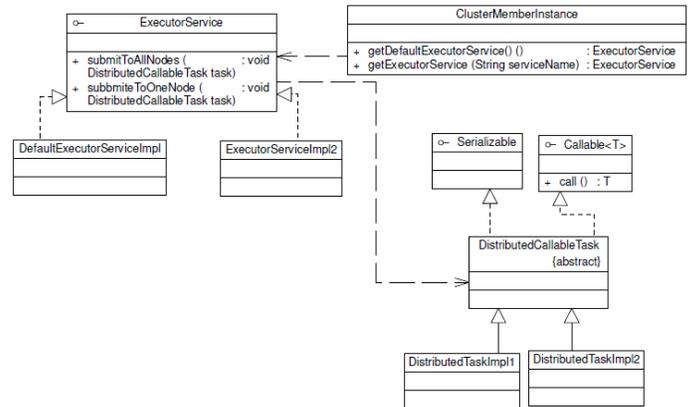


Fig. 17. Class Diagram of the Task Distribution Layer.

B. Sequence Model

Figure 18 illustrates the sequence diagram which describes an example of deployment of a distributed task in the cluster.

The agent begins by soliciting the local cluster client instance to retrieve the Distributed Task Execution service. This operation returns a DefaultExecutorService object configured and linked to the local cluster instance.

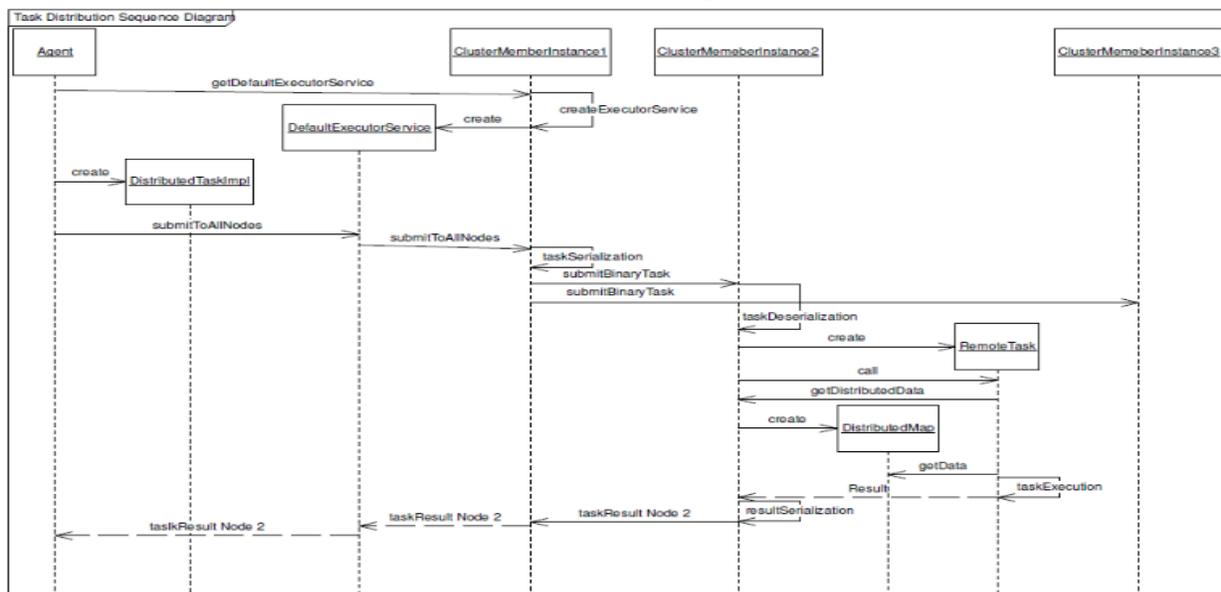


Fig. 18. Sequence Diagram of a Distribution Task Example.

After instantiating the implementation of the distributed task, the agent calls the ExecutorService object to submit the code for that task to all nodes in the cluster. The latter relies on the local cluster instance to do this. The DistributedTaskImpl object is first serialized in binary format before submitting this binary code to all instances in the cluster.

Each remote cluster instance that receives this code deserializes the object implementing the task code and then configures it by binding it to the local cluster instance. Then the remote cluster instance executes the call method of the distributed task.

Often in the distributed task code, we need to retrieve the data to be processed that is distributed in the grid as shared memory by calling the getDistributedData () operations of the local cluster instance. Then the result of the execution is returned to the cluster instance that submits this task. This result is returned to the agent who created the task.

VI. HIGHLIGHT ON THE MIDDLEWARE PERFORMANCE

The present middleware aims to optimize usage performance to verify this objective, we have monitored and carried out several measurements during the execution of the multi-agent system.

A. System Status after Maincontainer Launch

Figure 19 indicates an optimization of threads number just after the launch of the platform with a reduction of CPU use.

B. System Status after Container1 Creation

The following figure 20 shows an increase of the threads number after the deployment of a lightContainer “Container1” with its graphical interface. All usage of the system increase: CPU and memory occupation.

C. System Status after Container2 Deployment

Figure 21 present an evolution of the performance status after the creation of a second LightContainer “Container2”. At the creation moment, there is a pic of threads that is optimized just after the launch by eliminating all inactive threads.

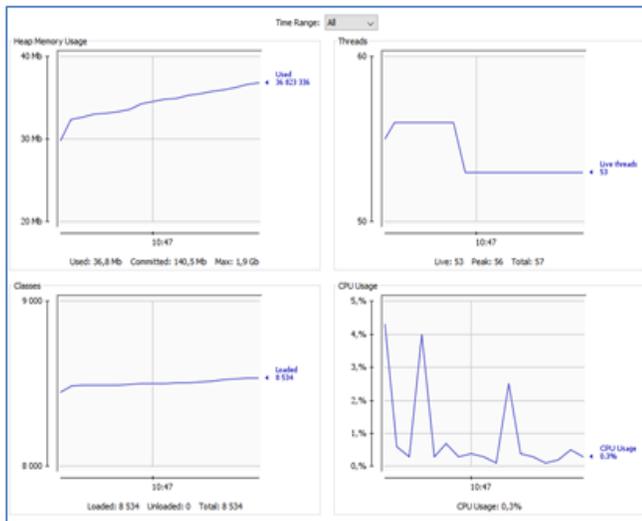


Fig. 19. Overview Performance Measurement – After MainContainer Launch.

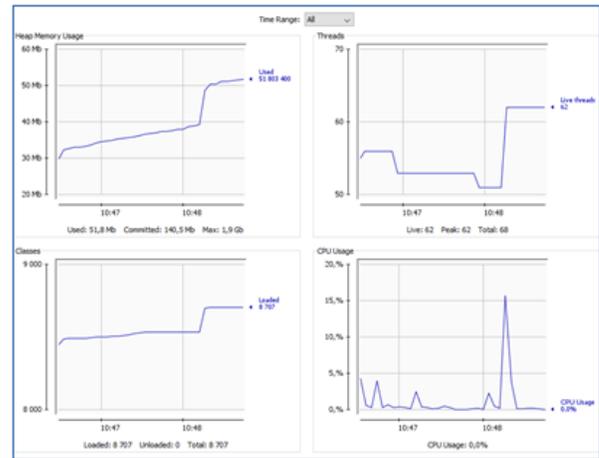


Fig. 20. Performance Measurement – After Container1 Deployment.

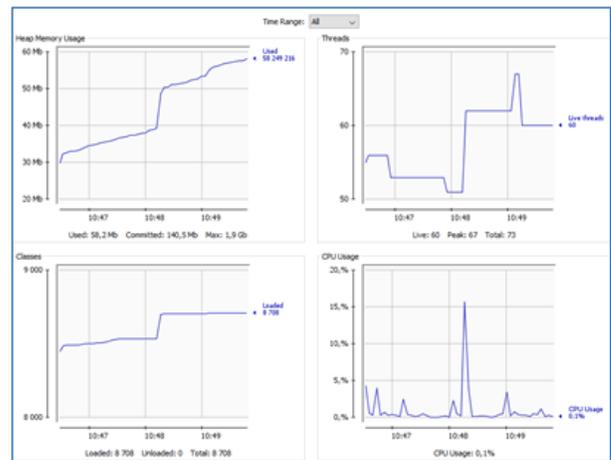


Fig. 21. Performance Measurement – After Container2 Deployment.

D. System Status after Migration Process from Container1 to Container2

The figure 22 illustrates a liberation of many threads and memory after the agent migrates.

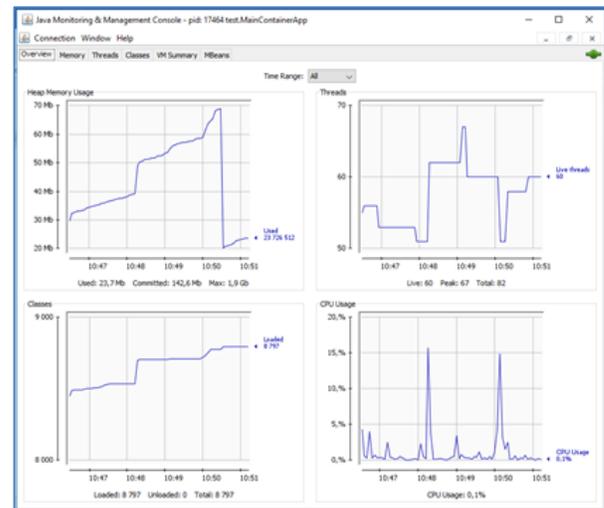


Fig. 22. Performance Measurement – After Agent Migration.

E. System Status after an Agent Communication

Figure 23 visualizes that in case of an agent communication act, some threats are used to send the message and are destructed just after optimizing also the CPU and memory usage.

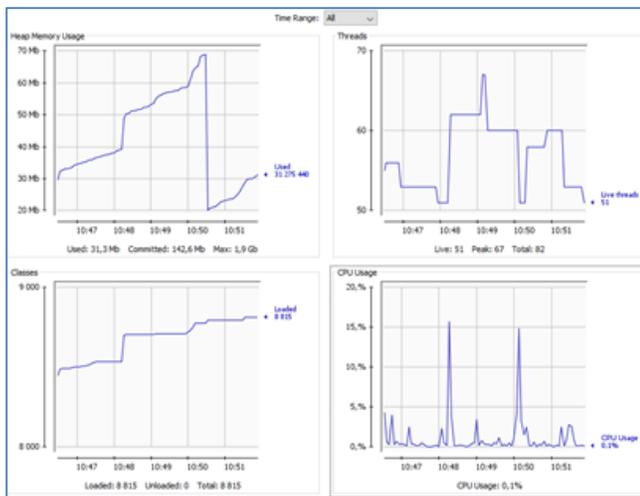


Fig. 23. Performance Measurement – After Agent Communication.

All these use cases show that the present middleware mobilize threats, CPU and memory just as needed, and optimizes these performance metrics dynamically.

VII. CONCLUSION

We presented in this article a scalable multi micro agent middleware based on reactive programming and designed for massively distributed systems and High-Performance Computing. This middleware is modular, based on seven APIs separating the creation/management of micro-agent, the communication pattern, the learning pattern, the data & distribution models, and the creation of the cluster and its monitoring.

The main objective is to find a reliable solution to design and build applications of massively distributed systems enabling cooperation, scalability, communication efficiency, resilience, and fault tolerance. We based the data & computing distribution approach on Hazelcast mechanism, which is efficient in term of data storage, cache computing structure &

tasks distribution. Several performance metrics were explored after implementing the proposal middleware, that show optimization of CPU usage, memory allocation and threads mobilization.

To confirm the performance of this solution, we are going to implement it in a big data context with a massively distributed architecture. The results of this implementation and the performance measurements will be published in a future article.

ACKNOWLEDGMENT

This project has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 777720.

REFERENCES

- [1] E. Ahmed, I. Yaqoob, I. A. Targio Hashem & al. : "The role of big data analytics in Internet of Things". In: Computer Networks, vol. 129, pp 459-471, December 2017.
- [2] R. Todd Evans, M. Cawood, S. Lien Harrell & al. : "Optimizing GPU-enhanced HPC system and cloud procurements for scientific workloads". In: High Performance Computing, pp. 313-331, June 2021.
- [3] M. Youssfi, O. Bouattane, J. Bakkoury & M. O. Bensalah "A new massively parallel and distributed virtual machine model using mobile agents". In: 2014 International Conference on Multimedia Computing and Systems (ICMCS), pp. 407-414, April 2014.
- [4] Youssfi M., Bouattane O., Bensalah M. : "A parallel computational model based on mobile agents for high performance computing". In: Contemporary Engineering Sciences, vol. 8, no. 15, pp. 677- 698, 2015.
- [5] J. M. Alberola, J. M. Such, V. Botti, A. Espinosa, A. Garcia-Fornes : "A scalable multiagent platform for large systems". In Computer Science and Information Systems Journal, vol. 10, N. 1, 2013.
- [6] F. Ezzrhari, M. Youssfi, O. Bouattane, V. Kaburlasos : "Scalable multi agent system middleware for HPC of big data applications". In : 2020 International Conference on Intelligent Systems and Computer Vision (ISCV), June 2020.
- [7] P. Rathore, D. Kumar, J. C. Bezdek, S. Rajasegarar, M. Palaniswami "A rapid hybrid clustering algorithm for large volumes of high-dimensional data". In: IEEE transactions on knowledge and data engineering, 2018.
- [8] FIPA Agent Communication Language Specifications. <http://www.fipa.org/repository/aclspecs.html>, last accessed October 2021.
- [9] F. Ezzrhari, H. Bensag, M. Youssfi, O. Bouattane & O. K. Abra : "Towards a New Micro Agents Middleware for Massively Distributed Systems". In: 2018 6th International Conference on Multimedia Computing and Systems (ICMCS), May 2018.
- [10] HAZELCAST. <https://docs.hazelcast.com/hazelcast/latest/index.html>, last accessed October 2021.

Expert System in Enhancing Efficiency in Basic Educational Management using Data Mining Techniques

Fuseini Inusah¹, Yaw Marfo Missah², Najim Ussiph³, Frimpong Twum⁴
Kwame Nkrumah University of Science and Technology
Department of Computer Science
Kumasi, Ghana

Abstract—The importance of basic education is well noted in every country. Proper planning and utilization of resources at the basic level, helps in leveraging the success of education at all other levels of education in a country. Ghana is noted to be the country that spends higher in education than its West African counterparts. In Ghana, attempts made to plan by predicting and projecting expenditure as well as the available resources to manage basic education are not accurate enough to address the challenges of education in the country. With the issue of COVID 19 pandemic, more expenditure is realized in managing educational institutions as more resources are needed in observing the protocols to curtail the pandemic. This throws a serious challenge to the effective and efficient utilization of the limited resources in the country. In this paper, the data from the Ministry of Education is analysed using data mining techniques. This has helped to identify the inaccuracies in the data. Inaccurate population projection affects the Key Performance Indicators (KPIs) in education because population is a common denominator for educational indicators. A proposed expert system is to be developed to assist in managing the situation.

Keywords—Basic education; data mining; educational management; expert system; population

I. INTRODUCTION

The 2030 agenda for sustainable development clearly highlights inclusivity as well as equitable quality education for all manner of learners to promote lifelong learning opportunities for all [1]. The importance of equity and inclusivity in education is noticed across the globe. Nations have devoted resources to campaign for all manner of people to be sent to school. Fairness in the provision of resources as well as treatment of learners in schools are also stressed on to make all manner of learners comfortable in school. Some of these include the laws to make learning environments disability friendly.

According to [2] equity is securing the rights of learners throughout their educational lives to make them achieve their dreams in life. Proper arrangements and implementation of policies should be done to ensure all learners achieve their aims for going to school. For the aspect of inclusion, it is seen as responding to the differences of need among learners by increasing their participation through learner friendly environment. Proper provision of resources and the blending of culture with content with reference to the ability of the

learner will enable all manner of learners to stay in school. The policies to ensure that all children of school going ages are in school will help in achieving inclusivity and reduce exclusion in education. Due to this, nations are paying serious attention to education to help in achieving the target. As education is a major aspect determining the development of a country, every nation pays attention to education. With the use of computers in handling educational data, there are very large databases which comprises of the enrolment of learners, available educational resources, cost of educating a learner, provision of educational equity for gender, inclusivity of all manner of learners in education etc. These larger data are accumulated automatically and manually in educational institutions which eventually constitute the Educational Management Information for the nation or country. Ghana is a middle income country. The educational system of Ghana (then Gold Coast) was one of the strongest in West Africa till it gained independence in 1957. According to [3], several educational reforms have been made in the country after independence just to achieve the desired quality of education the country is yearning for. This however has proved fatal due to the politicization of the educational policies and the unnecessary interference of political leaders in the management of education in the country. Resources are not adequately provided to the basic schools to enable in laying a solid foundation for effective teaching and learning. The unfortunate aspect is the manipulation of educational data to hype a political administration as the most efficient in management in the history of politics in the country.

Ghana has an educational system comprising of 11 years basic education, 3 years secondary education and 4 year basic degree for tertiary education. The focus of this study is basic education comprising of Pre-school, Primary education and Junior High School education. With ten regions and two hundred and sixteen districts, Ghana has about 41,598 public schools [4]. These schools are located in the 216 districts in the country. Each district has education directorate to manage activities and projects of the education. Information on enrolment, infrastructure, teacher availability, furniture and other educational resources are collected annually by the Ministry of Education in the Educational Management Information System (EMIS). This EMIS is the major source of information to the government of Ghana and every school is mandated by law to provide the information as reasonably

required. Despite all these efforts, there are still more challenges in the form of inaccurate data for the education sector. These inaccuracies are largely attributed to errors in data entry.

Education forms a major chunk of the expenditure of the budget of Ghana. The medium term expenditure framework for 2018-2021 released by the Ministry of Finance (MoF) showed a total expenditure for 2018 as GH¢ 9,258,839,827, estimate for 2019 is GH¢ 9,191,126,089 and 2020 figure of GH¢ 9,191,126,089. Out of these figures, 2018 figure for basic education alone is GH¢ 3,158,421,772. That of 2019 is GH¢ 3,161,130,849 and 2020 figure is GH¢ 3,161,130,849 [5]. This means that over thirty five percent (35%) of the expenditure from the Ministry of Education (MoE) is from basic education management.

Both the 6% or more recommendation of a country's GDP to be spent on education by UNESCO and the 20% recommendation by Global Partnership for Education (GPE) on governments' budgets are exceeded by Ghana [6] [7]. The World Bank [8] in a research also finds that, comparing Ghana to any of the other 13 Economic Community of West African States (ECOWAS) countries, Ghana is leading in terms of expenditure in education. According to [9], the annual growth rate of Ghana for the 2010 census was 2.2%. With a population growth without a decay, there is an increasing rate for the population per annum. This increase requires the provision of educational needs in basic schools to cater for the increasing population of school going ages. Government interventions are noticed in this direction in the form of provision of schools to increase access for the growing population. It implies that governments of Ghana are making efforts to improve the education sector. Donor agencies such as Non-Governmental Organisations (NGOs) also spend a lot of their resources to support basic education. Despite these heavy investments made to improve the basic education sector, the quality of education in the country is not improving as expected because there is no accurate way of predicting and forecasting to assist in proper planning and judicious use of resources. Resources directed to the sector seems not to be properly allocated and the various activities and projects carried out in the various metropolis, municipals and districts are not of higher priority to improve education at the various levels. Sometimes the interventions carried out are not accurately done.

Basic education in Ghana comprises of three different levels of education namely; Pre- school, Primary education and Junior High School level. The Pre-School consist of crèche or nursery and kindergarten. However, the Ghana Education Service formerly recognizes the Kindergartens in public schools as the starting point of basic education which is two years level to prepare a child for primary education. The primary level consists of six years of educational progression starting from primary 1 to 6. This is made up of lower and upper levels. It takes the highest amount of government expenditure for basic schools. The Junior High School consist of three year progression which starts from JHS 1 to JHS 3 [10]. Data from these three levels are combined in this paper

and analysed using data mining tools to achieve the objectives of the research.

In [11], it is seen that an intelligent system for predicting educational information is very relevant in predicting and making projections. These systems must employ more sophisticated methodologies to boast the data mining techniques in other to solve modern problems. This can be applied in the field of education in managing resources to improve the educational indicators. Conducive learning environments can be created to enable both teachers and learners stay in school and also have effective teaching and learning. Learners can be made the number one priority to desist from spending unnecessarily high expenditure on education. With this, educational institutions could plan well by making projections and predictions and direct resources to where they are needed.

In other to plan accurately and direct resource to where they are needed, there is a need for a competent system where resilient models are used to make forecast. This model could identify pattern in educational data, identify the challenges of education, make predictions and also propose solutions in the form of interventions. To fully identify the needs of education and truly utilize resources, unstructured data such as nature of school and learners (rural or urban) can be added to enable in classifying schools for better predictions. These are aspects difficult for a human expert to handle.

The educational offices that are in charge of managing educational resources in the country play a vital role in directing and allocating educational resources. They can help in minimizing cost and maximize efficiency in the education sector if accurate and reliable information is collected at the various educational institutions. If there can be higher efficiency and proper allocation of resources in education, more improvements will be seen in the Key Performance Indicators (KPIs). Also, personal interest of the individuals in managing educational resources will be eliminated to pave way for the needed improvements in basic education.

The aim for this research is to improve the management of basic education in Ghana by analyzing the existing data from the Ghana Statistical Service (GSS) and the Ministry of Education (MoE) to identify the challenges in data management and propose a system to assist management to enhance efficiency in decision making. Specifically, the study seeks to trace the anomalies in the data of Ghanaian education sector using data mining techniques and propose a resilient and sustainable model for a system to address the challenges.

The remaining part of the work is organized as follows: Section II is on the related work from the perspective of basic education in Ghana and the parameters used to calculate the indicators. Section III is the proposed methodology for the problem. Section IV is the findings for the quantitative data and the results represented in tables and graphs for visualization and the section the qualitative data from the extracts of the reports is also presented in this section. Section V is the conclusion drawn from the results as a global and local problem.

II. RELATED WORK

A. Basic Education in Ghana

Performance in the education sector is grouped in access and quality of education in the country. These Key Performance Indicators (KPIs) for measuring access of basic education are measured by parameters such as; admission rates, enrolment rates, availability of schools as well as classrooms, availability of teachers and teaching and learning resources, etc. The quality of basic education on the other hand is measured by the availability of qualified teachers in the schools as well as conducive teaching and learning environment coupled with improved teaching and learning materials to enable the learner acquire knowledge. Major parameters to measure access and quality of education as KPIs are; Gross admission rate, net admission rate, gross enrolment rate, net enrolment rate, pupil classroom ratio, pupil trained teacher ratio, gender parity index and the completion rates. All these indicators make use of the population of school going ages as a common denominator. The pattern for population growth for the children of basic school going ages is seen in an increasing other for the decade 2001-2010 in the EMIS data. For the second decade of 2011-2019, the EMIS data sees a fluctuation in population growth without any justifiable reason, the decrease in the population figures, corresponded to an improvement in results of the parameters for measuring the KPIs for the years. This is an inaccuracy that may result in an attempt to decrease the common denominator in other to see an improvement in the results. Selected indicators for this study are; Gross Enrolment Rate (GER), Net Enrolment Rates (NER) and the Gender Parity Index (GPI). These indicators are selected purposefully because the data is readily available for all levels and for the 20 years duration. The parameters and formulas for the indicators are seen as follows.

B. Population of School Going Age

This is the first parameter in measuring educational performance and the common denominator in calculating educational indicators. It is the total number of children who fall within the school going age for a particular level of learning. Inability to get this indicator accurately will affect almost all the educational indicators. The population of basic school going age in Ghana ranges from 4 years to 14 years. The pre-primary education which is two year Kindergarten (KG) is the beginning. Ideally, a child of four years should be in KG 1 and complete at the age of 5. The primary school going age starts from 6-11 years. A child of six years should be in primary 1 and complete at the age of 11 years. JHS school going age starts from 12 years to 14 years. A child of 12 years should be in JHS 1 and complete at the age of 14. The Ghana Statistical Service is mandated by law to provide these population figures and the rate of population growth.

C. Educational Indicators on Enrolment

1) *Gross enrolment rate*: This is the total enrolment in schools for a particular level (irrespective of age) as a ratio of school-age population corresponding to the same level of education in a given school year expressed as a percentage. For the KG, the school age population is 4 to 5 years. For primary, it is 6 to 11 years and for JHS it is 12 to 14 years.

The main reason behind this indicator is to know the level of participation in education by the population at a given time. It shows the ability of the educational system to enroll students. It can be compared to Net Enrolment Rate (NER) to indicate the extent of over-aged and under-aged enrolment. The appropriate age for Pre- school (KG) is 4 and 5 years. The appropriate age for primary school is 6 to 11 years and that of JHS is 12 to 14 years. Formula for the indicator is seen below.

$$\text{KG GER} = \frac{\text{Total Enrolment}}{\text{Total Population aged 4-5 years}} \times 100 \quad (1)$$

$$\text{Primary GER} = \frac{\text{Total Enrolment}}{\text{Total Population aged 6-11 years}} \times 100 \quad (2)$$

$$\text{JHS GER} = \frac{\text{Total Enrolment}}{\text{Total Population aged 12-14 years}} \times 100 \quad (3)$$

The Gross Enrolment Rate in the Ghanaian basic education has increase to an admirable rate. However, there are still some challenges in terms of inappropriate ages in the various levels.

2) *Net enrolment rates*: This is the total enrolment of students for a particular level within the appropriate school going ages expressed as a ratio of the total population of the appropriate age in percentages. It is the age specific enrolment which seeks to know the available learners in school who are at a level in school at the right ages.

$$\text{KG NER} = \frac{\text{Total Enrolment age 4-5}}{\text{Total Population aged 4-5 years}} \times 100 \quad (4)$$

$$\text{Primary NER} = \frac{\text{Total Enrolment aged 6-11}}{\text{Total Population aged 6-11 years}} \times 100 \quad (5)$$

$$\text{JHS NER} = \frac{\text{Total Enrolment age 12-14}}{\text{Total Population aged 12-14 years}} \times 100 \quad (6)$$

3) *Gender parity index*: This is a ratio of ratios. It is the ratio of the female gross enrolment rate to that of the male gross enrolment rate for a given level of education. The main aim is to find out the ratio of females participation in school compared to males in other to know female level of participation in schools. It can be calculated for all levels of education.

$$\text{GPI} = \frac{\text{Female Gross Enrolment Rate}}{\text{Male Gross Enrolment Rate}} \quad (7)$$

D. Data Mining

According to [12] data mining is a technique of examining data in a statistical perspective to extract relevant information about the data for informed decision making. It is a useful technique that enables an analyst to expose detailed information about data and enable users of the data to make predictions and projections on the data. In the paper [13] which is about a survey in recent big data technology, global view of main big data technologies as well as different system layers are provided to assist data technologist. It is revealed that as populations keep increasing and businesses as well as educational institutions keep increasing, databases are increasing at extremely faster rates as records or entries of transactions and details are recorded. As a survey paper, specific techniques of data mining and how those techniques

are to be used in carrying out task in data mining are not captured. This does not give much detail to the data technologist to build on. According to [14] in the paper Educational data mining in predicting students' performance, the use of data mining in analyzing educational data has now become a necessity due to the volumes of information on students' performance in educational institutions. In the paper [15], data mining is applied across organizations for cross analysis and easy identification of pattern to enable new institutions escape the challenges old institutions experience. In [16], innovative data mining methodology for the creation of new service ideas is considered. An association rule clustering using similarity measure was used in this paper to develop new graphs as sub-graph having exceptionalities capable of partially contributing to creating novel services. It was recommended for information in larger databases and capable of using data from different sources. This however is limited to services in data mining and the service one will choose for mining data strongly depends on the nature of the task to be performed.

The use of data mining has become a new normal in almost all aspects of the economy. This is evidence of the importance of data mining in the era of big data. In the paper [17] not only numerical figures are analyzed using data mining techniques but text can also be analyzed as in text mining techniques. The use of data mining is however not common in dealing with management of educational data. There is no enough evidence on datamining applications in the field of educational management of basic education.

According to [18] two major categories of data mining task has been identified i.e. descriptive data mining and predictive data mining. The former refers to the data mining task that tends to give a general description of the information on the current data set. This information is necessary in knowing the data and understanding what type of information it is. The latter tends to make forecasting on existing data sets. This is good for prediction and projections where models are develop.

E. Using Data Mining Techniques in Expert System

Expert system is an aspect of artificial intelligence that has gained much attention in management and decision making. It is a computer program design to mimic the expertise of the human expert. It takes the knowledge of the domain expert and stores it in a system to assist non experts in decision making. This enhance efficiency in decision making by increasing speed, accuracy and easy to use.[19].

In [20], data mining based expert system was used to determine the blood, hormone and obesity range for breast cancer. This was an automated diagnostic system designed to help medical and biomedical engineering studies. An accuracy level of 90.52% was realized using more scientific analysis accompanied by convincing mathematical evidence. A paper by [21] which is on accessing data mining rules through expert systems stressed on documenting and reporting extracted knowledge for successful application of practical data mining. The methodology proposed was on data mining rules based on expert systems to transform different data mining rules to domain knowledge in an expert system. This was done by the

use of attributes presented by the user as facts or goals to determine forward and backward chaining. A case study was also used in demonstrating the applicability of the rules.

According to [18], knowledge management is an important aspect in business management and competition in 21st century. This is very efficient when combined with data mining techniques .Fuzzy data mining was used in machine learning for expert systems development in the paper [22] using association based rule mining in fuzzy algorithms where knowledge representation was developed with unsupervised learning.

F. Data Mining in Education

The role of data mining in education can be seen in [22] where students performance in universities and the relationship with student and teacher behaviors are analyzed using data mining tools. Data mining can be used to predict students' enrolment, student profiling, curriculum development, students' complaints, course completion, course selection and placement, allocation of educational resources, performance of both, student and the teacher, dropout and relationship management. All these aspects help in identifying the challenges and finding appropriate solutions to the problems. The paper however does not demonstrate how these aspects identified are analyzed and interpreted using the appropriate data mining techniques.

A research by [23] which was to test the performance of students in the Waikato data mining environment indicates the need for proper design of algorithms to handle education related problems in other to help improve the quality of data mining in education. This can be done by the used of data mining techniques to extract the information from already existing information of the country on education. Such information can reveal the pattern of the data to get the challenges and the appropriate interventions to solve the problems. In [24], the benefits of educational data mining is clearly indicated as huge data management and pattern recognition of educational data is seen. This justifies the reason for the use of data mining to be combined with expert system to enable in effective decision making it is however worthy to note that the application of data mining in education is mostly on higher level neglecting the basic level of education which is the core or foundation for education.

III. METHODOLOGY

This research is analytical and descriptive research which makes use of both qualitative and quantitative data. The data is secondary data from the Ministry of Education and the Ghana Statistical Service reports from 2001 to 2019. RapidMiner studio 9.10 is the datamining software used. Purposeful sampling has been used to select the Key Performance Indicators in basic education. The data mining techniques proposed to be employed are classification and regression trees (CART) to design the model for prediction. Rule based inferencing is to be used in the expert system to store the knowledge of the domain expert. Cross validations is carried out at all levels to ensure accuracy and reliability. For better identification of needs of schools, the difference of schools with reference to geographical location and abilities

should be considered. Not all pupils and all schools have the same needs. Rural schools may not have the same needs as urban schools and well-endowed schools may not also have the same needs as less-endowed schools. The model is design purposely for predictions and projections to enable in accurate planning. The flowchart for the model and the tree structure to predict and make projections are presented in Fig. 1 and 2, respectively.

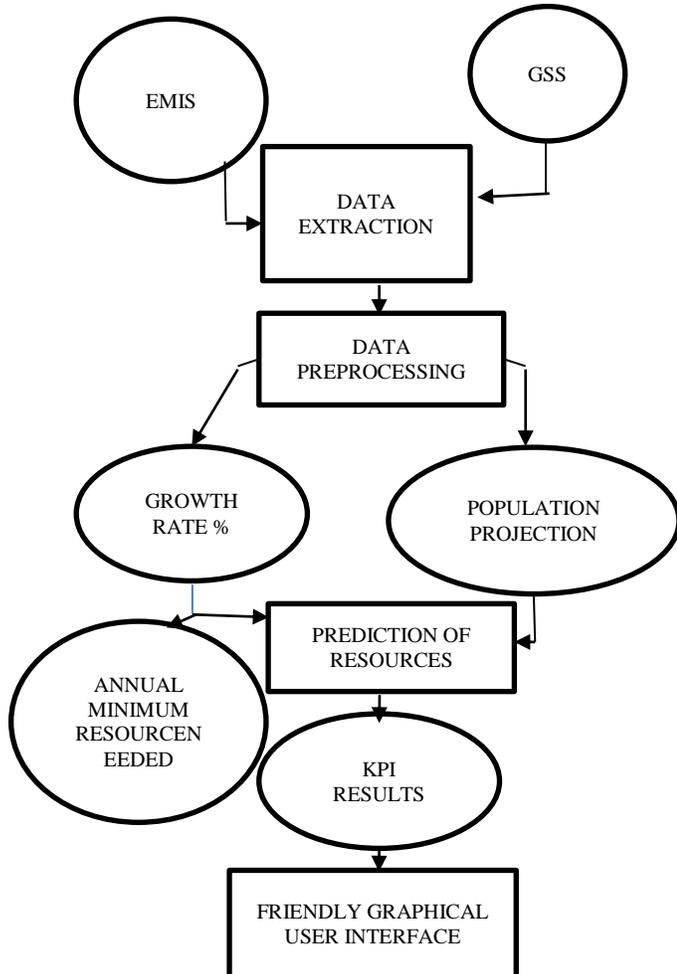


Fig. 1. Flowchart of the Proposed Model.

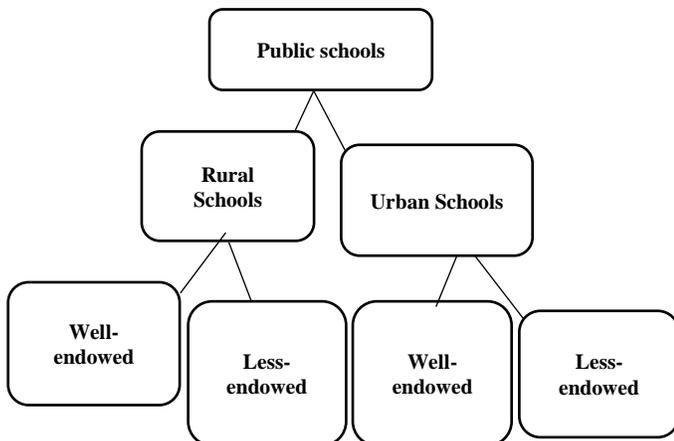


Fig. 2. Tree Structure of Basic School.

Fig. 1 is a flowchart for the proposed system. Data is extracted from the EMIS and GSS databases as inputs. This is to enhance automatic interactions to reduce the errors associated with human data entry in calculating the educational indicators. The processing of the data is done with consideration of the growth rates and the population projections. This will enhance accurate prediction of the resources needed for the future population of school going ages to help in improving the results of the educational indicators. A user friendly interface will be interacted by the user to produce the results.

In Fig. 2, a structure of basic schools is presented. Some schools are in urban areas while others are in rural areas. By the GSS standards, a community with population of 5000 or more is an urban area while those with less than 5000 are rural areas. For the aspect of resource provision, not all basic schools are having requisite teaching and learning resources for effective lesson delivery. Those with resources are seen as well-endowed while those without adequate resources are seen as less-endowed.

The results of the selected parameters for the indicators are presented in the findings of the research in tables and graphs. This is to enable simple understanding of the result for the average reader. As stakeholders of education are not well equipped with data mining methodologies, complex or technical presentation of the findings using data mining techniques may result to their inability to understand the findings of the research.

IV. FINDINGS AND RESULTS

The major challenge of basic education in Ghana is inaccurate planning and implementation of policies due to inaccurate data. Most of the parameter for the Key Performance Indicators (KPIs) is not giving accurate indication of the status of education in the country. For instance, the population of school going ages as captured in the Educational Management Information System (EMIS) as compared to the population projection by the Ghana Statistical Service (GSS) is not agreeing. Table IV is a result comparing the two. The specific findings are presented based on the selected parameters for the KPIs for the various levels of education

A. Presentation of Quantitative Data

The population of school going ages fluctuates considering 2011 to 2019 data from the EMIS reports produced by the Ministry of Education. As this parameter is the common denominators, it may be an attempt by stakeholders to project an increase or improvement in other parameters to measure the KPIs. Comparing the population projection from the GSS to that of the figures used, the difference is very significant. Table I shows the result.

As Kindergarten and primary schools have higher enrolments, the decrease in figure is seen at these two levels for the year 2012 to 2016. The junior high school with relatively lower numbers also sees this from the year 2015 to 2017. Fig. 3 represents kindergarten figures, Fig. 4 represents the Primary school figures and Fig. 5 represents the Junior High School figures.

TABLE I. COMPARING EMIS DATA TO GSS DATA ON POPULATION PROJECTION

Year	2.2% Growth Rate Expected Population of Basic School	POP. From EMIS Data	Variance
2010/2011	7306823	7306823	
2011/2012	7452959	7482201	(29242)
2012/2013	7602019	7085800	(516219)
2013/2014	7754059	6969422	784637
2014/2015	7909140	7169277	739863
2015/2016	8067323	7173470	893853
2016/2017	8228669	7336614	892055
2017/2018	8393243	7638343	754900
2018/2019	8561108	7840346	720762

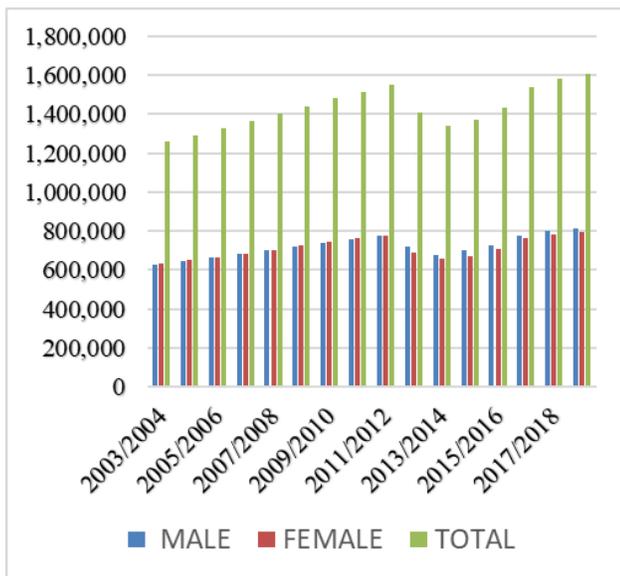


Fig. 3. Kindergarten Population of School Going Age.

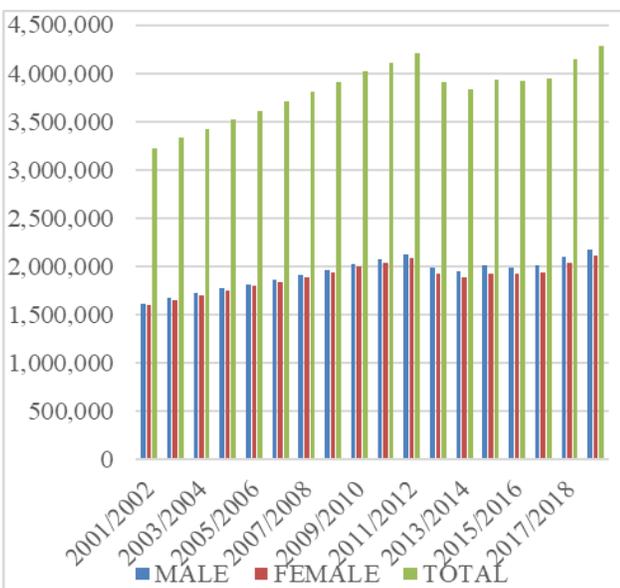


Fig. 4. Primary School Population Trend for School Going Age.

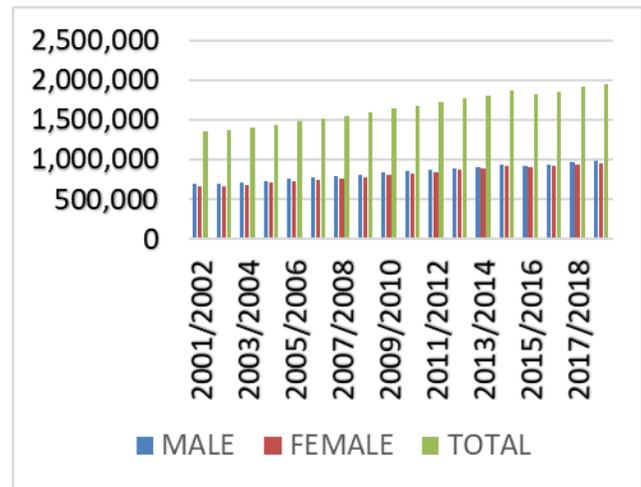


Fig. 5. JHS Population of School Going Age.

The results of the parameters for the various levels are analysed according to levels of education to give a clearer picture of how the inaccuracies in data management results to irregular pattern in the population trend. From Fig. 3, 4 and 5, the populations of school going ages for the various levels indicate a rise from the year 2001/2002 academic year to 2011/2012 academic year and then experienced a fall which indicates the population decay for the year 2012/2013 academic year to the year 2015/2016 academic year. This corresponds to a perceived improvement in the result for the educational indicators for the years in which the population figures were reduced as seen in Tables II, III and IV. The effect can be seen from the year 2012 to 2016 for both kindergarten and primary school. Tables II, III and IV represent the results for Kindergarten, Primary and Junior High School, respectively.

TABLE II. KINDERGARTEN EDUCATION KEY PERFORMANCE INDICATORS

YEAR	GER	NER	GPI
2001/2002	21%	15%	0.95
2002/2003	21.80%	19.00%	0.97
2003/2004	50.60%	34.40%	0.98
2004/2005	56.50%	38.50%	0.98
2005/2006	75.20%	50.00%	1
2006/2007	80.80%	55.80%	0.99
2007/2008	89.70%	62.60%	0.98
2008/2009	92.90%	63.60%	0.99
2009/2010	97.30%	58.70%	0.98
2010/2011	98.40%	60.10%	0.98
2011/2012	99.40%	64.20%	0.98
2012/2013	113.80%	74.80%	1.03
2013/2014	123.00%	90.80%	1.01
2014/2015	128.80%	82.70%	1.04
2015/2016	123.80%	79.50%	1.01
2016/2017	115.60%	74.60%	1
2017/2018	112.40%	74.60%	1
2018/2019	113.90%	73.80%	0.99

TABLE III. PRIMARY EDUCATION KEY PERFORMANCE INDICATORS

YEAR	GER	NER	GPI
2001/2002	80%	59%	0.96
2002/2003	75.70%	55.90%	0.92
2003/2004	78.40%	55.60%	0.93
2004/2005	83.30%	59.10%	0.93
2005/2006	86.40%	68.80%	0.96
2006/2007	90.80%	78.60%	0.96
2007/2008	95.00%	82.90%	0.96
2008/2009	94.90%	88.50%	0.96
2009/2010	94.90%	83.60%	0.96
2010/2011	96.40%	77.80%	0.97
2011/2012	96.50%	81.70%	0.97
2012/2013	105.00%	84.10%	0.99
2013/2014	107.30%	89.30%	0.99
2014/2015	110.40%	91.00%	1
2015/2016	111.30%	91.50%	1.01
2016/2017	111.40%	91.10%	1.01
2017/2018	106.20%	89.30%	1
2018/2019	105.30%	87.30%	1

TABLE IV. JUNIOR HIGH SCHOOL KEY PERFORMANCE INDICATORS

YEAR	GER	NER	GPI
2001/2002	64%	30%	0.88
2002/2003	63.40%	36.90%	0.88
2003/2004	65.60%	29.50%	0.88
2004/2005	70.20%	31.60%	0.88
2005/2006	70.40%	41.60%	0.9
2006/2007	74.80%	50.70%	0.9
2007/2008	78.80%	52.90%	0.92
2008/2009	80.60%	47.80%	0.92
2009/2010	79.50%	47.50%	0.92
2010/2011	79.60%	46.10%	0.93
2011/2012	80.60%	46.10%	0.94
2012/2013	82.20%	47.80%	0.93
2013/2014	82.00%	49.20%	0.95
2014/2015	85.40%	49.00%	0.96
2015/2016	88.0%	50.30%	0.97
2016/2017	86.80%	49.70%	0.98
2017/2018	86.10%	48.50%	1
2018/2019	86.20%	48.40%	1.02

As the population of school going age is the common denominator for the parameters measuring the KPIs, it should be made the basic parameter for projecting enrolment and predicting the resources needed to cater for the children of school going ages. Using already existing enrolment in school to project future enrolment and predict the resources needed may not be accurate since educational interventions are geared towards getting every child of school going age in school. If the policies work effectively, the trend of enrolment may not be in the pattern of current enrolment.

Comparatively the increase in population with a corresponding increase in enrolment in schools should be taken into consideration by management when providing educational resources to the basic education. As indicated in literature, access to quality education is a right but not a privilege. The Ghanaian basic education is however creating inequality by depriving some children of school going ages the right to resources to enable them learn even though they are in school.

B. Presentation of Qualitative Data Extracts from Reports

Comparing total enrolment in school to the availability of classrooms, it reveals congestion in schools as well as the availability of classes held in open air. This may scare other children of school going age to go to school. The findings from the analysis of statements in the reports from both the Ministry of Education and the Directorates for Ghana Education Service reveals the following statements.

The number of seating places and writing places are far below the total enrolment in basic schools. This means that there are some pupils who are still in school without furniture to accommodate them for effective learning. Even when comparing number of sitting places to that of the writing places, there is still a variance with a deficit of writing places which means that some pupils just sit for lessons but cannot write anything due to inadequate furniture.

Teaching and learning resources such as textbooks and other learning equipment are inadequate and a corresponding diminishing numbers in basic school. The pupil textbook ratio as well as the availability of curriculum materials for teachers to prepare and teach is reducing. These affect the quality of teaching and learning even if there are trained teachers in the schools.

The deployment of qualified teaching staff to schools for effective teaching and learning is also a very serious challenge. With the relatively lower ratio of pupil trained teacher ratio, the qualified teachers are concentrated in well-endowed schools which are usually in cities. This starves the rural deprived schools from qualified staff. Quality of teaching and learning is therefore compromised in the rural deprived schools as educational resources to improve them are woefully not adequate in those schools.

There should be a system that links the population figures from the Ghana Statistical Service to that of the Ministry of Education to enhance automatic interaction of the two in order to eliminate the human errors introduced in the calculation of the educational indicators. This system will help in making accurate projections for careful planning. The challenges of basic education in the country could be eliminated if such a system is in place. The future of basic education in Ghana can clearly be determined with this system as there will be an improvement in the management of resources. This will help in improving the quality of education at the basic level and also help in leveraging that success for high levels of learning.

V. CONCLUSION

Globally, the use of data mining to manage large data is recognized by researchers. The application of data mining in

education is also seen in many publications to demonstrate how data mining is relevant in education. However, the basic education level is relegated in data mining while concentration is on higher levels of learning. Attention is also given to learner attributes, performance and demographic factors in applying data mining on educational data. Educational resources availability and allocation in schools is not given serious attention by researchers in data mining especially at the basic level of learning. This makes it difficult in the accurate identification of challenges at the basic level which subsequently affects the higher levels of learning as the child progresses. With the inadequate experts in educational management, the use of data mining in expert system to assist in managing the education sector is the best approach. This will help to reduce the inaccuracies and also enhance the efficiency of management. Directors and other managers of educational institutions are usually teachers who are able to rise through the ranks in the Education Service (ES). These people may not have the expertise in management since management is a technical aspect. The use of expert system will therefore assist them to effectively manage the education sector.

REFERENCES

- [1] R. B. Johnston, "Arsenic and the 2030 Agenda for sustainable development," *Arsen. Res. Glob. Sustain. - Proc. 6th Int. Congr. Arsen. Environ.* AS 2016, pp. 12–14, 2016, doi: 10.1201/b20466-7.
- [2] H. J. Kim, P. Yi, and J. I. Hong, "Are schools digitally inclusive for all? Profiles of school digital inclusion using PISA 2018," *Comput. Educ.*, vol. 170, no. May, p. 104226, 2021, doi: 10.1016/j.compedu.2021.104226.
- [3] I. M. M. G., "Trajectories of Education Policy-Making in Ghana: Exploring the Journey To Depoliticisation Process," *Adv. Soc. Sci. Res. J.*, vol. 6, no. 2, 2019, doi: 10.14738/assrj.62.6160.
- [4] I. Management, "Ministry of Education, Science and Sports Report on Basic Statistics and Planning Parameters for Basic Education in Ghana," 2018.
- [5] Ministry of Education Ghana, "Ministry of Education; Programme Based Budget Estimates for 2019," *Minist. Educ.*, vol. 32, no. 161, pp. 66–66, 2019, doi: 10.1136/adc.32.161.66.
- [6] OCDE, "The Future of Education and Skills: Education 2030," *OECD Educ. Work. Pap.*, p. 23, 2018, [Online]. Available: [http://www.oecd.org/education/2030/E2030_Position_Paper_\(05.04.2018\).pdf](http://www.oecd.org/education/2030/E2030_Position_Paper_(05.04.2018).pdf).
- [7] Global Partnership for Education, "Guidelines for the Monitoring of National Education Budgets," no. February, 2019.
- [8] P. Schools, P. Schools, W. Bank, U. B. Education, and T. Basic, "REPORT ON BASIC STATISTICS AND PLANNING PARAMETERS FOR BASIC EDUCATION IN GHANA - 2016 / 2017," pp. 1–22, 2017.
- [9] GSS, "2010 Population and Housing Census, summary of Report of final results," *Ghana Stat. Serv.*, pp. 1–117, 2012, doi: 10.1371/journal.pone.0104053.
- [10] N. Bidwell and L. Junck, "Affordability Report," 2019, [Online]. Available: www.a4ai.org.
- [11] M. Ashraf, M. Zaman, and M. Ahmed, "An Intelligent Prediction System for Educational Data Mining Based on Ensemble and Filtering approaches," *Procedia Comput. Sci.*, vol. 167, no. 2019, pp. 1471–1483, 2020, doi: 10.1016/j.procs.2020.03.358.
- [12] I. Kreso, "Data mining privacy preserving: Research agenda," no. August, pp. 1–29, 2020, doi: 10.1002/widm.1392.
- [13] A. Oussous, F. Z. Benjelloun, A. Ait Lahcen, and S. Belfkih, "Big Data technologies: A survey," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 30, no. 4, pp. 431–448, 2018, doi: 10.1016/j.jksuci.2017.06.001.
- [14] A. Abu, "Educational Data Mining & Students' Performance Prediction," *Int. J. Adv. Comput. Sci. Appl.*, vol. 7, no. 5, pp. 212–220, 2016, doi: 10.14569/ijacsa.2016.070531.
- [15] G. Ahmad, M. Tanvir, and A. Al, "Cross-Organizational Information Systems: A Case for Educational Data Mining," *Int. J. Adv. Comput. Sci. Appl.*, vol. 8, no. 11, pp. 169–175, 2017, doi: 10.14569/ijacsa.2017.081122.
- [16] A. M. Karimi-Majd and M. Mahootchi, "A new data mining methodology for generating new service ideas," *Inf. Syst. E-bus. Manag.*, vol. 13, no. 3, pp. 421–443, 2015, doi: 10.1007/s10257-014-0267-y.
- [17] K. Thakur and V. Kumar, "Application of Text Mining Techniques on Scholarly Research Articles: Methods and Tools," *New Rev. Acad. Librariansh.*, vol. 0, no. 0, pp. 1–25, 2021, doi: 10.1080/13614533.2021.1918190.
- [18] T. Parlar and S. K. Acaravci, "International Journal of Economics and Financial Issues Using Data Mining Techniques for Detecting the Important Features of the Bank Direct Marketing Data," *Int. J. Econ. Financ. Issues*, vol. 7, no. 2, pp. 692–696, 2017, [Online]. Available: <http://www.econjournals.com>.
- [19] F. Inusah and A. A. Amponsah, "An Expert System to Assist Businesses in Financial Decision Making to Enhance Efficiency," 2018.
- [20] S. B. Akben, "Determination of the Blood, Hormone and Obesity Value Ranges that Indicate the Breast Cancer, Using Data Mining Based Expert System," *Irbm*, vol. 40, no. 6, pp. 355–360, 2019, doi: 10.1016/j.irbm.2019.05.007.
- [21] B. Boutsinas, "Accessing data mining rules through expert systems," vol. 1, no. 4, pp. 657–672, 2002.
- [22] V. E. Mirzakanov, "Value of fuzzy logic for data mining and machine learning: A case study," *Expert Syst. Appl.*, vol. 162, p. 113781, 2020, doi: 10.1016/j.eswa.2020.113781.
- [23] G. S. Gowri, R. Thulasiram, and M. A. Baburao, "Educational Data Mining Application for Estimating Students Performance in Weka Environment," *IOP Conf. Ser. Mater. Sci. Eng.*, vol. 263, no. 3, 2017, doi: 10.1088/1757-899X/263/3/032002.
- [24] A. Bilal Zorić, "Benefits of Educational Data Mining," *J. Int. Bus. Res. Mark.*, vol. 6, no. 1, pp. 12–16, 2020, doi: 10.18775/jibrm.1849-8558.2015.61.3002.

Machine Learning for Predicting Employee Attrition

Norsuhada Mansor¹, Nor Samsiah Sani²

Center for Artificial Intelligence Technology
Faculty of Information Science & Technology
Universiti Kebangsaan Malaysia
Bangi, Malaysia

Mohd Aliff³

Quality Engineering Research Cluster
Instrumentation and Control Engineering
Malaysian Institute of Industrial Technology
Universiti Kuala Lumpur, Johor, Malaysia

Abstract—Employee attrition has become a focus of researchers and human resources because of the effects of poor performance on organizations regardless of geography, industry, or size. In this context, the use of machine learning classification models to predict whether an employee is likely to quit could greatly increase the human resource department's ability to intervene on time and possibly provide a remedy to the situation to prevent attrition. This study is conducted with an objective to compare the performance machine learning techniques, namely, Decision Tree (DT) classifier, Support Vector Machines (SVM) classifier, and Artificial Neural Networks (ANN) classifier, and select the best model. These machine learning techniques are compared using the IBM Human Resource Analytic Employee Attrition and Performance dataset. Preprocessing steps for the dataset used in this comparative study include data exploration, data visualization, data cleaning and reduction, data transformation, discretization, and feature selection. In this study, parameter tuning and regularization techniques to overcome overfitting issues are applied for optimization purposes. The comparative study conducted on the three classifiers found that the optimized SVM model stood as the best model that can be used to predict employee attrition with the highest accuracy percentage of 88.87% as compared to the other classification models experimented with, followed by ANN and DT.

Keywords—Artificial neural networks; decision tree; employee attrition; machine learning; support vector machines

I. INTRODUCTION

Machine learning is one of the artificial intelligence technologies that provide systems with the ability to automatically learn and improve from experience or gain human-like intelligence without explicit programming. In other words, machine learning focuses on developing computer programs that can access data and use it to learn for themselves [1]-[4]. Machine learning (ML) is one of the fastest-growing fields of research and has been developed and applied successfully to a wide range of real-world domains [5] – [9]. This study presents a comparative analysis of three machine learning algorithms, i.e., DT, Support Vector Machines (SVM), and Artificial Neural Networks (ANN), to predict employee attrition.

Employee attrition in an organization can mean the reduction of employees through normal means, such as retirement and resignation, clients due to old age, or retrenching them due to change in the target demographics of the organization. The high rate of employee attrition is a major issue in an organization as it greatly impacts them. When

employees leave an organization, they carry with them invaluable tacit knowledge, which is often the source of competitive advantage for the organization [10]. Employee attrition causes the organization to bear the cost of business disruption, hiring and training new staff. On the other hand, higher retention means less hiring and training costs and more experienced workers to the company workforce over time. Organization nowadays has given a great business interest in understanding the drivers of staff attrition to reduce employee attrition. As a result, prediction on employee attrition and identifying the major contributing factors that lead to attrition becomes an important objective of an organization in order to enhance its human resource strategy [11].

The IBM Human Resource Analytic Employee Attrition and Performance dataset used in this paper is a publicly available dataset from Kaggle Dataset Repository. It was IBM's fictional dataset created by IBM data scientists. The dataset includes four (4) major components: employee satisfaction, income, seniority, and demographics data. The dataset contains several attributes influencing the predicted variable named 'Attrition' which signifies whether an employee left the company or not from 1,470 instances and 35 attributes. The identified class is labeled as 'Attrition' with 237 instances of 'Yes' and 1233 instances of 'No' having imbalanced data ratio of 1:5.

The purpose of this study is to conduct a comparative study to develop machine learning models, i.e., DT, SVM, and ANN, for predicting probable employee attrition and compare between the algorithms in terms of their accuracy and efficiencies.

II. RELATED WORK

Human resources are considered an important aspect of an organization, and voluntary employee attrition has been identified as a key issue. Reference [10] in his study focused on identifying employee-related attributes to predict employee attrition using decision tree algorithms.

The classification has been identified as an important issue in the emerging field of data mining. Over the years, there have been several studies on classification algorithms. Data mining algorithms must be efficient and scalable for the effective extraction of information from huge amounts of data in many data repositories or dynamic data streams. The key criteria are efficiency, scalability, performance, optimization, and the ability to execute in real-time that drives the development of many new data mining algorithms [12]. Two

(2) important performance indicators for data mining algorithms are the accuracy of a classification and the time taken for training. These indicators are mainly useful for selecting the best algorithms for classification or prediction tasks in data mining [13].

A study conducted by [14] using the IBM HR Employee Attrition & Performance dataset indicated the imbalance in the retrieved data. The correlation plot and histogram visualization had been performed to indicate the correlation between the continuous variables in the model during the data

exploration stage. Subsequently, the SMOTE (Synthetic Minority Oversampling Technique) was employed to balance the Attrition class.

The performance measurements observed in many literature reviews are mainly related to finding the best accuracy and speed to build a machine learning model. Table I briefly documents the literature review findings related to a comparative study on employee attrition using the machine learning classification algorithms:

TABLE I. RELATED WORK ON EMPLOYEE ATTRITION

No.	Author	Objective of Study	Classification Techniques Studied	Recommendation of Classification Techniques by Author
1.	Saradhi and Palshikar [15]	To predict employee churn	Naive Bayes, SVM, Logistic Regression, Decision Trees and Random Forests	SVM
2.	Alao and Adeyemo [10]	To analyze employee attrition using Decision Tree Algorithms	C4.5 Decision Tree, C5 Decision Tree, REPTree, CART (Simple Cart)	C5 Decision Tree
3.	Punnoose and Pankaj [16]	To predict employee turnover in organizations using machine learning algorithms	Logistic Regression, Naive Bayes, Random Forest, K-Nearest Neighbour (KNN), Linear Discriminant Analysis (LDA), SVM, Extreme Gradient Boosting (XGBoost)	Extreme Gradient XGBoost
4.	Alaskar, Crane and M. Alduailij [17]	To predict when workers will leave. It proposed a combination of five ML algorithms with three techniques for feature selection.	logistic regression, decision tree (DT), naïve Bayes, support vector machine (SVM) and AdaBoost	DT
5.	Mohbey [14]	To predict which customer or employee will leave their current company or organization	Naïve Bayes, SVM, decision tree, random forest, and logistic regression	DT
6.	Srivastava, D. K., & Nair, P. [18]	To analyze employee attrition using predictive techniques	ANN	ANN
7.	Frye et al. [19]	To present a model for predicting employee attrition	Logistic Regression, KNN, Random Forest	Logistic Regression
8.	Khera and Divya [20]	To predict employee turnover using machine learning techniques	SVM	SVM
9.	Ozdemir, Coskun, Gezer and Gungor [21]	To automatize the prediction of employee attrition utilizing data mining methods	Support Vector Machine (SVM), Random Forest, J48, LogitBoost, Multilayer Perceptron (MLP), K-Nearest Neighbors (KNN), Linear Discriminant Analysis (LDA), Naive Bayes, Bagging, AdaBoost, Logistic Regression	SVM
10.	Tharani and Raj [22]	To predict an employee's intention to leave the organization in the immediate future and identify the key features that influence the employee's intention to leave the organization	Logistic Regression and XG boost	XG boost

III. METHODOLOGY

A. Data Preprocessing

1) *Data description*: The initial step in carrying out this study is performing a data pre-preprocessing task. This study produces a data quality report to detect outliers and any unusual pattern about the dataset using statistical methods. Tables II and III show the data quality report of the dataset.

2) *Detecting outliers*: In addition to the above data quality report, forty-five (45) outliers were detected using the Interquartile Range filter based on the initial raw dataset, and the outliers were then checked. Those findings require further preprocessing, which are data cleaning, data reduction, and data transformation. There are also no missing values that are in existence, and the given data is complete.

3) *Data visualization*: An overview to understand each attribute pattern should be carried out and examined through data visualization. From the data visualization, we can see that a few attributes need to be examined to ensure accuracy during the model classification process. Fig. 1 shows the data visualization of each attribute in the dataset.

4) *Data cleaning and reduction*: The dataset is considered high dimensional as it consists of 35 attributes. Any irrelevant attributes that are not contributing to the objectives of this

study should be removed. Based on the data quality report in Table III and data visualization in Fig. 1, ‘EmployeeCount,’ ‘StandardHours’ and ‘Over18’ features can be removed in view that the cardinality/distinction is ‘1’, which means it has the same values throughout the data. Other than that, ‘EmployeeNumber’ is found not useful for the modeling and prediction process and can be removed from the dataset. No spelling inconsistencies were detected as inconsistencies may cause problems in later merges or transformations. Further description of data cleaning and reduction is explained in Table IV.

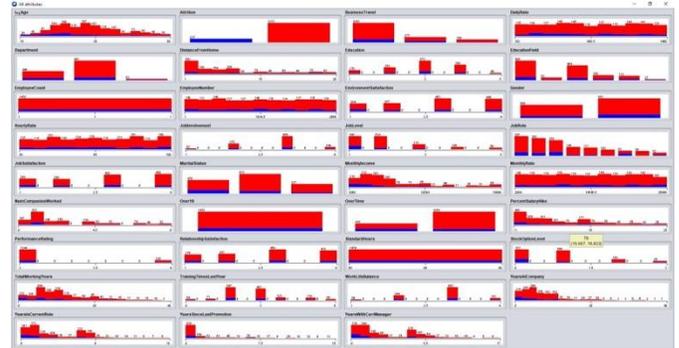


Fig. 1. Data Visualization.

TABLE II. THE DATA QUALITY REPORT (CONTINUOUS ATTRIBUTES)

No	Feature Name	Count	% of Missing Value	Cardinality	Min	1st Qrt	Mean	Median	3rd Qrt	Max	Std. Dev
1	Age	1470	0	43	18.00	30.00	36.92	36.00	43.00	60.00	9.14
2	DailyRate	1470	0	886	102.00	465.00	802.49	802.00	1157.00	1499.00	403.509
3	DistanceFromHome	1470	0	29	1.00	2.00	9.19	7.00	14.00	29.00	8.11
4	Employee Count	1470	0	1	1.00	1.00	1.00	1.00	1.00	1.00	0.00
5	Employee Number	1470	0	1470	1.00	491.25	1024.865	1020.5	1556.00	2068.00	602.024
6	Hourly Rate	1470	0	71	30.00	48.00	65.89	66.00	83.00	100.00	20.33
7	MonthlyIncome	1470	0	1349	1009.00	2911.00	6502.93	4919.00	8380.00	19999.00	4707.96
8	Monthly Rate	1470	0	1427	2094.00	8047.00	14313.103	14235.50	20462.00	26999.00	7117.79
9	NumCompaniesWorked	1470	0	10	0.00	1.00	2.69	2.00	4.00	9.00	2.50
10	PercentSalaryHike	1470	0	15	11.00	12.00	15.21	14.00	18.00	25.00	3.66
11	StandardHours	1470	0	1	80.00	80.00	80.00	80.00	80.00	80.00	0.00
12	TotalWorkingYears	1470	0	40	0.00	6.00	11.28	10.00	15.00	40.00	7.78
13	TrainingTimesLastYear	1470	0	7	0.00	2.00	2.80	3.00	3.00	6.00	1.29
14	YearsAtCompany	1470	0	37	0.00	3.00	7.01	5.00	9.00	40.00	6.13
15	YearsInCurrentRole	1470	0	19	0.00	2.00	4.23	3.00	7.00	18.00	3.62
16	YearsSinceLastPromotion	1470	0	16	0.00	0.00	2.19	1.00	3.00	15.00	3.22
17	YearsWithCurrManager	1470	0	18	0.00	2.00	4.12	3.00	7.00	17.00	3.57

TABLE III. THE DATA QUALITY REPORT (CATEGORICAL ATTRIBUTES)

No.	Feature Name	Count	% of Missing Value	Card.	Mode	Mode Freq.	Mode %	2nd Mode	2nd Mode Freq.	2nd Mode %
1	Attrition	1470	0	2	No	1233	84	Yes	237	16
2	BusinessTravel	1470	0	3	Travel Rarely	1043	71	Travel Frequently	277	19
3	Department	1470	0	3	R & D	961	65	Sales	446	30
4	Education	1470	0	5	3	473	32	4	340	23
5	Education Field	1470	0	6	Life Science	606	41	Medical	464	32
6	Environment Satisfaction	1470	0	4	3	453	31	4	446	30
7	Gender	1470	0	2	Male	882	60	Female	588	40
8	Job Involvement	1470	0	4	3	868	59	2	375	25
9	Job Level	1470	0	5	1	543	37	2	534	36
10	Job Role	1470	0	9	Sales Exec	326	22	Research Scientist	292	20
11	Job Satisfaction	1470	0	4	4	459	31	3	442	30
12	Marital Status	1470	0	3	Married	673	46	Single	470	32
13	Over 18	1470	0	1	Y	1470	100	-	-	-
14	Over Time	1470	0	2	No	1054	72	Yes	416	28
15	Performance Rating	1470	0	2	3	1244	85	4	226	15
16	Relationship Satisfaction	1470	0	4	3	459	31	4	432	29
17	Stock Option Level	1470	0	4	0	631	43	1	596	41
18	Work Life Balance	1470	0	4	3	893	61	2	344	23

TABLE IV. DESCRIPTION OF ATTRIBUTES AND PRE-PROCESSING ACTION

No.	Feature Name	Type of Data	Type of Data	Data Description	Pre-processing action/Findings
1	Age	Continuous	Numeric	The age of individual employee	Min = 18, max = 60 Normalize, Discretize
2	Attrition	Categorical	Nominal	Employee leaving the company (Yes, No)	Set to class
3	BusinessTravel	Categorical	Nominal	Business travel frequency (No Travel, Travel Frequently, Travel Rarely)	Retain
4	DailyRate	Continuous	Numeric	Salary Level	Normalize, Discretize
5	Department	Nominal	Nominal	Employee department (HR, R&D, Sales)	Retain
6	DistanceFromHome	Continuous	Numeric	The distance from work to home	Min = 1, Max = 29 Normalize, Discretize
7	Education	Categorical	Numeric	Level of education attained (1 = 'Below Collage', 2 = 'College', 3 = 'Bachelor', 4 = 'Master', 5 = 'Doctor')	Change to Nominal
8	EducationField	Nominal	Nominal	Field of education (HR, Life Sciences, Marketing, Medical Sciences, Others, Technical)	Retain
9	EmployeeCount	Continuous	Numeric	Count of instance	Cardinality = 1 - To remove
10	EmployeeNumber	Continuous	Numeric	Employee ID	Cardinality = 1470 - To remove
11	EnvironmentSatisfaction	Categorical	Numeric	Employee satisfaction with the environment (1 = 'Low', 2 = 'Medium', 3 = 'High', 4 = 'Very High')	Change to Nominal
12	Gender	Categorical	Nominal	Female, Male)	Retain
13	HourlyRate	Continuous	Numeric	Hourly Salary	Normalize, Discretize
14	JobInvolvement	Categorical	Numeric	Job Involvement (1 = 'Low', 2 = 'Medium', 3 = 'High', 4 = 'Very High')	Change to Nominal
15	JobLevel	Categorical	Numeric	Level Of Job (1 to 5)	Change to Nominal

16	JobRole	Categorical	Nominal	(1=Hc Rep, 2=Hr, 3=Lab Technician, 4=Manager, 5= Managing Director, 6=Research Director, 7= Research Scientist, 8=Sales Executive, 9= Sales Representative)	Retain
17	JobSatisfaction	Categorical	Numeric	Satisfaction with the job (1= 'Low', 2 = 'Medium', 3 = 'High', 4 = 'Very High')	Change to Nominal
18	MaritalStatus	Categorical	Nominal	(1=Divorced, 2=Married, 3=Single)	Retain
19	MonthlyIncome	Continuous	Numeric	Monthly Salary	Min = 1 009 Max = 19 709 Normalize, Discretize
20	MonthlyRate	Continuous	Numeric	Monthly Rate	Normalize, Discretize
21	NumCompaniesWorked	Continuous	Numeric	No. Of Companies Worked At	Min = 0 Max = 9 Normalize, Discretize
22	Over18	Categorical	Nominal	(1=Yes, 2=No)	Cardinality = 1 To remove
23	OverTime	Categorical	Nominal	(1=No, 2=Yes)	Retain
24	PercentSalaryHike	Continuous	Numeric	Percentage Increase In Salary	Normalize, Discretize
25	PerformanceRating	Categorical	Numeric	Performance Rating	Min = 3, Max = 4 Change to Nominal
26	RelationshipSatisfaction	Categorical	Numeric	Relations Satisfaction (1 = 'Low', 2 = 'Medium', 3 = 'High', 4 = 'Very High')	Change to Nominal
27	StandardHours	Continuous	Numeric	Standard Hours	Cardinality = 1 - To remove
28	StockOptionLevel	Categorical	Numeric	Stock Options	Min = 0, Max = 3 Change to Nominal
29	TotalWorkingYears	Continuous	Numeric	Total Years Worked	Normalize, Discretize
30	TrainingTimesLastYear	Continuous	Numeric	Hours Spent Training	Min = 0, Max = 6 Change to Nominal
31	WorkLifeBalance	Categorical	Numeric	Time Spent Between Work And Outside (1 'Bad' 2 'Good' 3 'Better' 4 'Best')	Change to Nominal
32	YearsAtCompany	Continuous	Numeric	Total Number Of Years At The Company	Min = 0, Max = 40 Normalize, Discretize
33	YearsInCurrentRole	Continuous	Numeric	Years In Current Role	Min = 0, Max = 18 Normalize, Discretize
34	YearsSinceLastPromotion	Continuous	Numeric	Last Promotion	Min = 0, Max = 15 Normalize, Discretize
35	YearsWithCurrManager	Continuous	Numeric	Years Spent With Current Manager	Min = 0, Max = 17 Normalize, Discretize

5) *Normalization and discretization:* During the data transformation in the preprocessing stage, feature scaling or normalization is applied. Normalization is a method used to standardize the range of independent variables or features of data [23]. Applying feature scaling or normalization can avoid dependency on the choice of measurement units on attributes. This process made the range of features of data fall between 0 and 1. The data cleaning and reduction were performed, which include the discretization process and change of attribute type from numerical to nominal. Four (4) attributes were removed based on the findings above, leaving the remaining 30 attributes. No outliers were detected after the interquartile filter was regenerated.

6) *Feature selection:* The next preprocessing part in machine learning is feature selection, which involves selecting features in the data and removing irrelevant and redundant information as much as possible to reduce the dimensionality of the dataset. Feature selection is a process of data reduction

that helps to improve accuracy, reduce overfitting, reduce training time and identify the fields that are most important and predictive for a given analysis. For this study, the top fifteen (15) out of 30 attributes had been selected based on several attribute selection methods that are Correlation Attribute, Gain Ratio Attribute, and Symmetrical Uncertainty Attributes as depicted in Table V:

Based on Table V, the selected fifteen (15) selected attributes that are used for the modeling phase are: Overtime, StockOptionLevel, JobLevel, MaritalStatus, YearsAtCompany, MonthlyIncome, YearsWithCurrManager, TotalWorkingYears, BusinessTravel, Age, YearsInCurrentRole, JobRole, JobInvolvement, EnvironmenSatisfaction, and WorkLifeBalance.

7) *Training dan test data:* For this experiment, resample filter function is used, the data is divided into two sets of data, which are the training and testing data with a split ratio of 80:20 as per Table VI.

TABLE V. FEATURE SELECTION RESULT

Correlation Attribute		Gain Ratio Attribute		Symmetrical Uncertainty Attribute	
Rank	Attributes	Rank	Attributes	Rank	Attributes
0.24612	Overtime	0.0464	Overtime	0.0533	Overtime
0.1543	StockOption Level	0.0185	StockOption Level	0.0278	JobLevel
0.1373	JobLevel	0.0184	JobLevel	0.0266	StockOption Level
0.1172	MaritalStatus	0.0149	JobRole	0.0244	JobRole
0.1124	YearsAtCompany	0.0147	MonthlyIncome	0.0239	MonthlyIncome
0.0854	MonthlyIncome	0.0142	MaritalStatus	0.0200	TotalWorkingYears
0.0734	YearsWithCurrManager	0.0123	TotalWorkingYears	0.0200	MaritalStatus
0.0705	TotalWorkingYears	0.0121	YearsAtCompany	0.0187	YearsAtCompany
0.0644	BusinessTravel	0.0117	YearsWithCurrManager	0.0186	YearsWithCurrManager
0.05838	Age	0.0104	Age	0.0173	Age
0.0581	YearsInCurrentRole	0.0102	BusinessTravel	0.0158	YearsInCurrentRole
0.0577	JobRole	0.0099	YearsInCurrentRole	0.0131	BusinessTravel
0.0574	JobInvolvement	0.0083	JobInvolvement	0.0117	JobInvolvement
0.0549	EnvironmenSatisfaction	0.0051	EnvironmenSatisfaction	0.0077	EnvironmenSatisfaction
0.0485	WorkLifeBalance	0.0046	WorkLifeBalance	0.0064	WorkLifeBalance

TABLE VI. SPLIT OF DATA

Dataset	No of Instances
Training with k-fold cross-validation	1,176
Test	294
Total	1,470

8) *Model validation technique*: The k-fold cross-validation is applied to the training set in view of its simplicity. Generally, it results in a less biased or less optimistic estimate of the model trained as compared to the other methods, such as the simple train/test split. Apart from that, this method is chosen as compared to the other training methods in view of the limited data sample in this study. Hence, the cross-validation technique splits the data into k groups, and it enables the model to be trained and validated on different sets iteratively. Overfitting refers to a situation where a machine-learning model cannot generalize or match the unseen dataset well. A strong indication of machine learning overfitting is whether the testing or validation dataset error is greater than the training dataset. There are different ways to resolve overfitting; cross-validation is an effective preventive against overfitting. [24].

9) *Imbalanced data*: The data quality report indicated an imbalance in the class distribution, with 237 tuples predicted as ‘Yes’ and 1233 tuples predicted as ‘No.’ Data imbalance is a well-known issue in classification problems, where one class is frequently far more prevalent than the others. Class imbalance usually degrades the real performance of a classification algorithm by poorly predicting the minority class, which is often the center of attention for a classification problem. Imbalanced data requires techniques that can deal with unequal misclassification costs [25]. Hence, the SMOTE

technique is applied to overcome the imbalance class at a 200% oversampling degree with five nearest neighborhoods on the training dataset. Using SMOTE, the minority class is over-sampled from 194 to 582 ‘Yes’ instances by creating “synthetic” examples rather than by over-sampling with replacement as shown in Table VII.

B. Machine Learning Classification Algorithms

This section explains the three (3) algorithms that are used in this study:

1) *Decision Tree (DT)*: DT is defined as a tree that classifies instances by sorting them based on feature values. The trees are made up of three fundamental segments: the root node, internal node, and leaf node as shown in Fig. 2. In a DT, each node represents a feature or attribute of the instance to be classified, each branch represents a test result, and leaf nodes represent class labels or class distribution. Classification of instances starts from the root node and is sorted based on their feature values. A sample of the decision tree, which is a flowchart like a tree structure, is as illustrated.

The basic algorithm for decision tree induction is a greedy algorithm that constructs decision trees in a top-down recursive divide-and-conquer manner [18]. C4.5 is an algorithm used to generate a decision tree based on information theory. C4.5 is known as J48 for Java. The classifiers, like filters, are organized in a hierarchy.

TABLE VII. NUMBER OF INSTANCES BEFORE AND AFTER SAMPLING (SMOTE)

Classification Model	No. of instances	Majority Class (“No” Attrition)	Minority Class (“Yes” Attrition)
Before Sampling	1176	982 (84%)	194 (16%)
After Sampling	1564	982 (63%)	582 (37%)

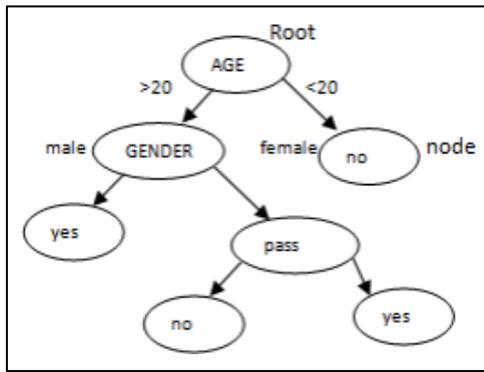


Fig. 2. Decision Tree.

The decision tree is induced by various algorithms. However, as it grows deeper, it happens that sometimes it generates unwanted and meaningless, and this is called overfitting. Therefore, pruning is needed to reduce the size of the tree that is too large and deep. The problem of noise and overfitting reduces the efficiency and accuracy of data [18]. There are various decision tree induction algorithms and various pruning parameters. In this study, pruning parameters such as the confidence factor and the number of objects (at the leaf node) were tuned to improve the DT classifier's performance.

2) *Support Vector Machines (SVM)*: SVM is known as a popular supervised algorithm in machine learning. Also, based on literature, SVM is also commonly used for employee attrition dataset. SVM acts as a classifier that categorizes the data into different 'classes' or as a regression function to estimate the numerical value of the desired output based on a linear combination of features for both linear and non-linear data [27]; SVM is known as SMO.

In relation to his study, the SVM model which is based on the training dataset, will try to generalize the input data based on their features and make a prediction. SVM machine learning will then produce a model that predicts the test data's target values [27]. The basic idea of SVM is to separate classes with maximum margin created by hyperplanes.

The tuning parameter in SVM includes the kernel, regularization parameter (C parameter), and gamma. Polynomial and exponential kernels calculate separation lines in a higher dimension called kernel tricks [27].

3) *Artificial Neural Networks (ANN)*: ANN is a machine learning technique that acquires knowledge through learning and is used to solve classification problems. The ANN can be organized in different topologies/architectures. There are different types of ANN architectures like feedforward and recurrent neural network. The most common neural network model is the Multilayer Perceptron (MLP), a non-linear predictive model that learns through training and is a feedforward network.

The objective in ANN in generic MLP is to find an unknown function f which relates the input vectors in X to the output vectors in Y ,

$$Y = f(X) \tag{1}$$

Where $X=[n \times k], Y=[n \times j]$.

n = number of training patterns.

k = the number of input nodes/variables.

j the number of output nodes/variables.

During the training of the dataset, the function f is optimized, where the network output for the input vectors in X is as close as possible to the target values in Y . Matrices X and Y represent the training data. The function f , for ANN architecture, is determined by the adjustable network weights. In ANN, the learning rate can be configured with a small positive value, often in the range between 0 and 1 [28].

C. Machine Learning Tasks Result

For this study, four (4) measures are used to compare the performance of the three (3) classifiers being studied i.e., J48, SVM, and ANN. Those four (4) common measures of the classifier are the accuracy rate, error rate, root mean square error (RMSE), receiver operating characteristic (ROC), and the time taken or speed to build a model. The prediction accuracy is defined as the percentage of correct prediction divided by the total number of predictions. The RMSE indicates an absolute measure of the fitness of the training dataset. A lower value of RMSE indicates a better fit. ROC tells how much the model is capable of distinguishing between classes. The time taken or the speed to build a model is another important consideration in choosing the best classifier model [4].

At the initial stage, the modeling task was carried out on the training dataset using the default parameter of each classifier, and SMOTE resampling technique was applied using 10-Fold cross-validation. Comparison of classifier performance is given in Table VIII.

As seen from the table, the following findings in the initial process of modeling were identified:

- 1) ANN had the highest accuracy result at 86.76% while SVM showed the lowest at 81.97%.
- 2) ANN showed the best RMSE with the lowest value of 0.3359.
- 3) ANN showed the best ROC at the highest value of 0.922.
- 4) J48 achieved the best time to build a model at 0.02 sec.

TABLE VIII. COMPARATIVE RESULT BETWEEN CLASSIFIERS USING 10-FOLD CROSS-VALIDATION ON DEFAULT PARAMETER ON THE TRAINING DATASET

Performance Measure	J48	SVM	ANN
Accuracy (%)	82.80	81.97	86.76
Error Rate (%)	17.20	18.03	13.24
RMSE	0.3756	0.4246	0.3359
ROC	0.853	0.808	0.922
Time taken to build model (second)	0.02	2.02	164.22

Machine learning algorithms can be optimized or configured in order to elicit different modeling behavior. Hence, in the next part, parameter tuning is conducted to optimize the model's current performance. The model will then be tested out with the unseen data after the parameter tuning is done on the model.

D. Parameter Tuning

Parameter tuning involves the process of optimizing the performance of a model, that is, to have the best result for each measurement. Parameter tuning is an important step in modeling as it is by no means the only way to improve performance.

1) *J48*: For the Decision Tree (*J48*) classifier, the value of the confidence factor and Minimum Number of Objects are tuned to achieve the best model and to avoid overfitting.

a) *Confidence factor*: The default confidence factor obtained above was run at 0.25. Table IX shows the results of confidence factor parameter tuning ranging from 0.1 to 1.0 run on the *J48* model.

The confidence factor parameter is tuned in DT to test the effectiveness of post-pruning. Post-pruning is the process of evaluating the decision error that is the estimated percent of misclassifications, at each decision junction and propagating this error up the tree. Fig. 3 shows that the highest accuracy of 83.57% at 0.4 confidence factor and the accuracy of 82.61% remains constant starting at 0.6 confidence factor. Hence, the 0.4 confidence factor parameter is the optimal value for *J48* classifier since increasing the confidence factor leads to lower accuracy.

b) *Minimum number of objects*: Also, parameter tuning is also conducted to get the optimal value for a minimum number of objects. For this study, the value of a minimum number of objects ranging from 0 to 30 is tuned at the confidence factor of 0.4. Table X shows the results for the minimum number of objects pruning parameter:

The minimum number of objects specifies the number of instances at the leaf node as a threshold value which means it specifies the minimum number of data separations per branch [26]. Fig. 4 shows that after the minimum number of objects of 1, the accuracy decreases when the minimum number of objects increases. The highest accuracy is at the parameter of 1 (minimum is 0 and cannot be a negative value) for the minimum number of objects with an accuracy of 84.40%. Hence, the minimum number of objects of 1 is the optimal number for the model.

2) *SVM*: The performance of the SVM classifier depends on the use of different kernel parameters in view that an appropriate kernel will provide a learning capability to SVM. For this experiment, as proposed in the literature, three (3) kernel functions were used for comparison in parameter tuning, which are the polynomial kernel, radial basis function (RBF) kernel, and Pearson VII kernel function (PUK) [29]-[31]. The regularization parameter (C) for these different kernels is tuned to improve the SVM model performance. The C determines how much penalty is given for misclassification.

The result of the kernel with C tuning is indicated in Table XI as follows.

TABLE IX. CONFIDENCE FACTOR TUNING FOR DT

Confidence Factor	Accuracy (%)	Error Rate (%)
0.2	81.84	18.16
0.4	83.57	16.43
0.6	82.61	17.39
0.8	82.61	17.39
1.0	82.61	17.39

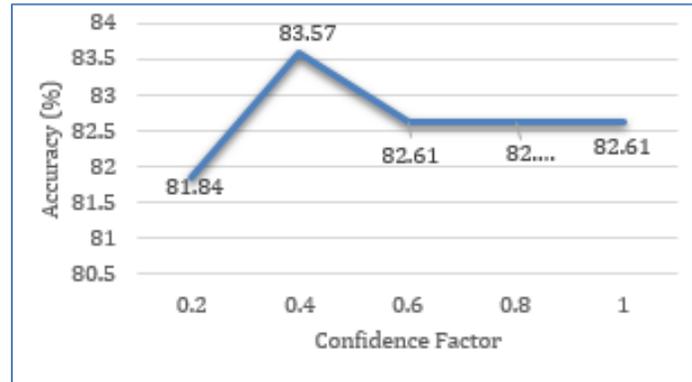


Fig. 3. Effect of Confidence Factor Tuning to Accuracy.

TABLE X. MINIMUM NUMBER OF OBJECTS TUNING FOR DT

Minimum Number of Objects	Accuracy (%)	Error Rate (%)
0	84.21	15.79
1	84.40	15.60
2 - default	83.57	16.43
5	83.38	16.62
10	79.80	20.20
15	78.71	21.29
20	77.69	22.31
25	77.11	22.89
30	76.15	23.85

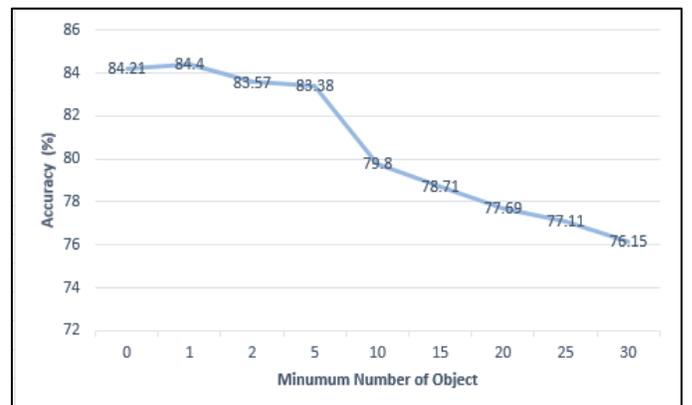


Fig. 4. Effect of MinNumObject Tuning to Accuracy.

TABLE XI. KERNEL AND REGULARIZATION PARAMETER (C) TUNING FOR SVM

Kernel	Regularization Parameter (C)	Accuracy (%)	Error Rate (%)	RMSE	ROC	Time taken to build model (s)
Polykernel	1	81.97	18.03	0.4246	0.808	2.19
	10	81.59	18.41	0.4291	0.806	6.57
Radial Basis Function (RBF)	1	82.23	17.77	0.4216	0.795	4.23
	10	85.23	14.77	0.3843	0.842	2.01
	100	86.51	13.49	0.3673	0.860	10.01
	200	85.55	14.45	0.3801	0.850	5.04
PUK	1	88.43	11.57	0.3402	0.847	3.68
	10	88.87	11.13	0.3335	0.853	5.36
	100	88.87	11.13	0.3335	0.853	5.35
	200	88.87	11.13	0.3335	0.853	5.67

The tuning result showed that the SVM model with PUK kernel produced the best fit with the highest accuracy of 88.87% and the lowest RMSE of 0.3335 compared to the other kernel when C is set to 10 using the PUK kernel. There is no change in the accuracy after the C value of 10; hence, the value is already optimized. This experiment also showed that the choices of kernel function gave an insightful effect on the performance of the SVM model for the employee attrition dataset after the parameter tuning.

3) ANN: In ANN, parameter tuning is performed by adjusting the learning rate. Table XII, Fig. 5 shows the performance result with parameter tuning on the learning rate.

TABLE XII. LEARNING RATE TUNING FOR ANN

Learning Rate	Accuracy (%)	Error Rate (%)	RMSE	ROC	Time taken to build model (s)
0.3	86.76	13.24	0.3359	0.922	84.27
0.4	87.98	12.02	0.3274	0.925	86.41
0.5	87.66	12.34	0.3329	0.924	90.86
0.6	87.08	12.92	0.3457	0.905	87.85

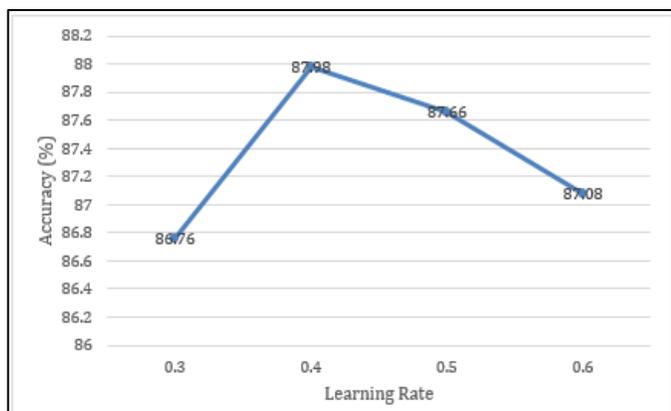


Fig. 5. Effect of Learning Rate Tuning to Accuracy.

The tuning result showed that ANN performed the best at a learning rate of 0.4 with an accuracy of 87.98%, and the time taken is 86.41sec as an optimal value. This algorithm was initially chosen in view of its capacity to detect all possible interactions between variables. However, even though this study used a small dataset with only 15 attributes after feature selection, ANN requires more time to create the model and requires more machine resources/capacity than the other machine learning algorithms. Moreover, the accuracy of 87.98% is still lower than the SVM. Hence, it is a less favorable option for this type of dataset.

E. Regularization

Regularization is basically a technique that was used to overcome the overfitting problem of a model. Overfitting refers to an occurrence where the model learns both the target function and noise during the training, which affects the performance of that model on the test/unseen data.

Regularization reduces the variance of the model without a substantial increase in its bias. In this study, few regularization techniques were performed to limit overfitting. As explained above, the tuning parameter is applied in each of the classifiers and is used as part of the regularization techniques to control the impact on bias and variance. As the value of parameter tuning rises, it reduces the coefficients' value, thus reducing the variance to avoid overfitting but not losing any important properties in the data. However, underfitting will occur when the model starts to lose important properties after a certain value, and this leads to the rising of bias in the model. Therefore, the value chosen during parameter tuning must be carefully selected [32].

Moreover, this study uses pruning to reduce the size of a decision tree to overcome overfitting. The SMOTE oversampling technique was applied to treat imbalanced minority classes in the dataset. Also, the use of the 10-fold cross-validation method, which is a resampling procedure, has given a coherent result and is used to overcome the overfitting issue in the dataset. Generally, regularization refers to a broad range of techniques for artificially forcing the machine learning model to be simpler and increase generalization chances.

IV. RESULTS AND DISCUSSION

A. The Effect of Feature Selection on Classification Accuracies

The 10-fold cross-validation test option enables the accuracy improvement of 15 attributes in comparison to 30 attributes. The result is depicted in Table XIII.

Based on the table, the results indicated that the use of top 15 attributes through feature selection has very much reduced the time taken to build the model from 330.23sec to 28.01sec without affecting the accuracy much where there is only a slight change from 85.96% to 85.13%.

TABLE XIII. THE EFFECT OF FEATURE SELECTION

Classification Model	Before feature Selection (30 attributes)				After Feature Selection (15 attributes)			
	Accuracy (%)	RMSE	ROC	Speed (sec)	Accuracy (%)	RMSE	ROC	Speed (sec)
J48	84.48	0.3608	0.603	0.02	84.56	0.3619	0.602	0.01
SVM	87.00	0.3605	0.723	3.79	86.87	0.3623	0.659	1.77
MLP	86.39	0.3440	0.839	326.42	83.95	0.3737	0.780	82.25
Average	85.96	0.3551	0.722	330.23	85.13	0.3660	0.680	28.01

TABLE XIV. PERFORMANCE COMPARISON BETWEEN DT, SVM AND ANN CLASSIFIERS

Classifier/ Results	Dataset	Accuracy (%)	Error Rate (%)	RMSE	ROC
DT – J48	Training	84.40	15.60	0.3704	0.850
	Test	80.95	19.05	0.4038	0.633
SVM	Training	88.87	11.13	0.3335	0.853
	Test	87.76	12.25	0.3499	0.990
ANN	Training	87.98	12.02	0.3274	0.925
	Test	85.03	14.97	0.3571	0.88

From the result in Table XI, SVM is revealed to be the best model that separates the class that can later be used to decide the class of a new set of data in predicting attrition. SVM ranks first at an accuracy rate of 88.87% (with parameter tuning at C=10 under the PUK kernel) while closely followed by ANN at 87.38%. DT showed the lowest accuracy rate of 84.40%. The performance measure result of the test dataset also showed a close result as compared to the training data and does not exceed the training result. It is proved that the model is not overfitted, and it is useful for predicting attrition for the new unseen dataset.

V. CONCLUSION

The comparative study on IBM Human Resource Analytic Employee Attrition and Performance was conducted to evaluate the classification models, i.e., J48, SVM, and ANN. SVM model stood at the best accuracy, RMSE, and Speed value after parameter tuning and regularization. Each of the three (3) classifiers used in this study has advantages and limitations; thus, evaluation is required to determine its suitability to solve the problem in relation to the dataset being studied.

B. Comparative Result between Classifiers after Parameter Tuning and Regularization using 10-Fold Cross-Validation

Table XIV shows the result obtained after the parameter tuning and regularization are applied for each classifier. The result in the training dataset below represents the best result for each classifier after applying parameter tuning and regularization. The results were then be compared with the unseen/test data.

As data preprocessing may affect the outcomes of the final model be interpreted, hence a tremendous effort is emplaced during the preprocessing stage for this study as it took a considerable amount of processing time. Several challenges and critical constraints faced in this study include the limited size of the dataset, imbalanced class, and high dimensional dataset. Hence, data preprocessing is an important stage to ensure only relevant features are selected for the training set.

The crucial part during the modeling stage is the parameter tuning conducted for each algorithm as different parameters require a different setting. In this study, this fact is proven when the initial accuracy for SVM was the lowest with no parameter tuning applied. However, SVM showed the highest accuracy after the parameter tuning due to its capacity to handle high-dimensional data with the use of different kernel functions. Also, the regularization technique is applied throughout the experiment to overcome the issue of overfitting during the modeling phase.

This paper is mainly focusing on the comparative study of the machine learning model to predict whether an employee would leave the company or not given an employee attrition dataset. Hence, future work may look into identifying the key features that lead to employee attrition. Apart from that, the use of the hyperparameter tuning approaches like grid search or random search can further be deliberated to find the best combination of parameters to enhance the model to ensure its efficiency and scalability.

ACKNOWLEDGMENT

The authors would like to thank Universiti Kebangsaan Malaysia (UKM) and Ministry of Education, Malaysia (MOE) under the FRGS/1/2018/ICT02/UKM/02/6) for funding and supporting this research.

REFERENCES

- [1] S. Das, A. Dey, A. Pal and N. Roy, "Applications of artificial intelligence in machine learning: Review and prospect," *Int. J. Comp. Appl.*, vol. 115, pp. 31–41, January 2015.
- [2] A. Abu, R. Hamdan, R. and N.S. Sani, "Ensemble Learning for Multidimensional Poverty Classification," *Sains Malaysiana*, vol. 49(2), pp.447-459 2020.
- [3] Nor Samsiah Sani, Abdul Hadi Abd Rahman, Afzan Adam, Israa Shlash and Mohd Aliff, "Ensemble Learning for Rainfall Prediction" *International Journal of Advanced Computer Science and Applications*, vol. 11(11), pp. 153-162, 2020.
- [4] Nor Samsiah Sani, Ahmad Fikri Mohamed Nafuri, Zulaiha Ali Othman, Mohd Zakree Ahmad Nazri and Khairul Nadiyah Mohamad, "Drop-Out Prediction in Higher Education Among B40 Students" *International Journal of Advanced Computer Science and Applications*, 11(11), pp. 550-559, 2020.
- [5] A. B. Abdulkareem, N. S. Sani, S. Sahran, Z. A. A. Alyessari, A. Adam et al., "Predicting covid-19 based on environmental factors with machine learning," *Intelligent Automation & Soft Computing*, vol. 28 (2), pp. 305–320, 2021.
- [6] N. S. Sani, I. I. S. Shamsuddin, S. Sahran, A. H. A. Rahman, and E. N. Muzaffar, "Redefining selection of features and classification algorithms for room occupancy detection," *International Journal on Advanced Science, Engineering and Information Technology*, vol. 8, pp. 1486-1493, 2018.
- [7] S. Shabudin, N. S. Sani, K. A. Z. Ariffin and M. Aliff, "Feature Selection for Phishing Website Classification," *International Journal of Advanced Computer Science and Applications*, vol. 11(4), pp. 587-595, 2020.
- [8] R. Hamdan, A. Abu and N. S. Sani. "Does Artificial Intelligence Prevail in Poverty Measurement?." In *Journal of Physics: Conference Series*, vol. 1529(4), pp. 042082. IOP Publishing, 2020.
- [9] Z. A. Othman, A. A. Bakar, N. S. Sani, and J. Sallim, "Household Overspending Model Amongst B40, M40 and T20 using Classification Algorithm." *International Journal of Advanced Computer Science and Applications*, vol. 11(7), pp. 392-399, 2019.
- [10] D. Alao and A. B. Adeyemo, "Analyzing employee attrition using decision tree algorithms," *Comput., Inf. Syst., Dev. Inform. Res. J.*, vol. 4, pp. 17–28, March 2013.
- [11] J. Rohan, A. Shahid, S. Saud, and J. Ramirez, "IBM HR analytics employee attrition & performance," January 2018 [Online] http://inseaddataanalytics.github.io/INSEADAnalytics/groupprojects/January2018FBL/IBM_Attrition_VSS.html#business_problem.
- [12] H. Jiawei and M. Kamber, *Data Mining: Concepts and Techniques*, Burlington, MA: Morgan Kaufmann, 2001.
- [13] S. O. Akinola and O. J. Oyabugbe, "Accuracies and training times of data mining classification algorithms: An empirical comparative study," *J. Softw. Eng. Appl.*, vol. 8, pp. 470–477, September 2015.
- [14] K.K Mohbey, "Employee's Attrition Prediction Using Machine Learning Approaches," In *Machine Learning and Deep Learning in Real-Time Applications*, pp. 121-128, 2020.
- [15] M. E. Kara, S. Ü. O. Firat and A. Ghadge, "A data mining-based framework for supply chain risk management," *Computers & Industrial Engineering*, vol. 139, pp. 1-12, 2020.
- [16] R. Punnoose and A. Pankaj, "Prediction of employee turnover in organizations using machine learning algorithms: A case for extreme gradient boosting," *Int. J. Adv. Res. Artif. Intel.*, vol. 5, pp. 22–26, October 2016.
- [17] L. Alaskar, M. Crane and M. Alduailij, "Employee Turnover Prediction Using Machine Learning," In *International Conference on Computing*, pp. 301-316, 2020.
- [18] D. K. Srivastava and P. & Nair, "Employee attrition analysis using predictive techniques," in *Int. Conf. Inform. Commun. Technol. for Intell. Syst.*, pp. 293–300, March 2017.
- [19] A. Frye, C. Boomhower, M. Smith, L. Vitovsky, and S. Fabricant, "Employee attrition: What makes an employee quit?." *SMU Data Sci. Rev.*, vol. 1, pp. 1–29, 2018.
- [20] S. N. Khera and Divya, "Predictive modelling of employee turnover in Indian IT industry using machine learning techniques," *Vis. J. Bus. Perspect.*, vol. 23, pp. 12–21, March 2018.
- [21] F. Ozdemir, M. Coskun, C. Gezer and V.C Gungor, "Assessing Employee Attrition Using Classifications Algorithms," In *Proceedings of the 2020 the 4th International Conference on Information System and Data Mining*, pp. 118-122, May 2020.
- [22] S.M. Tharani and S.V. Raj, "Predicting employee turnover intention in IT&ITeS industry using machine learning algorithms," In *2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC)*, pp. 508-513, 2020.
- [23] S. Srivastava, "Weka: A tool for data preprocessing, classification, ensemble, clustering and association rule mining," *Int. J. Comput. Appl.*, vol. 88, pp. 26–29, February 2014.
- [24] T. Shah, "About train, validation and test sets in machine learning," *Towards Data Science*, 6 Dec. 2017.
- [25] A. Singh and A. Purohit, "A survey on methods for solving data imbalance problem for classification," *Int. J. Comput. Appl.*, vol. 127, pp. 37–41, October 2015.
- [26] N. Patel and S. Upadhyay, "Study of various decision tree pruning methods with their empirical comparison in WEKA," *Int. J. Comput. Appl.*, vol. 60, pp. 20–25, December 2012.
- [27] J. Cervantes, F. Garcia-Lamont, L. Rodriguez-Mazahua and A. Lopez, "A comprehensive survey on support vector machine classification: Applications, challenges and trends," *Neurocomputing*, vol. 408, pp. 189-215, 2020.
- [28] D. S. Jat, P. Dhaka and A. Limbo, "Applications of statistical techniques and artificial neural networks: A review," *Journal of Statistics and Management Systems*, vol. 21(4), pp. 639-645, 2018.
- [29] D. Tien Bui, B. Pradhan, O. Lofman and I. Revhaug, "Landslide susceptibility assessment in Vietnam using support vector machines, decision tree, and Naive Bayes Models," *Math. Probl. Eng.*, pp. 1–26, July 2012.
- [30] K. A. Abakar and C. Yu, "Performance of SVM based on PUK kernel in comparison to SVM based on RBF kernel in prediction of yarn tenacity," *Indian J. Fibre Text. Res.*, vol. 39, pp. 55–59, 2014.
- [31] M. Abdul Rahman, N.S. Sani, R. Hamdan, Z. Ali Othman and A. Abu Bakar, "A clustering approach to identify multidimensional poverty indicators for the bottom 40 percent group," *Plos one*, vol. 16(8), pp. e0255312, 2021.
- [32] Y. Li, C. Wei and T. Ma, "Towards explaining the regularization effect of initial large learning rate in training neural networks," In *Advances in Neural Information Processing Systems*, pp. 11674-11685, 2019.

Finding Good Binary Linear Block Codes based on Hadamard Matrix and Existing Popular Codes

Driss Khebbou¹, Reda Benkhouya², Idriss Chana³, Hussain Ben-azza⁴

Ecole Nationale Supérieure d'Arts et Métiers, Moulay Ismail University, Meknès, Morocco^{1,4}

Faculty of Sciences, Ibn Tofail University, Kénitra, Morocco²

Ecole Supérieure de Technologie, Moulay Ismail University, Meknès, Morocco³

Abstract—Because of their algebraic structure and simple hardware implementation, linear codes as class of error-correcting codes, are used in a multitude of situations such as Compact disk, backland bar code, satellite and wireless communication, storage systems, ISBN numbers and so more. Nevertheless, the design of linear codes with high minimum Hamming distance to a given dimension and length of the code, remains an open challenge in coding theory. In this work, we propose a code construction method for constructing good binary linear codes from popular ones, while using the Hadamard matrix. The proposed method takes advantage of the MacWilliams identity for computing the weight distribution, to overcome the problem of computing the minimum Hamming distance for larger dimensions.

Keywords—Binary linear codes; code construction; minimum hamming distance; error-correcting codes; weight distribution; coding theory; hadamard matrix

I. INTRODUCTION

The basic digital communication chain includes a source, a communication channel, and a receiver. The message is sent from the source to the receiver through a channel. Unless there is an ideal channel, interference will corrupt the message and cause errors, which can be controlled by an error-correcting code. Thus, inner code redundancy is added to the original message downstream of the source. In fact, this redundancy upstream of the receiver is used to correct potential errors without retransmission.

In his fundamental article [1], Shannon showed via his channel coding theorem, the existence of error-correcting codes (ECC), theoretically allowing to transmit data in a channel with a small probability of error, whatever the noise level in the channel. However, the theorem does not specify how to create these codes. Thus the issue of implementing good error-correcting codes remains open in the field of information theory [2]. Great effort has been constantly devoted to constructing error-correcting codes to totally or almost achieve the channel capacity, following Shannon's work. In this way, Arikan developed the first codes (polar codes) with proven capacity, explicit construction, and low coding and decoding complexity [3], with the implementation of their multi-kernel designs [4]. This paper's inspiration comes from the coding process of polar code.

It is difficult to construct explicitly good codes with the best properties. Therefore, working with the already existing codes, with good properties, could be one of construction

alternatives [5]. Thus to determine if the code would be good enough, Markus Grassl made a bounds database [6] for the minimum distance of linear block codes over $GF(q)$, with $q \leq 9$, for given length and dimension, including construction details. Hence, if its parameters allow the current bounds to be achieved, the code is called 'good'.

One of the most recent methods to construct good binary linear block codes is presented in [7]. It consists in constructing linear codes from the Hadamard matrix and Bose–Chaudhuri–Hocquenghem (BCH) codes [8]. However, this method suffers from the problem of computing the minimal Hamming distance for higher code dimensions and it is used only for BCH codes. In this paper, a new method to produce good binary linear block codes based on the Hadamard matrix and some popular error-correcting codes often used in coding theory [9], [10] is presented. It allows to design many good binary linear block codes with considerable error-correcting capability. This method extends the approach presented in [7] for larger dimensions by exploiting the MacWilliams identity to overcome the problem of computing the minimal distance on the one hand, and to confirm the technique for codes other than BCH codes [8] on the other hand.

The remainder of this paper is structured as follows. In the next section, we detail some of the concepts required in this work, such as linear block codes, dual code of linear block code, MacWilliams identity, and Hadamard matrices. We present a new method of searching good binary linear codes in the third section. In the fourth section, we improve the proposed method by the set of good binary linear block codes found. Finally, we give an interpretation of the results before concluding the paper.

II. NOTATION AND PRELIMINARIES

In digital transmission, binary error-correcting codes denoted as $[n, k, d_{min}]$, can be employed to limit the incidence of word errors. Converting a k -bit word to an n -bit codeword ($n > k$), is the coding process. This conversion creates a code C with 2^k n -bit codewords chosen from a set of 2^n codewords. It has three main parameters: the length of codeword n , the dimension of coded block message k and the minimum Hamming distance between codewords d_{min} . This minimum distance ensures that a codeword will not be transformed, due to noise, into another codeword, and it allows to get the error correction capability.

A. Linear Block Codes Theory

A binary linear code is a sub-vector space over \mathbb{F}_2^n with dimension k . The code is a set of 2^k codewords, each one is a linear combination of the k basis vectors, that form a $k * n$ generator matrix, $G \in \mathbb{F}_2^{k*n}$. In other words, the codeword space \mathcal{V} of the code can be obtained as follow:

$$\mathcal{V} = \{c = u * G | u \in \mathbb{F}_2^k\} \quad (1)$$

Where $u = (u_0, u_1, \dots, u_k)$ is called the message to be sent, and $c = (c_0, c_1, \dots, c_n)$ is the codeword produced after encoding the message u .

The one-to-one correspondence between messages and codewords is a fundamental force of block codes; thus, a message is successfully retrieved if the decoder identifies its equivalent codeword. So, the minimum Hamming distance parameter of a code allows defining a difference limit between two valid codewords. It is the outcome of:

$$d_{min}(C) = \min\{d(c, c') : c, c' \in C \text{ and } c \neq c'\} \quad (2)$$

In the case of binary linear block codes, the minimum Hamming distance is equivalent to the smallest non-zero weight of a codeword of C , so that the weight of a codeword c is the number of its non-zero symbols. It is defined as:

$$w(c_i) = \begin{cases} 1 & \text{if } c_i \neq 0 \\ 0 & \text{if } c_i = 0 \end{cases} \Rightarrow w(c) = \sum_{i=1}^n w(c_i) \quad (3)$$

Another way to define a linear code is to use a matrix $H \in \mathbb{F}_2^{n*(n-k)}$ called parity-check matrix, which yields:

$$C = \{(c_1, c_2, \dots, c_n) | (c_1, c_2, \dots, c_n) * H^T = 0\} \quad (4)$$

So, for each linear block code $C(n, k, d_{min})$ defined by its generator matrix whose rows structure a basis of a linear vector subspace, another linear block code exists. It is called dual code C^\perp , known by length n , dimension $(n - k)$, and the vector space consisting of all orthogonal vectors (codewords) with the linear code C vectors. This means that two n-tuples x and y are orthogonal if their inner product is zero:

$$(x, y) = \sum_{i=1}^n (x_i, y_i) = 0 \quad (5)$$

If $G = [I_k | P]$ is the generator matrix of a linear code $C(n, k, d_{min})$ in the systematic form, then the generator matrix of its dual code is called parity-check matrix, such as:

$$H = [P^\perp | I_{n-k}] \quad (6)$$

B. Weight Distribution and MacWilliams Identity

As mentioned above, the minimum distance is the lower weight $w(c)$ as defined in (3), of a nonzero codeword among all of the 2^k codewords in linear code. The importance of this parameter lays in the error correction capacity of the code through $d_{min} = 2t + 1$, where t denotes the number of errors that the code is capable of correcting. However, the minimum distance does not give an idea about the other codewords' weight.

Acquiring knowledge of a code's weight distribution is essential and allows the computation of its analytical performance [11]. The weight distribution of an error-correcting code is a vector of size n whose i^{th} element

indicates the number of codewords having the weight $(i - 1)$. Otherwise, the weight distribution can be expressed in polynomial form as follows:

$$W(z) = w_0 + w_1z + \dots + w_{n-1}z^{n-1} \quad (7)$$

where w_i is the number of codewords with weight i obtained by (3).

Although the weight distribution does not inherently identify a code, it provides useful information that has both practical and theoretical significance. MacWilliams equation [12], a series of linear relations between the weight distributions of a code and its dual, is one of the most fundamental conclusion in weight distributions.

Let C be a $(n, k, d)_q$ linear code over \mathbb{F}_q^n with enumerator polynomial $W(z) = \sum_{i=0}^n w_i z^i$, and let $W^\perp(z)$ be the enumerator polynomial of the dual code C^\perp . Then:

$$W^\perp(z) = q^{-k}(1 + (q - 1)z)^n W\left(\frac{1-z}{1+(q-1)z}\right) \quad (8)$$

C. Hadamard Matrix

The Hadamard matrix H_m is a square matrix of order m , with m being a power of 2, and entries in $\{-1, +1\}$ as

$$H_m H_m^T = m I_m \quad (9)$$

Sylvester presented the first examples of these matrices in 1867 [13], before naming them Hadamard matrices in 1893 [14], after Hadamard who generalized them for orders other than 2^m . Many employments for these matrices have been found in telecommunications and signal processing. In fact, the use of Hadamard matrices to construct efficient error-correcting codes is one of the reasons that increased interest in discovering new Hadamard matrix constructions.

In a binary case, we can replace $\{-1, +1\}$ of H_m by $\{1, 0\}$ then H_m is obtained by the following technique:

$$\begin{aligned} H_1 &= [0] \equiv [1] \\ H_2 &= \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \\ H_m &= H_2 \otimes H_{m/2} \end{aligned} \quad (10)$$

where \otimes denotes the Kronecker product.

The orthogonality of the Hadamard matrix (9) guarantees that each permutation of rows or columns yields another Hadamard matrix [15].

III. NEW METHOD TO FIND GOOD BINARY LINEAR CODES

In [7], a method based on the outcome of the Kronecker product, between the Hadamard matrix and the redundant part of a generator matrix of a Bose, Ray-Chaudhuri et Hocquenghem (BCH) code is presented, to construct good binary linear codes. It allows us, from a (n, k, d_{min}) BCH code and a Hadamard matrix of order m , to build good binary linear codes having a given dimension $k' < 20$ and length $n' = m * n$. However, for higher dimensions, this approach has a problem to calculate the minimum Hamming distance, it is one of the open problems [16] in the field of information theory for large dimensions.

So for dimensions $k' > 20$, the method presented in [7] remains restricted according to the performance of a simple computer to calculate the minimum distance for codes with dimensions greater than 20. In this work, we practically took advantage of the dual properties of linear block codes and MacWilliams identity as it can be seen in figure 1 and outlined in the steps below, in order to fix this issue and validate the process by constructing good codes with high dimensions.

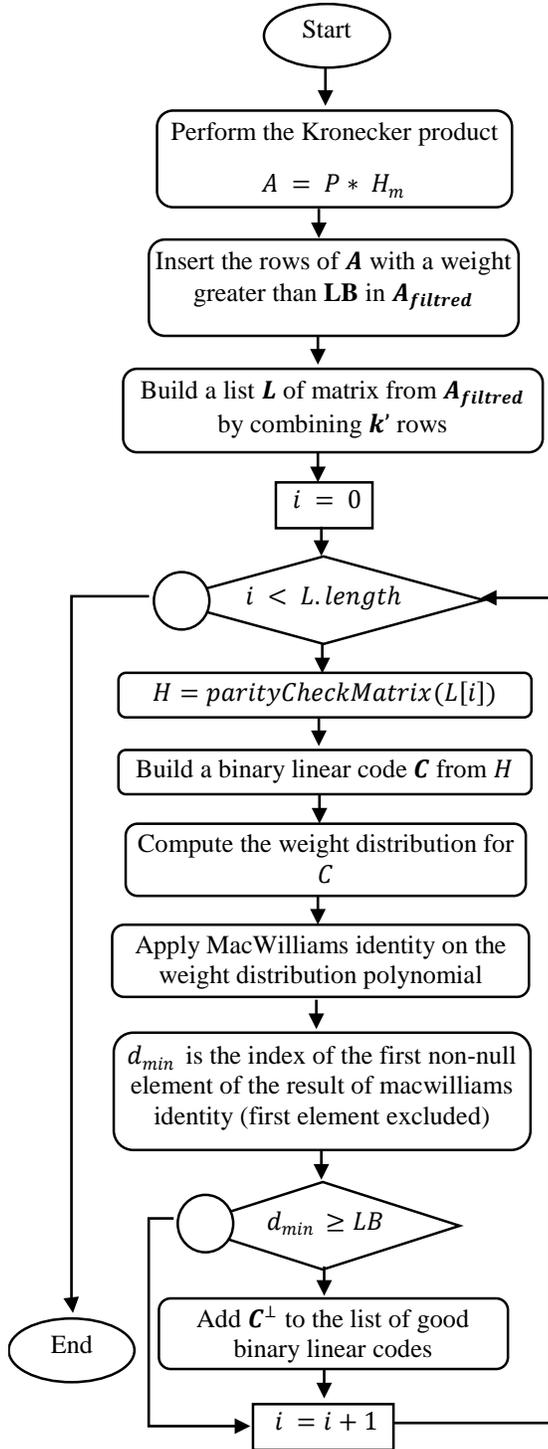


Fig. 1. New Method to Find Good Binary Linear Codes using MacWilliams Identity to Reduce the Complexity of the Minimum Distance Computation.

The technique consists of treating the minimum Hamming distance computation problem of the larger dimensions by searching good binary linear codes via their dual codes, with small dimensions, and calculating the weight distribution obtained using the identity of MacWilliams identity as described in (8). By definition, the minimum Hamming distance of a linear code corresponds to the smallest weight of its codewords, so it is obvious to extract the minimum distance of a linear code from its weight distribution, it corresponds to the index of the first non-null element of the weight distribution of a linear code (first element excluded, because it corresponds to the zero's codeword).

The details of the method we propose to improve the dimensions of the constructed good binary linear codes are developed in the following steps. Let's use:

- P : $n * (n - k)$ matrix extracted from a generator matrix of the popular used code in the systematic form.
- LB : Lower bound is the best-known minimum distance found in all pre-existing works.
- H_m : Hadamard matrix of order m .
- k' : Dimension of the desired code to be built.
- H : Parity check matrix constructed as described in (6).
- C^\perp : Dual code constructed from the parity check matrix H .
- $parityCheckMatrix()$: Function to transform a generator matrix to parity check matrix.
- $A_{filtred}$ the matrix A after the elimination of unnecessary rows (rows whose weight is less than LB).

Inputs: P, k', LB

Outputs: List of (n', k', d') binary linear codes.

- Step1:** Perform the kronecker product between the P and H_m .
Step2: Insert the rows of the step1 result whose weight is less than LB in $A_{filtred}$.
Step3: Generate matrices from the output of step 2 by combining k' rows.
Step4: From step 3, for each matrix G :
 - Extract the parity matrix H from G .
 - Build a dual code by H .
 - Compute the weight distribution of the dual code
 - Apply (8) on the weight distribution already computed.
 - d' is the index of the first not null element in the weight distribution obtained by (8).
Step5: If $d' \geq LB$ then add the code to the list of $(n' = m(n - k), k', d')$ good binary linear codes.

Let's give an example: Consider, the matrix A derived from the Kronecker product between the Hadamard matrix of order $m = 4$ and the redundant part matrix P extracted from the generator matrix of $(7,4,3)$ BCH code. i.e.

$$A = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 0 & 1 \end{pmatrix} \otimes \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \end{pmatrix}$$

$n' = 12$ is the length of suspect codes that can be constructed. Although the minimum distance of a linear code is equal to the minimum weight of the code, and the rows of a generator matrix are also codewords, it is consequently necessary to eliminate the rows whose weight is less than the lower bound (LB). Note $A_{Filtered}$ the matrix A after the elimination of unnecessary rows.

$$A_{Filtered} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 & 0 \end{pmatrix} \quad (11)$$

For example, to build a code with dimension $k' = 8$, proceeding to the construction of a code with $k' = 4$. In other words, it would be sufficient to check-in a space of size 2^4 instead of searching in a space of dimension 2^8 . From [17], the best-known minimum distance (LB) for $n' = 12$ and $k' = 8$ is 3, so $A_{Filtered}$ will be obtained by eliminating all rows with a weight less than 3 as defined in (11).

By combining 4 rows of $A_{Filtered}$ as a generator matrix of a suspect (12,4,x) code, calculating the weight distribution of the code and applying the MacWilliams identity, codes with the following weight distribution is obtained:

$$[1, 0, 0, 16, 39, 48, 48, 48, 39, 16, 0, 0, 1]$$

Which means that the minimum distance of the linear code is 3 and it contains 16 codewords of weight 3.

IV. EXPERIMENTAL RESULTS

Three types of results are presented in this section; the first one is obtained by the new method mentioned in the previous section, the second is an extension of [7] for the Golay and Reed-Muller codes, and the third one is based on the codes of the first result. All programs have been implemented in GAP via the GUAVA package over F_2 and F_3 [18].

A. Results Obtained using the MacWilliams Identity

The method as defined in [7], through a computer calculations with Intel(R) Core(TM) i5-4210U RAM 4 CPU @1.70GHz configuration, does not permit to generate good

binary linear codes with a dimension greater than 20. But, for dimensions greater than 20 and using the same computer, the new approach helps us to verify the validity of the concept, for dimensions greater than 20, and it allowed us to find new good binary linear codes. Table 1 describes the set of good binary linear codes with larger dimensions ($k > 20$), built using BCH codes by applying the presented approach.

In [7], it is focused on the construction of good binary linear codes from the Hadamard matrix and BCH codes. In this work, we tried to apply the approach for other codes with good properties. Table 2 describes the good codes constructed from Golay code (23,12).

Applicability of the technique for Reed-Muller codes produced satisfactory results, as shown in table 3.

TABLE I. GOOD BINARY LINEAR CODES USING BCH CODES

Rate	Code $[n, k, d]$	d_{magma}	Lower bound
0,86	[30,26,2]	2	2
0,9	[30,27,2]	2	2
0,93	[30,28,2]	2	2
0,71	[32,23,4]	4	4
0,75	[32,24,3]	3	4
0,84	[32,27,2]	2	2
0,87	[32,28,2]	2	2
0,69	[36,25,4]	4	5
0,72	[36,26,4]	4	4
0,78	[37,29,3]	3	4
0,76	[38,29,4]	4	4
0,55	[40,22,7]	7	8
0,6	[40,24,7]	7	7
0,62	[40,25,6]	6	6
0,72	[40,29,4]	4	5
0,75	[40,30,3]	3	4
0,78	[60,47,6]	6	6
0,83	[60,50,3]	3	4
0,81	[60,49,4]	4	4
0,84	[78,66,4]	4	4

TABLE II. GOOD BINARY LINEAR CODES USING GOLAY CODE

Rate	Code $[n, k, d]$	d_{magma}	Lower bound
0,86	[22,14,4]	4	4
0,68	[22,15,4]	3	4
0,9	[22,17,3]	3	3
0,93	[22,18,2]	2	2
0,71	[22,20,2]	2	2

TABLE III. GOOD BINARY LINEAR CODES USING REED-MULLER CODES

Rate	Code $[n, k, d]$	d_{magma}	Lower bound
0,5	[16,8,5]	5	5
0,56	[16,9,3]	3	4
0,75	[16,12,2]	2	2
0,81	[16,13,2]	2	2
0,63	[22,14,4]	4	4
0,59	[22,13,4]	4	5
0,81	[22,18,2]	2	2

B. Good Extended and Punctured Binary Linear Codes

Extending and puncturing code are two methods of code construction [19], which maintain the code dimension k while varying its length n . In the case of extending code, parity bits are added, which can contribute to increase a minimum distance. Whereas puncturing removes parity bits, which can lead to decrease a minimum distance. Let us $C_{ext}(n+1, k)$ a binary linear code who is the extended code of the linear $C(n, k)$. The extension is completed by adding a new coordinate (parity check bit) to each codeword of C so that the codeword length goes up. Put differently, each codeword $v_{ext} = (v_1, v_2, \dots, v_n, v_{n+1})$ of the extended code C_{ext} is generated by attaching a coordinate to the codeword $v = (v_1, v_2, \dots, v_n)$ from C , in order that $v_{n+1} = \sum_{i=1}^n v_i$, where sum is modulo 2 addition in binary case.

In this reflection, new good codes were defined by applying the extending and puncturing to the good codes mentioned in Tables 1, 2, and 3, as well as to the codes contained in related previous work [7]. Table 4 shows all the good extended and punctured binary linear codes found.

C. Interpretation

Lately, error-correcting code designers have been concerned with finding a high code rate which is defined as the ratio of the number of information symbols k to the length of codeword n , to take maximum advantage of the capacity of the channel.

In this work, the focus is on error-correcting codes with a rate greater than 0.5. Most of the constructed codes have a minimum Hamming distance equal to the lower bound, allowing us to identify them as well as good binary linear error-correcting codes. In some of the results above, for given n' and k' , most of the codes are found with the same wanted minimum distance (LB) existing in [6], and the chosen one is the one with the smallest number of codewords with minimum weight in the weight distribution. However, it should be mentioned that just a few codes with the lower limit have been reported in the literature for the codes that did not achieve the LB , and that the research discovered multiple different codes with the lower limit ($LB - 1$).

In comparison to the results obtained in [7], the technique provided in this paper allows us to construct good binary linear codes with larger dimensions and good properties. Unlike previous research, instead of shedding light on BCH codes only, the strategy yields positive outcomes for a variety of different codes, such as Golay and Reed-Muller codes.

All of the good codes discovered in this and previous research have been validated in software, designed to solve algebra problems MAGMA [20], [21], which supports several coding theories.

The exponential explosion of possible combinations, from $A_{filtered}$, of suspect codes for higher dimensions continues to be a problem of finding good codes observed during this work. This issue will continue to be a source of reflection in the future. The main objective of this simulation is to demonstrate that the proposed methodology is applicable to larger dimensions as well as codes other than used codes.

TABLE IV. GOOD EXTENDED AND PUNCTURED BINARY LINEAR CODES

Rate	Code $[n, k, d]$	d_{magma}	Lower bound
0,54	[11,6,4]	4	4
0,61	[13,8,4]	4	4
0,52	[17,9,4]	4	5
0,63	[19,12,4]	4	4
0,65	[23,15,4]	4	4
0,73	[23,17,4]	4	4
0,72	[33,24,4]	4	4
0,53	[41,22,7]	8	8
0,83	[59,49,4]	4	4
0,81	[61,50,4]	4	4

V. CONCLUSION

In this paper, an extension of the method of constructing good linear codes from BCH codes and Hadamard matrices, stated in the literature to higher dimensions and for other popular codes. In this way, a set of good binary linear block codes were discovered by exploring the duality of linear codes and MacWilliams identity on the one hand, and by extending and puncturing the discovered results on the other. The majority of the found codes match the bound of the existing codes in the literature. The search issue for good error-correcting code search problem is very large for most standard search techniques. In this case, and to overcome the problem of the exponential explosion of the number of combinations, genetic algorithms can be an efficient way to find good solutions in a relatively short time, and it can be a research direction for future work.

REFERENCES

- [1] C. E. Shannon, "A Mathematical Theory of Communication," Bell System Technical Journal, vol. 27, no. 3, pp. 379–423, 1948, doi: 10.1002/j.1538-7305.1948.tb01338.x.
- [2] D. Joyner and J.-L. Kim, Selected Unsolved Problems in Coding Theory. Birkhäuser Basel, 2011. doi: 10.1007/978-0-8176-8256-9.
- [3] E. Arıkan, "Channel Polarization: A Method for Constructing Capacity-Achieving Codes for Symmetric Binary-Input Memoryless Channels," IEEE Transactions on Information Theory, vol. 55, no. 7, pp. 3051–3073, Jul. 2009, doi: 10.1109/TIT.2009.2021379.
- [4] F. Gabry, V. Bioglio, I. Land, and J.-C. Belfiore, "Multi-kernel construction of polar codes," in 2017 IEEE International Conference on Communications Workshops (ICC Workshops), May 2017, pp. 761–765. doi: 10.1109/ICCW.2017.7962750.
- [5] M. Tomlinson, C. J. Tjhai, M. A. Ambroze, M. Ahmed, and M. Jibril, "Good Binary Linear Codes," in Error-Correction Coding and Decoding: Bounds, Codes, Decoders, Analysis and Applications, M. Tomlinson, C. J. Tjhai, M. A. Ambroze, M. Ahmed, and M. Jibril, Eds. Cham: Springer International Publishing, 2017, pp. 101–136. doi: 10.1007/978-3-319-51103-0_5.
- [6] G. Markus, "'Bounds on the minimum distance of linear codes and quantum codes.'" Online available at <http://www.codetables.de>. Accessed on 2021-08-04."
- [7] D. Khebbou, R. Benkhrouya, and I. Chana, "Construction of Some Good Binary Linear Codes Using Hadamard Matrix and BCH Codes," in Proceedings of Sixth International Congress on Information and Communication Technology, Singapore, 2022, pp. 523–532. doi: 10.1007/978-981-16-2377-6_49.
- [8] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," Information and Control, vol. 3, no. 1, pp. 68–79, Mar. 1960, doi: 10.1016/S0019-9958(60)90287-4.
- [9] I. Reed, "A class of multiple-error-correcting codes and the decoding scheme," Transactions of the IRE Professional Group on Information

- Theory, vol. 4, no. 4, pp. 38–49, Sep. 1954, doi: 10.1109/TIT.1954.1057465.
- [10] Marcel Golay, “Notes on Digital Coding.” 1949.
- [11] L. Bolcar, “Weights of Linear Codes and their Dual,” Academic Festival, Apr. 2020, [Online]. Available: <https://digitalcommons.sacredheart.edu/acadfest/2020/all/102>.
- [12] J. MacWilliams, “A theorem on the distribution of weights in a systematic code,” The Bell System Technical Journal, vol. 42, no. 1, pp. 79–94, Jan. 1963, doi: 10.1002/j.1538-7305.1963.tb04003.x.
- [13] J. J. Sylvester, “LX. Thoughts on inverse orthogonal matrices, simultaneous signsuccessions, and tessellated pavements in two or more colours, with applications to Newton’s rule, ornamental tile-work, and the theory of numbers,” The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science, vol. 34, no. 232, pp. 461–475, Dec. 1867, doi: 10.1080/14786446708639914.
- [14] J. Hadamard, Resolution D’une Question Relative Aux Determinants - in Bulletin des Sciences Mathematiques, Septembre 1893, 1st Edition. See Description, 1893.
- [15] A. LaClair, “A Survey on Hadamard Matrices,” Chancellor’s Honors Program Projects, May 2016, [Online]. Available: https://trace.tennessee.edu/utk_chanhonoproj/1971.
- [16] M. Askali, A. Azouaoui, S. Nouh, and M. Belkasm, “On the Computing of the Minimum Distance of Linear Block Codes by Heuristic Methods,” International Journal of Communications, Network and System Sciences, vol. 5, no. 11, Art. no. 11, Nov. 2012, doi: 10.4236/ijcns.2012.511081.
- [17] Grassl, Markus, “Bounds on the minimum distance of linear codes and quantum codes.” <http://www.codetables.de>.
- [18] “The GAP Group,” 2015. <http://www.gap-system.org>.
- [19] V. Pless and W. C. Huffman, Eds., “Basic concepts of linear codes,” in Fundamentals of Error-Correcting Codes, Cambridge: Cambridge University Press, 2003, pp. 1–52. doi: 10.1017/CBO9780511807077.002.
- [20] W. Bosma, J. Cannon, and C. Playoust, “The Magma Algebra System I: The User Language,” Journal of Symbolic Computation, vol. 24, no. 3, pp. 235–265, Sep. 1997, doi: 10.1006/jsco.1996.0125.
- [21] J. Cannon and W. Bosma, “Handbook of Magma Functions,” Jan. 2008.

EFPT-OIDS: Evaluation Framework for a Pre-processing Techniques of Automatic Ophtho-Imaging Diagnosis and Detection System

Sobia Naz¹

Research Scholar
Department of Electronics and
Communications Engineering
PES College of Engineering
Mandya, Karnataka, India

Dr.Radha Krishna Rao K.A²

Professor and Head
Department of Electronics and
Communications Engineering
PES College of Engineering
Mandya, Karnataka, India

Dr. Shreekanth T³

Project Manager
L&T Technology Services
Mysore, India

Abstract—The modalities of FUNDUS images and the availability of public domain data sets provides a starting point in designing an ecosystem for developing an automatic detection of degenerative early-stage Glaucoma and Diabetic Retinopathy, and other eye-related diseases. The existing techniques for these operations lack flexibility and robustness in their design implementation and are limited to only certain preprocessing requirements. However, the existing methods are useful but provide lower performance when the FUNDUS image quality degrades due to misalignment of lens opening in camera and poor functioning of visual sensors. This paper presents a unified framework that mechanizes different preprocessing techniques to benefit the Ophtho-imaging diagnosis and disease detection process. The proposed framework facilitates on-demand data treatment operations that include image interpolation, brightness adjustment, illumination correction, and noise reduction. The proposed techniques for FUNDUS image enhancement provide better PSNR and SSIM-performance metrics for image quality than existing popular image enhancement techniques when tested on two standard publicly available datasets. The contribution of the proposed framework is that it offers flexible and effective mechanisms that meet dynamic preprocessing operations on an on-demand basis to prepare better data representation for building machine learning models. The framework can also be used in real-time for eye disease diagnosis by an ophthalmologist.

Keywords—Pre-processing; FUNDUS image; glaucoma; diabetic retinopathy; interpolation; image enhancement

I. INTRODUCTION

The multidomain research modality is gaining popularity with the ever-increasing availability of the dataset, computing platform, and ecosystem, along with the advancement of the technologies like artificial intelligence (AI) and machine learning (ML) [1]. Many of the system processes aim to obtain complete automation in the enterprise's applications. The health care industry is one of the fastest adopting sectors after defense and another industrial automation [2]. The research statistics reveal that the stake of AI in medical imaging is approximately USD 264 billion by 2026 [3]. This paper focuses on medical imaging, namely, Fundus Imaging for the specialized healthcare section called ophthalmology, which deals with diagnosing and treating eye-related disease

Glaucoma from preprocessing perspectives. It is essential to know the modality of the Fundus image capturing aspects to understand the inclusion of the noises or redundancies that require preprocessing operation for the human vision system (HVS). The ophthalmic photographers capture the retina image using a specially designed fundus camera [4]. Fundus images are quite popular; the ophthalmologists found it suitable to diagnose Glaucoma or diabetic retinopathy [5]. The fundus images produce shallow and non-uniform contrast conditions between the retinal structural elements and the background and due to which the ophthalmologist faces difficulty to analyze it. However, the clarity is found by practicing an injective of the contrasting chemical during the fundus angiogram, but it sometimes affects the patient's health conditions [6]. The image enhancements techniques provide an alternate noninvasive way to enhance the fundus image quality for the HVS.

Further, with the increasing number of patients related to eye diseases and the lack of adequate ophthalmologist experts, investment is needed to build an automated system that can diagnose eye diseases using AI and ML. There is a critical requirement of preprocessing on Fundus images to obtain a higher accuracy for segmentation and feature extraction for learning models. The essential and effective preprocessing techniques include 1) fundus image enhancement for contrast and brightness adjustment 2) Interpolation for uniform dataset images 3) Region of Interest (ROI) localization for vessel removal by cropping for higher accuracy by the learning model. The existing literature is rich in treating medical image quality but, with a limited scope, does not consider all the essential preprocessing techniques in a single framework. Also, the existing techniques implemented using recursive operation suffers from substantial computational complexity that hinders its applicability in the real-time scenario. In this regard, the proposed work suggests a unified preprocessing framework consisting of different types of enhancement and image correction techniques that can meet the dynamic preprocessing requirement without depending on the requirement of an external source. The current research work also proposes a image enhancement techniques based on the convolution operation to filter the noise in frequency domain

and enhance the contrast without affecting the diagnostic quality of the image. The rest of the sections of this paper includes: related work in Section II, research problem in Section III description of the dataset is presented in Section IV. The modeling of the proposed preprocessing framework is discussed in Section V. Result analysis for the proposed preprocessing approaches is given in Section VI, and the overall contribution of this paper is summarized in Section VII.

II. RELATED WORK

Over the past few years, several techniques have been introduced to enhance fundus images before diagnosing optic disc for inspecting the condition of the diseases or Glaucoma that affect the eye. A work carried out by Sudeshna, and Santi [7] presents an automatic model to identify retinal lesions, where the curvelet transform technique is used for the edge enhancement and dark and brighter areas of retinal lesions are optimized using a bandpass filter. However, this approach requires a higher computational time. Image contrast enhancement using adaptive histogram equalization (AHE) was quite popular; the study by Bharkad [8] has applied AHE on the green component of the retinal to enhance the contrast for segmenting optic disk. A similar approach has been considered in the study of Jebaseeli et al. [9] to enhance the green component towards improving the contrast of the blood vessels. The work of Bhatt et al. [10] considers AHE on the red component of the retinal image for normalizing contrast. On the other hand, the median filtering approach is considered for the smoothing optic disc regions. However, AHE-based contrast enhancement provides improvements at the cost of reduced gray level, which may associate with loss of image intelligibility. In the study of Sahu et al. [11], the authors have demonstrated that CLAHE based preprocessing is appropriate for the refining fundus image quality. The work done by Rahim et al. [12] suggested multiple approaches to enhancing the fundus image towards the recognition of blood vessels for diabetic retinopathy using AHE, CLAHE, and Mahalanobis Distance techniques applied over the green channel of the fundus image. However, the Mahalanobis Distance method shows effective performance compared to the other two methods. In the study of Elloumi et al. [13], the authors presented a pipeline for image enhancement for the fundus image captured from the smartphone. They suggested that image enhancement can be better achieved by adopting the CLAHE and Butterworth filtering approach to reduce high-frequency noise present in the smartphone-captured fundus image. However, this approach may suffer from some real problem that has not been explored and addressed in this work. Bala et al. [14] adopted a joint approach of AHE and curvelet features for denoising retinal images. AHE is considered for optimizing ringing in this approach, and specular noises and curvelet features are considered for edge-preserving during denoising operation. The use of a quadratic filter can also be seen in the study of Hari et al. [15] to localize diabetic retinopathy. Abdallah et al. [16] presented their work to address the excessive smoothing issues caused by linear filters and conducted a performance assessment of different diffusion filters to improve contrast and sharpness of the fundus image for disease analysis. A de-hazing technique

is adopted in Vinodhini et al. [17] to correct non-uniform illumination in fundus image intensity, and contrast enhancement is performed using CLAHE followed by an adaptive median filter. Bhardwaj et al. [18] evaluated mathematical morphology for optic disc segmentation and blood vessel extraction. The work carried out by Hassan and Hassanien [19] developed an automated system to extract the retinal vasculature from the fundus images using preprocessing and segmentation mechanisms. The preprocessing operation over the fundus image is carried in multiple steps, where the first step is the fundus image resizing. The global mean value is computed for the brightness pixel, and further windowing-mean operation is carried to compute an enhanced image. Apart from AHE, CLAHE, Morphology, median filtering, and curvelet transform, Retinex-based preprocessing schemes have also been introduced to enhance the contrast of the Fundus or retinex images. The work of Sadia et al. [20] and Mahmood et al. [21] demonstrated the effectiveness of multi-scale retinex based preprocessing techniques for high-quality enhancement by eliminating uneven illumination in the image intensity. The adoption of hybrid approaches is also seen in some studies. A recent work by Sathananthavathi and Indumathi [22] uses a particle swarm optimization approach with gamma correction to improve and achieve optimal enhancement on the fundus image. Alwazzan et al. [23] used wiener filters with CLAHE to enhance the color fundus image. Bataineh and Almotairi [24] adopted bilateral filters to highlight the visual feature of the fundus image. However, all these techniques have significant dependency on large computational resource requirements due to their implementation strategy's recursive nature. Irrespective of having many suitable techniques, the ophthalmologist and machine learning modelers for Ophthalmology requires an integrated framework that can be used for both diagnostic purposes and data perpetrator.

III. RESEARCH PROBLEM

Despite several research efforts, the existing schemes for the preprocessing fundus image still have substantial issues that need to be improvised with a unique implementation strategy. Based on review analysis, it has been found that most of the existing researchers have adopted common techniques such as Gamma correction Adaptive Histogram, CLAHE, and Retinex, for fundus image preprocessing. However, these techniques offer better results, but at the same time, they may suffer a lack of flexibility and performance challenges when applied on different datasets as the existing techniques are particular to their objectives. Along with the issue of robustness and flexibility, the existing schemes suffer from the overhead of computational complexity and take longer runtime. Therefore, it is necessary to design an integrated framework to meet the preprocessing requirements by solving dynamic problems in order to achieve flexible, computationally efficient, and effective fundus image enhancement. The model must be robust enough to complement ophthalmologist diagnosis needs and be an easy tool to generate data for automated ophthalmological disease model learning.

IV. DATASET DESCRIPTION

The proposed work for designing an evaluation framework, EFPT- OIDS, provides an ecosystem to visualize the raw images from the different datasets for the ophthalmologist, Ophtho-data scientist, and analytics. The EFPT- OIDS is evaluated on two publicly accessible standard datasets (Ds) = {CHASEDB1, DRIONS-DB}. The summary of these datasets are highlighted in Table I:

A. CHASEDB1

The CHASEDB1 is a reference database of retinal blood vessel segmentation provided by Child Health and Study England (CHASE). The database was obtained from a health survey conducted in London over 200 primary schools, and 20 fundus images of 14 children were captured at 30o Field of View with a resolution of 1280×960 to prepare the CHASE dataset. The data set is publicly available to facilitate researchers for experimental purposes. The fundus images in this database are associated with uneven illumination background and low contrast of blood vessels. The 28 images that make up the CHASEDB1 database are divided into a testing set (20 Fundus images) and a training set (8 Fundus images).

B. DRIONS-DB

DRIONS database is subjected to digital fundus image for optic nerve segmentation and open to public access for research purposes. The dataset was prepared using images belonging to the patient (male 46.2 % and female 53.8%) subjected to Caucasian ethnicity. About 76.9 % of patients were suffering from eye hypertension, and 23.1 % of patients were suffering from chronic simple Glaucoma disease. The dataset contains 110 color images having a resolution of 600 x 400, and two experts manually segmented the optic disc.

TABLE I. DESCRIPTION OF DATABASES

SI. No	Databases	Resolution	Number	Application
1	CHASEDB1	1280 x 960	28	Blood vessels segmentation
2	DRIONS-DB	600 x 400	110	Optic nerve segmentation

V. DESIGN OF PROPOSED EFPT-GDS

The fundus images contain an uneven illumination due to various real-time constraints like lightning condition, misalignments of retinal and camera focus, and faults in the camera that degrades fundus images. These images require preprocessing towards enhancement from both HVS and computer vision system (CVS) analysis viewpoints. Also, exploration of the FI dataset and its Interpolation is the requirement for preprocessing. The core component of the framework includes i) FI visualization, ii) FI Interpolation, iii) Region of Interest extraction and iv) Existing and Proposed enhancement.

A. Fundus Image Visualization

The framework creates a pointer for the location (Dp) of the dataset. Further, the encoded image representation (Ie) gets concatenated as (Dp ∪ Ie) (Dn, where, Dn is the locator $\forall Ie \in Dp$, the list of $\forall Dn$ gets updated into a structure (Is) as {(Ie)_i,

Ts, M}, where i= total number of the $Ie \in Dp$, Ts is time stamping. M is the size of Ie in bytes. For $\forall Ie \in Is$, perform sampling and quantization to get the digitized equivalent matrix as I[m,n,d], where m is several rows, n is the number of columns, and d is the number of dimensions, for original fundus image, d=3 as [R, G, B] color space. Finally, the framework displays $Ie \in Is: Dp$. Fig. 1 illustrates 'k=5' number of $Ie \in Is: Dp$ The Ophthalmologist can use the FI visualization tool to diagnose eye diseases, whereas this facility of the framework is helpful for the modeler to data exploration.



Fig. 1. Visualization 'k' Fundus Images from a Chosen Dataset CHASEDB1 and DRIONS-DB ($Ie \in Is: Dp$).

B. Fundus Image Interpolation

The ophthalmologists require an eye image with highly distinct retina layers to diagnose glaucoma [25]. Fundus photography aims to provide such imaging methodologies in their imaging process [26]. Though the ophthalmic photographer adopts various field strategies to achieve the perceived enhanced sharpness in the Fundus imaging, it requires additional processing by computing image processing. The requirement of the down sampling and up a sampling of fundus images (FI) arises while the development of computing models for the automatic detection of Glaucoma (ADG)[27] and other eye-related diseases. One such requirement includes maintaining the equal size of the fundus images from different datasets for validating the developed model of automatic disease detection (ADD) on the different datasets as different datasets maintain different sizes of the FI [28-29]. The lowest resolution of the $\forall FIo \in Dp$ is set to a threshold = {Rth, Cth} of the target size of scaling to obtain an

interpolated or scaled fundus image (FIs). The framework includes a tool for FI interpolation using the nearest neighbours as in algorithm 1. The algorithm takes the input of original funds image-(FIo), and after processing, it provides interpolated enhanced fundus image-(FIs). The algorithm computes the size of FIo as row size (nR) and column size (nC). The system then initializes the variables Rth (Target image row size) and Cth (target image column size) as a threshold to obtain an interpolated fundus image.

Algorithm-1: Fundus Image Interpolation

Input: FIo, Rth, Cth

Output: FIs

Process:

Start

1. $[nR, nC] \leftarrow f_1(FIo)$
2. Initialize Rth, Cth
3. Compute:
 - a. $R_0, C_0 \leftarrow f_2(FIo)$
4. Compute: IposR, IposC
 - a. $I_{posR} \leftarrow f_r(\sum_{i=1}^{nR \cdot R_0} / R_0)$
 - b. $I_{posC} \leftarrow f_r(\sum_{i=1}^{nC \cdot C_0} / C_0)$
5. $[RFIo, GFIo, BFIo] \leftarrow f_3(FIo, C_H)$, // where, $C_H \in R, G, B$
6. $RI \leftarrow f_{RI}(RFIo(IposR), IposC)$
7. $GI \leftarrow f_{GI}(GFIo(IposR), IposC)$
8. $BI \leftarrow f_{BI}(BFIo(IposR), IposC)$
9. Create a matrix of zeros: $M \leftarrow []_{nrT \times nrC \times 3}$
10. Append: RI, GI, BI $\rightarrow M$
11. $FIs \leftarrow M$

End

In the next step, the system computes the ratio (R_0, C_0) of target image size and size of FIo using explicit function f_2 described in equation 1 and equation 2.

$$R_0 = \frac{R_{th}}{nR} \quad (1)$$

$$C_0 = \frac{C_{th}}{nC} \quad (2)$$

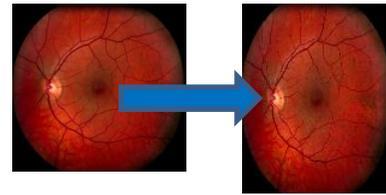
Further, a function $f_r(\)$ is applied over the interpolated position to compute normalized the row-wise pixel position- (I_{posR}) and column-wise pixel position- (I_{posC}) considering R_0, C_0 , and the size of FIo as given in equation 3 and equation 4.

$$I_{posR} = f_r(\sum_{i=1}^{nR \cdot R_0} / R_0) \quad (3)$$

$$I_{posC} = f_r(\sum_{i=1}^{nC \cdot C_0} / C_0) \quad (4)$$

Where $fr()$ denotes rounding to the nearest integer. In the next step of the algorithm, the system performs row-wise and column-wise Interpolation considering red-(RFIo), green (GFIo), and blue-(BFIo) components extracted from the FIo. Further, Interpolation for all three components, such as red component-(RI), green component-(GI), and blue component-(BI) is computed. In the next step, the algorithm creates a matrix-(M) of zeros with size R_{th} and C_{th} . Further, it performs an appending operation that resamples the interpolated RGB component's pixel value in matrix M to generate an enhanced interpolated image (FIs) outcome. In Fig. 2, the rescaling of the fundus input image using nearest-neighbour Interpolation is carried out, and the output fundus images are constructed

with the specified dimension without losing details of the fundus image.



Input Fundus Image (512 x 576) Rescaled Fundus Image (700 x 500)

Fig. 2. FI Interpolation using Nearest Neighborhood Interpolation Method.

C. Region of Interest Extraction

Since the input FI in the dataset comes with different resolutions and fields of views (FOVs). To extract the region of interest and eliminate the background from the input FI, the proposed framework adopts an adaptive cropping method that creates an interactive rectangular mask to cover the RoI region of the input FI. The tool comes with a flexible approach to operate at the ease of the user on the rectangular mask. Fig. 3 illustrates the RoI extraction from FI.

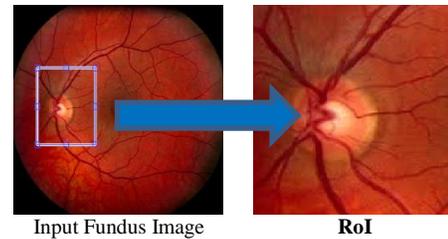


Fig. 3. RoI Extraction using user Interactive Cropping Method.

In Fig. 3, the left-hand side image is the input or target image, and the right-hand side is the RoI extracted from the input fundus image using a rectangular mask provided by the cropping tool.

D. Gamma Correction for Fundus Image Enhancement

The operator gamma (γ) performs encoding of the luminance of the input fundus images. The representation of this correction is popular by the name Gamma-Correction, and it is characterized as in eq.5.

$$I_{output} = C \times (I_{input})^\gamma \quad (5)$$

In this method, the input image (I_{input}) is mapped to the I_{output} by applying operator, C as a constant and γ as encoding and decoding factor, which ranges as $0 \leq \gamma \leq 1$ for a compressed domain but in the process of the image enhancement, an optimal value of it needs to be arrived based on the best PSNR.

In a particular context where only the gamma correction is suitable, the framework provisions manual adjustment of γ to arrive at a better visual perception from the HVS viewpoint. However, it imposes a loss of intrinsic properties, therefore not suitable form feature retention objective.

In Table II, the performance of gamma correction is evaluated with different values of γ ranging from 0.25 to 1.25 for each dataset considered in the proposed study. It can be analyzed that the value of PSNR varies depending on the value of γ operator. Fig. 4 shows that the graph trend exhibits the consistency of enhancement with the highest PSNR score at a similar range for three datasets. However, one advantage is that the value of γ can be adjusted flexibly depending on the requirement of image analysis.

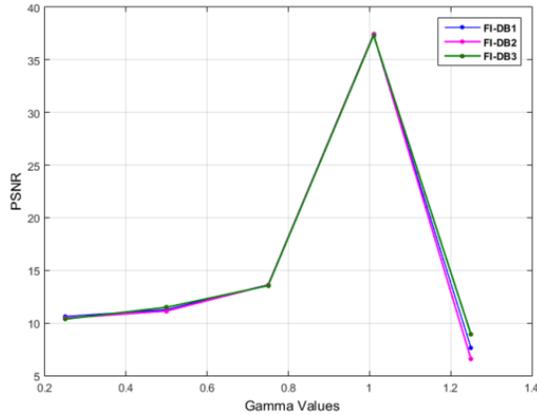


Fig. 4. Observations of the PSNR with Gamma Value Ranging from 0.25 to 1.5.

E. Equalization of the Histogram

The typical relationship between the Gray points and their frequency indicates the histogram of the FI defined in equation 6 below:

$$FI(k) = P_n / N \tag{6}$$

Where $FI(k)$ is the histogram of FI, where k indicates the gray points of an FI, P_n is the total number of the pixels in the gray point k , and N is the summation of all the pixels; therefore, the $FI(k)$ is the probability distribution of k . The process of the equalization of the histogram adopts a mapping procedure, where each pixel of the input FI is mapped to a new value as $FI(i) \rightarrow FI(j)$ using a mapping function $Mf(i)$ to get a dynamic range of the output image $FI(o)$ such that:

$$FI(i) = Mf(i) = (FI(0)-1) \sum_{k=0}^i FI(k) \tag{7}$$

Table III demonstrates a quantitative assessment of histogram equalization with different images from the particular datasets, which shows a little better pixel distribution than gamma correction. The quantitative evaluation of the Histogram Equalization technique is performed on various dataset images with their probability distribution of the pixels and the PSNR values. In this method, the larger and smoother areas get over-enhanced, which affects the disappointing appearance. If the fundus images are captured in the low lighting conditions, then the outputs are darker and contain larger smooth regions. Therefore, the histogram equalization process over-enhances the fundus images.

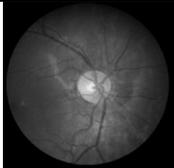
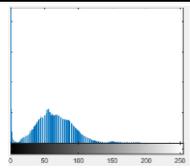
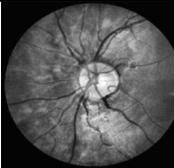
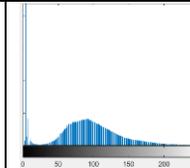
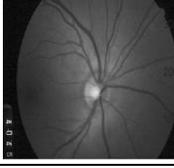
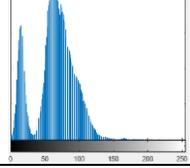
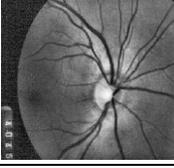
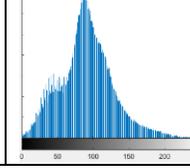
TABLE II. QUANTITATIVE ASSESSMENT OF GAMMA CORRECTION WITH VALUE RANGING FROM 0.25 TO 1.5 (3 DATASETS)

	Input Image	$\gamma = 0.25$	$\gamma = 0.5$	$\gamma = .75$	$\gamma = 1.01$	$\gamma = 1.25$
DS1						
PSNR =		10.6271	11.2672	13.6460	37.2933	7.6411
DS2						
PSNR =		10.4552	11.1387	13.6083	37.4164	6.5681

TABLE III. QUANTITATIVE ASSESSMENT OF HISTOGRAM EQUALIZATION ON DIFFERENT FUNDUS IMAGES

Dataset	Original Image	Enhanced Image	PSNR
DS1			8.6827
DS2			10.2113

TABLE IV. QUANTITATIVE ASSESSMENT OF CLAHE ON DIFFERENT FUNDUS IMAGES

Dataset	Original Image		Enhanced Image		PSNR
DS1					20.381
DS2					17.6048

F. Contrast Limited Adaptive Histogram Equalization: CLAHE

In order to overcome the limitations of the histogram equalization-based enhancement of FI, a method of CLAHE is evaluated, which minimizes the artifacts that resemble noise associated with the uniform regions. The typical process of the CLAHE-for-FI includes the redistribution process of the histogram and intra-block bilinear interpolation. The internal process of the CLAHE-for-FI initially partitions the original FI into a number of the blocks of size $B \times B$, and then on each block, the HE-for-FI is implemented. In the process of the HE-for-FI includes three significant operations as {Hsit, Clipp, Redistribution}, the specific mapping procedure provides a cumulative distribution from the clipped histogram. Further, the bilinear Interpolation provides the filtered blocks of the noises so that based on the height of the clips the contrast is enhanced. The clip-point (Cp) is computed as in equation 8 as below:

$$Cp = P/Q(1 + (K/100) \times \theta_{max}) \quad (8)$$

Where P is the pixels in each Block (Bi) of the FI, Q is the dynamic range in the Bi, θ_{max} is the maximum value of the slope, and K is the clip-factor ranging between [0:100]. The performance evaluation on various dataset images is tabulated in Table IV below with their probability distribution of the pixels and the PSNR values. The block-wise operation used in CLAHE-for-FI provides the enhancements into the contrast in a lower computational complexity. Thus, the operations where the large dataset requires to be fed in the learning models to achieve lower computational complexities during the preprocessing stage of the contrast enhancement, the CLAHE-for-FI is preferable to the HE-for-FI.

G. Retinex

A Retinex is an image enhancement technique used to adjust contrast and address illumination issues in the image. The algorithm considers logarithmic single-channel intensity images to be processed. The computing steps for Retinex based image enhancement are discussed in algorithm 2. The explicit function $f_1()$ takes the original fundus image (FI_{ori}) that provides the corresponding number of rows(nR) and columns(nC), which indicates the height(H) and width(W), respectively, of the fundus image (FI). The system then initializes a variable nI as the number of enhanced fundus image iterations. The maximum color value (Mcv) from the

fundus input image (FI_{ori}) gets computed using another explicit function $f_2()$, which defines the scale of the values possible for the color intensities. Further, an initial shift(s) computation gets performed using equation 9, as shown below.

$$S = \sum_{i,j} 2^{(f_3(\log_2(f_{min}(nR,nC))))-1)} \quad (9)$$

Where, $i = 1$ to nR and $j = 1$ to nC .

Algorithm 2: Retinex based Fundus image Enhancement

Input: FI_{ori}

Output: FI_e

Start

1. $[H, W]: [nR, nC] \leftarrow f_1(FI_{ori})$
2. Initialize nI
3. Compute: Mcv
4. $Mcv \leftarrow f_2(I)$
5. Perform initial shift:

$$S \leftarrow \sum_{i,j} 2^{(f_3(\log_2(f_{min}(nR,nC))))-1)}$$

6. $Op_{[]_{m \times n}} \leftarrow Mcv \times \sum_{i,j} n_{(nR,nC)}$
7. Till the condition $|S| \geq 1$
8. do check: for each nI
 - Hs $\leftarrow f_4(0, S)$
 - Vs $\leftarrow f_4(S, 0)$
9. end
10. $S = (-S)/2$
11. Stop
12. $FI_e \leftarrow \frac{Op + Op}{2}$

End

The explicit function $f_3()$ is used for truncating the numbers in nR and nC to integer, i.e., closer to zero, and the function $f_{min}()$ is used to compute the smallest element from the nR and nC. In the next step of the computation, the system performs initialization of the old product (Op) to scale all pixel values of nR, and nC equal to the value of Mcv, as shown in equation 10.

$$Op = Mcv \times \sum_{i,j} n_{(nR,nC)} \quad (10)$$

Where, $n = 1$.

However, the absolute value of S is greater or equal to 1 than for each nI. In that case, the system performs horizontal (Hs) and vertical shift (Vs) comparison operation using function $f_4()$, with an input argument of shift row (Sr) and

shift column (Sc). The algorithm initializes the variable UOp as updated Op, which gets computed based on the condition where the sum of the Sr and Sc is greater than zero. The value of UOp is updated with Mcv fas expressed in equation 8.

Once the condition of (|S| >= 1) becomes false, then the final enhanced Fundus image (FI_e) is obtained as in equation 11.

$$FI_e = \frac{UOp + Op}{2} \quad (11)$$

The core function of the Retinex algorithm focuses on dynamic ranges and color stability. When capturing an image by fundus imaging devices, it may be possible that certain conditions may cause the image to have a low dynamic range or poor color stability. The color of an object in images remains unchanged under various lighting conditions perceived by HVS, which is called color stability. The key mechanism of Retinex is the estimation of illumination. The Retinex algorithm is based on the path, recursion, and center-surround mechanism to enhance details and textures in the image by illumination removal. Table V exhibits the qualitative outcome of the preprocessing technique based on the Retinex algorithm for different fundus image samples with their probability distribution of the pixels and the PSNR values.

H. Proposed Image Enhancement

The fundus images usually suffer from the noises and correct poor luminance due to the absence of an element extent in the picture sensor of the fundus camera and the wrong setting of the lens opening in the camera. The proposed algorithm for fundus image enhancement uses the convolution property in order to mitigate all forms of distortions in the frequency levels. This handles the dark level of the fundus image and adjusts the contrast improved distribution of pixel density within the restricted range. The computing steps for the proposed image enhancement algorithm is discussed in algorithm 3. In the proposed algorithm, the explicit function f1() takes the original fundus image (FI_{ori}) that gives the corresponding number of rows(nR) and columns(nC), which indicates the height(H) and width(W), of the fundus image (FI). The centroidal

components P and Q get evaluated as H/2 and W/2. The system initializes the maximum high frequency and low-frequency co-efficient as: {rH, rL} and the other co-efficient: {hm, d0} as per the frequency adjustment requirements of the fundus image contrast.

Algorithm 3: Proposed Enhancement Technique

Input: FI_{ori}
Output: FI_e
Start

1. [H,W]:[nR,nC] ← f1(FI_{ori})
2. Compute: P and Q
3. P ← H/2 and Q ← W/2
4. Initialize, rH, rL, hm, d0
5. For ∀ pixel ∈ FI_{ori}
6. Compute → [H̄]_{m,n} using equ (12)
7. L̄ ← ∑[log(FI_{ori}) + 1]
8. Apply fast Fourier transformation
9. F ← f2(L̄)
10. Fo ← F̄ ⊙ H̄
11. Fb ← f3(Fo)
12. FI_e ← |e^{Fb}|

End

and brightness. Further, for each element of every row, the computation takes place as in equation 12 to update the vector [H̄]_{m,n}.

$$[\bar{H}]_{m,n} = (rH - rL) \times (1 - e^{-hmc}) + rL \quad (12)$$

Where, coefficient c can be numerically expressed as follows:

$$c = \left(\frac{\left(\sqrt{(i - P/2)^2 + (j - Q/2)^2} \right)^2}{d0} \right) \quad (13)$$

Where, i = 1 to m and j = 1 to n. The low-frequency co-efficient (L) computes as in equation 14.

$$\bar{L} = \sum[\log(I) + 1] \quad (14)$$

TABLE V. QUANTITATIVE ASSESSMENT OF RETINEX ALGORITHM ON DIFFERENT FUNDUS IMAGES

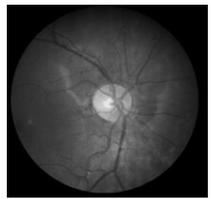
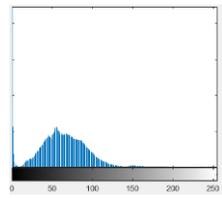
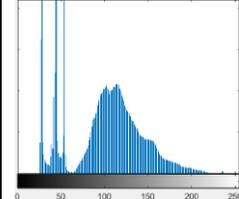
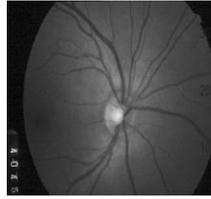
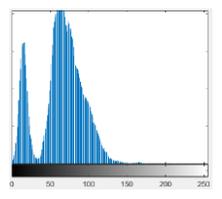
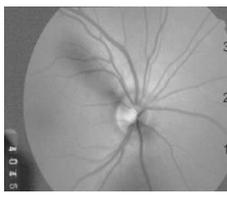
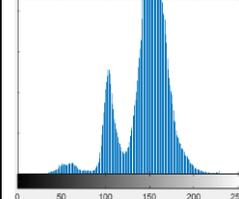
Dataset	Original Image		Enhanced Image		PSNR
DS1					14.9519
DS2					8.8829

TABLE VI. QUANTITATIVE ASSESSMENT OF THE PROPOSED IMAGE ENHANCEMENT TECHNIQUE ON DIFFERENT FUNDUS IMAGES

Dataset	Original Image		Enhanced Image		PSNR
DS1					23.3258
DS2					29.5686

In the next step, an explicit function $f_2()$ is used for two-dimensional fast Fourier transformation (2D-FFT) that takes \vec{L} to provide the corresponding co-efficient as \vec{F} . Many of the border frequency (Fb) components are not centered, which gets centered by using explicit function $f_3()$ for applying inverse 2D-FFT on filout portions (Fo). The value of filout is the vector product of \vec{F} and \vec{H} . The final enhanced fundus image (FI_e) yields better visual perception as per the co-efficient adjustments with the operations, as in equation 7.

$$FI_e = Abs(e^{Fb}) \tag{15}$$

In Table VI, a quantitative analysis of the proposed image enhancement algorithm for different fundus image samples is presented. The fundus image enhancement using a proposed method is produced based on the convolution operation linear combinations of the neighboring input image pixels.

VI. RESULT ANALYSIS

This section discusses the outcomes and performance analysis of the proposed framework concerning PSNR and SSIM quality metrics. The implementation and design of the proposed framework are carried out on a numerical computing tool MatLab. A detailed description of the performance metrics for evaluating existing techniques and proposed techniques for fundus image preprocessing is discussed as follows:

A. PSNR (Peak Signal to Noise Ratio)

This metric computes the value in decibels (dB) between the original and enhanced fundus images as a visual quality measurement. The higher value of PSNR indicates a better visual perception. There exists a fundamental relationship between the error and PSNR. Whenever the fundus image

undergoes a treatment of enhancement while reconstructing the image, and if there are some losses, it is measured by mean square error (MSE), and the peak error is mapped with PSNR. The value of PSNR is as in equation 17, which uses MSE as in equation 16.

$$MSE = \frac{\sum_{m,n} [I_{org} - I_{enc}]^2}{m \times n} \tag{16}$$

$$PSNR = 10 \log_{10} \left(\frac{R^2}{MSE} \right) \tag{17}$$

Where R is the maximum variation in the I_{org} for double-precision, it is '1', and for 8-bit unsigned integer: 255.

B. SSIM (Structural Similarity Index)

SSIM represents a human visual system-oriented image quality metric that deals with the similarity between the input and output images. The computation of SSIM is carried out over multiple windows of an image as numerically represented as follows:

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c1)(2\sigma_{xy} + c2)}{(\mu_x^2 + \mu_y^2 + c1)(\sigma_x^2 + \sigma_y^2 + c2)} \tag{18}$$

Where, μ_x and μ_y both refer to the mean value of x and y, respectively, σ_x^2 and σ_y^2 denotes variance value of the x and y, respectively. σ_{xy} indicates covariance. The c1 and c2 represent constraints whose values lie in the range of pixel value 255.

1) *Visual outcome analysis:* This section presents a qualitative analysis to visualize the quality of the enhanced images obtained from implemented existing and proposed enhancement techniques. The visual outcome obtained from implemented techniques over two different images from both datasets is shown in Table VII.

TABLE VII. VISUAL OUTCOME OF DIFFERENT TECHNIQUES FOR THREE DIFFERENT FUNDUS IMAGES

	Input image	GrayScale	Gamma correction	Histogram	CLAHE	Retinex	Proposed
CHASEDB1 (Image_08R)							
DRIONS_DB (Image 068)							

In Table VI, qualitative analysis is shown from the perspective of HVS for each technique over two fundus images considered from different datasets. It can be clearly analyzed that the proposed image enhancement techniques provide a clear view of the enhanced fundus image compared to other techniques. In the case of gamma correction, the evaluation is carried out considering the fixed value of the gamma operator for each performance evaluation instance. The visual outcome exhibits that gamma-corrected images suffer from poor brightness. However, the performance of gamma correction largely depends on the gamma operator value. The adjustment of brightness tone can be adjusted by varying the value of the gamma operator between [0,1]. In the case of the histogram, the enhanced images are subjected to over brightness issue. The main disadvantage of histogram-based image enhancement is that the image is usually prone to over-amplification in comparatively uniform regions of an image. However, this limitation of the histogram is overcome by CLAHE as it limits the over-enhanced factor of the image. The CLAHE is mostly an adopted technique for image enhancement compared to the adaptive histogram technique. Also, the Retinex techniques do not provide better visual quality of the image, and the performance varies in each test case of the images. The comparative analysis based on quantitative assessment for each implemented technique in terms of PSNR and SSIM is shown in Table VIII.

2) Numerical outcome analysis: This section presents a quantitative analysis based on the numerical outcome concerning PSNR and SSIM value of input fundus images processed by implemented preprocessing techniques. The quantified value obtained for the enhanced output images is given in Table VIII as follows.

In Table VIII, the numerical analysis is shown for 20 fundus images taken from individual datasets for the performance evaluation of the proposed enhancement technique and existing technique. Therefore, a total of 40 fundus images, i.e., 20 fundus images, are taken from the CHASEDB1 dataset, and 20 fundus images from the DRIONS_DB dataset are enhanced using implemented techniques, including existing and proposed enhancement methods. The Numerical output is computed based on the mean value of PSNR for 20 fundus images processed via each individual preprocessing technique under consideration of the proposed work. Fig. 5 demonstrates the comparative analysis for assessing the effectiveness of the proposed system with the existing system based on the mean of PNSR score.

TABLE VIII. NUMERICAL OUTCOME

TECHNIQUES	Dataset: CHASEDB1(DS1)		Dataset: DRIONS_DB (DS2)	
	PSNR	SSIM	PSNR	SSIM
GC	13.7523	0.7684	15.0515	0.7150
AHE	9.9658	0.4869	10.0935	0.5687
CLAHE	20.8603	0.6178	18.4775	0.6569
RETINEX	14.1990	0.6186	10.1988	0.6631
PROPOSED	23.7442	0.9623	25.0495	0.8275

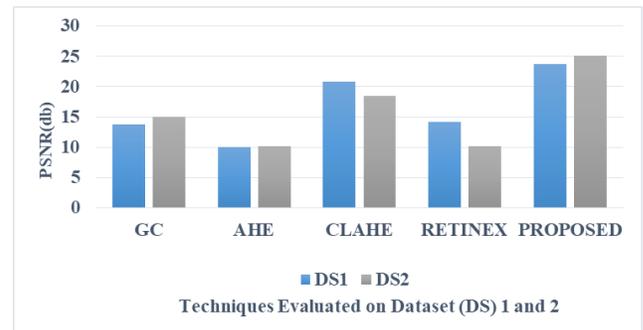


Fig. 5. Comparative Performance for different Preprocessing Techniques in Terms of PSNR.

From the comparative analysis in Fig. 5, it can be seen that the proposed image enhancement algorithm outperforms the other enhancement techniques regarding PSNR. However, after the proposed system, the CLAHE technique has maintained a good score of PNSR for different images compared to other existing techniques. In Fig. 6, a comparative analysis is presented based on the mean SSIM value obtained for each implemented technique. Based on the analysis, the proposed image enhancement technique outperforms the other enhancement techniques regarding SSIM. However, gamma correction has maintained a better mean SSIM for different images after the proposed system. It has been analyzed from both analysis that each method has a different performance score.

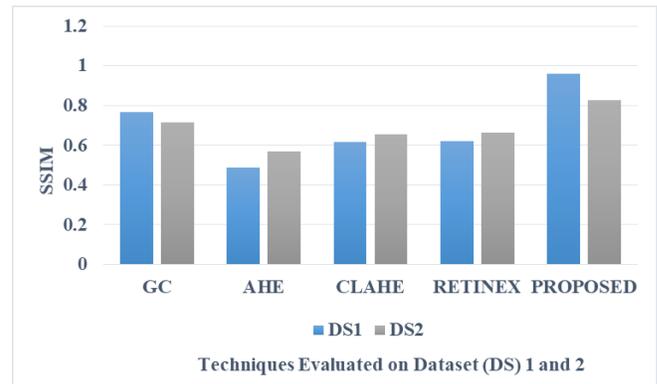


Fig. 6. Comparative Performance for different Preprocessing Techniques in Terms of SSIM.

The proposed enhancement technique has provided a better visual quality in the enhanced image. In the case of gamma correction, the PSNR and SSIM value is comparatively low compared to the proposed technique. The main disadvantage of gamma correction is that it has restricted precision, and multiple input values may be usually mapped to the same output or vice-versa. It applies adjustment of brightness on overall images. Hence, color space is also not perceptually evenly distributed.

Similarly, it has been analyzed that the adaptive histogram is also not suitable for fundus image enhancement. The histogram equalization algorithms provided unsatisfactory outcomes while dealing with fundus images obtained from a different dataset. This technique is associated with over-amplification of brightness and non-uniform distribution of

illumination images. It is because the histogram redistribution leads to unfitting pixel values in certain regions of the fundus image. The image processed with CLAHE yields a better outcome than the ordinary histogram equalization, gamma correction, and Retinex techniques. The CLAHE overcomes over-amplification in brightness as it operates on multiple fixed regions of the image known as tiles, in contrast to the overall image. However, CLAHE has certain limitations that, for certain images, it introduces noise application in flat tiles. CLAHE is computationally expensive compared to the ordinary histogram equalization technique and proposed technique. However, CLAHE outperforms other existing techniques in terms of PSNR and SSIM. But less effective compared to gamma correction in terms of SSIM. The Retinex technique is widely used in the literature to deal with poor illumination in the image. It has been analyzed that the performance of the Retinex technique quite varies for different images as its performance depends on the visual feature of images. It cannot be suitable for all types of fundus images. In Retinex based enhancements, reflectance is calculated as the image ratio to the smoothed version of the image, which is considered an approximation of illumination. The disadvantage of the retinex technique is that it can simultaneously offer dynamic compressions and visual tone reproduction. Also, the input image processed by retinex is prone to color distortion, loss of details due to halo artifacts in the output image. Another significant issue is observed while its execution is that it takes a long run time to process the image due to the involvement of the iterative process.

The proposed enhancement technique is quite flexible and evaluated with a large fundus image dataset and has a faster response time to execute preprocessing operation over input fundus image. The proposed enhancement technique takes very little run time as it adopts a simple implementation conceptually to process the input image in the frequency domain by constructing a filter vector based on different frequency coefficients and centroidal image components. On the other hand, the convolution operation in the image processing leads to yielding a better form of output enhanced fundus image. Remarkably, the proposed enhancement technique smoothens, sharpens the edges, and preserves the useful information in the output image. Based on the outcome obtained and comparative analysis, the proposed enhancement technique can be claimed to be efficient and suitable to operate on fundus images to draw a significant clinical conclusion towards eye-related disease detection.

VII. CONCLUSION

Medical imaging introduces a high degree of vision into the healthcare system, leading to widespread changes in the diagnosis and treatment of Glaucoma and diabetic retinopathy. The presence of noise, less contrast factor, and the reduction in fundus images' sharpness bring vagueness in the clinical analysis. This paper proposes an adaptive framework to carry out comprehensive image enhancement over fundus images. A user-friendly and interactive framework is introduced in the proposed study that allows users to select a desirable technique to address different issue-related images and meet preprocessing needs. The integration of the interpolation technique in the proposed framework allows the user or

ophthalmologist to deal with an imbalanced dataset consisting of variable sizes of images. The integration of the RoI extraction technique into the proposed framework is also an essential contribution, which will assist ophthalmologists in carrying out analysis on the interest area of the Fundus. Since the performance of each technique also depends on the visual characteristics of the input image. The selection of the enhancement techniques can be made based on performance metrics. In certain circumstances, multiple techniques can be checked with the input image, where the suitability of the selected technique is based on the output image quality metrics, i.e., PSNR and SSIM. Therefore, the proposed work contributes to providing deep analysis and understanding of the eye-related disease to provide better treatment. The study aimed to offer a flexible approach to diagnose the Fundus image deeply without compromising any performance-related issue. However, the scope of this framework is not only limited to the domain of fundus image enhancement. The uniqueness of the proposed framework is that it is adaptive and can be efficiently applied to other medical imaging domains, as it has layers of image enhancements techniques. In the future work, the enhanced image obtained from the proposed framework will be used to perform segmentation and glaucoma classification using machine learning technique.

REFERENCES

- [1] X. Gu, Y. Wong, L. Shou, P. Peng, G. Chen, and M. S. Kankanhalli, "Multi-Modal and Multidomain Embedding Learning for Fashion Retrieval and Analysis," in *IEEE Transactions on Multimedia*, vol. 21, no. 6, pp. 1524-1537, June 2019.
- [2] Alexander A, Jiang A, Ferreira C, Zurkiya D. An intelligent future for medical imaging: a market outlook on artificial intelligence for medical imaging. *Journal of the American College of Radiology*. 2020 Jan 1;17(1):165-70.
- [3] <https://www.openpr.com/news/1786173/global-ai-medical-imaging-market-to-grow-at-usd-264-85-billion-by-2026.html>.
- [4] M. C. V. Stella Mary, E. B. Rajasingh and G. R. Naik, "Retinal Fundus Image Analysis for Diagnosis of Glaucoma: A Comprehensive Survey," in *IEEE Access*, vol. 4, pp. 4327-4354, 2016.
- [5] Chalakkala RJ, Abdullaa WH, Hongb SC. Fundus retinal image analyses for screening and diagnosing diabetic retinopathy, macular edema, and glaucoma disorders. *Diabetes and Fundus OCT*. 2020 Apr 15:59.
- [6] Lapiere-Landry M, Carroll J, Skala MC. Imaging retinal melanin: a review of current technologies. *Journal of biological engineering*. 2018 Dec 1;12(1):29.
- [7] Sudeshna Sil Kar and Santi P. Maity, 'Automatic Detection of Retinal Lesions for Screening of Diabetic Retinopathy', *IEEE Transactions on Biomedical Engineering*, Vol.65, No.3, pp.608-618, March-2018.
- [8] Sangita Bharkad, 'Automatic Segmentation of Optic Disc in Retinal Images', *Biomedical Signal Processing and control*, Vol.31, pp.483-498, 2017.
- [9] Jebaseeli, T. Jemima, C. Anand Deva Durai, and J. Dinesh Peter, 'Segmentation of Type II Diabetic Patient's Retinal Blood Vessel to Diagnose Diabetic Retinopathy In Computer Aided Intervention and Diagnostics in Clinical and Medical Images', pp. 153-160. Springer, Cham, 2019.
- [10] Bhat, Shreenidhi H., and Preetham Kumar, 'Segmentation of Optic Disc by Localized Active Contour Model in Retinal Fundus Image', *Smart Innovations in Communication and Computational Sciences*, pp. 35-44, Springer, Singapore, 2019.
- [11] Sahu S, Singh AK, Ghreera SP, Elhoseny M. An approach for denoising and contrast enhancement of retinal fundus image using CLAHE. *Optics & Laser Technology*. 2019 Feb 1; 110:87-98.
- [12] H. Ab Rahim, A.S. Ibrahim, WMDW Zaki, A. Hussain, Methods to enhance digital fundus image for diabetic retinopathy detection, in: 2014

- IEEE 10th International Colloquium on Signal Processing & its Applications (CSPA), IEEE, 2014, pp. 221–224.
- [13] Y. Elloumi, M. Akil, N. Kehtarnavaz, A computationally efficient retina detection and enhancement image processing pipeline for smartphonecaptured fundus images, *J. Multimedia Inf. Syst.* (2018).
- [14] Anilet Bala A, Aruna Priya P, Maik V. Retinal image enhancement using adaptive histogram equalization tuned with nonsimilar grouping curvelet. *International Journal of Imaging Systems and Technology.*
- [15] Hari VS, Raj VJ, Gopikakumari R. Quadratic filter for the enhancement of edges in retinal images for the efficient detection and localization of diabetic retinopathy. *Pattern Analysis and Applications.* 2017 Feb 1;20(1):145-65.
- [16] Abdallah MB, Malek J, Azar AT, Belmabrouk H, Monreal JE. Performance evaluation of several anisotropic diffusion filters for fundus imaging. *International Journal of Intelligent Engineering Informatics.* 2015;3(1):66-90.
- [17] Vinodhini CA, Sabena S, Ramesh LS. A Robust and Fast Fundus Image Enhancement by Dehazing. In *International Conference On Computational Vision and Bio Inspired Computing 2018 Nov 29* (pp. 1111-1119). Springer, Cham.
- [18] Bhardwaj C, Jain S, Sood M. Automated optical disc segmentation and blood vessel extraction for fundus images using ophthalmic image processing. In *International Conference on Advanced Informatics for Computing Research 2018 Jul 14* (pp. 182-194). Springer, Singapore.
- [19] Hassan G, Hassanien AE. Retinal fundus vasculature multilevel segmentation using whale optimization algorithm. *Signal, Image and Video Processing.* 2018 Feb 1;12(2):263-70.
- [20] Sadia H, Azeem F, Ullah H, Mahmood Z, Khattak S, Khan GZ. Color Image Enhancement Using Multiscale Retinex with Guided Filter. In *2018 International Conference on Frontiers of Information Technology (FIT) 2018 Dec 17* (pp. 82-87). IEEE.
- [21] Mahmood Z, Muhammad N, Bibi N, Malik YM, Ahmed N. Human visual enhancement using Multi Scale Retinex. *Informatics in Medicine Unlocked.* 2018 Jan 1;13:9-20.
- [22] Sathananthavathi, V., Indumathi, G. Particle Swarm Optimization Based Retinal Image Enhancement. *Wireless Pers Commun* (2021).
- [23] Alwazzan, M.J., Ismael, M.A. & Ahmed, A.N. A Hybrid Algorithm to Enhance Colour Retinal Fundus Images Using a Wiener Filter and CLAHE. *J Digit Imaging* (2021).
- [24] Bataineh, B., Almotairi, K.H. Enhancement Method for Color Retinal Fundus Images Based on Structural Details and Illumination Improvements. *Arab J Sci Eng* (2021).
- [25] Carrillo, L. Bautista, J. Villamizar, J. Rueda, M. Sanchez and D. Rueda, "Glaucoma Detection Using Fundus Images of The Eye," 2019 XXII Symposium on Image, Signal Processing and Artificial Vision (STSIVA), Bucaramanga, Colombia, 2019, pp. 1-4,
- [26] A. Raj, A. K. Tiwari and M. G. Martini, "Fundus image quality assessment: survey, challenges, and future scope," in *IET Image Processing*, vol. 13, no. 8, pp. 1211-1224, 20 6 2019, doi: 10.1049/iet-ipr.2018.6212.
- [27] Mittal, K., Rajam, V.M.A. Computerized retinal image analysis - a survey. *Multimed Tools Appl* 79, 22389–22421 (2020).
- [28] Juneja, M., Thakur, S., Wani, A. et al. DC-Gnet for detection of Glaucoma in retinal fundus imaging. *Machine Vision and Applications* 31, 34 (2020).
- [29] Gómez-Valverde JJ, Antón A, Fatti G, Liefers B, Herranz A, Santos A, Sánchez CI, Ledesma-Carbayo MJ. Automatic glaucoma classification using color fundus images based on convolutional neural networks and transfer learning. *Biomedical optics express.* 2019 Feb 1;10(2):892-913.

A Delay-tolerant MAC Protocol for Emergency Care in WBAN Considering Preemptive and Non-preemptive Methods

Shah Murtaza Rashid Al Masud, Alope Kumar Saha

Department of Computer Science and Engineering
University of Asia Pacific, Dhaka, Bangladesh

Abstract—For facilitating pilgrims with no delay, quick and real-time emergency medical services at ritual sites a delay-tolerant Medium Access Control (MAC) protocol for the IEEE 802.15.6 standard based Wireless Body Area Networks (WBANs) has been proposed. Since MAC protocol is application-specific hence any particular MAC technique may not be appropriate for diverse applications. In this research work, we consider dealing with medical emergency traffics which is random, independent of each other and can be generated at any time. Moreover, emergency traffics must be transmitted ahead of normal medical data or emergency traffic with a lower severity level; because any delay in emergency data transmission may endanger patients' life. The proposed MAC protocol is compared with both preemptive and non-preemptive methods. Where, a modified MAC superframe (SF) structure, minimum backoff period and minimum Contention Window (CW_{min}) for quick data access to the IEEE 802.15.6 standard based EAP channel are also considered. The proposed delay-tolerant MAC protocol has been experimented with and simulated by the Castalia simulator which is based on the OMNeT++ platform. The experimental results show that data transmission using the preemptive method works faster with reduced delay than that of the non-preemptive method. Furthermore, the delay metric of the proposed delay-tolerant MAC protocol is analyzed, calculated and compared with the current Traffic-aware TA-MAC protocol. Results demonstrate that delay is relatively low during emergency data transmission using the proposed MAC in WBANs environment.

Keywords—WBAN; MAC; preemptive; non-preemptive; delay; emergency traffic

I. INTRODUCTION

Due to the huge medical concerns of pilgrimage at overcrowded Hajj ritual sites in Makkah and Madinah and Kumbh Mela in India, World Health Organization (WHO), Ministry of Health (MoH) of Saudi Government, and Government of India at different times provided with medical awareness guidelines for the pilgrims. During pilgrimage it is utmost important to identify pilgrims with serious medical issues and to provide them with adequate healthcare services [1-2]. In addition, a very few pilgrims' monitoring and healthcare technologies have been evolved including GPS, RFID, and WSN based ITS [3-7]. However, existing healthcare facilities are rarely able to observe urgent medical issues in an immediate and speedy way. Therefore, there is a vital need of emergent healthcare technology to abridge pilgrims' emergency medical problems.

According to the study [8-9], WBANs is an embryonic technology consists of numerous body sensors and a body coordinator and can be a greater option for medical applications at different health conditions. WBAN can deal with diverse traffic types including emergency, on-demand and normal traffic. In healthcare applications patients' data must be transferred ahead of other non-medical and low critical medical data because any data lost or delay may endanger the life. Among the WBANs heterogeneous traffics, emergency traffic is very unpredictable in nature. Emergency traffic can be produced in both regular and random manner. Generally, emergency traffics need to transfer in Contention-Free Phase (CFP) and non-scheduled mode which is opposite to normal medical traffic that can be sent in scheduled phase and in Contention Access Phase (CAP). However, the problem may occur during transmission of multiple emergency data concurrently that may result in inefficient transmission of medical data with severe delay, data lost and re-transmission, collision and excessive energy consumption.

Since, WBAN is energy and delay sensitive, hence, one particular communication technology and Medium Access Control (MAC) protocol will hardly be suitable for every possible WBAN applications. The IEEE802.15.6 standard based MAC protocol is anticipated to handle heterogeneous traffics where Exclusive Access Phase I and II (EAP I and II) is designed for emergency data access, Random Access Phase I and II (RAP) for on-demand traffics, and Managed Access Phase I and II (MAP) for normal medical traffics. But, EAP I and EAP II of MAC superframe (SF) structure work based on Contention Access Phase (CAP). CAP leads data traffic to contend with each other if multiple data aggregate at coordinator needs to simultaneously access the channel, which is the main reason for data collision and data loss which result in higher delay and excessive power consumption. Hence, there is a need for deploying appropriate priority and queue model for designing MAC protocol that should ensure high priority data to be given higher priority during transmission. The existing MAC superframe may not be suitable for critical data management for medical applications considering both IEEE 802.15.6 and IEEE 802.15.4 standards [10]. According to their research, for handling medical emergencies, CFP is proposed. But, to the best of our knowledge, emergency physiological data can be generated and transmitted at any time; hence, time-bounded scheme and technology may not be suitable for medical emergency applications. Moreover, unlike

the IEEE802.15.6 standard, the IEEE802.15.4 standard does not support data classification and prioritization features. Therefore, the IEEE 802.15.4 MAC superframe is also not suitable to be used for monitoring pilgrims' emergencies and critical health issues during Hajj, Kumbh Mela or any overcrowded event.

To tackle medical emergencies using WBANs, in our research we proposed delay-tolerant MAC protocol. For deploying delay efficient MAC for WBAN we primarily considered both preemptive and non-preemptive methods to effectively transmit pilgrims' data to the healthcare station. In non-preemptive method, packets that are in undergoing services are allowed to finish services first without disturbance even in the meantime if packets with higher priority arrive. Besides, in the non-preemptive method, the packet with the highest priority enters service first only when the server becomes idle or free. Thus, the non-preemptive priority model is not able to deliver medical data with a higher priority before data with a lower priority level, which results in higher delay. Hence, for tackling medical emergency situation, we finally considered preemptive method for developing delay-tolerant MAC protocol, because in this scheme, data with higher priority must access the channel or SF timeslot ahead of lower priority medical data thus results in lower delay in emergency data transmission with higher severity.

To experiment, analyze and validate the obtained results, the proposed delay-tolerant MAC protocol has been simulated with Castalia simulator which is based on OMNeT++ simulator. The result is analyzed considering both preemptive and non-preemptive methods. Moreover, the delay metric of the proposed delay-tolerant MAC protocol is compared with up-to-date Traffic-aware MAC protocol (TA-MAC). Results exhibit that delay is comparatively very low during transmission of emergency data with different severity levels using preemptive method in WBANs environment due to less queuing delay, no data re-transmission and no collision.

The rest of the research paper is structured as follows: Section 2 presents the related work. Classification of traffics, proposed modified MAC superframe structure, algorithms and network management procedures are explained in Section 3. Results are discussed in Section 4. Finally, the paper ends with conclusion in Section 5.

II. RELATED WORK

This section explores the literature in order to discover the existing MAC methods and techniques and their limitations that are already being designed and deployed for WBANs healthcare applications considering different Quality of Service (QoS) issues. The delay tolerant MAC protocol must consider WBANs heterogeneous traffic. The QoS proficient MAC protocol must consider diverse system requirements and network development challenges. Major challenges and requirements include data classification and prioritization, energy consumption issues of sensor nodes, delay in transmission, data rate and timely delivery of medical data. In WBANs applications, any loss of physiological data and excessive delay in transmission may jeopardize patients' life.

Considering WBANs MAC requirements and other environmental issues some researchers have designed and proposed several priority and QoS efficient MAC protocols for WBAN. An energy efficient Adaptive (A-MAC) MAC protocol has been proposed in [11]. In this IEEE 802.15.6 based MAC protocol, data are classified into three priority classes and an improved MAC superframe has also been proposed. The existing superframe is restructured into four different periods or phase such as beacon phase, aperiodic contention access phase, periodically scheduled phase or contention-free phase, and an inactive phase. The slots lengths (time duration) for access phases are being adjusted according to the priority level of data, moreover, body sensors must compete for accessing channel according to the channel access mechanism.

A radio wake-up mechanism based MAC protocol for WBAN is proposed in [12]. Authors consider data classification and prioritization to achieve the goal, which is 'prolong the network lifetime'. The protocol is designed according to the IEEE802.15.4 standard, where the superframe is also modified and improved. To represent the limited capacity of the buffers, an asymmetric hidden Markov model is also illustrated. Another MAC protocol that has been proposed by the authors [10] where emergency traffics are being classified into diverse data severity levels based on the threshold values. In addition, authors have suggested for the modification of the MAC superframe based on different time slots for accessing communication channel. To access the different channel, data is further divided into high priority and low priority data. Though data delay and throughput are presented in the result, however, energy consumption issue is not defined. Moreover, no direction is provided to handle various emergency data.

The authors [13] proposed IEEE802.15.4 based TA-MAC protocol of diverse phases of CAP and different levels of traffic priority. In the CAP, traffic-aware MAC utilizes the priority-based CSMA/CA procedure that is supported by the IEEE802.15.6 standard to satisfy WBANs standard; however, the protocol is restricted to IEEE802.15.4 standard. In [14], the IEEE 802.15.6 Traffic Priority based Channel Assignment Technique (TP-CAT) has been projected. Authors have recommended adaptive time slot management algorithms based on data threshold values for QoS efficient TP-CAT.

A novel Energy Efficient and Load Balanced Priority Queue Algorithm (ELBPQA) has been proposed [15], where, traffic criticality is defined by data priority levels such as low-medium-high priority data, and thus data are scheduled and transmitted. Data priority and modified superframe are proposed for the IEEE802.15.4 standard, and besides, CSMA/CA mechanism is used to tackle data with different priorities of energy-efficient MAC protocol [16]. A Markov model has also been proposed in order to identify the state of WBANs sensor nodes.

Authors [17] have proposed Traffic Adaptive Priority (TAP-MAC) MAC protocol with a revised MAC superframe structure. The goal of TAP-MAC is to reduce collisions and data re-transmission that results in lower delay and minimal energy consumption. Naturally, during CAP, low-priority

traffic cannot dominant over high-priority traffic thus results in lower throughput, higher delay and high energy consumption in WBAN [17]. The existing standard for data communication does not offer a differentiated QoS to the diverse traffic therefore, a Priority-based Adaptive (PA) MAC protocol for WBAN was proposed in [18]. In PA-MAC, data is classified into four different types. In this protocol, according to data priority level, MAC superframe timeslots are being dynamically allocated. The proposed protocol works based on well-designed IEEE 802.15.4 and IEEE 802.15.6 standards. The PA-MAC protocol cares more on traffics with higher priority than that of lower priority which affects the overall network quality.

The above mentioned MAC protocols have been proposed and designed on the basis of the IEEE 802.15.4 and the IEEE 802.15.6 standards. In WBANs communication, generally, higher-priority traffic is generally the lowermost loaded traffic and lower-priority traffic is typically the highermost loaded traffic, hence MAC protocols need to accept either one or both of the aforementioned concepts in order to ignore the harmful situation during data transmission considering diverse QoS including delay and energy consumption issues. In addition, there is an essential requisite to deliver and provide services with utmost importance to manage emergency medical packets and its severity levels. Hence, there is an utmost necessity to design and develop MAC protocol for WBAN that should deal with various QoS related issues along with the traffic-severity and priority of WBAN applications for real-time and quick monitoring of patients at overcrowded environment.

III. DELAY-TOLERANT MAC PROTOCOL FOR WBAN

A. Data Classification and Determination of Severity Levels

For WBANs coordinator it is less challenging to tackle one or a few emergency event than multiple emergency events simultaneously. To build a delay-tolerant MAC protocol for WBAN application, we classify the emergency traffic into six different categories based on the level of severity, which is presented in Table I. Data severity or criticality is basically meant by a level of medical urgency or emergency. Here in this research, we classified, ordered, organized, prioritized WBAN emergency traffic based on their QoS requisites for MAC which is necessitated for a novel solution in WBAN applications.

Emergency data is event triggered and relies on life-threatening situation to be generated. Hence, emergency data requires smooth and quick transmission in WBAN medium in an efficient way.

TABLE I. SEVERITY LEVEL OF DISEASES

Medical Syndromes/Diseases	Level of Severity
Respiratory Syndromes	Extremely severe traffic
Cardiovascular Problems	Very high severe traffic
Diabetes Mellitus	High severe traffic
Blood Pressure (BP)	Moderately severe traffic
Gastroenteritis	Low severe traffic
Body Temperature (BT)	Very low severe traffic

B. Modified MAC Superframe for Emergency Data Transmission

Based on the nature of WBAN operations and applications, the IEEE 802.15.6 and IEEE 802.15.4 based MAC superframe can be re-structured in to different time frame [8], where, beacon period of the same length encircles the entire timeslot of the superframe. Using the IEEE 802.15.6 standard and its associated MAC protocols, WBANs are supposed to transmit data in three different modes to access channels enabling beacon mode and non-beacon mode. Beacon mode supports MAC with superframe structure; on the other hand, non-beacon mode supports MAC with superframe and without superframe structure to operate in WBAN environment. The superframe is divided into two phases, such as aperiodic CAP and periodic scheduled access phase. CAP is non-scheduled and aperiodic in nature; moreover, CAP is random and dynamic. In IEEE 802.15.6 based CAP supports EAP 1 and EAP 2. It also supports RAP 1 and RAP 2 and the CAP slot itself. However, MAP is scheduled based access phase which is supported by CFP. The slots of superframe have different periods or duration, and lengths are identified based on the number of timeslots. Hence the MAC superframe structure can be improved and restructured by neutralizing definite time periods. In our research, we modify and update the existing MAC superframe in order to avoid data collision during simultaneous transmission of emergency medical data. The proposed MAC superframe structure is presented in Fig. 1.

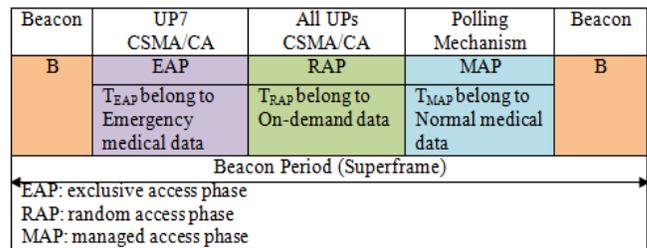


Fig. 1. Proposed MAC Superframe (SF) for WBAN.

Fig. 1 illustrated the proposed superframe for the delay-tolerant MAC protocol which is based on the synchronous mode of IEEE 802.15.6 standard. In our research, we combine EAP1 and EAP2 into EAP for emergency data transmission. In IEEE806.15.6 standard, user priority UP₇ defines the priority of the highest level over medical data of different classes including emergency and non-emergency medical data. Besides, in our proposed MAC mechanism, a combined version of Random Access Phase-RAP1 and RAP2 which is named as RAP is proposed for on-demand medical data. In addition, a combined version of Managed Access Phase-MAP1 and MAP2 which is named as MAP is suggested for normal medical or non-medical traffic. Normal medical or non-medical data is scheduled based whereas; emergency data requires random access in WBANs transmission medium.

In our research, we propose CSMA/CA mechanism for Extensive Access Phase-EAP along with preemptive method over non-preemptive method for contention-free data transmission. EAP is a combination of two contention access phases such as EAP 1, and EAP 2 has been proposed to deploy only for high priority traffic (emergency packets). On the

contrary, the RAP phase which is the addition of two random access phases RAP 1 and RAP 2 is proposed for on-demand traffic having the average user priority and MAP phase is assigned to the normal medical or non-medical traffics for the traffics with low user priority.

In this research, we deploy six different sensors for measuring different physiological parameters of patients. Physiological parameters are then classified based on data classification concepts of IEEE802.15.6 standard. The emergency data has the highest priority followed by medium priority for on-demand data and the lowest priority for normal medical data. For prioritizing the emergency data we define and classify the medical physiological data on the basis of severity level. According to our study [19-20], data severity level is defined based on the patients' symptoms, mortality rate and hospital admission at overcrowded ritual sites. Emergency data are non-periodic and random in nature and can be generated at any time. Besides, normal medical or non-medical data can be observed periodically. Moreover, using the data threshold values the emergency data and normal medical data can be differentiated easily. Therefore, the priority-severity index value of WBAN traffic is formulated by combining the highest user priority (P_7 : emergency data) and the index of different data severity level (S_1-S_6). The priority-severity level is defined using the formula $i = P_7S_i$ where $i=1-6$, that ranges from $P_7S_1-P_7S_6$ with WBANs user priority UP_7 followed by UP_6 for on-demand traffic (P_6 : on-demand traffic) and UP_5 for normal traffic (P_5 : normal traffic).

In WBAN communication, body sensors are supposed to sense or generate data, process data according to the methods applied and transmit data to body coordinator (Hub). In contrary, WBAN Hub or body coordinator collects data from sensors; processes and sorts data according to the methods and techniques applied; and then transmit data using appropriate transmission channel of MAC superframe (SF) structure for further processing. Table II presents the projected severity and priority index values.

TABLE II. SEVERITY-PRIORITY INDEX VALUE

WBAN UP as of IEEE 806.15.6	Severity Level of Emergency Traffic	Criticality-Priority Index Table	Types of Access Phases
$UP_7 = P_7$, indicates Emergency Medical Condition	$S_i = \{1,2,3,4,5,6\}$	Various Emergency Data Types: $P_7S_i = \{P_7S_1, P_7S_2, P_7S_3, P_7S_4, P_7S_5, P_7S_6\}$	Exclusive Access Phase EAP that combines EAP1 and EAP2
$UP_6 = P_6$, indicates High Priority Medical Data	$P_6S_i = 0$		Random Access Phase RAP that combines RAP1 and RAP2
$UP_5 = P_5$, indicates Medical Data	$P_5S_i = 0$		Managed Access Phase MAP that combines MAP1 and MAP2

C. The Roles of Sensor Nodes and Body Coordinator

In our proposed delay-tolerant MAC protocol, body coordinator allocates data transmission slot based on user priority levels which rely on different data types, criticality level of emergency data, and priority-severity index value as discussed earlier. Priority levels of different data values are generated by the nodes, except the on-demand data defined by the coordinator. Moreover, criticality levels of emergency data and non-critical normal medical data are specified by the coordinator. The coordinator also determines the priority-criticality index table, and then slots are assigned accordingly for transmitting data to the healthcare stations. In the proposed delay-tolerant MAC protocol we consider M/M/1 technique with both preemptive and non-preemptive methods where, traffics arrivals are determined by Poisson process. In this research, we also consider diverse user priority (UP_7-UP_5) and dissimilar severity level of medical emergency data.

In general, a body coordinator receives data, processes it and then transmits the data for further processing on the basis of the priority-severity level. In WBANs operations, multiple emergency events may occur at any moment of time; thus, specifying the roles of each node which is either sensor or hub is urgent to schedule according to the level of criticality and priority. At body coordinator level, an emergency traffic is classified based on data received from the sensors according to the priority severity index values. Hence, upon receiving the packets from physiological sensors, the hub is to use its severity index values to classify the emergency data and express the following resolutions or determinations:

1) If any emergency data exceeds the threshold value as compared to the severity-priority index values, then the status of that precise data will be defined as severe or critical.

2) Moreover, if any data derived from the sensor node (let's consider as on-demand traffic) categorised as on-demand traffic and no corresponding data or type is found in the severity-priority index values, then the health status will be designated as non-critical but an emergency. Also, since the related traffic is designated as an emergency, the coordinator, if required, may include a replica of the data related to the new findings to its severity-priority index table for improvement of the severity index before transmitting it.

3) Finally, if data traffic comes from the sensor or source node, which is categorised as normal, then the pilgrims' health status will be nominated normal medical.

The following Fig. 2 presents the functions of WBAN hub to determine heterogeneous physiological data, data classification, and delay-tolerant channel access mechanism. Moreover, we explain the severity level of data as presented in Fig. 3.

1) The traffic is called as extremely severe traffic, if the severity-priority index value $P_7S_i = P_7S_1$ (the highest severity level of emergency data).

2) The traffic is very high severe traffic, if the severity-priority index value $P_7S_i = P_7S_2$.

- 3) The traffic is high severe traffic, if the severity-priority index value $P_7S_i=P_7S_3$.
- 4) The traffic moderate severe traffic, if the severity-priority index value $P_7S_i=P_7S_4$.
- 5) The traffic is low severe traffic, if the severity-priority index value $P_7S_i=P_7S_5$.
- 6) The traffic is very low severe traffic, if the severity-priority index value $P_7S_i=P_7S_6$.

D. Relevant Algorithms and Slot Allocation in Modified MAC Superframe Structure

A slot allocation mechanism for MAC superframe has been proposed by the type of data according to threshold values from body sensor nodes and order of criticality level of both emergency and non-emergency data traffic from body coordinator node at different pilgrims' health conditions. For this, emergency traffic is categorised into six types based on the criticality level of vital signs as discussed earlier.

Pseudo code: Heterogeneous physiological data determination, classification and delay-tolerant channel access mechanism

Input: Threshold parameter of sensed physiological data

Sensing Element: Various sensors

Output: Classification of medical data, access to communication channel

Begin

//Patients' medical data received by Sensors and coordinate to Hub for further processing

1. **if** data exceeds (> or <) threshold limit **then**
data is classified as emergency medical data;
Set the priority level UP7;
Define the delay-tolerant preemptive or non preemptive methods for lower delay communication;
EAP of SF is selected to transfer data and access the channel using CSMA/CA mechanism;
 2. **elseif** data exceeds (> or <) or within (<>)threshold limit **then** data is classified as on-demand medical data;
Set the priority level UP6;
Data to be transmitted as requested by healthcare station;
RAP of SF is selected to transfer data and access the channel using CSMA/CA mechanism;
 3. **elseif** data within (<>) threshold value **then**
data is classified as normal medical data;
Set the priority level UP5;
Data is transmitted using scheduled access mechanism;
MAP of SF is selected to transfer data
 4. **else**
Repeat step 1
 5. **end if**
- End**

Fig. 2. Identification of Heterogeneous Traffic.

Pseudo code: Determine the severity level of emergency medical data at WBSN Hub

Input:

T: Traffic or patients' physiological data

P_1C_i : Severity-priority index value

Output:

Emergencies events classification based on data severity level

Begin

// for every arrive data from the sensor node

1. **if** (data type == emergency)&&(P₇S_i == P₇S₁) **then**
T nominates as extremely severe traffic
 2. **elseif** (data type == emergency)&&(P₇S_i == P₇S₂) **then**
T nominates as very high severe traffic
 3. **elseif** (data type == emergency)&&(P₇S_i == P₇S₃) **then**
T nominates as high severe traffic
 4. **elseif** (data type == emergency)&&(P₇S_i == P₇S₄) **then**
T nominates as moderately severe traffic
 5. **elseif** (data type == emergency)&&(P₇S_i == P₇S₅) **then**
T nominates as low severe traffic
 6. **elseif** (data type == emergency)&&(P₇S_i == P₇S₆) **then**
T nominates as very low severe traffic
 7. **else**
- if** (data type == on-demand)&&(P₇S_i == 0) **then**
T nominates as on-demand
14. **end if**
 15. **else**
 16. **if** (data type == no event or normal)&&(P₇S_i == 0) **then**
T nominates as normal traffic
 17. **end if**
 18. **end if**
 19. **end**

Fig. 3. Body Coordinator's Role to Deal with Emergency Traffic

If the coordinator at any moment of time receives emergency data from a sensor, then it assigns EAP slot to this particular traffic based on the CSMA/CA mechanism. Here there is no need for finding the criticality level of that emergency traffic because it has been received from the single sensor node.

When two or more than two emergency traffics are received by the coordinator at a time, it invokes the severity-priority index value as illustrated earlier in Table II. Upon classification phase, depending on the traffic types, data are to be distributed among the queues. All emergency data shall proceed to slot EAP based on their criticality level and queuing process. Traffic queuing process at the data transmission scheme of the MAC level is illustrated in Fig. 4. Emergency traffic is life-threatening, so excessive delay and data loss can worsen the health condition or life of the pilgrims. Hence it is vital to ensure no data loss and minimal delay in emergency traffic.

In our research, we assume, on-demand and normal traffic are not life-threatening. RAP phase is allocated for on-demand traffics which are contention-based, since this traffic is considered as not life-threatening so low to moderate contention for the slots are acceptable when there is multiple such traffics. For normal traffic, a scheduled access phase MAP is assigned so that data traffic can access the channel at a specific period. Again, since this traffic is assumed as not life-threatening so low to moderate contention and delay for the slots are acceptable when there is multiple such traffics. The queuing process for emergency data transmission is presented in Fig. 4.

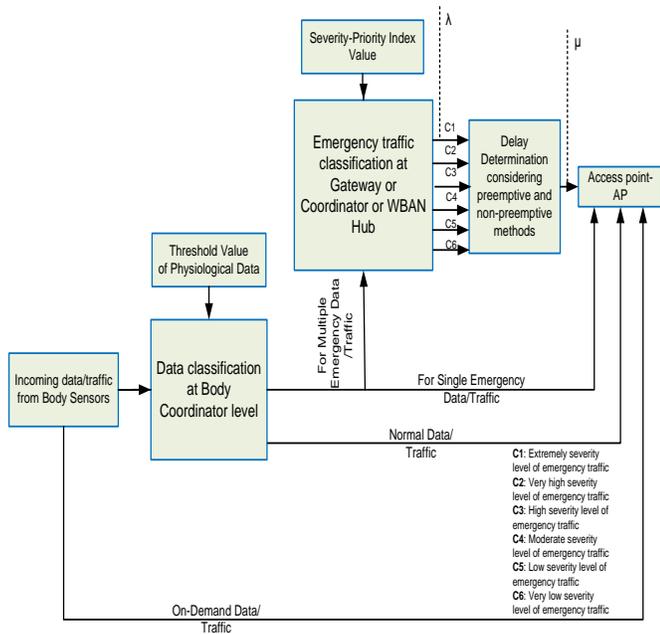


Fig. 4. Queuing Process of Emergency Data Transmission through MAC Protocol.

Preemptive method is time-critical and applicable for emergency traffic which is random in nature. In addition, preemptive method allows data with the highest precedence access the communication channel ahead of data with lower precedence. The preemption technique is illustrated in Fig. 5.

Non-preemptive method is non-time-critical and applicable for normal medical traffic and even can be utilized for the emergency traffic with different severity levels in WBAN communication. Normal medical traffic can be of time bounded or scheduled in nature. The non-preemption technique is illustrated in Fig. 6.

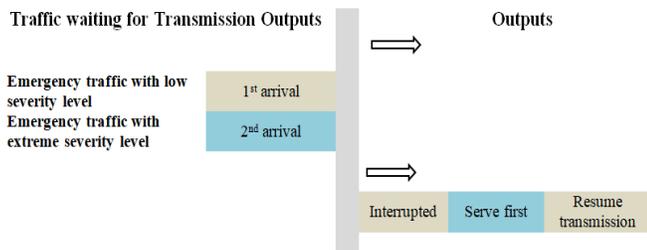


Fig. 5. Schematic Diagram of Preemption.

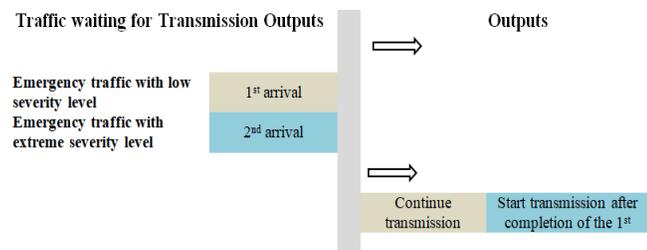


Fig. 6. Schematic Diagram of non-preemption.

For the proposed delay-tolerant MAC protocol we deploy CSMA/CA mechanism for handling emergency traffic of WBAN. Since the proposed MAC is supposed to transmit emergency traffic with different severity levels hence, the length of backoff counter (BC) should be set to minimal and data transmission is occurred when BC=0 which is presented in Fig 7. In addition, the length of Contention Window (CW) of MAC superframe (SF) is varied according to the type of applications. In our research, CW is fixed to minimum as CW=CW_{min} for emergency data transmission, however, for non-emergency cases the CW is set to CW_{max}.

E. Mathematical Analysis of the Proposed Delay-tolerant MAC Protocol Considering Preemptive Method

In our research, the queuing delay is measured using the deployment of various queue methods as explained earlier in this research paper. The queue model has been proposed in our research demonstrates service time as queuing delay that is being served in the system. The delay is calculated as follows, where; λ is data or traffic arrival rate, μ is the service rate of traffic, traffic intensity rate is denoted by ρ , according to our research, $E(n)$ is the average number of critical data in the queue, $E(t)$ is average or mean delay time for any kind of traffic or data.

$$\text{Extremely severe traffic: } E(t_{p7s1}) = \frac{\frac{1}{\mu}}{1-\rho_{p7s1}} \tag{1}$$

$$\text{Very high severe traffic: } E(t_{p7s2}) = \frac{E(n_{p7s2})}{\lambda p7s2} = \frac{\frac{1}{\mu}}{(1-\rho_{p7s1})(1-\rho_{p7s1}-\rho_{p7s2})} \tag{2}$$

$$\text{High severe traffic: } E(t_{p7s3}) = \frac{E(n_{p7s3})}{\lambda p7s3} = \frac{\frac{1}{\mu}}{(1-\rho_{p7s1}-\rho_{p7s2})(1-\rho_{p7s1}-\rho_{p7s2}-\rho_{p7s3})} \tag{3}$$

$$\text{Moderately severe traffic: } E(t_{p7s4}) = \frac{E(n_{p7s4})}{\lambda p7s4} = \frac{\frac{1}{\mu}}{(1-\rho_{p7s1}-\rho_{p7s2}-\rho_{p7s3})(1-\rho_{p7s1}-\rho_{p7s2}-\rho_{p7s3}-\rho_{p7s4})} \tag{4}$$

$$\text{Low severe traffic: } E(t_{p7s5}) = \frac{E(n_{p7s5})}{\lambda p7s5} = \frac{\frac{1}{\mu}}{(1-\rho_{p7s1}-\rho_{p7s2}-\rho_{p7s3}-\rho_{p7s4})(1-\rho_{p7s1}-\rho_{p7s2}-\rho_{p7s3}-\rho_{p7s4}-\rho_{p7s5})} \tag{5}$$

$$\text{Very low severe traffic: } E(t_{p7s6}) = \frac{E(n_{p7s6})}{\lambda p7s6} = \frac{\frac{1}{\mu}}{(1-\rho_{p7s1}-\rho_{p7s2}-\rho_{p7s3}-\rho_{p7s4}-\rho_{p7s5})(1-\rho_{p7s1}-\rho_{p7s2}-\rho_{p7s3}-\rho_{p7s4}-\rho_{p7s5})} \tag{6}$$

And applying Little's law of Queuing theory we get,

$$E(t_{p7si}) = \frac{E(n_{p7si})}{\lambda p7si} = \frac{\frac{1}{\mu}}{(1-\sum_{i=1}^{n-1} \rho_{p7s_i})(1-\sum_{i=1}^n \rho_{p7s_i})} \tag{7}$$

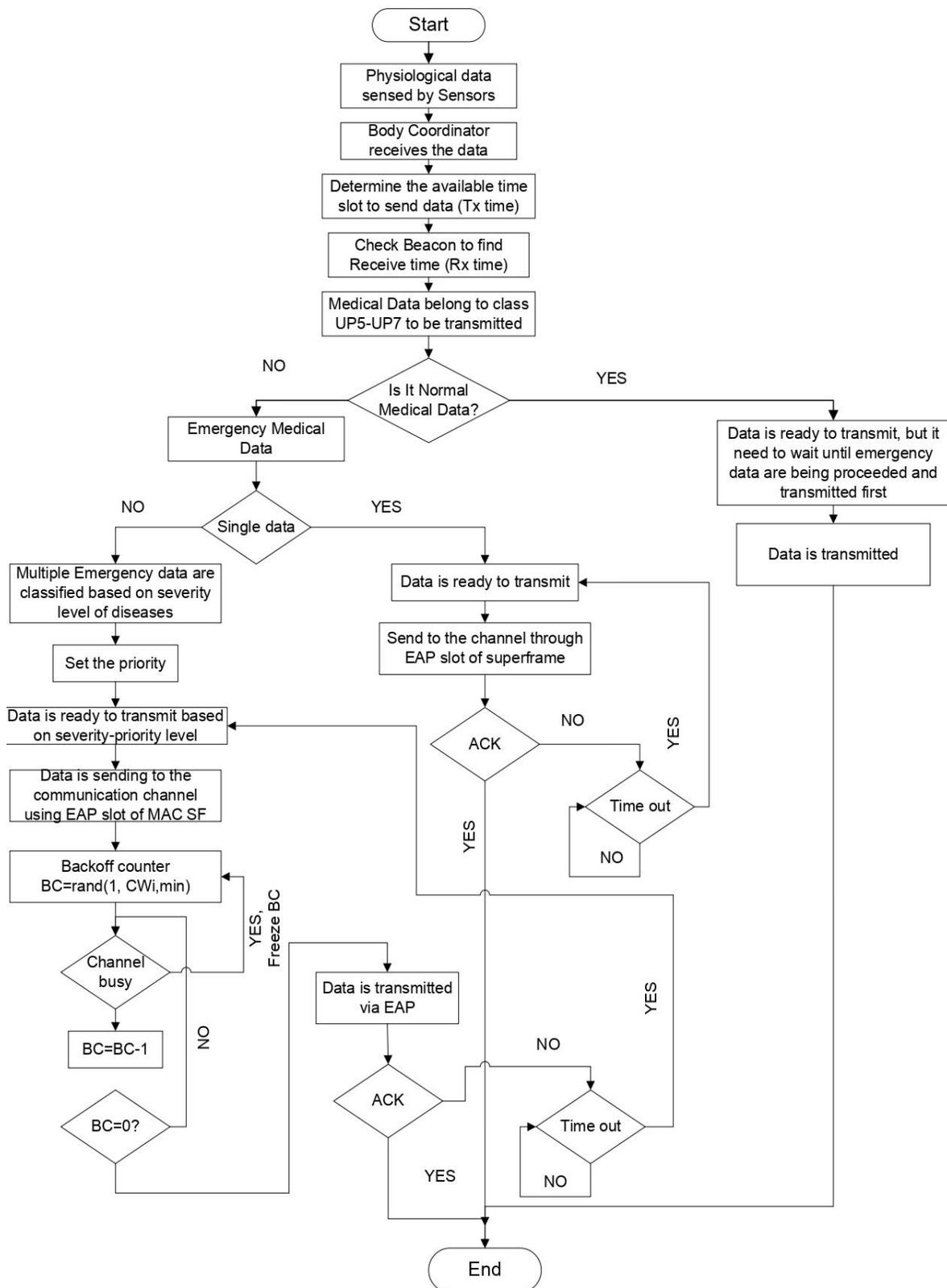


Fig. 7. CSMA/CA Mechanism and Relevant Operational Flowchart of the Proposed Delay-tolerant MAC Protocol.

F. Mathematical Analysis of the Proposed Delay-tolerant MAC Protocol Considering Non-Preemptive Method

In fact, by introducing Little's law in our research work and the property of PASTA (Poisson Arrivals See Time Averages), $E(n_{p1c1})$ and $E(t_{p1c1})$ can be defined directly without expressing the probabilities P_n . According to PASTA, in the system, an average number of customers seen by an arriving customer equals $E(n_{p7s1})$ and each of the customers has a service time (residual) with mean $\frac{1}{\mu}$. Additionally, patient must wait for its own service time. Hence, the average or mean time for extremely severe data can be formulated as, where the queue delay is determined considering the packets in service plus the packets that are already buffered in the queue.

$$E(t_{p7s1}) = \frac{E(n_{p7s1})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho_{p7s2} + \rho_{p7s3} + \rho_{p7s4} + \rho_{p7s5} + \rho_{p7s6}) \quad (8)$$

$$E(t_{p7s1}) = \frac{E(n_{p7s1})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho - \rho_{p7s1}) \quad (9)$$

Very high severe data processing: The very high severe data packet has to wait for the extremely severe data in service and very high severe data or packets in the queue. The delay can be found using the following formula:

$$E(t_{p7s2}) = \frac{E(n_{p7s1})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho_{p7s3} + \rho_{p7s4} + \rho_{p7s5} + \rho_{p7s6}) \quad (10)$$

$$E(t_{p7s2}) = \frac{E(n_{p7s1})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho - \rho_{p7s1} - \rho_{p7s2}) \quad (11)$$

High severe data processing: The high severe packet has to wait for the extremely severe packet and very high severe packets in service and high severe data or packets in the queue. The delay can be found using the following formula:

$$E(t_{p7s3}) = \frac{E(n_{p7s1})}{\mu} + \frac{E(n_{p7s2})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho_{p7s4} + \rho_{p7s5} + \rho_{p7s6}) \quad (12)$$

$$E(tp7s3) = \frac{E(n_{p7s1})}{\mu} + \frac{E(n_{p7s2})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho - \rho_{p7s1} - \rho_{p7s2} - \rho_{p7s3}) \quad (13)$$

Moderately severe data processing: The moderate severe data has to wait for the extremely severe packet, very high severe packet and high severe packet in service and moderate severe data or packets in the queue. The delay can be found using the following formula:

$$E(t_{p7s4}) = \frac{E(n_{p7s1})}{\mu} + \frac{E(n_{p7s2})}{\mu} + \frac{E(n_{p7s3})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho_{p7s5} + \rho_{p7s6}) \quad (14)$$

$$E(t_{p7s4}) = \frac{E(n_{p7s1})}{\mu} + \frac{E(n_{p7s2})}{\mu} + \frac{E(n_{p7s3})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho - \rho_{p1c1} - \rho_{p1c2} - \rho_{p1c3} - \rho_{p1c4}) \quad (15)$$

Low severe data processing: The low severe data has to wait for the extremely severe packet, very high severe packet, high severe packet and moderate severe data in service and low severe data or packets in the queue. The delay can be found using the following formula:

$$E(tp7s5) = \frac{E(n_{p7s1})}{\mu} + \frac{E(n_{p7s2})}{\mu} + \frac{E(n_{p7s3})}{\mu} + \frac{E(n_{p7s4})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho - \rho_{p7s1} - \rho_{p7s2} - \rho_{p7s4} - \rho_{p7s5}) \quad (16)$$

$$E(tp7s5) = \frac{E(n_{p7s1})}{\mu} + \frac{E(n_{p7s2})}{\mu} + \frac{E(n_{p7s3})}{\mu} + \frac{E(n_{p7s4})}{\mu} + \frac{1}{\mu}(\rho_{p7s6}) \quad (17)$$

Very low severe data processing: The low severe data has to wait for the extremely severe packet, very high severe packet, high severe packet, moderate severe data and low severe data in service and very low severe data or packets in the queue. The delay can be found using the following formula:

$$E(tp7s6) = \frac{E(n_{p7s1})}{\mu} + \frac{E(n_{p7s2})}{\mu} + \frac{E(n_{p7s3})}{\mu} + \frac{E(n_{p7s4})}{\mu} + \frac{E(n_{p7s5})}{\mu} + \frac{1}{\mu} + \frac{1}{\mu}(\rho - \rho_{p7s1} - \rho_{p7s2} - \rho_{p7s4} - \rho_{p7s5} - \rho_{p7s6}) \quad (18)$$

$$E(tp7s6) = \frac{E(n_{p7s1})}{\mu} + \frac{E(n_{p7s2})}{\mu} + \frac{E(n_{p7s3})}{\mu} + \frac{E(n_{p7s4})}{\mu} + \frac{E(n_{p7s5})}{\mu} + \frac{1}{\mu} \quad (19)$$

IV. RESULT AND DISCUSSION

A. Simulation Environment

The proposed delay-tolerant MAC protocol has been experimented and simulated using Castalia simulator which is based on OMNeT++ platform. Castalia is built for network of low-power embedded devices.

B. Simulation Parameters

To evaluate the competency of delay-tolerant MAC protocol, different scenarios are being considered including network size (number of nodes) and diverse traffic size. Varied network size has been considered ranging from 1 to 6 sensor nodes. In addition, different traffic sizes have been taken ranging from 16 bytes to 127 bytes. WBAN operating range is considered ranging from 5 to 10 meters with operational frequency of 2.4 GHz and channel bandwidth is 250 kbps. Simulation parameters are depicted in subsequent Table III.

TABLE III. MAC SIMULATION PARAMETERS

Parameters	Values
Total Nodes	6
Body Coordinator	1
Data Transmission Range	3m to 5m
mMaxBANSize	< 64 Nodes
MAC and Superframe Structure	IEEE 802.15.6 Standard
Channel Mode	Wireless
MAC Superframe Size	Total 255 Slots
MAC Superframe Duration	122.88 ms
Simulation Runtime	150 Seconds
Operating Frequency	2.4 GHz ISM
Bandwidth	Up to 250 kbps
Packet Size	Variable, up to 512 bytes
macMaxCSMABackoffs	*So far there is no specific unit
Beacon size	40 bytes

C. Performance Evaluation and Results Discussion

In order to performance evaluation of the proposed delay-tolerant MAC protocol, different scenarios are considered including network size (number of sensor nodes) and diverse traffic size. In our proposed MAC model we assume WBAN with a star topology. We also set EAP1, EAP2, RAP1, RAP2 and CAP to zero for the proposed MAC superframe (SF) structure and set to EAP, RAP and MAP for diverse traffics. The proposed delay-tolerant MAC protocol is compared considering both preemptive and non-preemptive methods for analyzing the performance. Moreover, the delay is compared with Traffic-aware MAC (TA-MAC) protocol for further validation of the proposed scheme.

D. First Scenario

The first scenario portrays the delay comparison considering both preemptive and non-preemptive methods considering varying nodes. For analysis delay we considered heterogeneous emergency traffic with different levels of severity. Fig. 8 presents the WBAN situation where the total number of nodes or network size increases from 1 to 6. From the obtained result it has been seen that the queue delay considering preemptive and non-preemptive methods for different emergency data increases with the increasing network size. In general, if the network size or number of nodes increased in the network then the delay is also increased proportionally almost in all the cases as depicted in Fig. 8. Moreover, the proposed MAC protocol performs better in term of delay by applying preemptive method in the network than that of non-preemptive method.

In non-preemptive method, the delay is increased for the transmission of emergency traffics because traffic with higher severity level has to wait until traffic with lower severity level complete its transmission which is already being served. However, the proposed delay-tolerant MAC works better with preemptive method because in this method emergency traffic with higher severity levels proceed ahead of normal medical data or emergency data with lower severity level. Form the experiment it is obtained that WBAN with single node and preemptive method takes 35.87 ms whereas the same network model with non-preemptive method takes almost 50 ms for data transmission using the modified MAC superframe and required EAP channel. Moreover, the delay is increased in all the cases if the nodes number is also increased using both queue methods. From our experiment it is found that WBAN with six nodes and preemptive method takes almost 58.50 ms whereas the same network model with non-preemptive method takes almost 72 ms for data transmission which is much higher than that of the preemptive method.

E. Second Scenario

The second scenario analyses the delay efficiency of proposed MAC by considering different severity levels of emergency traffic. The results are obtained on the basis of different traffic sizes which are fluctuating from 16 bytes to 127 bytes.

Fig. 9 shows the obtained delay by implementing preemptive method for our proposed MAC model for different

severity levels and the result differs with varied packets (medical) sizes up to 127 bytes. According to the results obtained as presented in Fig. 9, it is shown that for low sized packets (16 bytes) and for extremely severe traffic delay is calculated as 5.78 ms. In contrary, for low sized packets (16 bytes) but for very low severe traffic delay is calculated as 8 ms. It has been observed that the overall delay is increased in the network if the packets sizes up and for 127 bytes packets the delay is measure as 8.12 ms and 11.89 ms respectively for extremely severe traffic and very low severe traffic in WBAN communication.

On the other hand, Fig. 10 shows the obtained delay by implementing non-preemptive method for our proposed MAC model for different severity levels with varied packets sizes fluctuating from 16 bytes to 127 bytes. According to the results obtained as presented in Fig. 10, it is shown that for low sized packets (16 bytes) and for extremely severe traffic delay is calculated as 9.3 ms. In contrary, for low sized packets (16 bytes) but for very low severe traffic delay is calculated as 11.1 ms. It has been observed that the overall delay is increased in the network if the packets sizes up and for 127 bytes packets the delay is measure as 11.2 ms and 14.8 ms respectively for extremely severe traffic and very low severe traffic in WBAN communication.

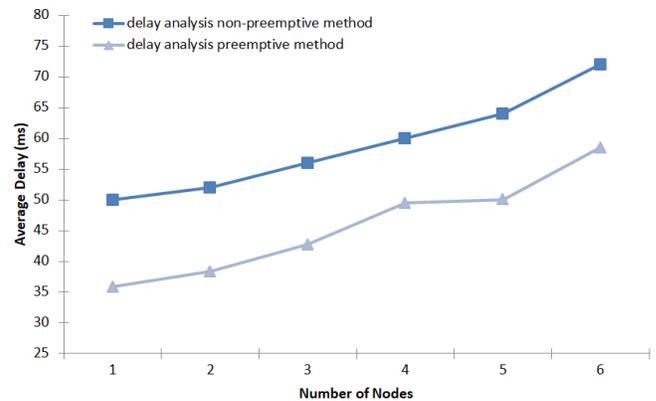


Fig. 8. Delay Comparison of Emergency Data Transmission Considering Preemptive and Non-preemptive Methods.

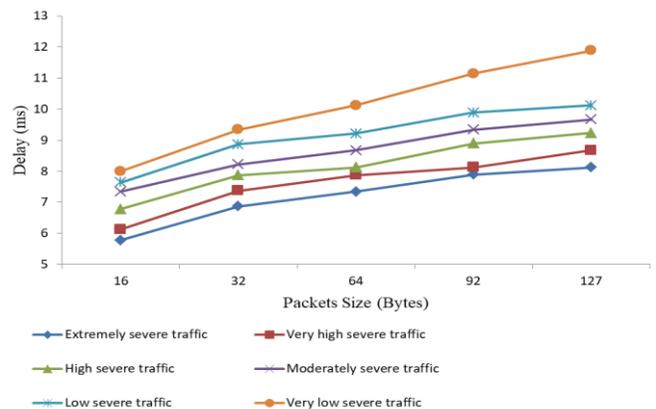


Fig. 9. Delay Assessment of Emergency Traffic Considering Preemptive Method.

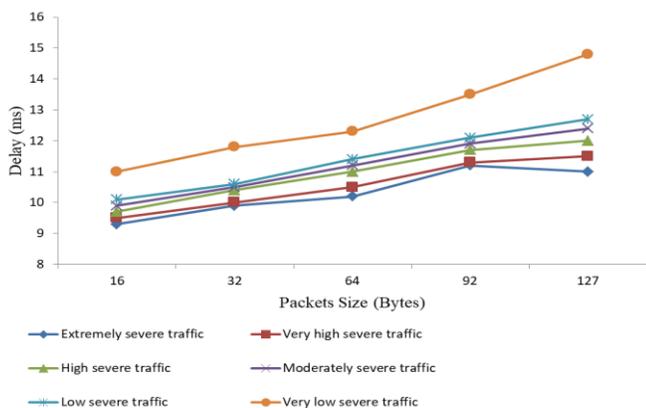


Fig. 10. Delay Assessment of Emergency Traffic Considering Non-Preemptive Method.

Moreover, our proposed delay-tolerant MAC protocol with both queue methods has been compared with up-to-date Traffic-aware (TA-MAC) protocol and it has been found that our proposed model with preemptive method performs much better than TA-MAC in terms of delay in data transmission in WBAN environment, whereas non-preemptive method based approach consumes more time for data transmission as presented in Fig. 11. According to the results obtained, it is shown that for low sized packets (16 bytes) and for extremely severe traffic delay is calculated as 5.78 ms. In contrast, for low sized packets (16 bytes) but for very low severe traffic delay is calculated as 8 ms using the preemptive method. However, TA-MAC requires 6.3 ms for extremely severe traffic and 9.11 ms for very low severe traffic transmission in WBAN.

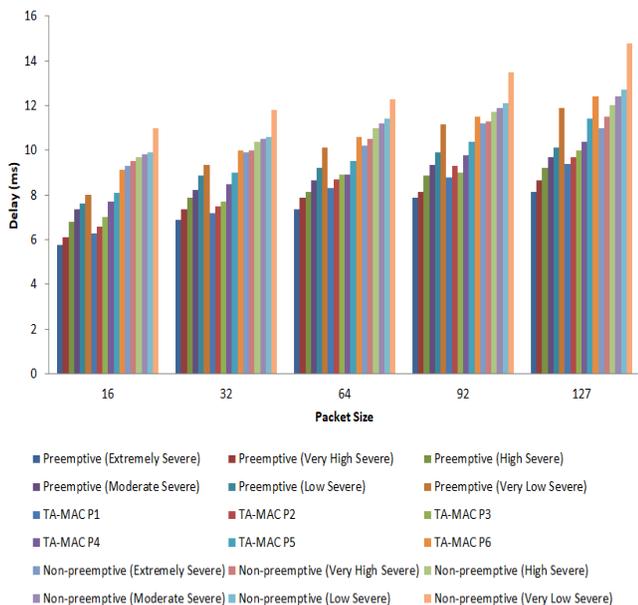


Fig. 11. Delay (ms) is Analysed on the basis of Data Severity Level Considering Various Packet Size.

F. Third Scenario

The third scenario portrays the delay comparison between the proposed delay-tolerant MAC protocol and TA-MAC protocol. For analysis delay we considered heterogeneous emergency traffic with different levels of severity. Fig. 12 presents the WBAN situation where the network size increases from 1 to 6 nodes. Considering 6 as a maximum number of nodes, the queue delay of the delay-tolerant MAC protocol is lower than that of the competitive TA-MAC protocol.

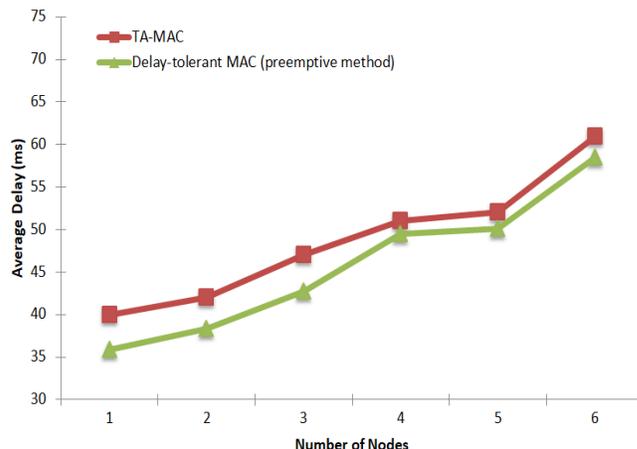


Fig. 12. Delay (ms) Comparison between Proposed MAC and TA-MAC.

V. CONCLUSION

In order to facilitate patients' with real-time and quick healthcare services at crowded sites we propose WBANs delay-tolerant MAC protocol. We designed the MAC protocol on the basis of M/M/1 preemptive method for dealing with emergency data. However, to analyze the delay efficiency we compare the proposed MAC with both preemptive and non-preemptive methods. In addition, to design the delay-tolerant MAC for monitoring pilgrims' emergency conditions we categorized emergencies based on level of severity. We proposed an improved MAC superframe structure and algorithms are also developed for better management of sensor nodes and body coordinator at WBANs MAC level. Moreover, minimum backoff period and minimum Contention Window (CM_{min}) are considered for quick access to the IEEE 802.15.6 standard based EAP channel. The proposed delay-tolerant MAC protocol has been experimented via simulation and verified using Castalia simulator which is based on OMNeT++ platform. The proposed MAC scheme is designed to handle the emergency situation with different severity levels and during the experiment it has been shown that data transmission using the preemptive method works faster with reduced delay than that of the non-preemptive method. Furthermore, the proposed delay-tolerant MAC protocol is analyzed and compared with up-to-date TA-MAC protocol considering its delay matrix. Results demonstrate that delay is relatively low during emergency data transmission in WBANs environment. Our future research plan is to extend the existing work using other queue models including M/G/1 and relevant techniques considering WBANs heterogeneous traffics.

ACKNOWLEDGMENT

We would like to convey our sincerest appreciation to University of Asia Pacific, Dhaka, Bangladesh for providing us with admirable research environment.

REFERENCES

- [1] Aldossari M, et.al.; Health issues in the Hajj pilgrimage: a literature review. *East Mediterr Health J.* 2019;25(10):744–753.
- [2] Hajj guidelines by Ministry of Health (MoH), Kingdom of Saudi Arabia : <https://www.moh.gov.sa/Hajj/Documents/Languages/English.pdf>.
- [3] Osman, M, “Hajj guide systems – past, present and future”, *International Journal of Emerging Technology and Advanced Engineering*, vol.4, no. 8, pp. 25-31, 2014.
- [4] Aladdein Amro, “Pilgrims’ Hajj Tracking System.” *Contemporary Engineering Sciences*, Vol. 5, No. 9, pp. 437-446, 2012.
- [5] Mohandes, M, et.al., “Pilgrim tracking and identification using wireless sensor networks and GPS in a mobile phone”, *Arabian Journal for Science and Engineering*, vol. 38. No. 8, pp. 2135-2141, 2013.
- [6] Memish, Z., “Emergence of medicine for mass gatherings: lessons from the Hajj”, *The Lancet infectious diseases*, vol. 12, no. 1, pp. 56-65, 2012.
- [7] Hamhoum, F., “Supporting pilgrims in navigating densely crowded religious sites”, *Personal and Ubiquitous Computing*, vol. 16, no. 8, pp. 1013-1023, 2012.
- [8] IEEE. (2012). IEEE Standard for Local and Metropolitan Area Networks - Part 15.6: Wireless Body Area Networks. In *IEEE Std 802.15.6-2012*. <https://doi.org/10.1109/IEEESTD.2012.6161600>.
- [9] Ghassan Ahmed Ali and Shah Murtaza Rashid Al Masud, “Routing Optimization in WBAN using Bees Algorithm for Overcrowded Hajj Environment” *International Journal of Advanced Computer Science and Applications (IJACSA)*, 9(5), 2018.
- [10] Gouda, K. C., et. al., “Implementation of Traffic Priority Aware Medium Access Control Protocol for Wireless Body Area Networks”, *Springer Link*, 1 (7), 2019.
- [11] Yuan, D., et.al., “An Adaptive MAC Protocol Based on IEEE802.15.6 for Wireless Body Area Networks”, *Wireless Communications and Mobile Computing*, 1 (9), 2019.
- [12] Rismanian Yazdi, et. al., “A Priority-Based MAC Protocol for Energy Consumption and Delay Guaranteed in Wireless Body Area Networks”, *Wireless Personal Communications*, May 2019.
- [13] Bhandari, S. et.al., “A MAC Protocol with Dynamic Allocation of Time Slots Based on Traffic Priority in Wireless Body Area Networks”, *International Journal of Computer Networks & Communications*, 11(4), 25–41, 2019.
- [14] Ambigavathi, M., et. al., “Traffic Priority Based Channel Assignment Technique for Critical Data Transmission in Wireless Body Area Network”, *Journal of Medical Systems*, 42(11), 2018.
- [15] Sridharan, D., et. al., “Energy efficient and load balanced priority queue algorithm for Wireless Body Area Networks”, *Future Generation Computer Systems*, 88 (February 2019), 586–593.
- [16] Rasheed, M. B., et. al., “Delay and energy consumption analysis of priority guaranteed MAC protocol for wireless body area networks”, *Wireless Networks*, 23(4), 1249–1266, 2017.
- [17] Henna, S., et. al., “A fair contention access scheme for low-priority traffic in wireless body area networks”, *Sensors*, 17 (9), 2017.
- [18] Moh, S. et. al., “A priority-based adaptive MAC protocol for wireless body area networks”, *Sensors*, 16 (3), 2016.
- [19] Ansar Munir Shah, Abdelzahir Abdelmaboud, Khalid Mahmood, Mahmood ul Hassan and Muhammad Kashif Saeed, “eHealth WBAN: Energy-Efficient and Priority-Based Enhanced IEEE802.15.6 CSMA/CA MAC Protocol” *International Journal of Advanced Computer Science and Applications (IJACSA)*, 9(4), 2018.
- [20] Shah Murtaza Rashid Al Masud, et. al., 'Preemptive Queue Based Modified MAC Superframe for WBSN to Efficiently Transmit Pilgrims' Heterogeneous Data at Ritual Sites: An Analytical Approach'. *IICSNS (International Journal of Computer Science and Network Security)*, Korea, October 2020 Edition (Vol. 20, No: 10). Indexed in ESCI, Thomson Reuters (ISI).

Transformer based Contextual Model for Sentiment Analysis of Customer Reviews: A Fine-tuned BERT

A Sequence Learning BERT Model for Sentiment Analysis

Ashok Kumar Durairaj¹, Anandan Chinnalagu²
Department of Computer Science, Govt. Arts College
(Affiliated to Bharathidasan University Tiruchirappalli)
Kulithali, Karur, India

Abstract—The Bidirectional Encoder Representations from Transformers (BERT) is a state-of-the-art language model used for multiple natural language processing tasks and sequential modeling applications. The accuracy of predictions from context-based sentiment and analysis of customer review data from various social media platforms are challenging and time-consuming tasks due to the high volumes of unstructured data. In recent years, more research has been conducted based on the recurrent neural network algorithm, Long Short-Term Memory (LSTM), Bidirectional LSTM (BiLSTM) as well as hybrid, neutral, and traditional text classification algorithms. This paper presents our experimental research work to overcome these known challenges of the sentiment analysis models, such as its performance, accuracy, and context-based predictions. We've proposed a fine-tuned BERT model to predict customer sentiments through the utilization of customer reviews from Twitter, IMDB Movie Reviews, Yelp, Amazon. In addition, we compared the results of the proposed model with our custom Linear Support Vector Machine (LSVM), fastText, BiLSTM and hybrid fastText-BiLSTM models, as well as presented a comparative analysis dashboard report. This experiment result shows that the proposed model performs better than other models with respect to various performance measures.

Keywords—Transformers model; BERT; sequential model; deep learning; RNN; LSVM; LSTM; BiLSTM; fastText

I. INTRODUCTION

The RNN, LSTM, gated recurrent neural network (GRNN) and BiLSTM models are some of the various sequence models [1] for NLP tasks, language modeling, and machine translation. The Google research team introduced (Year 2017) the first Transformer and the first transduction model that replaces the recurrent layer with attention. The first Transformer model was used for language translation (English to France and English to German) tasks and the results showed that it outperformed all other neural model architecture with convolutional or recurrent layers [2]. Fig. 1 shows the Transformer architecture and the build blocks of BERT model. In this Transformer architecture, input sequence $(x_1, x_2, x_3, \dots, x_n)$ mapped for symbol representation of encoder to the continuous sequence representation of decoder $(z_1, z_2, z_3, \dots, z_n) = z$ the z decoder generates the $(y_1, y_2, y_3, \dots, y_m)$ sequence symbol of an element output at a time.

Model generates the symbols based on the output of previously generated symbols as an additional input, it uses the auto-regressive method at each step for next generation of symbols [2]. The overall Transformer architecture is based on self-attention with fully connected encoder and decode.

BERT is a pre-trained, an open-sourced (Year 2018) [3] and transformer-based language model from Google. It's designed to pre-train bidirectional (left and right) text representations from unlabeled text [4]. The BERT_{BASE} and BERT_{LARGE} are two original models. The base model consists of 12 Encoders and bidirectional self-attention, while the large model consists of 24 Encoders and 16 bidirectional heads. BERT model is pre-trained on 800 million words from BooksCorpus and English Wikipedia's unlabeled text of 2.5 billion words. As BERT is pre-trained with large unlabeled text datasets, this model can be easily fine-tuned for small datasets that are specific to an NLP task like sentiment prediction on customer or employees' reviews and question-answer system for chatbot applications.

Fig. 2 shows the neural network architecture of BERT's deep bidirectional and OpenAI GPT's unidirectional (Left-to-Right) contextual models [1], in which the unidirectional model generates a representation for each word based on other words in the same sentence. The BERT bidirectional model represents both the previous and next context in a sentence. However, the context free Word2vec and Glove models generate a word representation based on each word in the vocabulary.

There are many organizations that rely on reviews to improve customer experience and increase revenue of their products and services. Positive sentiments are one of the key factors for the success of several online businesses. However, determining the context of the review, polarity, and sentiment in textual content of customer reviews remain a challenge. The custom and hybrid deep learning models (LSTM, BiLSTM, fastText and fastText-BiLSTM) perform higher in textual datasets compare to traditional models [Naive Bays (NB), Logistic Regression (LR), Decision Tree (DT), Random Forest (RF), and Support Vector Machines (SVM)].

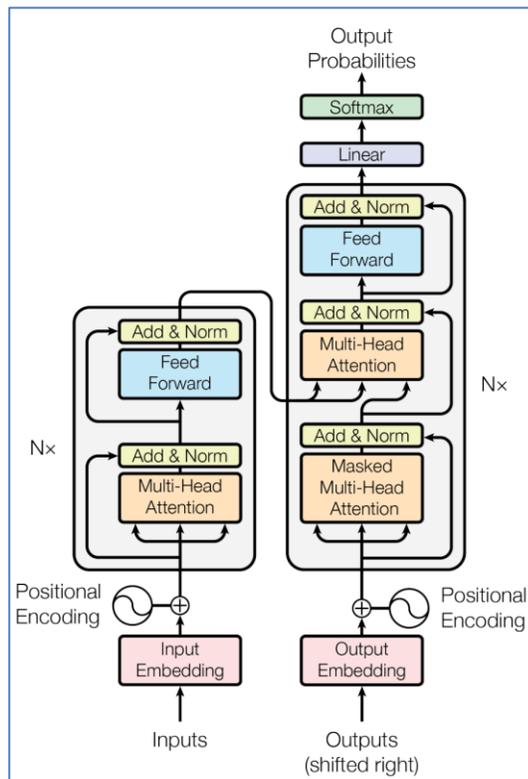


Fig. 1. Multi-layer Transformer Architecture.

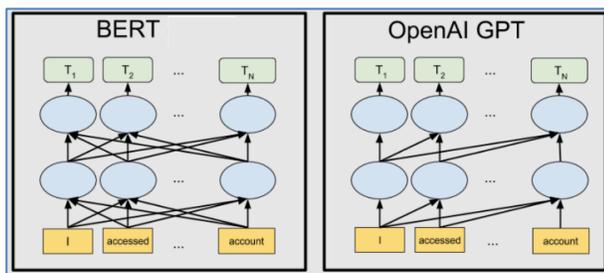


Fig. 2. BERT and OpenAI GPT Neural Network Architecture.

Evaluating Transformer based models and comparing their results with other state-of-the-art LSTM models are important for identifying the best model to utilize for Sentiment Analysis applications. Several researchers have used traditional models for sentiment analysis on datasets of customer reviews and discussed about their experience and issues occurred from it. These issues include time consumption of tasks such as data pre-processing, preparation for testing and training the datasets, as well as problems in performance and accuracy. We identified the gap in leveraging the pre-trained BERT model for datasets of customer reviews and found that the pre-trained model solves the problems and issues that traditional models have.

The pre-trained BERT model's performance, accuracy and approach motivated the authors to experiment with this model for customer sentiment analysis. The main objectives and contributions are as follows;

- Overcome known challenges of SA model performance, accuracy and context-based prediction.

- Train BERT-base-based model on Twitter, IMDB Movie Reviews, Yelp, and Amazon customer reviews datasets to improve the accuracy and performance of the model.
- Evaluate the custom deep learning sequential model of BiLSTM, hybrid fastText-BiLSTM model and linear models of LSVM, fastText models using the same datasets.
- Compare the results of the BERT model with the results of the deep learning sequential and linear model.
- Customize the data pre-processing steps for hybrid and linear model training.
- Fine-tune the hyperparameters for fastText-BiLSTM models.

This paper presented with several recent BERT and SA related research papers reviews and major contributions from various researchers in Section II. The literature reviews of BERT, fastText, BiLSTM, and LSVM models are presented in Section III. The experimental setting and model evaluation results are discussed in the Section IV. In Section V, concluded this paper with model results, findings of this research work and future work.

II. RELATED WORK

Recently, many researchers evaluated BERT model for many NLP tasks. In this section, presented most recent research papers on SA and pre-trained BERT models.

In 2021, [5] evaluated RNN+LSTM and BERT model for sentiment analysis to detect cyberbullying based on Twitters Spanish language dataset. The evaluation results show the accuracy and performance of the BERT model outperformed RNN+LSTM by 20%. Based on evaluation the bert-base-multilingual-uncased and Bert-large-uncased models show more accuracy. However, BERT model requires higher configuration of the computational environment. A challenge researchers face is finding the investment on a grand-scale infrastructure to train the models. There are many BERT-based SA experimental research, case studies and review papers presented for Arabic aspect-based [6], Italian Twitter SA [7] and Bangla-English Machine Translation [8].

In 2021, [9] present a large-scale open source pre-trained BERTweet model for English Tweets. BERTweet used for Part of speech (POS), recognition of Named entity and text classifications. Experimental result shows that it outperforms XLM-Rbase and RoBERTabase models, all these models are having a same architecture of BERT-base. There are several models available as open-sourced, whereas other models are inaccessible to be customized for commercial use.

In 2020, [10] presented a research article about a question answering (QA) system based on LSTM, multilingual BERT and BERT+vnKG models. They had used crafted Vietnam tourism QA dataset for this experiment and evaluated three models with the same data. The experimental result shows the proposed model outperformed other model in terms of time and the accuracy.

In 2021, [11] conducted an Aspect-based SA study on consumers product reviews data. They have proposed two BERT models for aspect extraction, sentiment classification using parallel and hierarchical aggregation methods based on hierarchical transformer model [12]. The following Fig. 3 and Fig. 4 show the parallel and hierarchical models. Study result shows that applying their proposed model approach improved the model performance and eliminate the need of further model training.

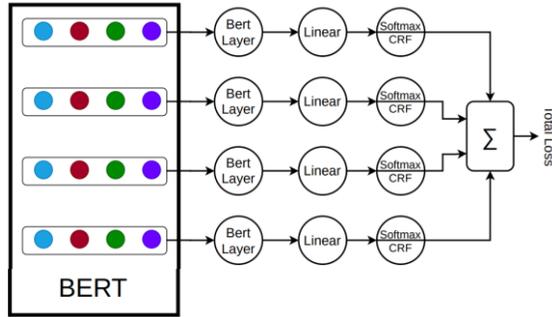


Fig. 3. Parallel Aggregation Model.

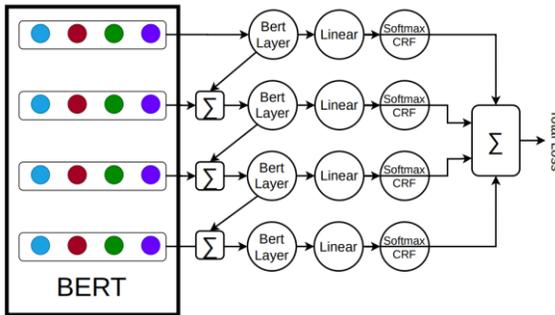


Fig. 4. Hierarchical Aggregation Model.

In 2021, [13] presented a research paper on attentions and hidden representation of learned pre-trained BERT models for aspect-based SA (ABSA) on reviews datasets. This research study found that BERT uses the aspect representation dedicated to semantics of the domain and self-attention head encode the context of the words. In 2021, [14] conduct a experiment based on Aspect-level SA (ABSA) using ALM-BERT model on consumer datasets, ALM-BERT model show the better performance than the other models.

In 2021, [15] presented BERT-based SA models research paper, in this research analyzed Github, Jira web portal comments and Stack Overflow posting datasets related to Software Engineering. comments. Authors used vanilla BERT, fine-tuned ensemble BERT and compressed DistilBERT models [16] and based on F1 score measure the ensemble and compressed BERT models improved performance by 6-12% over other model. Another research study conduced by [17] on GitHub dataset and the expermental results show 94% accuracy of emotion classification.

In 2021, [18] published an article of SA models comparative analysis od machine and deep learnings models, SA research work carried out by using Naive Bayes (NB), Support Vector Machine (SVM), LSTM and BERT-based

uncased model on consumer reviews and rating dataset from Amazon, Flipkart e-commerce platforms. Binary classification of consumer sentiment is categorized as positive and negative. This research study results show that deep learning BERT uncased model improved performance, and higher accuracy of sentiment predictions compared [19][20] to other machine learning models.

III. PROPOSED MODEL AND METHODOLOGY

Proposed sentiment analysis frameworks and models' architectures present with data pre-processing steps in the following section.

A. Data Pre-processing

We've developed python scripts for data pre-processing steps, customized the scripts and steps sequences based on dataset. Our custom script consists of data cleansing, reduction of unwanted data, data transformation and validations steps.

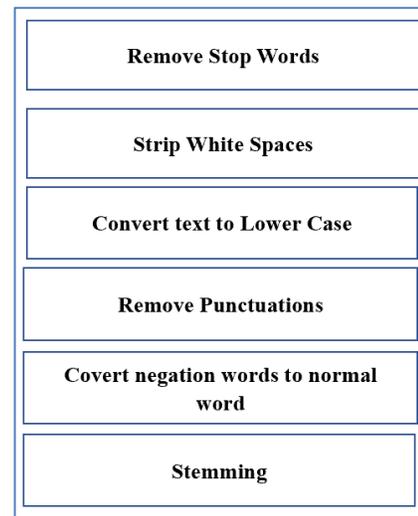


Fig. 5. Data Pre-processing Steps.

The above Fig. 5 shows data pre-processing steps. For this experiment, Twitter, IMDB Movie Reviews, Yelp, Amazon customer reviews datasets are used for training and testing the models. To improve the data quality, model performance and accuracy, performed the following pre-processing tasks: converted text to lowercasing text and removed stop words, converted negation words to normal word, removed white spaces, special characters, punctuations, stripping recurring headers from the text and stemming.

B. Proposed BERT Model

We propose fine-tuned BERT-base-cased model for sentiment prediction on customer reviews datasets. The advantage of BERT model is that it was pre-trained on large corpus of raw texts data. These models are used for Masked Language Modeling (MLM) and Next Sentence Prediction (NSP) and these pre-trained models can be fine-tuned for downstream applications [2]. BERT-base fine-tuned SA model framework is represented in Fig. 6. This framework consists of the following four components, input data pre-processing, Tokenization of input text for model, BERT-base-cased model and classification layer.

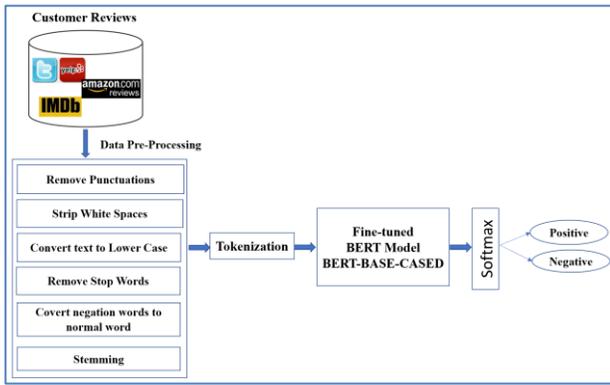


Fig. 6. BERT-base-cased Sentiment Analysis Framework.

The input layer generated tokens for given pre-processed text, the following Fig. 7 shows the embedding layers of tokenization of sentences. The Token embeddings is the sum of segment and position embeddings. These embeddings are learned specific token from WordPiece token vocabulary [4].

To train the model on customer review dataset, we follow the pre-train procedure with Adam optimizer from Hugging Face. following Fig. 8 shows the training history of BERTmodel on our dataset, the model training result show the close to 100% accuracy after 10 epochs. We've evaluated the pre-trained model and the evaluation result show 95% accuracy on our test dataset.

Fine-tuned the hyperparameters for higher accuracy and performance for customer reviews datasets. The Softmax function applied in the output layer to get the predicted probabilities of sentiment values. Here are the questions for probabilities and Softmax.

$$Probability = \frac{Numerator}{Denominator} \quad (1)$$

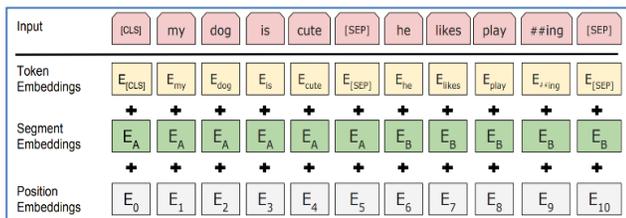


Fig. 7. Input Representation of BERT Model.

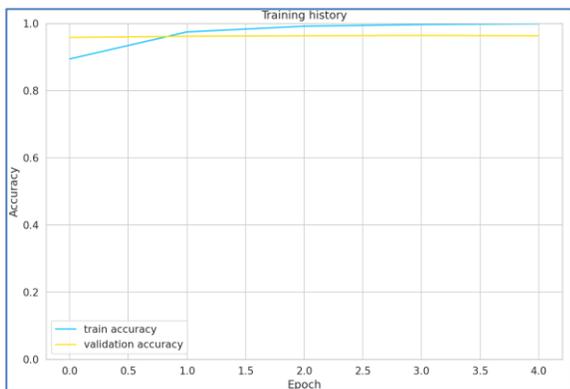


Fig. 8. Model Training History.

Softmax performs the transform on $x_1, x_2, x_3 \dots x_n$ numbers.

$$\text{softmax}(x_i) = \frac{e^{x_i}}{\sum_{j=1}^n e^{x_j}} \quad (2)$$

C. FastText, BiLSTM and FastText-BiLSTM Models

The Fig. 9 shows the neural networks SA framework used for this experimental research. These models are based on fastText and LSTM architectures.

FastText introduce by Facebook AI research (FAIR) lab for text representation and classification, it's a lightweight method and works on generic hardware with multicore CPU, the fastText models show faster performance, accuracy during model training and evaluation [21]. A new extension of the continuous skipgram and Continuous Bag of Words (CBOW) model like word2vec word embedding is introduced by fastText, where each word is represented as a bag of character n -grams. fastText model is Pre-Trained on Wikipedia dataset (294 languages) [22]. To compare with BERT model result, we evaluate customer review dataset using fastText model.

Authors build a two novel multilayer sequence processing custom models using BiLSTM and hybrid fastText-BiLSTM. it consists of two LSTM units and multilayers, one unit taking the input in a forward direction and other unit taking the input in a backward direction [23]. In this experiment, our main goal is to compare the BERT model result with authors The Hybrid fastText-BiLSTM and custom multilayer BiLSTM. Models consist of 196 memory units, 128 Embedding Layer, 5 Dense Layer and Softmax activation function at output layer. The LSTM unit consists of input, output and forget gates and these three gates are the activation of sigmoid function; the sigmoid output value is between 0 and 1, when gates are blocked the value is 0 and gates allow the input to pass through when the value is 1. The following are the equations of sigmoid and input, output and forget gates.

$$\text{sig}(t) = \frac{1}{1+e^{-t}} \quad (3)$$

$$i_t = \sigma(\omega_i[h_{t-1}, x_t] + b_i) \quad (4)$$

$$o_t = \sigma(\omega_o[h_{t-1}, x_t] + b_o) \quad (5)$$

$$f_t = \sigma(\omega_o[h_{t-1}, x_t] + b_f) \quad (6)$$

σ represents sigmoid function,

x_t represents input at current timestamp.

h_{t-1} represents LSTM block output of previous state at timestamp t-1.

$\omega_i, \omega_f,$ and ω_o are representing weight of input, forget and output gates.

b_i, b_o and b_f are representing bias for input, output, forget gates.

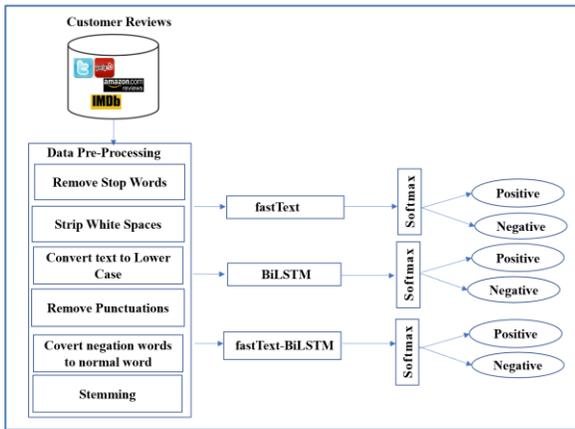


Fig. 9. FastText, BiLSTM and FastText-BiLSTM Models.

D. LSVM Model

Linear SVM (LSVM) is a most frequently used supervised learning algorithm for classification problems. SVM has two types of classifiers Linear [24] and Non-Linear. In Linear Classifier separates the data in a liner order and a data point considered as a p-dimensional vector, but the best hyperplane consider one which maximize the margin. The text can be categorized linearly using the SVM’s linear kernel and LSVM [25] works well with lot of features and also less parameters to optimize for training the model. We used linear kernel for this experiment. Fig. 10 shows the LSVM architecture and SA framework used for this experiment.

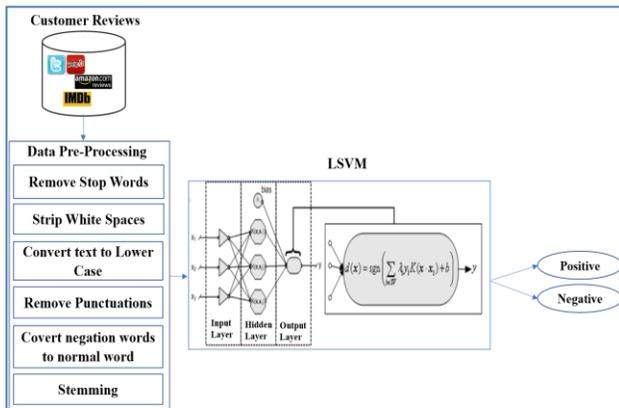


Fig. 10. Linear SVM (LSVM) Model.

Here is the equation for linear kernel function $k(x, y)$, given by the inner product $\langle x, y \rangle$, and c represent the optional constant.

$$k(x, y) = x^T + c \tag{7}$$

IV. EXPERIMENTAL SETTING AND RESULTS

There are four models and two environments used for this experiment. The data source, dataset, environment settings, fine-tuned hyperparameters and experimental results are presented in the following sub-sections.

A. Data Source and Dataset

There are multiple data sources are available online for customer reviews data, we have obtained publicly available

Twitter, IMDB Movie Reviews, Yelp and Amazon customer reviews datasets from Kaggle.com. Total 778631 customer reviews finalized after preprocessing the raw dataset and split the dataset 545041 (70%) for training and 233590 (30%) for testing the models. The data pre-processing steps are explained in the proposed model Section III. Models have trained and tested after fine-tuning the hyper parameters.

B. Experimental Environments

Training and evaluation of the BERT model is used through the Google Colaboratory cloud environment, while a standard server is used for training and evaluating the fastText, LSVM and SA-BLSTM models. Table I lists the details and components used for this experiment.

TABLE I. EXPERIMENTAL ENVIRONMENTS

Environment #1	Description
Model	BERT-base-cased
Transformer	Hugging face
Server Configuration	Google Colab Cloud
Programming Language & Tool	PyTorch, Python 3.8.8 Jupyter Notebook 6.3.0
Environment #2	Description
Model	fastText, LSVM and SA-BLSTM
Server Configuration	Windows 64-bit Operating System with Intel core i7 processor, 16 GB Memory.
Word Embedding	fastText Library and Keras Encoder
Programming Language & Tool	Python 3.8.8 Jupyter Notebook 6.3.0
Libraries and Frameworks	fastText, Pandas, Numpy, Seaborn, Matplotlib, Nltk, Scikit-learn, Keras

C. Parameters Fine-tuning for Models

Table II lists the values of parameters set for these models.

TABLE II. PARAMETERS SETTINGS

Model	Parameters	Value
BERT	Mode	Bert-base-cased
	Transformer	Hugging Face
	Batch Size	16
	Token Length	160
	Epoch	10
	Learning Rate	0.0002
	Optimizer	Adam
	Loss	Softmax
LSVM	Unigram, Bigram, Trigram	Linear
	Kernel	
fastText	Unigram, Bigram, Trigram	10
	Epoch	
	Learning Rate	
	Loss	
BLSTM	Epoch=10	10
	Learning Rate	0.01
	Loss=softmax	Softmax
fastText-BLSTM	Epoch	10
	Learning Rate	0.01
	Loss	Softmax

D. Performance Measures

The models evaluated are based on accuracy, recall, precision and F1 score while the performance measures are calculated based on the True Positive (TP), True Negative (TN), False Positive (FP) and False Negative (FN) matrix. The following Table III lists the values of performance measures.

TABLE III. EVALUATION METRIC

Table with 5 columns: Models, TP, FP, TN, FN. Rows include BERT, LSVM, fastText, BiLSTM, and fastText-BiLSTM.

The following are the equations to calculate the performance measures:

Precision = tp / (tp + fp) (8)

Recall = tp / (tp + fn) (9)

F1 Score = 2 * (Precision * Recall) / (Precision + Recall) (10)

Accuracy % = (tp + tn) / (tp + fp + tn + fn) * 100

The following Table IV and Table V show the performance measures and sentiment score of the models.

TABLE IV. MODELS PERFORMANCE MEASURES

Table with 5 columns: Model, Accuracy %, Recall, Precision, F1. Rows include BERT, LSVM, fastText, BiLSTM, and fastText-BiLSTM.

TABLE V. SENTIMENT SCORE

Table with 3 columns: Models, Positive, Negative. Rows include BERT, LSVM, fastText, BiLSTM, and fastText-BiLSTM.

The results of the accuracy are compared with other researchers' model results for the same datasets. The result showed BERT and fastText models' accuracy are 90% compared to other models. Table VI shows the comparison of model accuracy. Our experimental results performance measures show that fine-tuned Pre-trained BERT model scores highest F1 score of 0.90 and hybrid fastText-BiLSTM

model scores F1 score of 0.89 and other models scored less than 0.85. BERT shows the best result as a state-of-the-art model with respect to performance, accuracy, training and testing on customer reviews datasets.

TABLE VI. COMPARE MODELS ACCURACY SCORE

Table with 4 columns: Et.al, Dataset, Model, Accuracy %. Rows include Ashok and Anandan, Geetika Gautam, Seyed-Ali Bahrainaian, Neethu M.S, and Dhiraj Gurkhe.

V. CONCLUSION AND FUTURE WORK

The proposed BERT model outperforms in terms of accuracy and model performance compare to other models. The results of the fastText model showed low accuracy when unigram and bigram methods were used for training the model. The overall model training and data preparation tasks took less time for BERT model in comparison to others. This experiment reveals that the BERT model required more computational resources to train compared with other traditional models. The fastText model performed well with a standard server environment with minimal computational resources compare to other models. The fine-tuned BERT model simplifies the sentiment analysis tasks on large datasets.

A proposal for future research can be made to build transformer models for various domains, and framework for a continuous model trained to streamline data processing methods. In the future, more work will be done to conduct pre-training a BERT-base model on datasets of customer reviews for sentiment analysis and detecting emotions.

REFERENCES

[1] Connor Holmes, Daniel Mawhirter, Yuxiong He, Feng Yan, Bo Wu, "GRNN: Low-Latency and Scalable RNN Inference on GPUs", In Fourteenth Eurosys Conference (Eurosys '19) https://doi.org/10.1145/3302424.3303949, March, 2019.

- [2] Ashish Vaswani, Noam Shazeer, Niki Parmar, Jakob Uszkoreit, Llion Jones, Aidan N. Gomez, Lukasz Kaiser, Illia Polosukhin, "Attention is all you need". 31st Conference on Neural Information Processing Systems (NIPS), Long Beach, CA, USA, December, 2017.
- [3] Jacob Devlin and Ming-Wei Chng, Research Scientists Google AI Lanaguage, "https://ai.googleblog.com/2018/11/open-sourcing-bert-state-of-art-pre.html", November 2, 2018. Accessed on 10/30/2021.
- [4] Jacob Devlin, Ming-Wei Chang, Kenton Lee, Kristina Toutanova, "BERT:Pre-training of Deep Birirectional Transformers for Lanaguage Understanding" Google AI Lanaguage, arXiv:1810.04805v2 [cs.CL] 24 May, 2019.
- [5] Diego A. Andrade-Segarra1, Gabriel A. Leon-Paredes 2, "Deep Learning-based Natural Language Processing Methods Comparison for Presumptive Detection of Cyberbullying in Social Networks", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. 5, May, 2021.
- [6] Mohammed M.Abdelgwad, Taysir Hassan A Soliman, Ahmed I.Tabloba and Mohamed Fawzy Farghaly, "Arabic aspect based sentiment analysis using BERT", arXiv:2107.13290v2 [cs.CL] 28 September, 2021.
- [7] Marco Pota, Mirko Ventura, Rosario Catelli, Massimo Esposito, "An Effective BERT-Based Pipeline for Twitter Sentiment Analysis: A Case Study in Italiana", Sensors, MDPI Article, December 2020.
- [8] M. A. H. Akhand, Arna Roy, Argha Chandra Dhar and Md Abdus Samad Kamal, "Recent Progress, Emerging Techniques, and Future Research Prospects of Bangla Machine Translation: A Systematic Review", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 12, No. September, 2021.
- [9] Dat Quoc Nguyen, Thanh Vu and Anh Tuan Nguyen, "BERTweet: A pre-trained lanaguage model for English Tweets". Proceeding of the 2020 EMNLP, pages 9-14. November 16-20, 2020.
- [10] Truong H. V Phan and Phuc Do, "BERT+vnKG: Using Deep Learning and Knowledge Graph to Improve Vietnamese Question Answering System", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 7, July, 2020.
- [11] Akbar Karimi, Leonardo Rossi, Andrea Prati, "Improving BERT Performance for Aspect-Based Sentiment Analysis", Department of Engineering and Architecture, University of Parma. Italy. March, 2021.
- [12] Luca Bacco, Andrea Cimino, Felice Dell'Orletta, and Mario Merone, "Explainable Sentiment Analysis: A Hierarchical Transformer-Based Extractive Summarization Approach", MDPI, Electronics 2021, 10, 2195. https://doi.org/10.3390/electronics10182195. September, 2021.
- [13] Hu Xu, Lei Shu, Philip S. Yu, Bing Liu, "Understanding Pre-trained BERT for Aspect-based Sentiment Analysis", Department of Computer Science, University of Illinois at Chicago, IL, USA. Proceedings of the 28th International Conference on computational Linguistics, Barcelona, Spain, December, 2020.
- [14] Guangyao Pang, Keda Lu, Xiaoying Zhu, Jie He, Zhiyi Mo, Zizhen Peng, and Baoxing Pu, "Aspect-Level Sentiment Analysis Approach via BERT and Aspect Feature Location Model", Hindawi, Wireless Communications and Mobile Computing, Volume 2021, Article ID 5534615, 13 pages. https://doi.org/10.1155/2021/5534615. 2021.
- [15] Himanshu Batra, Narinder Singh Punn, Sanjay Kumar Sonbhadra, and Sonali Agarwal, "BERT-Based Sentiment Analysis: A Software Engineering Perspective", Indian Institute of Information Technology Allahabad, India, arXiv:2106.02581v3 [cs.CV], Jun, 2021.
- [16] Prakhar Ganesh, Yao Chen, Xin Lou, Mohammad Ali Khan, Yin Yang, Hassan Sajjad, Preslav Nakov, Deming Chen, Marianne Winslett, "Compressing Large-Scale Transformer-Based Models: A Case Study on BERT", https://doi.org/10.1162/tacl.00413. Transactions of the Association for Computational Linguistics, vol. 9, pp. 1061–1080, Jun, 2021.
- [17] Mrityunjay Singh, Amit Kumar Jakhar, Shivam Pandey, "Sentiment analysis on the impact of coronavirus in social life using BERT model", Social Network Analysis and Mining, Licence to Springer-Verlag GmBH Austria, part os Springer Nature. February, 2021.
- [18] M.P.Geetha and D.Karthika Renuka, "Improving the performance of aspect based sentiment analysis using fine-tuned Bert base Uncased model", International Journal of Intelligent Networks 2 (2021) 64–69. Jun, 2021.
- [19] Fatima-ezzahra Lagrari and Youssfi Elkettani, "Customized BERT with Convolution Model: A New Heuristic Enabled Encoder for Twitter Sentiment Analysis", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 10, October, 2020.
- [20] Majdi Baseiso and Saleh Alzahrani, "An Empirical Analysis of BERT Embedding for Automated Eassay Scoring", (IJACSA) International Journal of Advanced Computer Science and Applications, Vol. 11, No. 10, October, 2020.
- [21] A. Joulin, E. Grave, P. Bojanowski, and T. Mikolov, "Bag of tricks for efficient text classification", Facebook AI Research arXiv:1607.01759v3 [cs.CL], August, 2016.
- [22] Piotr Bojanowski, Edouard Grave, Armand Joulin, and Tomas Mikolov, "Enriching Word Vectors with Subword Information", Facebook AI Research, arXiv:1607.04606v2 [cs.CL] 19 Jun, 2017.
- [23] Karthik Gopalakrishnan and Fathi M. Salem, "Sentiment Analysis Using Simplified Long Short-term Memory Recurrent Neural Networks", Department of Electrical and Computer Engineering, Michigan State University USA. arXiv:2005.03993v1[cs.CL]. May, 2020.
- [24] Surbhi Arora, "SVM: Difference between Linear and Non-Linear Models", 4 February, 2020.
- [25] Alexandre Kowalczyk, "Support Vector Machine Succinctly", Syncfusion Inc, https://www.syncfusion.com/succinctly-free-books/confirmation/support-vector-machines-succinctly October, 2017.

A New Energy-efficient Multi-hop Routing Protocol for Heterogeneous Wireless Sensor Networks

Rowayda A. Sadek¹, Doha M. Abd-alazeem², Mohamed M. Abbassy³

Information Technology Department, Faculty of Computers & Artificial Intelligence, Helwan University, Cairo, Egypt¹
Information Technology Department, Faculty of Computers & Artificial Intelligence, Beni-Suef University, Cairo, Egypt^{2, 3}

Abstract—Energy use of sensor nodes efficiently and extending the lifetime of heterogeneous wireless sensor networks (HWSNs) is a main goal of HWSNs routing optimization methods, and therefore building an energy-efficient routing protocol becomes critical for HWSN performance improvement. They present an energy-efficient routing protocol based on the grey wolf optimizer (GWO) and the Tabu search algorithm (TSA) in this paper. Proposed routing system with primary objectives include clustering and the selection of cluster heads (CH) utilizing GWO with a fitness function based on the residual energy of sensor nodes and the average distance between CH and sink nodes base station (BS) due to the mobility of sensors, the quality of service (QoS) parameters such as reliability and energy consumption can be improved by discovering multiple optimized paths for data transmission from CH to BS and by TSA selecting the optimal route from CH to BS based on the forwarding of reliable route packets (FRRPs). The experimental results indicate that the proposed grey wolf optimizer with tabu Search Algorithm (GWO-TSA) can reduce HWSNs energy consumption by 10% and 20%, increase lifetime by 13% and 18%, and finally increase throughput by 6% and 14% when compared to the genetic algorithm with tabu search algorithm (GA-TSA) and grey wolf optimizer with crow search algorithm (GWO-CSA). When compared to GA-TSA & GWO-CSA, simulation reveals that the proposed GWO-TSA protocol improves HWSNs performance by minimizing energy consumption, maximizing network lifetime, and boosting network throughput.

Keywords—Heterogeneous wireless sensor networks (HWSNs); forwarding of reliable route packets (FRRPs); grey wolf optimizer (GWO); routing optimization; tabu search algorithm (TSA); quality of service (QoS)

I. INTRODUCTION

Wireless sensor networks (WSNs) connect the physical and digital worlds via many sensor nodes. Military surveillance, environmental monitoring, medical and healthcare applications all make use of WSNs. Because nodes are mobile, WSNs have a dynamic topology. This frequently results in the battery being unable to be changed or replaced, reducing the network's life, and it is critical to conserve energy and reduce the energy consumption of sensor nodes, as they are critical for communication in Wireless sensor networks. In the event of battery exhaustion, node and link failures may occur, necessitating the immediate suggestion of an alternate route to continue data transmission from the source to the destination, which requires additional energy. Thus, by establishing multiple paths for data communication, the overall efficiency, reliability, and integrity of the wireless sensor network can be

increased, and the network's traffic load can be distributed evenly [1].

Sensor nodes in WSNs are made up of wireless transceivers that can collect data from sensors and communicating with one another as in Fig. 1. A self-contained sensor node is a tiny device composed of four major components: sensing, computation, communication, and power. The sensor node's battery capacity is restricted, charging is difficult, and charging may be impossible [2].

There are two types of wireless sensor networks: heterogeneous and homogeneous as in Fig. 2. Heterogeneous wireless sensor networks are composed of sensor nodes with varying capabilities, including varying computational capabilities and sensing ranges, as well as certain sophisticated nodes [3]. The sensor node's primary function is to detect data from the environment and transmit it to the heterogeneous high-level node CH, which has high-level energy or communication capabilities as in Fig. 3. Advanced nodes may be equipped with greater memory and more powerful microprocessors/microcontrollers than cluster member nodes. The primary benefit of HWSNs is that it extends the life of the network, increases data transmission reliability, and reduces latency [4].

By reducing the transmission distance between the CH and the BS and optimizing the energy consumption of the sensor node, the clustering-based hierarchical routing protocol improves energy efficiency and network lifespan [5]. Clustering splits the region of WSNs sensing into many clusters. Each cluster's CH is responsible for connecting to other cluster members (CMs), collecting data from them, aggregating it, and transmitting it to the BS as in Fig. 4. As a consequence, how do you optimize your website? The most critical element of clustering-based routing protocols is the process of clustering and choosing CHs [6].

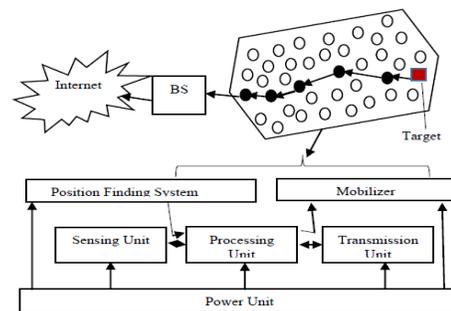


Fig. 1. Sensor Node Structure [16].

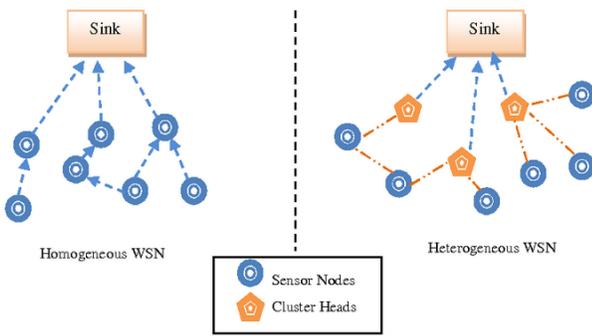


Fig. 2. Homogenous & Heterogeneous WSN [22].

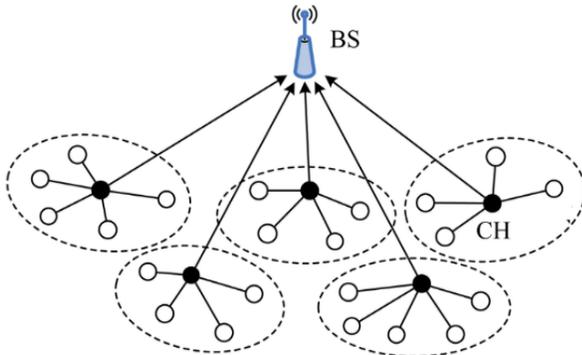


Fig. 3. Heterogeneous WSNs Structure.

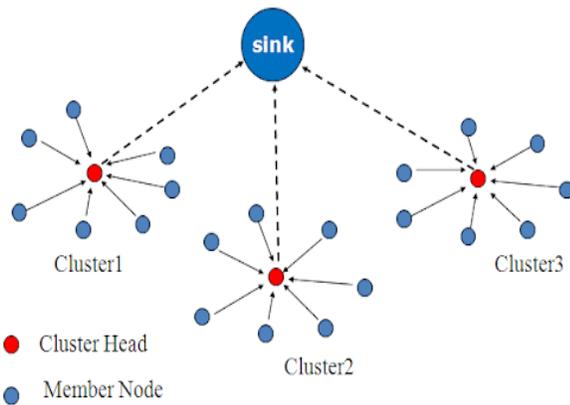


Fig. 4. WSN Clusters Structure [17].

Because a WSN is a self-organizing network, using a static topology increases the routing overhead, resulting in higher congestion and sensor node energy consumption [7]. With N nodes, the network is said to be enormous in size. Sensors are randomly distributed across a sensing range. Due to the large number of sensor nodes and their tight energy restrictions, as well as the frequent changes in topology, an energy-efficient routing method is critical. This may be achieved via the use of Tabu search, which is based on FRRPs. This search returns the optimal path. FRRPs packets are required for routing choices because they take into account path latency, node energy, and the frequency at which a node acts as a router. In wireless sensor networks, QoS requirements like as latency, throughput, and dependability must be considered [1].

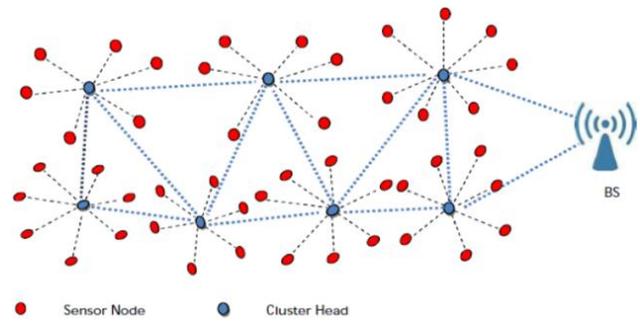


Fig. 5. Hierarchical Routing-Protocol Structure [17].

Routing techniques used in WSNs all have the aim of effectively using the limited resources available to sensor nodes to reduce energy consumption and prolong the network's lifespan [23]. Hierarchical Routing is the most often utilized routing algorithm in wireless sensor networks as in Fig. 5. Its primary objective is to control the energy consumption of sensor nodes effectively to optimize system lifespan and to sustain numerous clusters through multi-hop communication [25] [26]. Each cluster elects a cluster head who is responsible for aggregating data from cluster member nodes, while low-energy nodes may perform sensing duties. The primary objective is to minimize the number of messages delivered to BS. Clusters are generated using sensor energy storage and proximity to the cluster head [8] [24].

Due to the large number of sensor nodes that are subject to tight energy restrictions and frequent topology changes, the objective is to develop a routing protocol that controls node mobility and optimizes the routing process because of node mobility. The proposed GWO-TSA protocol, which operates on moving nodes in HWSNs, seeks to decrease energy consumption, increase WSN throughput, and prolong the network's life. Since the majority of HWSNs applications need dynamic routing methods, we want to manage the routing Process in such a way that it achieves the critical objective of reducing energy consumption and increasing network lifespan. This goal can be achieved by the use of GWO for clustering and optimize routing process by the selection of CHs by utilizing GWO with a fitness function based on the residual energy of sensor nodes and the average distance between CH and BS due to the mobility of sensor nodes and use TSA for selecting optimal route from CH to BS based on FRRPs.

The remainder of this paper is arranged as follow. Researcher's related work is described in Section II. Section III introduces routing optimization in WSNs, First introduce GWO, second grey wolf based Optimization for WSNs and finally TSA & its theoretical analyses. The Proposed Hybrid GWO-TSA protocol and presented in Section IV. Modeling of WSN explained in Section V. Experimental results and discussion are shown in Section VI Finally, Section VII concludes this paper.

II. RELATED WORK

Various researchers investigated issues related to the design of a routing protocol for a dynamic WSNs topology and its routing issues in order to send data from source nodes to the BS using a variety of techniques with the primary goal of

achieving routing optimization in WSNs by reducing sensor nodes' energy consumption, extending the network's lifetime, and increasing network performance.

A cluster head-based routing hierarchy method proposed for increasing the energy efficiency of WSNs by splitting the routing responsibility between a cluster head and a cooperative vice cluster head. The approach is similar to that of a TX/RX load balancing issue, except that the vice cluster head selection criteria are determined by the CH, resulting in a transparent temporary responsibility transfer procedure for all normal nodes in a cluster after the death of the cluster head. When compared to current vice cluster head-based techniques, the suggested system has the benefit of not needing time for each round's advertising phase, since the authority transfer procedure from a CH to its vice CH (VCH) does not interrupt WSN operation. According to simulation data, attaching a vice CH (VCH) node to share routing duties with a CH improves load balance across the WSN, thus prolonging its lifespan [9].

MLHP (Multi-level Hybrid Clustering Routing Protocol) was suggested as a technique for optimizing routing in WSNs using the GWO. To begin, the BS is critical in the CH selection process, and the second routing step utilizes GWO to transmit data to the BS. To save energy, nodes choose the most efficient route to the BS. & a third-stage clustering method based on a cost/fitness function calculated from the node's residual energy and the number of its neighbors. MLHP beat the other algorithms in terms of network lifespan, stability period, and residual energy [10].

Dynamic Cluster Formation Method was developed to prolong the network's lifespan. Based on coverage and connectivity, a WSNs is split into many clusters. The coverage range of a network is first confirmed by all nodes. This is done by broadcasting a message to all of the nodes in its vicinity. The nodes within the sensing range transmit an update message to that node. To decide which CH to utilize, the residual energy and delay time are used. To begin, each node sends a broadcast message to all other nodes. As a consequence, the node count is defined as the number of broadcast messages that a particular node receives. The delay time is calculated based on the number of nodes. The cluster head is the node with the lowest delay time and the most energy left. Clusters are generated by the cluster head. During data transmission, the energy of all nodes is drained. A threshold value is assigned to the energy of a node. When the energy of the CH falls below a predefined threshold, another node is selected as the cluster head based on the remaining energy and delay time. Therefore, clusters are generated dynamically by moving the cluster heads. Therefore, energy consumption is balanced, extending the network's life [2].

FIGWO (Fitness value-based Improved GWO) is an Energy-Efficient protocol that was implemented based on an improved GWO that utilizes a fitness Function to improve the selection of the optimal solution in GWO, resulting in a more balanced cluster structure and better distribution of CHs. It enhanced the process of choosing CHs by calculating a fitness value, which ensures that the cluster node nearest to the BS and

with the most energy is more likely to be selected as a CH. When a new CH is chosen, the transmission distance between each node and the BS is also changed. This reduces both the transmission distance between CHs and BS and the energy consumption of sensor nodes. As a consequence, the lifespan of the network may be prolonged. According to simulation findings, the suggested algorithm's performance was a fitness value that improved the discovery of the optimum solution in GWO, which ensures a more balanced cluster structure and a better distribution of CHs. When compared to other algorithms, this method consumes less energy, maintains network stability, and increases network throughput (amount of data received by BS) [6].

Routing Protocol Framework was developed with the following primary objectives: construct dynamic topology using a genetic algorithm with mutation operator, determine the optimal route for data transmission from CH to BS using the Tabu search approach, and improve service quality characteristics such as reliability and energy constraints by discovering various optimum paths. The suggested approach starts by clustering normal sensor nodes. Each cluster is given a CH using a genetic method. In GA, the fitness function is defined only in terms of energy dissipation. If the sensor nodes' remaining energy is more than the average energy of all live (active) nodes, the BS activates them to maximize energy efficiency. Then, using Tabu search, connect the member nodes to the cluster heads for data transmission. Due to the proposed protocol's optimal route selection technique, simulation results indicate that it may enhance service quality [1].

Routing technique based on the TSA and a fuzzy inference system (FIS) was proposed to enhance network stability, energy consumption, and packet delivery ratio (PDR). To get excellent results in WSN, this technique utilized the TSA method for neighborhood solution selection and next-hop selection. It then applied FIS to the TSA solutions generated, resulting in a route that complied with FIS requirements for data transmission between CH and BS. The FIS is computed by dividing CH by BS. The simulation findings indicate that the proposed protocol may enhance service quality by using an optimum route selection method for data transmission from CH to BS [11].

Optimum cluster head selection method based on a combination of GWO and CSA was created for extending the lifespan of WSNs by reducing the latency in data transmission from CH to BS, the distance between nodes and BS, and optimizing energy consumption. To address the issue of early convergence, which prevents it from traversing the search space efficiently, CSA is combined with the GWO method. To select CH efficiently, this hybridization of GWO and CSA algorithms preserves the trade-off between exploitation and exploration degrees in the search space throughout the clustering process. The proposed hybridization of the GWO and CSA protocols demonstrated that by lowering node energy consumption and balancing active and dead nodes, the lifespan of a WSN may be extended [12].

III. ROUTING OPTIMIZATION IN WSNS

A. Grey Wolf Optimizer

GWO is an intelligent algorithm that simulates the hierarchy and hunting process of wild wolf packs. Wolves have a four-tiered social structure. As shown in Fig. 6, alpha (α) wolves, beta (β) wolves, delta (δ) wolves, and omega (ω) wolves are ranked from top to bottom [18].

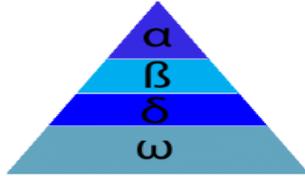


Fig. 6. Hierarchy of GWO [13].

Hunting behavior of the wolf is split into three phases: tracking and approaching prey, hunting, and encircling prey, and attacking prey. The GWO algorithm is led in its hunting (optimization) by, and, wolf is iteratively enhanced via the use of, and, [13] develops the following mathematical model of GWO:

1) *Encircling prey*: To mathematically simulate the wolf's encircling technique, GWO analyses two points in n-dimensional space and changes the location of one of the points in response to the position of the other. As in [13] and [14], the following formulae have been suggested to simulate this.

$$D = |C * X P(t) - X(t)| \quad (1)$$

$$X(t+1) = X P(t) - A * D \quad (2)$$

Where D is the distance between the source node (grey wolf) and Destination BS, t is the current iteration, X_p and X indicate the position vector of the prey (BS) and a grey wolf respectively, A and C are coefficient vectors which are calculated as follow as in [13] [14].

$$A = 2a * r1 - a \quad (3)$$

$$C = 2 * r2 \quad (4)$$

where components of a are decreased linearly from 2 to 0 with iteration, $r1$ and $r2$ are randomly generated vectors in [0, 1].

2) *Hunting*: Gray wolves can identify and approaching prey (BS). Alpha is primarily responsible for hunting, sleeping, and waking up. Beta and delta wolves may also take part in decision-making or other tasks on occasion. Grey wolves' hunting technique may be mathematically approximated using alpha, beta, and delta solutions to approximate the prey (BS) location. Each wolf may update its location using the equations described in [13] and [14].

$$D\alpha = |C1 * X\alpha - X| \quad (5)$$

$$D\beta = C2 * X\beta - X \quad (6)$$

$$D\delta = |C3 * X\delta - X| \quad (7)$$

$$X1 = X\alpha - A1 * D\alpha \quad (8)$$

$$X2 = X\beta - A2 * D\beta \quad (9)$$

$$X3 = X\delta - A3 * D\delta \quad (10)$$

$$X(t+1) = [X1(t) + X2(t) + X3(t)] / 3 \quad (11)$$

3) *Exploitation & Exploitation in attacking prey*: GWO reduced the value of a to mathematically simulate approaching the prey (BS). The fluctuation range of A is likewise reduced by a , where A is a random variable in the range $[a, a]$, with a decreasing from 2 to 0 over repetitions. When $|A| < 1$, candidate solutions tend to converge near the prey (BS) and diverge from it when $|A| > 1$. The adaptive values of a and A determine the shift between exploration and exploitation. When $|A| > 1$, the focus is on exploration, while when $|A| < 1$, the focus is on extraction.

Algorithm 1: GWO

```

Initialize the grey wolf population  $X_i$  ( $i = 1, 2, \dots, n$ )
Initialize  $\alpha$ ,  $A$  and  $C$ .
Calculate the fitness of each search agent.
 $X\alpha$  = the best search agent
 $X\beta$  = the second best search agent
 $X\delta$  = the third best search agent
While ( $t < \text{Max number of iterations}$ )
  for each search agent
    Update the position of the current search agent by (11).
  end for
  Update  $\alpha$ ,  $A$  and  $C$ .
  Calculate the fitness of all search agents.
  Update  $X\alpha$ ,  $X\beta$ ,  $X\delta$ 
   $t = t + 1$ ;
End while.
return  $X\alpha$ .

```

4) *Optimization for WSNS*: Because the communication process utilizes the majority of the energy in a wireless sensor network, power consumption may be reasonably lowered by carefully choosing the routing technology. The whole network life cycle is reduced as a result of improper data packet routing, and nodes responsible for forwarding data packets play a significant role in routing. An appropriate cluster head must be chosen in light of these issues. This is accomplished by using the remaining energy and the suggested protocol's distance to the BS. To minimize iterations, GWO is employed, in which a layered design splits the whole region into four levels, each with several duties. The first layer's nodes are referred to as leader nodes. When the number surpasses two, game theory may be used to elect the head. This technique results in substantial energy savings, extending the life of the whole network [19].

Cluster-based selection is used to determine which cluster heads are on the first layer and closest to the base station. If layer 1 has several nodes, the nodes' remaining energy is utilized to make a choice. GWO technique adheres to the Gray Wolf's leadership hierarchy. It has four distinct subspecies of grey wolves: alpha (α), beta (β), delta (δ), and omega (ω), each of which performs a specific function. The following actions must be taken to establish this leadership hierarchy in a wireless sensor network. Utilize hierarchical and cluster-based

architectures. Sensor nodes are placed in various levels based on their distance from the base station, with each layer consisting of several sensor nodes [15].

Each layer is separated by R , the first layer is separated by R , and the second layer is separated by $2R$. The network is similarly divided into four layers: layer 1, layer 2, layer 3, and layer 4. Clustering is determined by the sensor nodes' density, and the cluster's transmission radius will be $2R$. The cluster's chief (or)The leader is elected from the sensor nodes in layer 1, co-leaders are chosen from the nodes in layer 2, elders are elected from the nodes in layer 3, and members are elected from the nodes in layer 4, as shown in Fig. 7.

B. Tabu Search Algorithm

Tabu search is a meta-heuristic search method that avoids looping back to previously used routes by storing information about adjacent nodes in short-term memory called Tabu lists. Tabu lists include information about neighboring nodes' energy levels, their IDs, and status. To prevent loops, Tabu search utilizes memory based on recency to avoid some re-instancing within a certain time (this is done through a tabu list) [21]. As a result, the Tabu list stores the active routes that are accessible at each energy level. This kind of information is represented in the form of dynamic data packets termed FRRP, which are utilized during data transmission to determine the optimal way from the source to the sink among the many possible routes as in Fig. 8.

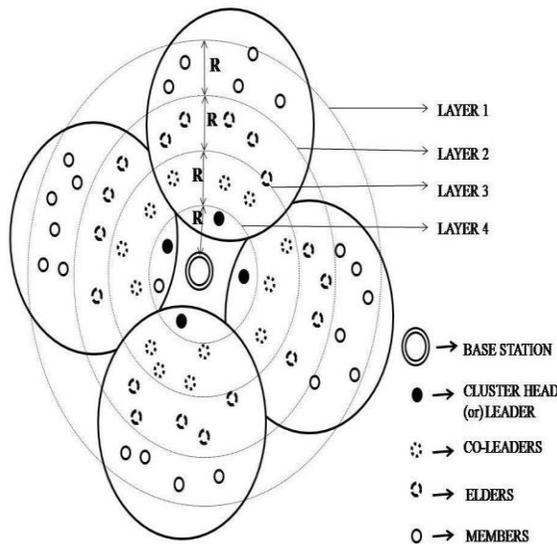


Fig. 7. A Grey-Wolf Optimization Approach [20].

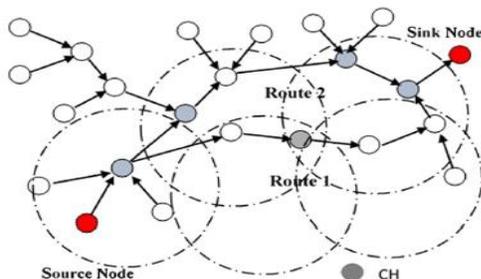


Fig. 8. Optimal Path Selection from Multiple Available Paths [1].

Algorithm 2: Tabu Search Algorithm

1. Start
2. Select An initial $x \in X$
3. Let $x^* = x$ { x^* denote the optimal solution recently founded}
4. Set the iteration number $k=0$.
5. $T = \emptyset$ (T is Tabu list).
6. If $S(x) \in T$ is empty.
7. Go to step 16
8. Else
9. $K=k+1$;
10. Select $\dots()$ $kx \in Sx - T$ such \dots that $(()) : (())$ $kxs \in$ Optimum $sxs \in Sx - T$
11. End if
12. $: ()$ $kx=sx$
13. If $C(x) < C(x^*)$
14. $X^* := x$
15. End if
16. If a number of iteration within a stipulated time has elapsed either in total
17. Upon reaching this step directly from step 6
18. Else
19. Update T (as subsequently identified)
20. Return to step 6.
21. End if
22. End

IV. PROPOSED GWO-TSA PROTOCOL

Proposed GWO-TSA Protocol combines the GWO method with a fitness function for clustering and a procedure for selecting CHs based on sensor node residual energy and the average distance between the CH and BS. Then, using TSA with FRRPs for optimum route selection from CH to BS, enhance QoS factors such as reliability and energy restrictions in WSN. The proposed GWO-TSA aims to improve WSN performance by reducing sensor energy consumption, extending the network's lifespan, and increasing network throughput.

A. Fitness Function

The proposed GWO-TSA identified CHs based on the GWO and computed their fitness values using Fitness Function (12), where the fitness value of a node is determined by its distance from the BS and residual energy.

$$F = w * (TD_{N-BS} - D_{CH-N}) + (1-w) * (E_t - E_r) \quad (12)$$

Where the w coefficient in the fitness function shows the contribution of the residual energy and distance parameters?

TD_{N-BS} - represents the total distance from all nodes to BS.

D_{CH-BS} - represents a distance from CH to its related Nodes in its cluster.

E_t - represents the total energy of nodes.

E_r - represents residual energy of nodes.

B. Steps of the Proposed GWO-TSA in a Dynamically Deployed WSN for Optimal Route Selection for Data Transmission from CH To BS in Fig. 9

1) Setup Initialization of the HWSN and deployment of sensor nodes.

2) Clustering using GWO with a fitness function based on the node's distance to the BS and residual energy for CHs

selection (grey wolves, alpha (α), beta (β), and delta (δ)) three optimum CHs.

3) Initiate TSA by generating FRRPs from (grey wolves, alpha (α), beta (β), and delta (δ)) three optimum CHs energy values for each sensor node and its distance from the BS and inserting them into the Tabu list.

4) Using the TSA method on the values in the Tabu list, choose the optimum route for data transfer from CH to BS from the possible routes in the Tabu list.

5) Remove FRRP from the Tabu list if it transmits from CH to BS.

6) Conduct an energy dissipation analysis and update the Tabu list.

7) Repeat steps 2–6 above until all data has been sent from CH to BS.

C. Improving QoS Parameters by using Proposed GWO-TSA

The GWO-TSA proposal is primarily concerned with network quality metrics like as network lifespan, node energy consumption, and network throughput as shown above in Fig. 10.

Dynamic networks, node deployment, network scalability, and network reliability are all linked issues. These issues have to be resolved in order to improve QoS in areas like as dependability, energy consumption, throughput, data loss, and network lifespan.

1) Node deployment: Instead of randomly dispersed nodes, GWO is utilized to deploy sensor nodes depending on their remaining energy and distance to the base station.

2) Formation of Dynamic Clusters: Network nodes this needed more time and energy for the findings to be moved into dynamic clusters and the CH selection process. This is enhanced using GWO with a Fitness Function to choose CHs based on two primary criteria (energy and distance to BS), which significantly lowers the amount of time and energy spent on the clustering process.

3) Network Scalability: The proposed GWO-TSA performance is unaffected by the number of sensors nodes but is influenced by the node's energy and distance to the base station.

4) Network Reliability: TSA identifies several optimal routes for data transmission from CH to BS to increase data transmission reliability; rather of using a single path, many paths may be utilized concurrently.

5) Network Throughput: Data transfer from CH to BS was improved by delivering data through several optimal routes identified by TSA. This allows load balancing to concentrate on nodes that influence the network's lifespan rather than on the whole network.

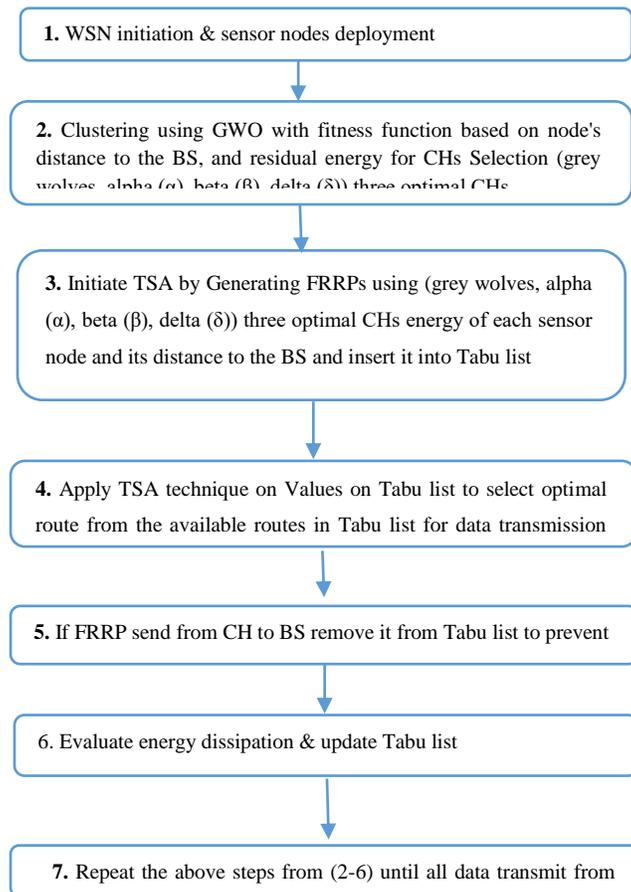


Fig. 9. Proposed GWO-TSA Main Steps.

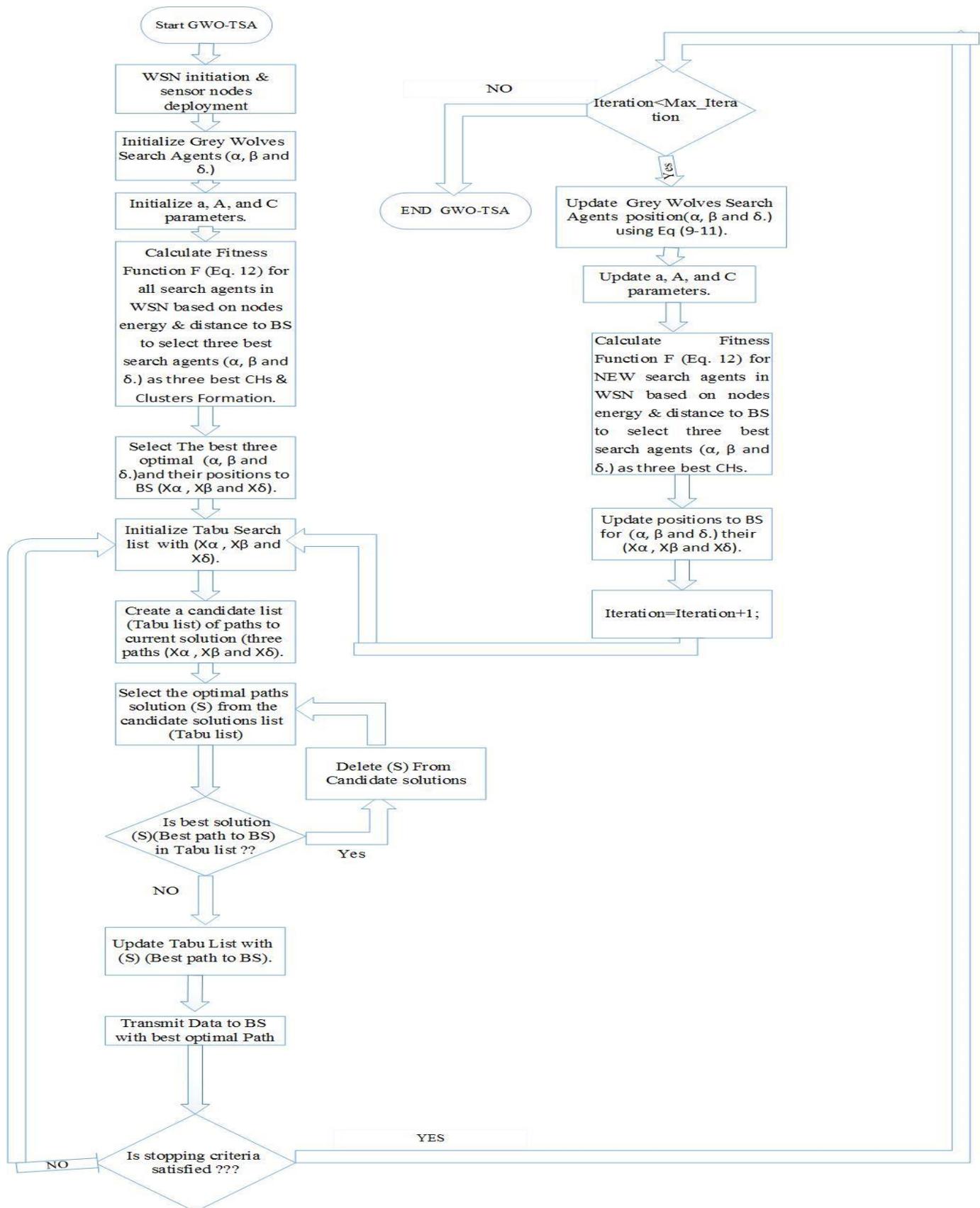


Fig. 10. Proposed GWO-TSA Protocol Flowchart.

V. MODELING OF WSNS

A. Energy Model

When transmitting an L-bit long data packet across the distance d, the energy model is utilized, as shown in [2]. Specifically, the amount of energy needed is:

$$E_{TX}(l, d) = l \times E_{elec} + l \times \epsilon_{fs} \times d^2, \text{ if } d < d_0$$

$$l \times E_{elec} + l \times \epsilon_{mp} \times d^4, \text{ if } d > d_0$$

Where E_{TX} indicates the energy transferred and E_{elec} indicates the energy used per bit by the transmitter or receiver circuit. The values for fs and mp are dependent on the transmitter amplifier type. The open space model is utilized if the distance between the transmitter and receiver is less than a threshold d_0 ; otherwise, the multi-path model is used. d_0 is often computed as follows:

$$d_0 = \epsilon_{fs} / \epsilon_{mp}$$

B. Simulation Model

1) Assumptions made for this routing:

- a) The sink (Base Station) is located inside the sensor field.
- b) Heterogeneous WSN.
- c) After deployment sensor nodes are unattended. So that recharging or changing of battery is not possible.
- d) Links are asymmetric because of nodes mobility.
- e) Mobility of the node is controllable and predictable.

Proposed GWO-TSA is done in MATLAB 2017b with 16GB RAM, 1TB HDD, and an i7 CPU. The GWO-TSA network and energy models were built in MATLAB to assess the algorithm's performance.

The following metrics used performance evaluation:

- 1) Network lifetime.
- 2) Network Throughput.
- 3) Network Residual /Remaining energy.

The proposed GWO-TSA aims to improve WSN by reducing sensor energy consumption, extending network lifespan, and increasing network throughput.

VI. RESULTS AND DISCUSSION

GWO-TSA algorithm is compared to GA-TSA) and GWO-CSA algorithms when the identical WSN simulation parameters Table I are being used.

Fig. 11 show Wireless sensor network simulation area as (200*200) m², where sensor nodes deployment and BS are in the center of the sensing area while Fig. 12 Heterogeneous WSN nodes.

A. Network Lifetime

It is used to determine the WSN's stability period; it is one of the most critical metric parameters in WSNs. We depict it as a series of alive & dead nodes with varying round counts.

Fig. 13 show number of alive sensor nodes for three comparative procedures with a varied number of rounds (0-

2800 rounds). Initially, when the number of rounds grew from 0 to 2800 number of alive nodes decreased. Proposed GWO-TSA, as shown in Fig. 13 maintains nodes alive for a greater number of cycles than the GA-TSA and GWO-CSA. Nodes remain viable for about 2780 rounds in the planned GWO-TSA, but only for approximately 2630 and 2260 rounds in the GA-TSA and GWO-CSA, respectively.

TABLE I. SIMULATION PARAMETERS

Simulation parameters	Value
Number of sensor nodes	100
Sensing Area	(200*200)
Position of the sink node	(100*100)
The initial energy of the sensor nodes	0.5J
Control packet size	2000
Data packet size	4096
Data Aggregation Energy	$E_{DA} = 50 \text{ nJ/bit}$
Transmitter/receiver energy	$E_{elec} = 50 \text{ nJ/bit}$
Transmitter Amplifier(free space)	$\epsilon_{fs} = 10 \text{ nJ/(bit. m}^2)$
Transmitter Amplifier (multi-path space)	$\epsilon_{mp} = 0.0013 \text{ pJ/(bit.m}^4)$
Maximum node speed	10 m/s
W	0.3

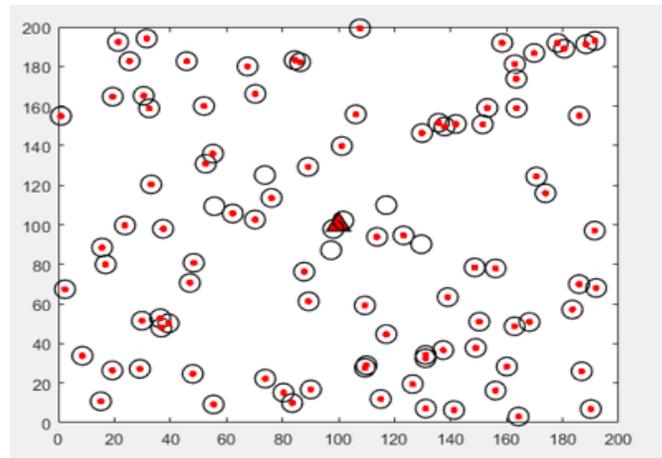


Fig. 11. Wireless Sensor Network Simulation Area.

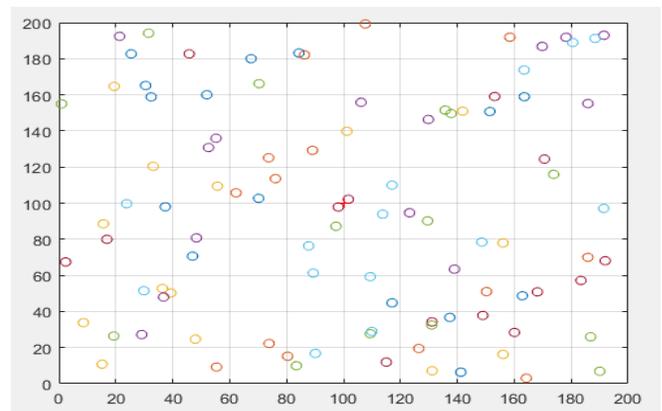


Fig. 12. Heterogenous WSN Nodes.

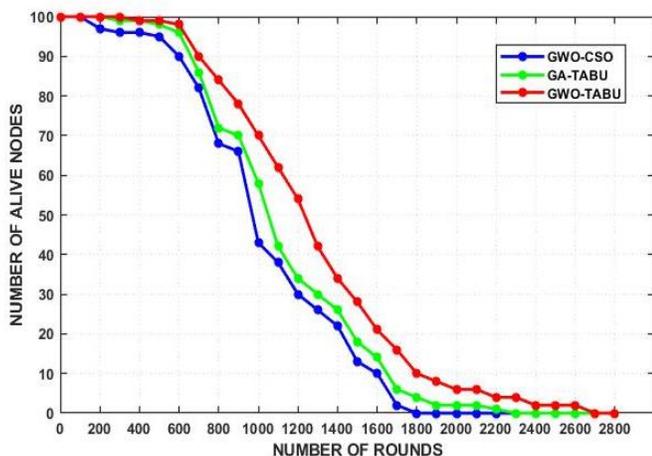


Fig. 13. Number of Alive Nodes in a different Number of Rounds.

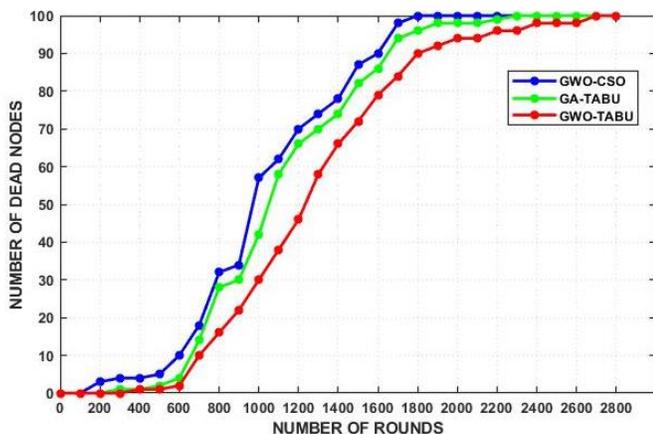


Fig. 14. Number of Dead nodes in a different Number of Rounds.

Fig. 14 show number of dead sensor nodes for three comparative procedures with a varied number of rounds (0-2800 rounds). Initially, the number of dead nodes increased as the number of rounds increased from 0 to 2800, as sensor nodes lost energy and their batteries became difficult to recharge. Fig. 14 shows that nodes died approximately at 2780 rounds in the proposed GWO-TSA, while they died at 2630 and 2260 rounds in the GA-TSA and GWO-CSA, respectively. Finally, the Dead & Alive nodes findings indicate that the proposed GWO-TSA reduces node energy consumption, which results in nodes being alive longer, which increases network lifespan, one of the most critical aspects in WSN performance.

Fig. 15 shows WSN lifetime with a different number of sensor nodes Start with 100 sensors until 1000 sensors node to show network lifetime for three compared protocols. Fig. 15 show that the proposed GWO-TSA enhances network lifetime by improving node energy consumption that leads to nodes alive more times. GWO-TSA improves network lifetime percentage by 13% & 18% over the compared protocols GA-TSA & GWO-CSA respectively.

B. Network Throughput

It's defined as the Number of packets received by BS from CHs, It's another necessary facto in WSN Routing optimization.

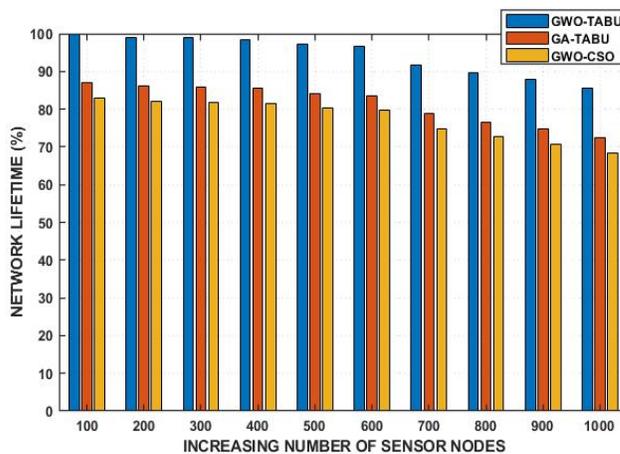


Fig. 15. Network Lifetime of a different Number of Sensor Nodes.

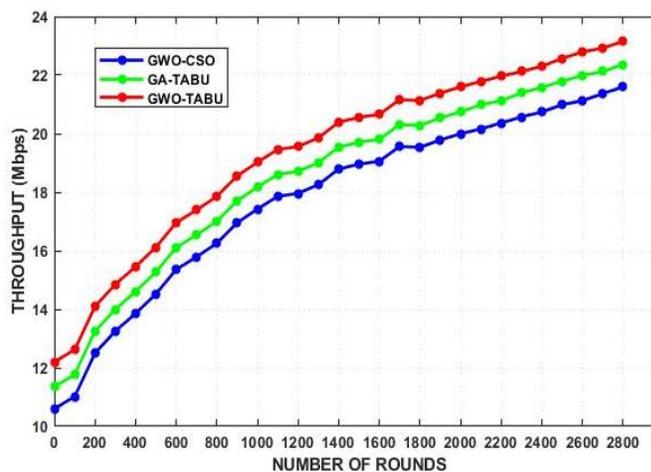


Fig. 16. Network Throughput with a different Number of Rounds.

Fig. 16 show Average of WSN Throughput with a different number of rounds from (0-2800 rounds) for three compared protocols. Fig. 16 shows that the proposed GWO-TSA increases Network Throughput over the compared GA-TSA & GWO-CSA protocols.

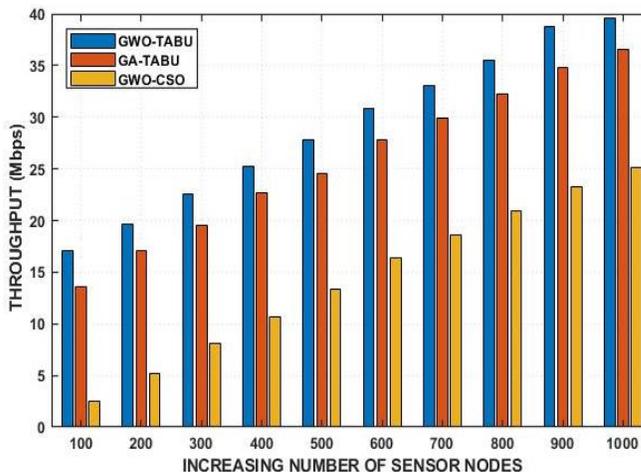


Fig. 17. Network throughput of a different Number of Sensor Nodes.

Fig. 17 show average of WSN throughput with a different number of sensors nodes Start with 100 sensors until 1000 sensors node to show network throughput for three compared protocols. Fig. 17, show that the proposed GWO-TSA improved network throughput percentage by 6% & 14% over GA-TSA & GWO-CSA respectively, this means GWO-TSA increases the number of bits sends by CHs to BS. GWO-TSA using GWO & Tabu search techniques for clustering & Cluster heads selection for transmitting aggregated data from cluster nodes to BS by CHs to save energy for data transmission this lead to increase network throughput.

C. 5 Network Residual Energy

Residual Energy is one of the most important Metric elements in WSN Routing Optimization because the main goal is to minimize nodes' energy consumption.

Fig. 18 shows average of WSN residual energy with a different number of rounds from (0-2800 rounds) for three compared protocols. Fig. 18, show that the proposed GWO-TSA increase Network Residual energy over the compared GA-TSA & GWO-CSA protocols.

Fig. 19 shows the Average of WSN residual energy with a different number of sensors nodes Start with 100 sensors until 1000 sensors node to show energy consumption for three compared protocols. Fig. 19, show that the proposed GWO-TSA enhances network residual energy by 10% & 20% over GA-TSA & GWO-CSA respectively. GWO-TSA enhances the energy consumption of sensor nodes by using the Tabu search technique for optimal route selection to reduce energy consumption that leads to increased residual energy of the network.

Table II explain the Performance of the proposed GWO-TSA over the compared protocols GA-TSA & GWO-CSA. The experimental results indicate that the proposed GWO-TSA enhances WSN Energy consumption by 10% and 20%, Increase in WSN Lifetime by 13% and 18% and finally Increase in WSN Throughput by 6% and 14% over GA-TSA and GWO-TSA respectively.

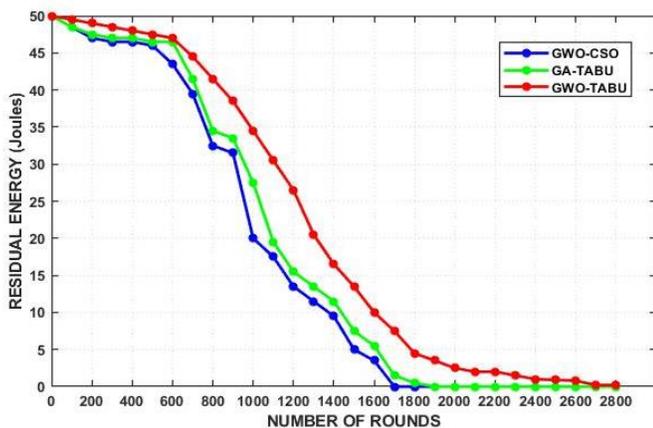


Fig. 18. Network Residual Energy with a different Number of Rounds.

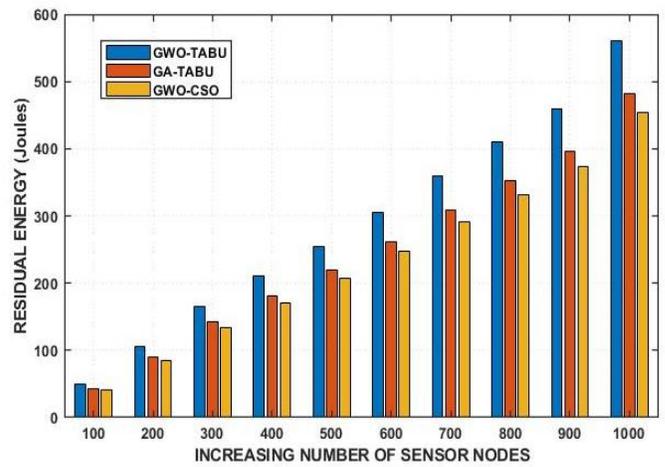


Fig. 19. Network Residual Energy of a different Number of Sensor Nodes.

TABLE II. PROPOSED GWO-TSA PERFORMANCE

protocols	WSN Performance		
	Energy consumption	Lifetime	Throughput
GA-TSA	10%	13%	6%
GWO-CSA	20%	18%	14%

VII. CONCLUSION

In this paper, we propose a new energy-efficient multi-hop routing protocol based on GWO and TSA, with the primary goal of optimizing routing by reducing the energy consumption of Sensor nodes, extending the lifetime of WSNs, and increasing network throughput. The proposed GWO-TSA protocol accomplished this goal by incorporating GWO into the CH selection process. By utilizing a fitness function based on the sensor node's energy residual and its distance to BS, TSA determined the optimal route from the CH to BS using FRRPs. The suggested GWO-TSA satisfies QoS requirements such as network scalability, since the proposed GWO-TSA's performance is unaffected by the number of sensor nodes but is influenced by the node's energy and distance to the base station, and network dependability. TSA identifies several optimal routes for data transmission from CH to BS to increase data transmission reliability; rather than using a single path, many paths may be utilized concurrently. Through simulations in MATLAB, it was shown that the proposed approach accomplished the route optimization goal by combining GWO and TSA.

ACKNOWLEDGMENT

I express my sincere gratitude and special thanks to my guides Assoc.Prof. Rowayda A.Sadek & Mohamed M.Abbassy for their constant help, encouragement and inspiration throughout the thesis work. Without their valuable guidance, this work would never have been a successful one. I would also like to thank my parents and my husband who have been the backbone, advisors and constant source of motivation throughout the work.

REFERENCES

- [1] P. Srinivasa Ragavan and K. Ramasamy, Optimized routing in wireless sensor networks by establishing dynamic topologies based on genetic algorithm, Springer,2019.
- [2] K. Johny Elma and Dr.S .Meenakshi, Dynamic cluster formation method to increase the lifetime of a wireless sensor network, International Journal of Computer Science and Information Security (IJCSIS) ,2017.
- [3] M. Kumar Singh, S. Intekhab Amin, S. Akhtar Imam , V. Kumar Sachan and A. Choudhary , A survey of wireless sensor network and its types, International Conference on Advances in Computing, Communication Control and Networking ,2018.
- [4] A. Kau & , Dr. S. Vatta, Implementation of LEACH, Hetero-LEACH, SEP and EEHC protocols using MATLAB in wireless sensor network , International Journal of Engineering Research & Technology (IJERT) ,2016.
- [5] H. Chaurasiya &Dr.S. Ghosh, Performance evaluation of energy-efficient cluster-based algorithms in wireless sensor network, International Journal of Advanced Trends in Computer Science and Engineering,2018.
- [6] X. Zhao, H. Zhu, S. Aleksic and Q. Gao, Energy-efficient routing protocol for wireless sensor networks based on improved grey wolf optimizer, KSII Transactions on Internet and Information Systems, 2018.
- [7] X. Zhao , S. Ren ,H. Quan and Q. Gao , Routing protocol for heterogeneous wireless sensor networks based on a modified grey wolf optimizer, Sensors ,2020.
- [8] S. Al-Khammasi, D. Alhelal and N. Salih Ali, Energy efficient cluster based routing protocol for dynamic and static nodes in wireless sensor network, TELKOMNIKA .2018.
- [9] Y R. Sadek, G. Selim and T. Abdel-Hakam, A novel energy efficient vice cluster head routing protocol in wireless sensor networks, IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS),2015.
- [10] N. A. Al-Aboody & H. S. Al-Raweshidy, Grey wolf optimization-based energy-efficient routing protocol for heterogeneous wireless sensor networks", IEEE, 2016.
- [11] A. Rai, and M. Sharma, Wireless sensor network using tabu searching algorithm and fuzzy inference system, International Journal of Recent Technology and Engineering (IJRTE) ,2019.
- [12] P. Subramanian, J. Martin Sahayaraj, S. Senthilkumar and D. Stalin Alex, A hybrid grey wolf and crow search optimization algorithm-based optimal cluster head selection scheme for wireless sensor network.", Springer, 2020.
- [13] Z. Ming Gao and J. Zhao, An improved grey wolf optimization algorithm with variable weights", Hindawi Computational Intelligence and Neuroscience ,2019.
- [14] P. HU , S. CHEN, H. HUANG, G. ZHANG, and L. LIU, " Improved alpha-guided grey wolf optimizer", IEEE Access ,2018.
- [15] M. Sharawi & E. Emary, " Impact of grey wolf optimization on wsn cluster formation and lifetime expansion", IEEE ,2017.
- [16] A. Rathee, R. Singh & A. Nandini, Wireless sensor network- challenges and possibilities, International Journal of Computer Applications, 2016.
- [17] M. Akhtar , A. Ali , Z. Ali , M. Hashmi and M. Atif, Cluster based routing protocols for Wireless Sensor Networks: An Overview", (IJACSA) International Journal of Advanced Computer Science and Applications ,2018.
- [18] H. Faris I. Aljarah, M. Al-Betar, and S. Mirjalili, Grey wolf optimizer: a review of recent variants and applications", Neural Computing and Applications,2018.
- [19] A. Yadav and S. Kumar, Energy efficient cluster formation in wireless sensor networks using particle swarm optimization, Indian Journal of Science and Technology,2017.
- [20] W. Long & S. Xu , " A novel grey wolf optimizer for global optimization problems, IEEE ,2016.
- [21] H. Orojloo & A. Haghghat , A tabu search based routing algorithm for wireless sensor Networks , Springer , 2016.
- [22] M. Singh Manshabia: Wireless sensor networks: a survey ", International Journal of Scientific & Engineering Research, 2016.
- [23] H. M. Salman, Survey of routing protocols in wireless sensor networks, nternational Journal of Sensors and Sensor Networks,2014.
- [24] A. Sabri , K. Al-Shqeerat, Hierarchical cluster-based routing protocols for wireless sensor networks – a survey, IJCSI International Journal of Computer Science Issues,2014.
- [25] A. Singh , Dr. S.B. Rana, Heterogeneous routing protocols in wireless sensor network: a survey, International Research Journal of Engineering and Technology (IRJET),2015.
- [26] S.P. Singh,S.C. Sharma, A survey on cluster based routing protocols in wireless sensor networks, International Conference on Advanced Computing Technologies and Applications (ICACTA),2015.

Improved GRASP Technique based Resource Allocation in the Cloud

Madhukar E¹

Associate Professor, CSE
Sreenidhi Institute of Science and Technology
Hyderabad, India

Ragunathan T²

Professor & Dean, CSE
SRM University
Amaravathi, India

Abstract—In the era of cloud computing, everyone is somehow using cloud resources. However, the resources are limited in the Cloud. Cloud vendors look for enhanced returns on investments. Promising return on investment is possible only when the cloud resources are scheduled efficiently to execute jobs within the stipulated time. However, brute force methods require exponential time to produce a schedule. Heuristic and meta-heuristic algorithms have been proposed in the literature to allocate resources to the jobs. These algorithms still suffer from slow convergence. To overcome this problem, researchers clubbed various heuristics and meta-heuristic to form a new hybrid algorithm. With the same motive, this paper explores the limitations of greedy random adaptive search and shows that learning through a fixed set search enhances efficiency. Based on the results, it can be concluded that the proposed algorithm is on par with existing hybrid meta-heuristic algorithms.

Keywords—Cloud computing; task scheduling; meta-heuristics; fixed set search; GRASP; resource allocation

I. INTRODUCTION

Cloud computing is one of the emerging technologies in this era. It creates a new paradigm in information technology and computing. Conventional computing methods are ousted by Cloud computing by making "usage of computing as a utility" [1] which is charged on pay-as-you-use provision similar to "utilities like water, electricity, gas, and internet" [1].

Cloud provides a metered service that automatically delivers services when and where they are needed. It provides virtualized, well-managed, abstracted, and on-demand compute, storage, and network services with a deep internet backbone.

While cloud computing has origins in Cluster, Parallel, and Grid computing, it differs in terms of virtualization, resource pooling, elasticity, and heterogeneity from these technologies. The Cloud imposes several challenges to provide the features.

The challenges range from security, privacy, scalability, fault tolerance, energy consumption, interoperability, and scheduling. Cloud vendors have to be cautious with all these challenges to dispense the service to the users. It is an arduous task to stick to the service level agreement (SLA). Violations of SLA lead to many legal problems.

Resource scheduling is required to balance the service provider's challenges and fulfill the cloud user's requirements.

However, resource scheduling is an NP-hard problem. With exhaustive search, it takes a longer time to give the schedule. Within a polynomial-time, it is not proven to give an optimal solution.

Cloud computing provides an infinite number of resources on demand. The users can focus on business innovations rather than focussing on the accumulation of physical resources. Its pervasiveness helps the users by providing the resources on-demand, convenient, and tailored to the requirements. Many start-ups can effectively utilize the services offered by cloud vendors. Special pricing schemes are offered to the corporate users, as the resources are needed at a large scale. The services can be divided into IaaS, PaaS, and SaaS. The phrase "everything as service" XaaS was termed in [2]. Many companies have moved to the Cloud to compute and store information. The characteristics of cloud computing benefit both cloud providers and users.

Three types of clouds exist based on their ownership. Public, private, and hybrid clouds fulfill the user's requirements. Public Cloud is made up of resources of third-party companies. Private clouds, in general, will be located on the premises of the organizations. Hybrid clouds consist of combined features of public and private clouds.

Resource scheduling in a Cloud computing environment is an important phenomenon. Researchers have been proposing new heuristic and metaheuristic algorithms. In this paper, an improved Greedy randomized adaptive search algorithm has been proposed. The learning mechanism is added to the existing algorithm. It is shown that the algorithm's simplicity is not lost even after the addition of the learning to the existing algorithm. Tasks will be allocated to the virtual machines with efficiency. The main objective is to minimize the makespan.

A. GRASP

The "Greedy Random Adaptive Search Procedure (GRASP)" [3] is one among many familiar meta-heuristic algorithms proposed by Feo and Resende. It helps to solve the NP hard problems, precisely like combinatorial problems. This algorithm has two phases in each iteration. The algorithm begins with a "randomized greedy allocation" [3]. The second phase will be added with a procedure of local search with existing solutions. If any improvement is added to the existing solution in the objective function, the new solution is considered a new incumbent solution. This procedure is

continued till it reaches an optimal solution or to stopping criteria. However, it has a limitation of not learning.

The addition of the local search method improves the performance of the metaheuristic algorithm. Hybridization is such a process that can combine one or more metaheuristics, to enhance efficiency. However, complexity may be increased if such hybridization is done.

Model-based heuristic algorithms are made up of identifying sets of parameters that define that model and help to find the target in the search space. These algorithms progressively modify their model after every iteration. In turn, the possibility of finding a quality solution is increased. The learning mechanism is part of Swarm intelligence, in which the information will be shared among the particles (components) so that the direction of the search will be changed. More emphasis is put on the learning mechanism in the recent past. In this phase, the focus is maintained to collect the information to enhance the quality of the solution.

GRASP algorithm falls into the class of population-based metaheuristics. The greedy function and stochastic model clubbed together to improve the efficiency of the algorithm. In addition to the GRASP, instances such as Semi-greedy heuristics[4] prove that rather than complex algorithms, simple algorithms also can give promising results.

In this paper, the boundaries of GRASP are extended by adding a learning mechanism [5]. A few examples of such methods are the "Dynamic Convexized method" [6] and "GRASP with Path relinking" [7]. These two algorithms show instances of intensified foraging behavior in the solution space. A significant level of improvement was shown with these methods.

The majority of the existing hybridized methods focus on the best quality solutions found so far to enhance the quality of the solution. However, algorithms like ACO use the elements of high-quality solutions with probability. The cross-entropy method (CE) [8] is akin to the concept in which the solutions are constructed based on the frequency of the elements from high-quality solutions. In the proposed algorithm, the focus is on the best elements of the finest solutions. The existing GRASP will be added with the theory of fixed set search to learn and select elements that direct towards the solution. Based on the prevalence of the elements which are part of high-quality solutions, a new solution is constructed.

II. RELATED WORK

Scheduling started way back in Johnson's proposed work [9] to use the machinery efficiently as part of manufacturing. Scheduling had taken new directions with the invention of operating systems in computers. However, scheduling methods which have been part of the operating system are not suitable for the Cloud.

The Grid computing algorithms were tailor-made to suit Cloud computing. Batch and online mode heuristic [10] algorithms are two types of requirements for scheduling in the Cloud. Min-Min, Max-min, Round robin, and FCFS are part

of batch mode. Most-fit task scheduling falls into online scheduling.

A. Deterministic and Exhaustive Algorithms

Online mode heuristic algorithms (OMHA) and batch mode heuristic algorithms (BMHA) [10] are two categories of scheduling algorithms in the Cloud. "First Come First Serve (FCFS), Round Robin(RR), Min- Min algorithms, and Max-Min algorithms come under BMHA. Most Fit Task Scheduling(MFTS) algorithms come under OHMA, in which schedule will be done when the job is received" [11]. First come, first serve, Shortest time remaining job, Priority scheduling, and Round-robin are not optimal for the Cloud.

The deterministic and exhaustive algorithms are two methods for scheduling algorithms. Both these methods are not suitable for large-scale environments like clouds. It is evident that finding the optimal solution within the polynomial-time for such NP-hard problems is not possible. The metaheuristic algorithms [12] could find the solutions within a short time by compromising the optimality. Simulated annealing(SA), Genetic algorithm (GA), Ant colony optimization, Particle swarm optimization (PSO) are a few such metaheuristic algorithms. Analytical Hierarchical processing was applied to prioritize the tasks in [13], which proved that there is some improvement in the makespan

B. Metaheuristic Scheduling Algorithms

The term "metaheuristic" was coined by Fred Glover in 1986 [14]. It indicates a heuristic with a non-problem-specific approach, and it is a combination of exploration and exploitation.

Applying metaheuristic algorithms for scheduling in the Cloud has become a common practice because of its efficiency. One among many such algorithms is ant colony optimization. It proved a significant improvement in the time complexity for optimization problems. It also proved that a near-optimal solution could be achieved by iteration after iteration. One such algorithm is proposed and applied by M. A Tawfeek et al. [15]. They compared with FCFS and round-robin algorithms. Since then, many researchers have shown some improvement by either hybridization or adding extra features.

Moon et al. [16] discuss ant colony optimization-based task scheduling. They claim that the global optimization problem was solved with slave ants by avoiding long paths where pheromone gets accumulated. Z. Chen *et al.* [17], used multiple populations in ACO to solve two objectives in the Cloud. They dealt with a new pheromone update by using non-dominated solutions from the global archive to guide a complementary heuristic to avoid the single-objective optimization.

In [18], the authors proposed an algorithm in which the greedy strategy is combined with the GA algorithm. They show that their method shows better results in task scheduling. The Differential algorithm in [19] was considered as one of the simple algorithms to search for the optimal solutions in the search space. To derive potential off-springs, better individuals were applied with the Taguchi method. In [20], the moth search algorithm and differential algorithms were

hybridized. In the presence of Levy flights, they used a differential evolutionary algorithm to enhance the exploitation potential and used phototaxis for explorations. In [21], the authors integrate project scheduling along with the workflow scheduling problem. Two artificial bee colony algorithms proposed by them help to solve the workflow scheduling. They claim that their method is practically applicable for complicated workflow scheduling problems. In [22], the researchers discuss the provision of resources with QoS such as makespan, cost, and task migration reduction. They show that their method achieves better results with their objectives with improved efficient artificial bee colony. In [23], by using whale optimization, they proposed a W-scheduler. Multi-objectives were proposed and compared with PBACO, SLPSOSA, and SPSO-SA. Agarwal et.al. [24], discusses the application of genetic algorithms. They discuss mainly the distribution of the load among the virtual machines. They compare it with FCFS and prove that their method outperforms in terms of QoS.

C. Maintaining the Integrity of the Specifications

The initial stages of the metaheuristic algorithm exhibit divergence, which covers a large search space, and decreases as the solution is near-optimal. Premature and slow convergence [12] are the problems with existing metaheuristic algorithms. The probability of achieving an optimal solution with high diversity is maximum. This high diversity suffers from slow convergence. Contrary to this, the convergence might be fast with a less accurate solution if divergence is less. To enhance the efficiency of the metaheuristic algorithm, it has become a general practice to add two or more metaheuristic algorithms to form a new hybrid algorithm.

Generally, three kinds of combinations [12] are used to hybridize the algorithms. The first type is a mix of population-driven and single solution-based algorithms. Combining two population-based algorithms is the second type, and the combination of metaheuristic and heuristic algorithms is the third type.

In [25] and [26], the authors fused the Genetic algorithm with the Particle swarm optimization algorithm (HGPSO) and the Genetic algorithm with Ant colony optimization (HGA-ACO), respectively. In the former algorithm, the initial population is generated by GA, and the individuals with good fitness are selected as candidates for PSO. In the latter, the efficient pheromone for ant colony optimization is initialized using a genetic algorithm. The ACO is used to improve GA solutions for crossover GA action. The findings of the experiments demonstrate that the suggested system performs well in terms of mission allocation and maintaining service efficiency parameters.

Two-hybrid metaheuristic algorithms have been introduced [27] by Ben Alla, H. et al. PSO, which is hybridized with fuzzy logic, is the first proposed algorithm. Simulated annealing is combined with PSO in the second algorithm. They use Dynamic dispatch queues for these algorithms. Discrete PSO has been combined [28] with a local search in which the authors use hill climbing for the avoidance of local optima. They claim that their algorithm has shown better performance in the minimization of makespan. In [29-

32], PSO and fruit fly algorithms (FOA) were merged. The essential parameters, position, and velocity of PSO have been redefined. With the help of a fruit fly smell operator, the issue of prematurity has been resolved.

III. PROPOSED WORK: IMPROVED GRASP ALGORITHM

Fixed set search and GRASP are combined to make an improvement in the performance of the algorithm to allocate jobs to VMs.

A. General Procedure for GRASP

As GRASP is an iterative process [3], each iteration consists of the construction phase and a local search phase. A feasible solution is built iteratively, one element at a time in the development process. The choice of the next element to be added is decided at each construction iteration by ordering all the elements in a candidate list with respect to a greedy function. The pseudocode for GRASP is presented in Fig. 1 with algorithm 1.

The advantage of choosing each element is calculated. The heuristic is adaptive because, during each iteration of the construction process, the benefit associated with each element is modified to accommodate the improvements made by the previous element's selection.

Algorithm 1. Pseudocode – GRASP

```
while GRASP Stop Criteria not Satisfied do
    create solution Sol using greedy random method
    local search (Sol)
    update if Sol is the new best
end while
```

Fig. 1. Pseudo Code for GRASP.

The "Restricted candidate list (RCL)" [3] is labeled by considering the list of best candidates. This technique makes it possible to obtain new solutions in every iteration of GRASP without compromising the power of adaptive greedy processes.

The procedure for creating the initial population is presented in algorithm 2, Fig. 2, J is a set of n jobs represented with J_1, J_2, \dots, J_n . In this discussion, tasks and jobs are considered the same for simplicity. VM is a set of virtual machines denoted with $VM_1, VM_2, VM_3, \dots, VM_n$. The greedy adaptive random search procedure is applied to generate an initial population Pop. This procedure is presented in Fig. 2 in algorithm 2.

Algorithm 2: Generate the initial population with GRASP

```
1.  $J = \{J_1, J_2, J_3, \dots, J_n\}$  is the set of jobs
2.  $VM = \{VM_1, VM_2, VM_3, \dots, VM_n\}$ 
3. Pop = { } // null
4. while not completed, do
5.     Pop = Pop U Apply GRASP and allocate jobs to VMs
6.     calculate the overall completion time
7. end while
8.  $R_{mbest} = AGRASP(Pop, n)$ 
9. end.
```

Fig. 2. Algorithm to Generate Initial Population and RCL.

The set of solutions generated by GRASP will be sorted according to the overall completion time. RCL is helpful in reducing the search space. Top 'm' best solutions considered, and in the present case, RCL is stored in the R_{mbest} . This procedure is presented in Fig. 3 in algorithm 3.

Algorithm 3: AGRASP

1. Algorithm(Pop,n)
 2. Sort the jobs in increasing order of execution time
 3. temp=Select top 'm' elements from the sorted list of jobs
 4. return(temp)
 5. end
-

Fig. 3. AGRASP for Best Solutions.

The solution created by GRASP may not be locally optimal. It adds benefits by applying local search. Iteratively, a local search algorithm operates by successively substituting the incumbent solution with a more robust solution in the neighborhood.

The right choice of the neighborhood structure with good neighborhood search techniques and a better initial solution leads to a thriving local search. Exponential time may be required for such a local optimization procedure as it starts arbitrarily. However, efficiency improves significantly with the best initial solution. As it is known that the initial population is generated with greedy random selection in the GRASP algorithm, the algorithm may not be optimal. But with the help of local search like, 2-opt, or 3-opt there can be improvements. The procedure for the local search is shown in the following algorithm 4 in Fig. 4.

Algorithm 4: Procedure for the Local search

1. Local search(LS(RCL))
 2. Swap two randomly selected allocations.
 3. Calculate the overall completion time.
 4. If the newly calculated completion time is less than the best
 5. best= new best
 6. end
-

Fig. 4. Algorithm for Local- Search.

B. Fixed Set Search (F-GRASP)

GRASP algorithm does not incorporate any learning in its iterations [5]. The idea of the addition of "learning" called fixed set search(FSS) was proposed in [5]. This added feature will not affect the simplicity of the GRASP algorithm in both calculations and complexity. This learning is used in this paper to address the scheduling in the Cloud.

To make fixed set search more efficient, two rules are used. First, the solution space can be minimized by fixing certain sections of the solution. Second if a large number of good solutions are considered, there might be some similarities among them. A fixed set is defined as the set created by these standard components. It is possible to discover a near-optimal solution by "filling the gap."

FS represents a fixed set. The set consists of the elements which help to generate the best solutions. The following requirements should be satisfied by the proposed method.

First, the engendered fixed set FS should consist of elements from the best solutions. Second, it should be able to generate random fixed sets. In turn, these sets should help to generate high-quality solutions. Third, feasible solutions should be generated from fixed set FS. Fourth, the capability to monitor the number of elements in the fixed set generated should be possible.

The random selection of high-quality solutions can achieve the first and second requirements. Select k random solutions from the set Pop and store in a set $R_{mbest} = \{R_1, R_2, R_3...R_k\}$. The set of edges $Ed = \{ed_{11}, ed_{12}...ed_{1j}, ed_{21}, ed_{2j}...ed_{ij}, ed_{ij}\}$, $i \in |J|, j \in |VM|$, denotes the solution. The representation ed_{ij} is used to indicate that job 'i' is delegated to VM 'j'. A cost function $C(ed_{ij}, R_{mbest})$ equal to '1' if $ed_{ij} \in R_{mbest}$ and '0' otherwise. If job 3 is allocated to VM 4, for example, and is present in R_1, R_2 , and R_4 . The cost function gets calculated as follows.

$$T(ed_{3,4}, \{R_1, R_2, R_3, R_4\}) = C(ed_{3,4}, R_1) + C(ed_{3,4}, R_2) + C(ed_{3,4}, R_3) + C(ed_{3,4}, R_4).$$

The count is 3.

$$T(ed_{i,j}, R_{mbest}) = \sum_{R_k \in R_{mbest}} C(ed_{i,j}, R_k) \quad (1)$$

The size of the FS has to be adaptable. It will be fixed to a value, and changes made as required. To simplify, Eq. (2) is used.

$$maxsize[i] = |J| - \left\lfloor \frac{|J|}{2^i} \right\rfloor \quad 'i' \text{ is the iteration number} \quad (2)$$

The fixed set size is initialized to $maxsize$ and changes after each iteration. If the number of jobs is 5, then the size of the fixed set can be considered as 3. This indicates that three assignments from the fixed set with the highest count for edges will be considered.

The notation F-GRASP is considered for fixed set search GRASP. Fig. 5 explains the procedure for finding the best allocation with F-GRASP. The notation Pop_n, R_{mbest} represent the initial population and RCL, respectively.

Algorithm 5. Pseudo-code for the fixed set search

1. Popn represents initial population using GRASP with n elements
 2. $R_{mbest} = \{R_1, R_2, R_3...R_k\}$ where $R_i \in Pop_n, i \in N, 1 \leq i \leq k$
 3. Count= $T(ed_{i,j}, R_{mbest})$ //find the frequency of each edge with Eq. (1)
 4. Set FS= $\{ed_1(jobi, vmk), ed_2(jobi, vmk), ... ed_{maxsize}(jobi, vmk) \}$
 5. Allocate the jobs to VMs according to FS.
 6. Allocate the remaining jobs according to GRASP
 7. while stopping criteria not reached do
 8. Apply local search to S
 9. end while
-

Fig. 5. Algorithm F-GRASP.

The set FS is used to store the edges with the highest allocation. By considering the fixed set with the highest count, an initial allocation in the solution space is done. The remaining allocation is done with the GRASP. By this, it reduces the number of iterations. After fixing the allocation, the total completion time will be calculated. The swap in the allocation of the jobs is done till there is no improvement in

the makespan. The same is explained with an example in section 4.

Table I is considered for the execution times of each job on every VM. $J_1, J_2, J_3, J_4,$ and J_5 are the given jobs. $VM_1, VM_2, VM_3, VM_4,$ and VM_5 are the VMs available for allocation. The challenge is to allocate the jobs to VMs with minimum makespan by the scheduler.

Table II consists of the initial population represented by Pop_n . For example, the representation $J_1 \rightarrow VM_1, J_5 \rightarrow VM_2, J_1 \rightarrow VM_3, J_3 \rightarrow VM_4, J_4 \rightarrow VM_5$ considered as one of the allocations.

For each allocation, fitness (total execution time) is calculated and sorted in ascending order of fitness function. Table III holds these values. Top 'm' best allocations considering fitness function are selected.

C. Worked Out Example

Table I is considered for the execution times of each job on every VM. $J_1, J_2, J_3, J_4,$ and J_5 are the given jobs. $VM_1, VM_2, VM_3, VM_4,$ and VM_5 are the VMs available for allocation. The challenge is to allocate the jobs to VMs with minimum makespan by the scheduler.

Table II consists of the initial population represented by Pop_n . For example, the representation $J_1 \rightarrow VM_1, J_5 \rightarrow VM_2, J_1 \rightarrow VM_3, J_3 \rightarrow VM_4, J_4 \rightarrow VM_5$ considered as one of the allocations.

For each allocation, fitness (total execution time) is calculated and sorted in ascending order of fitness function. Table III holds these values. Top 'm' best allocations considering fitness function are selected for allocation and presented in Table IV. This list is considered as RCL(Restricted Candidate List). R_{mbest} is the notation used for RCL. The allocation will be done randomly. As an example, an allocation of $J_3-J_5-J_4-J_1-J_2$ is considered. The execution time of J_3 on VM_1 is 11, J_5 on VM_2 is 10, J_4 on VM_3 is 14, J_1 on VM_4 is 9, J_2 on VM_5 is 9. The overall completion time $(11+10+14+9+9)$ is 53.

By applying a local search, there can be an improvement. However, in the proposed method, to reduce the number of swaps as part of 2-opt, a fixed set is introduced.

Equ. (2) calculates the size of the fixed set—the number of VMs=5. Hence the maxsize=3. From Table IV, allocation with minimum completion time is $J_3 \rightarrow VM_1, J_5 \rightarrow VM_2, J_4 \rightarrow VM_3, J_1 \rightarrow VM_4, J_2 \rightarrow VM_5$.

Frequency of the allocation is counted with variable Count. $Count(J_3, VM_1) = 1, Count(J_5, VM_2)= 2, Count(J_4, VM_3)= 1, Count(J_1, VM_4) = 1, Count(J_2, VM_5) = 4.$ From the values, it is evident that allocation of J_5 to VM_2 has a count as 2, and J_2 to VM_5 as 4. As the remaining counts are not considerable, the fixed set holds the two allocations. The fixed set is $FS=\{(J_5, VM_2), (J_2, M_5)\}$, therefore the new allocation is

$$\{ J_5 \rightarrow VM_2, J_2 \rightarrow M_5 \}$$

TABLE I. EXECUTION TIME OF JOBS ON EACH VM

Execution times of a job on a Virtual machine					
	VM ₁	VM ₂	VM ₃	VM ₄	VM ₅
J ₁	13	10	18	9	13
J ₂	19	18	15	11	9
J ₃	11	15	12	10	18
J ₄	11	15	14	11	19
J ₅	10	10	13	11	14

TABLE II. INITIAL POPULATION

Initial Population Pop _n				
VM ₁	VM ₂	VM ₃	VM ₄	VM ₅
J ₂	J ₅	J ₁	J ₃	J ₄
J ₃	J ₄	J ₅	J ₂	J ₁
J ₄	J ₅	J ₁	J ₃	J ₂
J ₁	J ₂	J ₃	J ₅	J ₄
J ₄	J ₃	J ₁	J ₂	J ₅
J ₁	J ₄	J ₃	J ₅	J ₂
J ₃	J ₅	J ₄	J ₁	J ₂
J ₅	J ₃	J ₂	J ₄	J ₁
J ₁	J ₃	J ₅	J ₄	J ₂
J ₄	J ₂	J ₁	J ₅	J ₃
J ₁	J ₂	J ₅	J ₃	J ₄
J ₄	J ₅	J ₃	J ₁	J ₂
J ₄	J ₂	J ₅	J ₃	J ₁
J ₂	J ₅	J ₄	J ₃	J ₁
J ₂	J ₄	J ₃	J ₅	J ₁

TABLE III. SORTED LIST OF VMs

Sorted list of allocation of jobs to VMs Pop _n					Total execution time
J ₃	J ₅	J ₄	J ₁	J ₂	53
J ₄	J ₅	J ₁	J ₃	J ₂	58
J ₁	J ₄	J ₃	J ₅	J ₂	60
J ₁	J ₃	J ₅	J ₄	J ₂	61
J ₃	J ₄	J ₅	J ₂	J ₁	63
J ₅	J ₃	J ₂	J ₄	J ₁	64
J ₄	J ₂	J ₅	J ₃	J ₁	65
J ₂	J ₅	J ₄	J ₃	J ₁	66
J ₄	J ₃	J ₁	J ₂	J ₅	69
J ₂	J ₄	J ₃	J ₅	J ₁	70
J ₁	J ₂	J ₃	J ₅	J ₄	73
J ₁	J ₂	J ₅	J ₃	J ₄	73
J ₂	J ₅	J ₁	J ₃	J ₄	76
J ₄	J ₂	J ₁	J ₅	J ₃	76

TABLE IV. SELECTION OF BEST CANDIDATES

R_{mbest} = Best Candidates selected from Pop_n					
J_3	J_5	J_4	J_1	J_2	53
J_4	J_5	J_1	J_3	J_2	58
J_1	J_4	J_3	J_5	J_2	60
J_1	J_3	J_5	J_4	J_2	61
J_3	J_4	J_5	J_2	J_1	63

The greedy random method can be applied to the remaining. For VM_1 the jobs J_1 , J_3 , and J_4 are the choices. As J_3 and J_4 are the same, VM_1 decisions cannot be taken. Move on to the next VM, i.e., on to VM_3 . J_3 's execution time is minimum on VM_3 . Based on this, J_3 is allocated to VM_3 . VM_4 is left with J_1 and J_4 . Here, J_1 having less execution time, hence assigned to VM_4 . VM_1 will be allocated with J_4 . VM_1 can be allocated either with J_3 or J_4 as they both have equal values. Here, J_3 is allocated to VM_3 . And VM_1 is left with J_4 and is allocated. The overall completion time is 51, which is the newly updated value. The best solution is shown in Table V.

TABLE V. FINAL ALLOCATION

VM_1	VM_2	VM_3	VM_4	VM_5	Completion time
J_4	J_5	J_3	J_1	J_2	51

IV. RESULT

The proposed algorithm is implemented in MATLAB R2020a. Computations are performed on a PC with Intel core™ i7 CPU@1.80-GHz with 8 GB of RAM. The comparison is done among three algorithms. The Genetic algorithm(GA), Fixed set search-GRASP from now considered as (F-GRASP), GRASP are chosen for comparison. The overall completion (makespan) time is calculated. The allocation with minimum overall completion time is considered as the best allocation. However, as the scheduling is NP-complete, the near-optimal allocation changes in each run. With 10 jobs, and in 100 iterations, the best makespan with the algorithms GA=140, F-GRASP=148, GRASP=160, with 200 iterations GA=134, F-GRASP=132, GRASP=133, 300 iterations GA=133, F-GRASP=130, GRASP=135, 400 iterations GA=133, F-GRASP=130, GRASP=132, and after 500 iterations GA=132 F-GRASP=129 GRASP=131, GA=132, F-GRASP= 130 GRASP=130. The results show that the proposed algorithm is equally competing with existing metaheuristic algorithms like the Genetic algorithm and GRASP. In some instances, it is showing better results than the algorithms with which it has been compared.

The usage of fixed set search reduces the search space. Thus it converges with the near-optimal solution faster than the other two algorithms. Fig. 6. represents the number of iterations on the X coordinate and best makespan on the Y coordinate. F-GRASP shows promising results with the Genetic algorithm and GRASP.

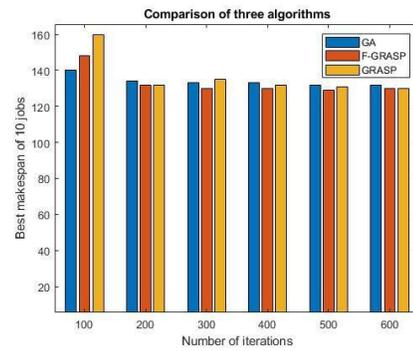


Fig. 6. Comparison of Makespan of F-GRASP with GA and GRASP.

V. CONCLUSION AND FUTURE WORK

This paper discusses the limitations of the GRASP algorithm. Learning is added to improve the efficiency of the algorithm. With the inclusion of a fixed set search, the learning is accomplished. The algorithm's search space reduces by accumulating the elements of high-quality solutions. The algorithm starts with a greedy random approach, and each iteration shows some improvement and finally reaches an optimal solution. The algorithm shows remarkable improvement in performance. While the addition of fixed set search and the 2-Opt algorithm strengthens the algorithm significantly, there is still space to test with 3-Opt or 4-Opt algorithms. The proposed algorithm is evaluated using MATLAB. The time complexity is $O(2^n n^2)$ and space complexity is $O(n^2)$. Alternative methods can be explored to reduce the time complexity. The open-source cloud platforms such as Open stack or Cloud stack by interested researchers with the proposed algorithm.

REFERENCES

- [1] Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the 5th utility. *Future Generation computer systems*, 25(6), 599-616.
- [2] Y. Duan, G. Fu, N. Zhou, X. Sun, N. C. Narendra and B. Hu, "Everything as a Service (XaaS) on the Cloud: Origins, Current and Future Trends," 2015 IEEE 8th International Conference on Cloud Computing, New York, NY, 2015, pp. 621-628, doi: 10.1109/CLOUD.2015.88.
- [3] Feo, T.A., Resende, MGC Greedy Randomized Adaptive Search Procedures. *JGloboptim* 6, 109–133(1995). <https://doi.org/10.1007/BF01096763>.
- [4] J.P. Hart and A.W. Shogan. Semi-greedy heuristics: An empirical study. *Operations Research Letters*, 6:107–114, 1987.
- [5] Jovanovic R., Tuba M., Voß S. (2019) Fixed Set Search Applied to the Traveling Salesman Problem. In: Blesa Aguilera M., Blum C., Gambini Santos H., Pinacho-Davidson P., Godoy del Campo J. (eds) *Hybrid Metaheuristics. HM 2019. Lecture Notes in Computer Science*, vol 11299. Springer, Cham. https://doi.org/10.1007/978-3-030-05983-5_5.
- [6] Zhu, M., Chen, J.: Computational comparison of GRASP and DCTSP methods for the Traveling Salesman Problem, pp. 1044–1048 (2017).
- [7] Festa, P., Resende, MGC: Hybridizations of GRASP with path-relinking. Talbi, E.G. (ed.) *Hybrid Metaheuristics. Studies in Computational Intelligence*, vol. 434, pp. 135–155. Springer, Heidelberg (2013). https://doi.org/10.1007/978-3-642-30671-6_5.
- [8] De Boer, P.T., Kroese, D.P., Mannor, S., Rubinstein, R.Y.: A tutorial on the cross entropy method. *Ann. Oper. Res.* 134(1), 19–67 (2005).

- [9] S. M. Johnson, "Optimal two- and three-stage production schedules with setup times included," *Naval Res. Logistics Quart.*, vol. 1, no. 1, pp. 61–68, 1954.
- [10] S. Dubey, V. Jain and S. Shrivastava, "An innovative approach for scheduling of tasks in cloud environment," 2013 Fourth International Conference on Computing, Communications and Networking Technologies (ICCCNT), Tiruchengode, 2013, pp. 1-8, doi: 10.1109/ICCCNT.2013.6726727.
- [11] E. Madhukar and T. Ragunathan, "Dynamic and Static Characteristics Based Algorithm to Allocate VMs to Jobs in the Cloud," in 2016 International Conference on Information Technology (ICIT), Bhubaneswar, 2016 pp. 81-86. doi: 10.1109/ICIT.2016.028.
- [12] Metaheuristic Scheduling for Cloud: A Survey Chun-Wei Tsai and Joel J. P. C. Rodrigues Senior Member, IEEE.
- [13] A. Makwe and P. Kanungo, "Scheduling in cloud computing environment using analytic hierarchy process model," 2015 International Conference on Computer, Communication and Control (IC4), Indore, 2015, pp. 1-4, doi: 10.1109/IC4.2015.7375723.
- [14] Mohamed Abdel-Basset, Laila Abdel-Fatah, Arun Kumar Sangaiah, Chapter 10 - Metaheuristic Algorithms: A Comprehensive Review, Editor(s): Arun Kumar Sangaiah, Michael Sheng, Zhiyong Zhang, In Intelligent Data-Centric Systems, Computational Intelligence for Multimedia Big Data on the Cloud with Engineering Applications, Academic Press, 2018.
- [15] M. A. Tawfeek, A. El-Sisi, A. E. Keshk, and F. A. Torkey, "Cloud task scheduling based on ant colony optimization," 2013 8th International Conference on Computer Engineering & Systems (ICCES), Cairo, 2013, pp. 64-69, doi: 10.1109/ICCES.2013.6707172.
- [16] YoungJu Moon, HeonChang Yu, Joon_Min Gil & JongBeom Lim. A slave ants based ant colony optimization algorithm for task scheduling in cloud computing environments. *Hum. Cent. Comput. Inf. Sci.* 7, 28 (2017). <https://doi.org/10.1186/s13673-017-0109-2>.
- [17] Z. Chen et al., "Multi-objective Cloud Workflow Scheduling: A Multiple Populations Ant Colony System Approach," in *IEEE Transactions on Cybernetics*, vol. 49, no. 8, pp. 2912-2926, Aug. 2019, doi: 10.1109/TCYB.2018.2832640.
- [18] Zhou, Z., Li, F., Zhu, H. et al. An improved genetic algorithm using greedy strategy toward task scheduling optimization in cloud environments. *Neural Comput & Applic* 32, 1531–1541 (2020). <https://doi.org/10.1007/s00521-019-04119-7>.
- [19] Jinn-Tsong Tsai, Jia-Cen Fang, Jyh-Horng Chou " Optimized task scheduling and resource allocation on cloud computing environment using improved differential evolution algorithm " <https://doi.org/10.1016/j.cor.2013.06.012>.
- [20] M.A. Elaziz, S. Xiong, K.P.N. Jayasena, et al., Task scheduling in cloud computing based on hybrid moth search algorithm and differential evolution, *Knowledge-Based Systems* (2019), <https://doi.org/10.1016/j.knsys.2019.01.023>.
- [21] Y. Liang, A. H. Chen and Y. Nien, "Artificial Bee Colony for workflow scheduling," 2014 IEEE Congress on Evolutionary Computation (CEC), Beijing, 2014, pp. 558-564, doi: 10.1109/CEC.2014.6900537.
- [22] Thanka, MR, Uma Maheswari, P. & Edwin, E.B. An improved efficient: Artificial Bee Colony algorithm for security and QoS aware scheduling in cloud computing environment. *Cluster Comput* 22, 10905–10913 (2019). <https://doi.org/10.1007/s10586-017-1223-7>.
- [23] Sreenu, K., Sreelatha, M. W-Scheduler: whale optimization for task scheduling in cloud computing. *Cluster Comput* 22, 1087–1098 (2019). <https://doi.org/10.1007/s10586-017-1055-5>.
- [24] Singh, P., Dutta, M. & Aggarwal, N. A review of task scheduling based on meta-heuristics approach in cloud computing. *Knowl Inf Syst* 52, 1–51 (2017). <https://doi.org/10.1007/s10115-017-1044-2>.
- [25] Senthil Kumar, A.M., Venkatesan, M. Task scheduling in a cloud computing environment using HGPSO algorithm. *Cluster Comput* 22, 2179–2185 (2019). <https://doi.org/10.1007/s10586-018-2515-2>.
- [26] Senthil Kumar, A.M., Venkatesan, M. Multi-Objective Task Scheduling Using Hybrid Genetic-Ant Colony Optimization Algorithm in Cloud Environment. *Wireless Pers Commun* 107, 1835–1848 (2019). <https://doi.org/10.1007/s11277-019-06360-8>.
- [27] Ben Alla, H., Ben Alla, S., Touhafi, A. et al. A novel task scheduling approach based on dynamic queues and hybrid meta-heuristic algorithms for cloud computing environment. *Cluster Comput* 21, 1797–1820 (2018). <https://doi.org/10.1007/s10586-018-2811-x>.
- [28] Mirsaeid Hosseini Shirvani, A hybrid meta-heuristic algorithm for scientific workflow scheduling in heterogeneous distributed computing systems, *Engineering Applications of Artificial Intelligence*, Volume 90, 2020, 103501, ISSN 0952-1976, <https://doi.org/10.1016/j.engappai.2020.103501>.
- [29] Bhushan, S. B., & Reddy, P. C. (2018). A Hybrid Meta-Heuristic Approach for QoS-Aware Cloud Service Composition. *International Journal of Web Services Research (IJWSR)*, 15(2), 1-20. doi:10.4018/IJWSR.2018040101.
- [30] Ayaluri MR, K. SR, Konda SR, Chidirala SR. 2021. Efficient steganalysis using convolutional auto encoder network to ensure original image quality. *PeerJ Computer Science* 7:e356 <https://doi.org/10.7717/peerj-cs.356>.
- [31] A. M. Reddy, V. V. Krishna, L. Sumalatha and S. K. Niranjana, "Facial recognition based on straight angle fuzzy texture unit matrix," 2017 International Conference on Big Data Analytics and Computational Intelligence (ICBDAC), Chirala, 2017, pp. 366-372, doi: 10.1109/ICBDACI.2017.8070865.
- [32] Ilaiah Kavati, A. Mallikarjuna Reddy, E. Suresh Babu, K. Sudheer Reddy, Ramalinga Swamy Cheruku, Design of a fingerprint template protection scheme using elliptical structures, *ICT Express*, 2021, ISSN 2405-9595, <https://doi.org/10.1016/j.icte.2021.04.001>.

Ada-IDS: AdaBoost Intrusion Detection System for ICMPv6 based Attacks in Internet of Things

A.Arul Anitha¹

Research Scholar, Department of Computer Science
St. Joseph's College (Autonomous)
Tiruchirappalli, Tamil Nadu, India
(Affiliated to Bharathidasan University, Tiruchirappalli)

Dr. L. Arockiam²

Associate Professor, Department of Computer Science
St. Joseph's College (Autonomous)
Tiruchirappalli, Tamil Nadu, India
(Affiliated to Bharathidasan University, Tiruchirappalli)

Abstract—The magical buzzword Internet of Things (IoT) connects any objects which are diverse in nature. The restricted capacity, heterogeneity and large scale implementation of the IoT technology tend to have lot of security threats to the IoT networks. RPL is the routing protocol for the constraint devices like IoT nodes. ICMPv6 protocol plays a major role in constructing the tree-like topology called DODAG. It is vulnerable to several security attacks. Version Number Attack, DIS flooding attack and DAO attack are the ICMPv6 based attacks discussed in this paper. The network traffic is collected from the simulated environment in the normal and attacker settings. An AdaBoost ensemble model termed Ada-IDS is developed in this research to detect these three ICMPv6 based security attacks in RPL based Internet of Things. The proposed model detects the attacks with 99.6% accuracy and there is no false alarm rate. The Ada-IDS ensemble model is deployed in the Border Router of the IoT network to safeguard the IoT nodes and network.

Keywords—IoT; ICMPv6; version number attack; DIS attack; DAO attack; Ada-IDS

I. INTRODUCTION

Internet of Things (IoT) is a network of embedded objects having unique identifier with sensing and actuation capacities and limited resources. IoT has the ability to connect any objects in the real world to the global network. Though IoT makes the people's life easier, it has lot of security issues and challenges. The privacy and security vulnerabilities increase as the global network includes greater number of connected devices from various fields and domain [1][2]. The large volume of connected devices in IoT network are uniquely identified using IPv6 addressing. IPv6 inherited several features from its previous version IPv4. So, it has the associated vulnerabilities of IPv4 and the specific security challenges of IPv6 [3]. These security threats have to be addressed in order to enhance the IoT security schemes.

IoT resource limited devices form Low-Power Lossy Networks (LLNs). To meet the requirements of the LLNs, the Routing Protocol for Low-Power Lossy Network (RPL) is designed. This RPL protocol is exposed to several security threats [4]. In RPL, the routing is performed by the control messages of the Internet Control Message Protocol version 6 (ICMPv6). The control messages construct a Destination Oriented Directed Acyclic Graph (DODAG). It is a tree structure with hierarchy of nodes with a single root node

called as Border Router which acts as a gateway to the global network [5].

The ICMPv6 messages are grouped as error messages and informational messages. The communication between the IPv6 nodes totally depends upon the ICMPv6 Protocol. It is also responsible for router and node configuration. The error messages have a preceding '0' in the high-order bit of the 'Type' field and the informational message contains a preceding '1' in the 'Type' field. ICMPv6 is the backbone of IPv6 and RPL as it has the building blocks such as DODAG Information Object (DIO), Destination Advertisement Object (DAO), DODAG Information Solicitation (DIS) and DAO-Acknowledgement (DAO-ACK) informational messages for constructing the DODAG for routing [6].

The root node initiates the DODAG formation by emitting DIO messages in a multicasting fashion. When a node receives the DIO message, based on the information available in the DIO message, it joins the DODAG and sends back the DAO message to the sender. Then it starts multicasting the DIO messages to its children. The DIO messages are regulated by the Algorithm. In order to identify the neighbors and join the DODAG, a node transmits DIS messages in a unicast or multicast manner. After receiving the DAO messages from the children, the parent node acknowledges the DAO message by sending DAO-ACK messages [7].

RPL and ICMPv6 protocols are prone to several security threats and attacks. According to Anthéa Mayzaud et al. [8], the attacks in RPL protocol are classified into three types such as attack against topology, attacks against resources and attacks against network. The attacks against the resources consumes more resources of the constrained devices, the attacks against topology cause sub-optimization and isolation in the topology and the attacks against the traffic creates security threats using the network traffic.

The ICMPv6 based attacks are created by manipulating the control messages. These attacks cause many damages to the networks. It also leads to Denial of Service (DoS) and Distributed Denial of Service (DDoS) in the resource constrained networks. Version Number attacks, DIS flooding attacks and DAO attacks are some of the ICMPv6 control message based attacks which lead to harmful effects in the IoT environment [9]. Machine Learning models are used to detect the intrusions from the network traces and log files. It is very

difficult to design IDS that performs well in terms of accuracy and less false alarm rate. Ensemble machine learning algorithms boosts the accuracy by combining many classifiers [10].

In this paper, an AdaBoost ensemble Intrusion Detection System called Ada-IDS is proposed to detect the Version Number attack, DIS flooding attack and DAO attacks in the IoT network. To develop this system, the IoT network communication traces are collected from the normal simulation environment and attack scenarios such as Version Number attack, DIS flooding attack and DAO attack. The Ada-IDS is developed by using the collected network traces. For that, the pre-processing and feature engineering processes are carried out on these collected data. Finally, an ensemble AdaBoost machine learning algorithms is applied on the collected dataset to build the Ada-IDS for detecting the ICMPv6 based attacks. The proposed Ada-IDS detects the Version Number Attack, DIS flooding attack and DAO attacks with 99.6% accuracy and with very less false alarm rate.

The rest of the paper is organized as follows: Section II explicates the related works of this research. The three ICMPv6 based attacks are explained in Section III. The Icmpv6 dataset used in this research and the proposed Ada-IDS is elaborately discussed in Section IV. The results obtained by the Ada-IDS model are presented in Section V. Finally, the Section VI concludes the paper.

II. RELATED WORK

Adnan Hasan Bdair et al. [11] critically reviewed the latest ICMPv6 based Intrusion Detection mechanisms with a special focus on the Denial of Service (DoS) and Distributed Denial of Service (DDoS) attacks. Three types of ICMPv6 based attacks such as ICMPv6 flood, ICMPv6 amplification and ICMPv6 protocol exploitation were addressed. Different types of Intrusion Detection systems for ICMPv6 based attacks were also explicated in this paper.

Arul Anitha et al. [12] proposed an Artificial Neural Network based Intrusion Detection System for Internet of Things using Multilayer Perceptron for detecting the Version Attacks and DIS attacks from the dataset collected from the Cooja Simulator and the proposed method classified the attacks and normal nodes correctly.

EmreAydogan et al. [13] developed a Centralized Intrusion Detection System for RPL based Industrial IoT using Genetic Programming concept. This system detects 'Hello Flood Attacks' and 'Version Number Attacks' using the Genetic Algorithm approach with 50 population and other default parameters. Network traces are not analyzed in this work.

Nour Mustafa et al. [14] developed an AdaBoost ensemble Network Intrusion Detection System (NIDS) by using Decision Tree (DT), Naive Bayes (NB) and Artificial Neural Network (ANN) algorithm. This system detects the application layer related IoT attacks. The UNSW-NB15 and NIMS botnet dataset were used to develop this ensemble model. According to their findings, the proposed model detects the attacks in the UNSW-NB15 dataset with 99.54% accuracy and NIMS botnet dataset with 98.29% accuracy.

Dan Tang et al. [15] proposed a multi-feature based AdaBoost system for detecting the low-rate Denial of Service (LDoS) attacks. At fixed time intervals the network traffics were captured and the obtained samples were analyzed using various statistical measures. The correlation scores between the features and the class labels were attained to choose the optimal feature set. Using the optimal features, the AdaBoost ensemble model was developed. NS2 simulator and a test-bed were used to evaluate the performance of the model and achieved 94.05% and 97.06% attack detection accuracy respectively.

A.R.Javed et al. [16] proposed an AdaBoost ensemble classifier to detect botnet attacks in connected vehicles. The decision tree algorithm was used as the base estimator and the cluster size was 100 in the AdaBoost algorithm. The performance of the AdaBoost classifier was compared with the decision tree, probabilistic neural network and sequential minimal optimization. According to their findings, the AdaBoost classifier outperformed other models and achieved 99.7% true positive rate and 99.1% accuracy.

Amin Shahraki et al. [17] performed a comparative analysis on various AdaBoost algorithms like Real Adaboost, Gentle Adaboost and Modest Adaboost using the well-known Intrusion detection datasets such as KDDCUP99, NSL-KDD, CICIDS2017, UNSW-NB15 and TRAbID. In this research, the authors identified that Gentle AdaBoost and Real AdaBoost performed better than the Modest AdaBoost algorithm. At the same time, the Modest AdaBoost algorithm was faster than the other AdaBoost algorithms.

III. ICMPV6 ATTACKS IN RPL BASED IOT

The ICMPv6 protocol is susceptible to various security threats and attacks. In this research, three ICMPv6 based attacks are implemented such as Version Number Attack DIS attack and DAO attack. The characteristics of these attacks are explained below:

A. Version Number Attacks

Version Number is an 8-bit number which denotes the Version of the DODAG topology. It is multicasted by the parent nodes using the DIO control message. Whenever there is an inconsistency in the DODAG, the global repair mechanism is initiated and the Version Number is updated by the root node. This updated information is multicasted from the root node via DIO control message. A Version Number Attacker without the knowledge of the root node updates the Version Number periodically and sends the updated version number using the DIO messages to its neighbors. On receiving this DIO message, the neighboring nodes join the global repair mechanism. Hence, the DODAG is reconstructed again and again. This malicious act affects the normal responsibilities of the legitimate nodes and consumes the constrained resources of the IoT devices. In the long run, it increases the control traffic while constructing the DODAG repeatedly in the network and this leads to Denial of Service (DoS) attacks [18][19].

B. DIS Flooding Attacks

This attack is created by manipulating the header details of the DIS messages. The DIS Control messages are used to probe its neighbors in order to join the DODAG. On receiving this DIS message, the neighbor nodes send back DIO messages to the sender. The Time duration for sending DIO messages is scheduled by the Trickle Timer. A DIS flooding attacker continuously multicasts DIS messages to its neighbors even though it received DIO message already. This heavy flooding of DIS messages in the network degrades the performance of the Network and leads to Denial of Service (DoS) attack [20].

C. DAO Attacks

DAO attack is generated by manipulating the DAO Control Message. When a Child node receives a DIO message from its parent, it has to send back a DAO message for maintaining the reverse root. The DAO message sent by the child node traverses multiple ancestors until it reaches the root node. A DAO attacker continuously transmits the DAO message to its parent list. All such unnecessary messages in the network have to be forwarded to the root node. It consumes more network resources and also prohibits the legitimate nodes to perform regular activities. Finally, the network will be in an inconsistent state which causes Denial of Service (DoS) attacks in the network [21].

These three attacks are created by using the ICMPv6 control messages which consumes more resources in the IoT network and reduces network performance. At last, all the three attacks lead to Denial of Service (DoS) attack which causes more damage to the RPL based IoT network.

IV. PROPOSED ADA-IDS MODEL

Network or Centralized Intrusion Detection System and Distributed Intrusion Detection System are the major two categories of IDS. In the centralized concept, the IDS is installed in the border router or a dedicated server. In the Distributed IDS, it is deployed in the client nodes. As the IoT nodes are resource constrained, the Distributed IDS concept is not suitable for limited resource devices.

The proposed Ada-IDS belongs to the Centralized IDS category. It monitors the nodes in the network and whenever there is an intrusion occurs, it raises an alarm to notify the admin about the issue. The various phases involved in developing the Ada-IDS are given in Fig. 1.

As it is given in Fig. 1, there are five phases for developing the Ada-IDS that are Data Collection Phase, Pre-Processing Phase, Feature Engineering Phase, Model Building Phase and Deployment Phase.

A. Data Collection Phase

The data is collected from the simulation environment. There are 50 normal client nodes, one root node and an attacker involved in the simulation. The Version Number Attack, DIS flooding Attack DAO attacks and a simulation without attacker are implemented in the Cooja simulator and the network traces from all these experimental setups were captured using the 6LoWPAN Analyzer tool. The simulation is performed for 30 minutes in each scenario. The captured packets are analyzed using the WireShark tool and the .pcap files were converted into .csv files. The file is named as 'Icmpv6.csv' that is used for building the Ada-IDS model. The collected dataset contains normal packets, Version Number Attacks, DIS flooding Attacks and DAO Attacks. The Normal and Attack instances are listed in Table I.

As it is given in Table I, there are 127684 samples in the dataset including 125184 Normal, 325 DIS Attacks, 1193 DAO Attacks and 982 Version Number Attacks. There are nine attributes in the dataset. The description of the dataset is given in Table II.

TABLE I. NORMAL AND ATTACK INSTANCES

S.No.	Type	No. of Packets
1.	Normal	125184
2.	DIS Attacks	325
3.	DAO Attacks	1193
4.	Version Number Attacks	982
Total		127684

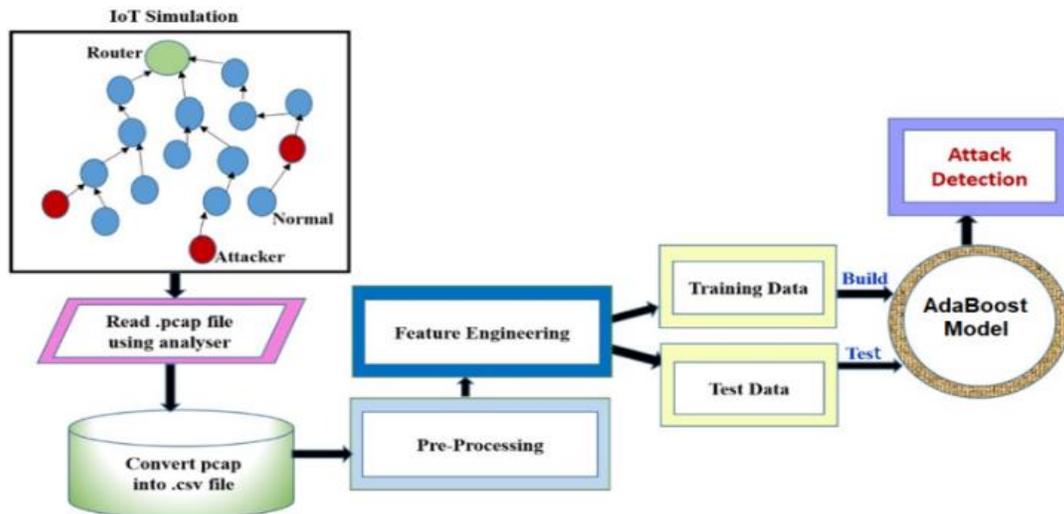


Fig. 1. Ada-IDS Model.

Table II explains the attributes of the Icmpv6 dataset. The screenshot with sample records captured using python code is shown in Fig. 2.

As it is given in Fig. 2, the Class field and Type field denote whether a packet is attack or normal. The Type field also gives the details of an attack as Version Attack, DIS Attack or DAO Attack.

TABLE II. DESCRIPTION OF THE ICMPV6 DATASET

S.No.	Attribute Name	Data Type	Description
1.	No.	Integer	Packet Number
2.	Source	String	Source Address of a packet
3.	Time	Float	Time represented in millisecond
4.	Destination	String	Destination Address of a packet
5.	Protocol	String	Protocol for Communication
6.	Length	Integer	Packet length in Bytes
7.	Info	String	Description about the protocol
8.	Class	String	The packet is Attack or Normal
9.	Type	String	Type of the Attack (Version, DIS, DAO)

B. Pre-Processing Phase

The dataset collected from the simulation environment has to undergo a pre-processing stage in order to be relevant for building the AdaBoost ensemble model. There are 394 missing values in Source and Destination fields. Since these two fields

represent the IPv6 address of the nodes, the missing values cannot be replaced by mean, median or mode values. A new value is given for the Source and Destination Addresses.

C. Feature Engineering

One hot encoding and label encoding are performed on the categorical features to make them relevant for the ML algorithms. The frequency encoding is applied for the 'Time' feature. The Class feature is created which separates the Normal data samples from the Attack samples. The Type feature categorizes the different types of attacks such as DIS Attack, DAO Attack and Version Number Attack. The feature 'No.' indicates the packet number which doesn't have any significance in predicting the target and hence it is eliminated from the dataset. The null values in the 'Source' feature are replaced by a dummy value 'a'. Similarly, the null values in the 'Destination' field are replaced by a dummy value 'b'. After the accomplishment of the pre-processing and feature engineering tasks, the dataset will look like the Fig. 3.

As shown in Fig. 3, all the categorical values of the dataset are converted into numerical values. Now, the dataset is relevant for model building.

D. Model Building Phase

The pre-processed dataset with eight features is used in this experiment. The combined dataset has 127684 data samples. 80% of the data samples are split into a training set which contains 102147 instances and the remaining 20% of data samples are treated as the test set which contains 25537 instances.

No	Source	Time	Destination	Protocol	Length	Info	Class	Type
1	fe80::212:742f:2f:2f2f	0	fe80::212:7425:25:2525	ICMPv6	76	RPL Control (Destination Advertisement Object)	Normal	Normal
2	fe80::212:740a:a:a0a	0.114	fe80::212:7410:10:1010	ICMPv6	76	RPL Control (Destination Advertisement Object)	Normal	Normal
3	fe80::212:741d:1d:1d1d	0.114	fe80::212:7421:21:2121	ICMPv6	76	RPL Control (Destination Advertisement Object)	Normal	Normal
4	fe80::212:742f:2f:2f2f	0.114	fe80::212:7425:25:2525	ICMPv6	76	RPL Control (Destination Advertisement Object)	Normal	Normal
5	fe80::212:740a:a:a0a	0.114	fe80::212:7410:10:1010	ICMPv6	76	RPL Control (Destination Advertisement Object)	Normal	Normal
...
127680	fe80::212:740b:b:b0b	431.709	fe80::212:7401:1:101	ICMPv6	76	RPL Control (Destination Advertisement Object)	Normal	Normal
127681	fe80::212:741f:1f:1fff	431.71	ff02::1a	ICMPv6	97	RPL Control (DODAG Information Object)	Normal	Normal
127682	fe80::212:7432:32:3232	431.71	fe80::212:7424:24:2424	ICMPv6	76	RPL Control (Destination Advertisement Object)	Attack	Version Attack
127683	fe80::212:740b:b:b0b	431.711	fe80::212:7401:1:101	ICMPv6	76	RPL Control (Destination Advertisement Object)	Normal	Normal
127684	fe80::212:741f:1f:1fff	431.712	ff02::1a	ICMPv6	97	RPL Control (DODAG Information Object)	Normal	Normal

127684 rows x 9 columns

Fig. 2. Screenshot with Sample Date.

	Source	Time	Destination	Protocol	Length	Info	Class	Type
0	58	3	29	0	76	4	0	0
1	21	4	15	0	76	4	0	0
2	40	4	25	0	76	4	0	0
3	58	4	29	0	76	4	0	0
4	21	4	15	0	76	4	0	0
...
127679	22	1	2	0	76	4	0	0
127680	42	2	37	0	97	2	0	0
127681	61	2	28	0	76	4	0	0
127682	22	1	2	0	76	4	0	0
127683	42	1	37	0	97	2	0	0

127684 rows × 8 columns

Fig. 3. Sample Data after Pre-processing.

E. AdaBoost Ensemble Model

An Ada-Boost (Adaptive Boosting) model is built to detect the Version Number Attack, DIS flooding attack and DAO attacks in the IoT environment. It was developed by Yoav Freund and Robert Schapire in 1996 as a classifier that uses ensemble boosting. Classifier accuracy is improved by combining multiple classifiers [22]. AdaBoost classifier creates a powerful classifier by combining several weak classifiers, resulting in a powerful classifier with high accuracy. The basic idea behind Adaboost is to train the data sample and adjust the classifier weights in each iteration, so that unusual observations can be accurately predicted [23]. Interactive training on a variety of weighted training examples should be used to fine-tune the classifier. It tries to minimize training error in order to provide the best fit possible for these examples in each iteration. The steps for obtaining the ensemble model are given below:

1) Adaboost begins by picking a training subset at random.

2) The AdaBoost machine learning model is trained iteratively by selecting the training set based on the accuracy of the previous training prediction.

3) It gives more weight to observations that were incorrectly classified, increasing the likelihood that these observations will be correctly classified during the next iteration.

4) Additionally, the trained classifier is given more weight in each iteration based on how accurately it classifies.

5) Classifiers that are more precise will be given more credit.

6) In this process, the training data is iterated until it fits perfectly, or until the specified maximum number of estimators has been reached.

In AdaBoost classifier, there are three basic parameters such as `base_estimator`, `n_estimator` and `learning_rate`. The parameters used in this research are given below:

- `base_estimator`: A weak learner is used to train the model. In this work, the default `DecisionTreeClassifier` is used to train the ensemble model.
- `n_estimator`: It specifies how many weak learners are used for training the model repeatedly. In this model 10 estimators are used. The performance is analyzed. Then increment by 10 until it reaches 100 estimators.
- `learning_rate`: The default learning rate is 1, it denotes the weights of the weak learner. In this ensemble model, the default learning rate is used.

In AdaBoost ensemble approach, weak learners are combined to improve accuracy, which is done iteratively by fixing the faults of the weak classifier. AdaBoost isn't prone to being overfit issue. Though AdaBoost has these advantages, the performance is degraded if there are outliers in the dataset.

F. Deployment Phase

The proposed Ada-IDS model is installed in the Border Router (Gateway). The Pseudo Code for the Ada-IDS is given in Fig. 4.

This Ada-IDS detects the icmpv6 based attacks such as Version Number Attacks, DIS flooding attacks and DAO attacks in RPL based IoT networks.

```
Pseudo Code for Ada-IDS  
Input: Network Traffic  
Output: Attack- DAO, DIS, Version or Normal  
  
1. implement Normal and Attack Scenarios in Cooja Simulator  
2. collect the packets from 6LowPAN Analyser tool  
3. analyse the packets using WireShark tool  
4. convert the packets into .csv format  
5. extract the features from the .csv file  
6. pre-process the features  
7. perform feature encoding  
8. select the relevant features  
9. split the Dataset into two parts:  
   - 80% Training data  
   - 20% Testing data  
10. learning_rate=1, base_estimator=DecisionTree Classifier  
11. for i=10 to 100 do: // Build AdaBoost Ensemble Model  
12.   n_estimator=i  
13.   build AdaBoost(learning_rate, base_estimator, n_estimator)  
14.   calculate training_time  
15.   test AdaBoost(learning_rate, base_estimator, n_estimator)  
16.   calculate testing_time  
17.   evaluate confusion_matrix, accuracy  
18.   evaluate precision, recall, f-Score  
19.   increment i by 10  
20. end for  
21. implement Ada-IDS Model in the Gateway  
22. return output
```

Fig. 4. Pseudo Code for Ada-IDS.

V. RESULT AND DISCUSSION

This section elaborates the results obtained by the AdaBoost ensemble model. After accomplishing preprocess and feature engineering phases, the dataset is split into two sets like training and testing set. The training set contains 80% of the original data samples and the testing set consists of 20% of the dataset. The No. of samples in both categories is given in Table III.

The training samples are used to build the AdaBoost ensemble model. The DecisionTreeClassifier is selected as the weak classifier to fine tune the model iteratively. The learning rate parameter takes the default value. The no. of base_estimator is initially given as 10. The training time and testing time with 10 base estimators are analyzed. The testing accuracy for the AdaBoost Classifier with 10 base estimators is noted. To check whether there will be any change in the accuracy with respect to the number of estimators, the base estimator is incremented by 10 until it reaches 100. Surprisingly, the accuracy is 99.6% and it is not affected by the number of estimators used for building the AdaBoost classifier. The parameters and accuracy of the AdaBoost ensemble model is listed in Table IV.

As it is given in Table IV, the learning_rate is constant of all experiments. The number of Decision Trees used for building the AdaBoost ensemble model for each experiment varies from 10 to 100. The accuracy obtained is the same in all experiments. The training time and testing time varies in each

experiment according to the no. of base estimators used. The relationship between the training time and the testing time is indicated by using Fig. 5.

As Fig. 5 depicts, the training time required for building the model is more compared to the testing time. Because, the training set contains 80% of data. Also when number of DecisionTreeClassifier increases, the training time also increases. So, there is a positive correlation between the number of samples, number of estimators and the training time. The testing time also varies according to the no. of estimators in each experiment. When more DecisionTreeClassifiers are included, the testing time also increases.

TABLE III. DESCRIPTION OF THE ICMPV6 DATASET

Type of Instance	Training (80%)	Testing (20%)	Total
Normal	100169	25015	125184
DAO Attack	79	246	325
DIS Attack	1115	78	1193
Version Attack	784	198	982
Total Samples	102147	25537	127684

TABLE IV. ADABOOST PARAMETERS AND ACCURACY

n_Estimator	Learning Rate	Training Time (Sec.)	Testing Time (Sec.)	Accuracy
10	1	0.62	0.069	0.996
20	1	1.77	0.092	0.996
30	1	1.662	0.163	0.996
40	1	2.406	0.355	0.996
50	1	2.937	0.272	0.996
60	1	4.881	0.363	0.996
70	1	5.21	0.357	0.996
80	1	6.627	0.428	0.996
90	1	5.561	0.786	0.996
100	1	6.923	0.872	0.996

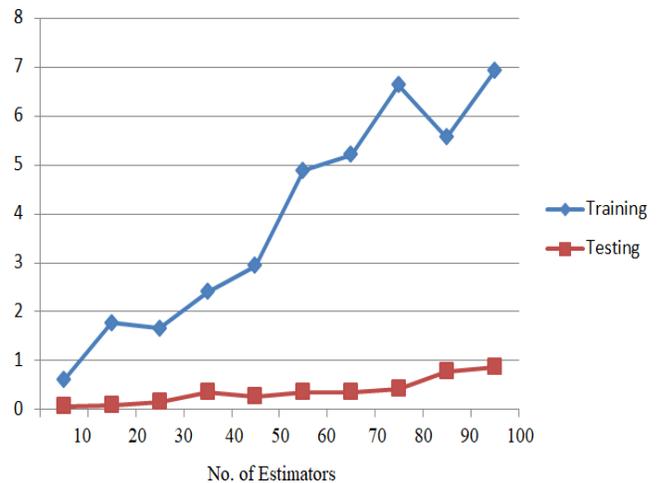


Fig. 5. Training and Testing Time Comparison.

A. Evaluation Metrics

There are three classes of attacks in the dataset. The confusion matrices are generated for each experiment which shows the actual and predicted class labels for each sample. To evaluate the performance of the models, the metrics such as accuracy, precision, Recall, F-Score are also computed [24].

- True Positive (TP): TP represents the correct classification of an attack packet as attack.
- True Negative (TN): TN specifies the correct classification of normal packets as normal.
- False Negative (FN): FN illustrates the wrong classification of an attack packet as normal. When this value increases, it affects the confidentiality and availability which are very important security concerns.
- False Positive (FP): FP signifies the incorrect classification where the normal packet is classified as attack.
- Accuracy: It denotes the ratio between the sum of correctly classified samples as normal and attack to the total instances. The formula for computing Accuracy is given in the Eq.1

$$\text{Accuracy} = (\text{TP} + \text{TN}) / (\text{TP} + \text{TN} + \text{FP} + \text{FN}) \quad (1)$$

- Recall (Sensitivity): Recall quantifies the number of correct positive predictions made out of all correct classifications that could have been made. Eq. 2 is the formula for calculating the sensitivity or recall.

$$\text{Recall} = (\text{TP}) / (\text{TP} + \text{FN}) \quad (2)$$

- Precision: It represents the total number of records that are correctly classified as attack divided by a total number of records classified as attack. The precision can be calculated according to the Eq.3.

$$\text{Precision} = (\text{TP}) / (\text{TP} + \text{FP}) \quad (3)$$

- F-Score: F-Score combines the properties of both precision and recall and it expresses them using a single measure. The formula for computing the F-Score is given in Eq.4.

$$\text{F-Score} = 2 * (\text{Recall} * \text{Precision}) / (\text{Recall} + \text{Precision}) \quad (4)$$

In this work, the CPU time for training the model and testing the model are also taken into account for each experiment. The confusion matrix obtained for each experiment is almost the same and it is given in Table V.

In Table V, the correctly classified samples in the testing set are given blue color text, but the misclassified samples are denoted by using red font color. As it is shown in the table, all normal events are identified correctly. There are very few misclassifications in other categories. Using the confusion matrix and by applying the equations Eq. 1 to Eq. 4, the accuracy, precision, recall and f1-score values are calculated and listed in Table VI.

TABLE V. CONFUSION MATRIX

	Normal	DAO Attack	DIS Attack	Version Attack
Normal	25015	0	0	0
DAO Attack	0	214	32	0
DIS Attack	0	21	57	0
Version Attack	0	0	38	160

TABLE VI. RESULTS FROM COFUSION MATRIX

n_Estimator	Accuracy	Precision	Recall	F-Score
10	0.996	0.99	1.00	1.00
20	0.996	0.99	1.00	1.00
30	0.996	0.99	1.00	1.00
40	0.996	0.99	1.00	1.00
50	0.996	0.99	1.00	1.00
60	0.996	0.99	1.00	1.00
70	0.996	0.99	1.00	1.00
80	0.996	0.99	1.00	1.00
90	0.996	0.99	1.00	1.00
100	0.996	0.99	1.00	1.00

As Table VI denotes, the Ada-IDS model, developed by using AdaBoost Ensemble model with DecisionTreeClassifier provides better results in terms of accuracy, precision, recall and f-score. The obtained confusion matrix is the same for all observations, so that it gives the same accuracy, precision, recall and f-score values. Since it doesn't have any false alarm-rate, it is suitable for anomaly detection. The Ada-IDS is implemented in the Border Router (6BR) to safeguard the connected devices in the IoT network.

VI. CONCLUSION

The security attacks are inevitable in RPL based Internet of Things as they have limited resources compared to other networks. In this paper, an ensemble IDS named Ada-IDS is developed using the AdaBoost ensemble model and it is deployed in the Border Router to protect the IoT network from Version Number Attack, DIS flooding Attack and DAO Attack. According to the experiments, this Ada-IDS ensemble model detected these three types of attacks with 99.6% accuracy and with no false alarm rate. Hence, it will act as an anomaly based Intrusion System. It is suitable for all IoT domains and it acts as a shield to protect the nodes from flooding of ICMPv6 messages, unnecessary version updates and bulk sending of the DAO message in the RPL based IoT network. Availability and reliability of the IoT nodes for their normal responsibilities are also ensured. To enhance this system further, more ICMPv6 related attacks can be included in the 'icmpv6.csv' dataset.

REFERENCES

- [1] Zhihan LV, Liang Qiao, Amit Kumar Singh and Qingjun Wang, "AI-empowered IoT security for Smart Cities", ACM Trans. Internet Technol. 21, 4, Article 99, July 2021, DOI: 10.1145/3406115.
- [2] Mahmoud Ammar, Giovanni Russello and Bruno Crispo, "Internet of Things: A survey on the security of IoT frameworks", Journal of

- Information Security and Applications, Vol. 38, pp.8-27, 2018, DOI: 10.1016/j.jisa.2017.11.002.
- [3] Lisandro Ubiedo, Thomas O'Hara, Maria Jose Erquiaga and Sebastian Garcia, "Current State of IPv6 Security in IoT", Stratosphere Research Laboratory, arXiv:2105.02710v1 [cs.NI] 5 May 2021.
- [4] Mohammed Aman Kareem and Shahab Tayeb, "ML-based NIDS to secure RPL from Routing Attacks", IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, DOI: 10.1109/ccwc51732.2021.937584.
- [5] Ge Guo, "A Lightweight Countermeasure to DIS Attack in RPL Routing Protocol", IEEE 11th Annual Computing and Communication Workshop and Conference (CCWC), 2021, DOI: 10.1109/CCWC51732.2021.9376041.
- [6] Omar E. Elejla, BahariBelaton, Mohammed Anbar and Ahmad Alnajjar, "A Reference Dataset for ICMPv6 based Flooding Attacks", Journal of Engineering and Applied Sciences, Vol.11, Issue: 3, pp: 476-481, ISSN: 1816-949x, 2016.
- [7] Antonio Arena, Pericle Perazzo, Carlo Vallati, Gianluca Dini and Giuseppe Anastas, "Evaluating and Improving the Scalability of RPL Security in the Internet of Things", Computer Communications, Volume 151, pp. 119-132, 2020, DOI: 10.1016/j.comcom.2019.12.062.
- [8] Anth ea Mayzaud, R emi Badonnel, Isabelle Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security, ACEEE a Division of Engineers Network, Vol.18, No.3, pp.459-473, 2016, DOI: 10.6633/IJNS.201605.18(3), hal-01207859.
- [9] Andrea Agiollo, Mauro Conti, Pallavi Kaliyar, Tsung-Nan Lin and Luca Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT", IEEE Transactions on Network and Service Management, Vol. 18, NO. 2, JUNE 2021, pp. 1178 – 1190, DOI: 10.1109/TNSM.2021.3075496.
- [10] Alaa Alhawaide, Izzat Alismaadi and Jiang Tang, "Ensemble Detection Model for IoT IDS", Internet of Things, 10035, 2021, DOI: 10.1016/j.iot.2021.100435.
- [11] Adnan HasanBdair, Rosni Abdullah, SelvakumarManickam and Ahmed K. Al-Ani, "Brief of Intrusion Detection Systems in Detecting ICMPv6 Attacks", Computational Science and Technology, Lecture Notes in Electrical Engineering 603, Springer Nature, DOI: 10.1007/978-981-15-0058-9_20.
- [12] A. Arul Anitha, L. Arockiam, "ANNIDS: Artificial Neural Network based Intrusion Detection System for Internet of Things", International Journal of Innovative Technology and Exploring Engineering, Volume: 8 Issue: 11, ISSN: 2278-3075, 2019.
- [13] EmreAydogan, S. Yilmaz, S. Sen, I. Butun, S. Forsstr om and M. Gidlund, "A Central Intrusion Detection System for RPL-Based Industrial Internet of Things," 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS), 2019, pp. 1-5, DOI: 10.1109/WFCS.2019.8758024.
- [14] Nour Moustafa, Benjamin Turnbull and Kim-Kwang Raymond Choo, "An Ensemble Intrusion Detection Technique based on proposed Statistical Flow Features for Protecting Network Traffic of Internet of Things", IEEE Internet of Things Journal, DOI: 10.1109/JIOT.2018.2871719.
- [15] Dan Tang, Liu Tang, Rui Dai, Jingwen Chen, Xiong Li and Joel J.P.C. Rodrigues, "MF-Adaboost: LDoS attack detection based on multi-features and improved Adaboost", Future Generation Computer Systems, Vol. 106 (2020), pp. 347–359, DOI: 10.1016/j.future.2019.12.034.
- [16] Abdul Rehman Javed, Zunera Jalil, Syed Atif Moqurrab, Sidra Abbas and Xuan Liu, "Ensemble Adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles", Transactions on Emerging Telecommunications Technologies, Wiley, 2020, DOI: 10.1002/ett.4088.
- [17] Amin Shahraki, Mahmoud Abbasi and Øystein Haugen, "Boosting algorithms for network intrusion detection: A comparative evaluation of Real AdaBoost, Gentle AdaBoost and Modest AdaBoost", Engineering Applications of Artificial Intelligence, Vol. 94, 103770, 2020.
- [18] Ahmet Arı, Siddika Berna  rs Yalın and Sema F. Oktu, "New lightweight mitigation techniques for RPL version number attacks", Ad Hoc Networks, Vol. 85, pp. 81-91, 2018, DOI: 10.1016/j.adhoc.2018.10.022.
- [19] Mayzaud A., Sehgal A., Badonnel R., Chrisment I., Sch onw lder J., "A Study of RPL DODAG Version Attacks", IFIP International Conference on Autonomous Infrastructure, Management and Security, AIMS 2014: Monitoring and Securing Virtualized Networks and Services pp 92-104, DOI: 10.1007/978-3-662-43862-6_12.
- [20] Cong Pu, "Spam DIS Attack Against Routing Protocol in the Internet of Things", International Conference on Computing, Networking and Communications (ICNC), IEEE, 2019, DOI:10.1109/icnc.2019.8685628.
- [21] Isam Wadhaj, Baraq Ghaleb, Craig Thomson, Ahmed Al-Dubai and William J. Buchanan, "Mitigation Mechanisms against the DAO Attack on the Routing Protocol for Low Power and Lossy Networks (RPL)", Green Internet of Things, IEEE Access, Volume: 8, 2020, DOI: 10.1109/ACCESS.2020.2977476.
- [22] Avinash Navlani, "AdaBoost Classifier in Python", DataCampTutorials, 2018, <https://www.datacamp.com/community/tutorials/adaboost-classifier-pyhton>, [Accessed on: 15th October, 2021].
- [23] Abdul Rehman Javed, Zunera Jalil, Syed Atif Moqurrab, Sidra Abbas and Xuan Liu, "Ensemble Adaboost classifier for accurate and fast detection of botnet attacks in connected vehicles", Transactions on Emerging Telecommunications Technologies, Wiley, 2020, DOI:10.1002/ett.4088.
- [24] Mohammad Almseidin, Maen Alzubi, Szilveszter Kovacs and Mouhammd Alkasassbeh, "Evaluation of Machine Learning Algorithms for Intrusion Detection System", IEEE Explore, ISSN: 1949-0488, 2017, DOI:10.1109/SISY.2017.8080566.

Analytical Framework for Binarized Response for Enhancing Knowledge Delivery System

Chethan G S¹

Assistant Professor, Department of Information Science and Engineering, JNN College of Engineering, Shimoga, Karnataka, India

Vinay S²

Professor and Head, Department of Information Science and Engineering, PES College of Engineering, Mandya, Karnataka, India

Abstract—The student feedback offer effective insight into their experience of knowledge transfer, routinely collected in academic institutions. However, the existing research literature lacks reporting whether the comments in education system are helpful or non-useful. Most of the existing works are limited to sentiment polarity computation only, and teacher evaluation is carried out without considering the aspects of the teaching. This study analyzes student comments and classifies comments as applicable and non-useful for the teacher scoring system. In the proposed research, the data considered is the student feedback collected from the teacher rating website. The study performed phase-by-phase text data modeling. First, exploratory analysis is carried out on the student feedback dataset to understand text data characteristics and features. Based on the exploratory analysis, appropriate steps are determined to perform preprocessing operations for data cleaning. Using natural language processing context, the study only focuses on removing stop words and common words that belong to both useful and non-useful contexts. BoW model is considered for features extraction, and two probabilistic supervised machine learning models are used for comment classification. The study outcome exhibits that Gaussian Naïve Bayes outperforms Multinomial Naïve Bayes in accuracy, precision, recall rate, and F1-score.

Keywords—Education; knowledge transfer; machine learning; natural language processing; student feedback

I. INTRODUCTION

Education is the key to success and serves as a foundation that enables people to learn about the society and world around them. People have a preconceived notion that getting an education gives them basic survival skills and is essential for good citizenship. However, education provides many opportunities in life through acquiring fundamental skills, values, ethics, morals, and life survival skills. Over the past decades, the trend of education has undergone tremendous evolutions. With the advent of technology tools and the Internet, people have raised many questions about the best teaching model. The upsurge of growth in the educational sector has a long history. The initial increase is related to personal background involving learning and memorization [1]. The upturn appeared in the education system in the early twentieth century regarding mass learning [2]. In the late 1990s, with the advent of computers and the Internet, teaching and learning methods have changed significantly. As a result, the trend of distance learning emerged parallel with the learning from books, libraries, and teaching on the blackboard. Over time, a revolutionary advancement in electronic and

network communication technologies has changed education. It induces a trend of online learning and knowledge delivery or transfer as a service at a global scale. The availability of digital platforms in the form of Information and Communication Technology (ICT) utilizes a knowledge-based learning model that will be made available to everyone by experts in various educational topics and domain disciplines [3-4]. The vision of education to all is being evidenced through different e-learning systems and MOOCS [5-6] like Khan Academy, Course era, NPTEL, etc. Various educational institutions and an educational corporate [7-8] race this. Such Institutions or learning platforms are continually looking for an efficient mechanism that can be utilized to improvise knowledge transfer and learning services. This improvement can be achieved by collecting feedback from students about the knowledge transfer by their teachers. According to the researchers [9], students' feedback provides a vital means for analyzing the student's level of understanding, attitude towards learning, and scoring teachers concerning the quality of knowledge transfer in the particular class or session. Thus, the students' feedback must be addressed efficiently by learning and education platforms to successfully enhance the quality of education in terms of helping to improve student achievement that can benefit society and the nation.

Students' feedback consists of both quantitative and qualitative information. Quantitative information such as personal feelings, beliefs, sentiments, and desires can be identified and handled easily. However, the qualitative data such as useful and non-useful comments may consist of positive and negative sentiments. Still, selecting helpful comments requires an effective classification mechanism to utilize the improvising education model and knowledge transfer services. In fact, in most cases, quantitative comments are considered, while qualitative comments are either treated manually or entirely ignored. Qualitative analysis can be performed with less data, but if the amount of information is large, a challenge will occur and be considered a text mining problem. Researches in the context of qualitative analysis of feedbacks in the education sector are relatively new. The previous study reported their contribution to student reviews mining using Natural Language Processing (NLP). The NLP-based approach uses dictionary- methods that use sentiment words match them with textual terms of comments to determine the polarity, how positive, negative, or neutral the words are like happy, sad, satisfied, dissatisfied, or angry [10-12]. Also, Machine Learning (ML) techniques such as Support

Vector Machine (SVM), clustering, neural network, and many more have been utilized in the literature to describe student understating from the various aspects level of teaching methodology, communication skills, and technical skills knowledge, etc. Though sentiment analysis plays a vital role in assessing learning effectiveness. However, most of the existing works are limited to finding the polarity of feedbacks. They do not focus on understanding and categorizing useful and non-useful review/comments patterns to effectively improve the learning organization's performance and formulate plans to enhance the knowledge transfer by teachers and students' learning experience.

Despite the variety of efforts and solutions available in the existing literature, the proposed study considers classifying helpful and un-useful comments as a text classification problem and offers an alternative approach to help score teachers, improve knowledge transfer services. In the proposed work, NLP and ML are applied to student feedback to classify valuable and useless comments benefiting learning platforms to overcome potential barriers to effective knowledge transfer services and the quality of learning processes. The idea of the proposed system is to present a novel computational framework to enhance the teaching-learning system in a digitized educational system. The importance of the research is briefed with respect to key contributions of this paper include.

- The paper highlights all the significant work carried out in a similar domain to extract unaddressed research problems.
- The paper presents a novel and simplified computational framework capable of analyzing the binary response in the form of valuable and non-useful remarks.
- The paper presents an exploratory analysis of the dataset of student response data from a teacher review site to recognize the characteristics of the feedback dataset and understate the requirement of preprocessing steps.
- The paper presents an intelligent filter to score the performance of teachers based on categorizing functional and non-useful patterns of comments using the probabilistic model-based supervised classifier.

If all the above stated research contribution is implemented than a novel framework is evolved which is capable to automating the teaching-learning experience enhancement, which doesn't exist in current research work or any commercial application. Apart from the above stated research contribution, the limitation of proposed study are viz. i) it doesn't address any distributed storage management over data center or in warehouse, ii) it doesn't address any form of security encapsulation for the extracted knowledge from the analyzed data, and iii) it doesn't consider analyzing any other language apart from English. The remaining parts of this paper are organized in the following manner: Section II. Presents brief discussion about existing techniques used for enhancing the education delivery as well as a management system. Section III discusses the motivational factors about this topic

and briefing of significant reasons behind the proposed work. Section IV describes a proposed solution to the identified research problem and detailed research methodology describing the exploratory study, preprocessing, and classification of valuable and non-useful comments. Section V discusses the experimental results presented to evaluate the proposed system's performance, whereas Section VI concludes the overall work carried out in this paper.

II. RELATED WORK

This section discusses the related work regarding improvement in education based on student attitude analysis and teaching evaluation using feedback.

In recent years, researchers have begun to score teachers and evaluate student understanding and attitude. For instance, Beatrice Tucker [13] investigated feedback and reviews from an Australian University's aggressive or unprofessional. The investigational analysis showed that 20 comments were recognized as abusive directed towards professors and teaching, and 34 comments were recognized as unprofessional directed towards education units. A recent study by Boca [14] showed an interesting work on analyzing factors that impact student learning and attitude towards online classes during the current pandemic situation. The author surveyed by preparing a questionnaire from 300 students from technical university Romania. The findings of this study reveal that online classes and materials are beneficial for most students in a pandemic situation. But also, students found this approach to learning stressful. This study has provided good background in the context of improving education to meet the needs of new generations. Similar efforts have been made by Wu et al. [15] and Zughoul et al. [16], where the authors have analyzed students' performances and attitudes towards teachers.

The remarkable use of text mining approaches to examine student reviews and comments has led to an excess of methods. Various ML and NLP-based approaches have been applied to the education field. The work of Dhanalakshmi et al. [17] examined different ML approaches and demonstrated effective of each ML technique under consideration. The authors showed Naïve Bayes is the most suitable ML approach to compute the probability of input comments directed to specific attributes. Meanwhile, the authors in the study of Nasim et al. [18] reported lexicon-based text analysis does not require extensive data and high processing power. Qi and Liu [19] used a latent Dirichlet allocation scheme to perform texting mining over the feedback provided by the student for MOOC courses. A matrix was constructed to describe comments regarding courses. Bi-long-short-term memory (LSTM), a deep learning approach, is used to classify the sentiments from the comments.

Liu et al. [20] developed a model opinion and topic mining to forecast the worldwide acceptance level of MOOC courses. The authors have obtained sentimental comments regarding improving knowledge transfer strategies and courses. Similarly, Weng et al. [21] designed a computing model based on the feedback regarding MOOC courses. The presented model was developed based on the sentiment analysis to help education providers understand the reason for changing students' sentiments and accordingly perform course

adjustment and teaching methods. The work carried out by Koufakou et al. [22] adopted the data analytics method to mine meaningful information from student reviews to assist teachers, and educational organizations gain insights into students' emotions and attitudes. Another work done by Leong et al. [23] considered messaging texts for carrying out teaching assessments. The authors have initially classified different contexts presented within the text messages and performed data modeling using a multi-level data analytics approach. The study finding shows sentiment analysis-based model is better to conduct teacher scoring and teaching evaluation. The authors in the study of Kumar and Jain [24] introduced a model in which significant features are first analyzed.

Then, TFIDF scores were used to select features for the classification. The classification of comments is done based on the sentiment analysis-based polarity prediction using Naïve Bayes. The result indicated that 81.06% of features were correctly predicted, and 89.67 % of accuracy was achieved in the comment classification. The researchers in Chetan and Vinay's [25] study focus on optimizing data storage related to knowledge delivery systems in a cloud-based e-learning system using an advanced data analysis method using a semantic-based approach. Kastrati et al. [26] presented work on systematic mapping of existing studies on the sentiment analysis of Students' feedback with dictionary-based approaches and Learning models. The findings of this study indicated that despite many challenges, education and teacher evaluation are booming concerning the application of learning mechanisms. The authors have also highlighted the requirement of structured datasets, standardized solutions, and increased focus on emotional expression and classification. A significant study carried out by Skedsmo and Huber [27] has presented an investigational analysis based on teacher evaluation regarding the valid measures and teacher involvement. The authors discussed the various issues associated with procedures adopted in the existing studies for teacher rating in this study. The author's contribution is an essential question of the relevance between teacher rating policies and existing research procedures. Zerihun et al. [28] showed that student learning experience and achievement indicators rated teachers similarly. The authors have developed a questionnaire oriented on the students' experiences, and a hypothesis in the questionnaire is made by exploring the literature. The hypothesized evaluation parameters were designed that consist of different factors such as evaluation and review, course structure and presentation, self-assessment, and engagement.

A study conducted by Sindhu et al. [29] presented a vital work relevant to the current research. The authors have focused on the extraction of qualitative information from the student's feedback. In this work, the authors considered various aspects of teaching and used supervised learning-based sentiment analysis using multi-layer LSTM. The first layer classifies the characteristics described within the comments, and further aspect-based sentiments polarity is predicted. The dataset used in this study is prepared based on the student's observations from the specific educational institution as a use case. The study outcome indicated good

accuracy regarding aspect-based prediction with 91% and sentiment polarity with 93%. This study has provided significant concern as it focuses on different aspects needed in the teacher evaluation process. However, none of the other studies considered teaching characteristics and other necessary attributes to classify useful and non-useful features from the student feedback data. Most of the existing research is limited to polarity computation, which is suitable to highlight the emotion and sentiments of students but not much significant to score teachers. Since the student's comments and feedback often consist of irrelevant, unprofessional, abusive words, which need to be analyzed whether it is valuable or not valuable for the context of scoring or rating the teacher. The following section presents the motivation and reason behind this study.

III. MOTIVATION

The discussion in the first section is carried out from the perspective of the education system and its improvement. In the present section, the discussion is carried out from the teachers' perspective and the influential factors that motivated and the reason behind the proposed work. A teacher has a significant role in everyone's life. Teachers engage students' minds to help in gaining knowledge and understanding the subject of interest. The teaching aspects from different perspectives are illustrated in Fig. 1.

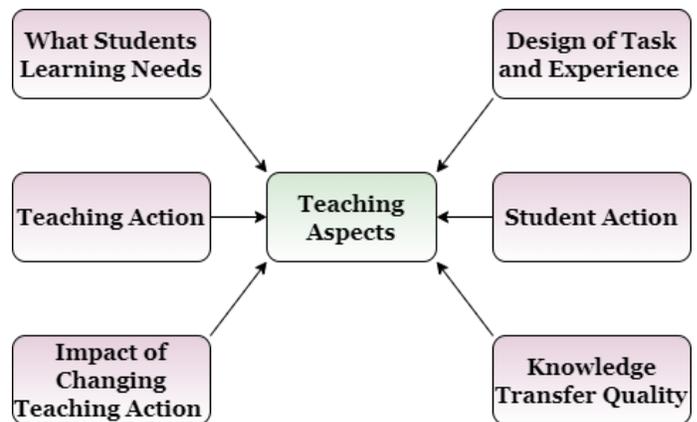


Fig. 1. An Illustration of Teaching Aspects.

In education, teachers have to contribute in several ways, including understanding their students, what student learning needs, what type of task design and assessments should be included. Another important thing is determining the quality of knowledge or teaching action required to create positive associations with students, make an operative learning environment, and establish proficiency and accountability. However, society is constantly evolving, and the performance requirements of education organizations and online learning platforms are also changing. The teaching profession is no exception except to bring about a change in academic life and professional commitments. In this regard, the requirements for teachers have become more and more complex. Although teachers try to do their best, sometimes the quality of knowledge deliverance is questioned. Reflecting on these changes and requirements in the current scenario, teacher scoring or rating systems have become more challenging and

complex. Rating teacher refers to accessing teaching skills, the approach of knowledge transfer, and teachers' achievement. Based on the discussion in the previous section, the sentiments analysis from students' feedback provides correlational attributes to score teachers and courses. Particularly in the context of education, the positive sentiments are believed to have good learning from the teachers, while negative sentiments believed to be knowledge transfer by teachers for their classes is not satisfactory. The sentiment analysis from textual data (student's feedback or comments) raises many technical challenges. A key challenge is understanding the essential features and classifying helpful and non-useful comments regarding scoring teachers. However, none of the existing research works have focused on this challenge. The proposed study believes that analyzing the sentiments from textual data is highly contextual as the wording meaning varies across different domains. For instance, in terms of education context, the word "extremely" indicates a negative sentiment in the comment-1 "She moves extremely fast, teaches different methods than the book."

However, the same word 'extremely' indicates a positive one in comment-2 "Extremely an important class". The word 'extremely' in both sentences reflects different sentiments. Let us consider another example with the same word that reflects positive sentiment in comment-3 "This is her favorite class and is extremely passionate about it". The comment-3 reflects positive sentiments, but it is not helpful because it does not describe any clear information and basis for improvement. Careful observation reveals that though comment-1 and comment-2 reflect different sentiments, they can be considered useful comments. They have significant intentions that contribute to improvising teaching methods and an effective learning environment. To get more clarity, let us see another example in terms of a different domain. The word "quickly" indicates a negative sentiment in the comment, "The explanation ended too quickly!". However, in a restaurant context, it means a positive sentiment in the comment "The service provided quickly". These examples show how important it is to understand the critical feature of comments to determine the valuable and non-useful comments regarding educational context.

It should also be noted here that useful and useless comments can be composed of positive and negative emotions, and the task is to determine or classify useful and useless. Unfortunately, most existing literature does not consider the above factors and generally divides comments into positive, negative, and sometimes even neutral. They do not consider the correlation between sentiment and the usefulness of comments, whether it is understood as a sentiment classification problem without considering salient features and contextual significance. In turn, this raises serious questions about the current approach to the rating or assessment of teaching aspects. In this sense, the vagueness in the existing literature leaves education providers and learning organizations with a constrained direction about an effective way to make new policies towards improving courses, knowledge transfer services, and reforming other units of education. The proposed research aims to present an effective intelligent filter to score teachers based on identifying helpful

and non-useful comments from student feedback. This work can be defined as a problem of text classification from the given comments in textual representation concerning helpful comment (Uc) and non-useful comment (Nc) aspect: $\{Uc, Nc; \exists \text{ comments } (c)\} \leftarrow \text{function } f \text{ such that } (c) = \{Uc, Nc\}$. The study performs phase-by-phase analytics of textual data to determine the main aspects to be taken into account for designing a teacher scoring model.

IV. PROPOSED SYSTEM

This section discusses the methodology and implementation strategy for the proposed system. The suggested work presents a significant contribution in the field of learning analytics. The study has been carried out to analyze substantial comments from the students' feedback rather than the sentiment polarity computation. The study considers that if good data analytics is carried out, then helpful and non-useful comments can be distinguished efficiently, positively impacting the teacher scoring system, thereby improving the quality of knowledge transfer in e-learning systems and academic institutions.

The workflow of the proposed system architecture is shown in Fig. 2, which has five core components: the first collection of text from the student's feedback; second exploratory analysis to understand characteristics of data and steps required in data cleaning in the third preprocessing, where irrelevant information associated with text data is excluded, and unique words specific to helpful comments are analyzed; fourth feature extraction is carried out using bag of word (BoW) model making text data suitable to fit in classification model; then designing an intelligent filter for classification of a useful and non-useful comment using the supervised classifier. All these processes are performed phase-by-phase, and a text cloud is used to visualize the essential words related to helpful and non-useful comments. The system uses the open-source Python programming language to perform modeling and implementation of the entire system.

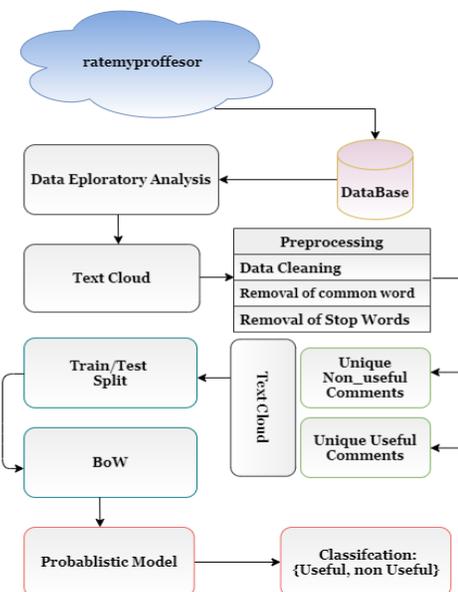


Fig. 2. Systematic Workflow of the Proposed System.

A. Data Aggregation

The data aggregation in the proposed research work is student feedback from the teacher review site. Academic institutions and online learning platforms often do not disclose their internal input or review by students to assess teaching quality. Several online platforms have emerged, which allow students to evaluate their teachers publicly. The most popular online evaluation platform is RateMyProfessors.com. Fig. 3 illustrates the online student learning and feedback sharing over the learning management system.

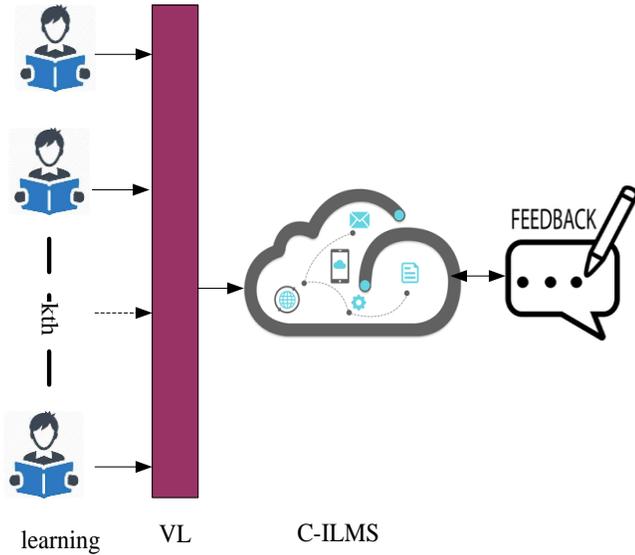


Fig. 3. The Conceptual Scenario of Learning and Feedback Sharing.

In Fig. 3, the conceptual scenario of e-learning or online system and the feedback sharing process is demonstrated. The students get education and knowledge via a virtual layer (VL) connected with a Cloud-Enabled Intelligent Learning Management System (C-ILMS). This kind of platform also allows students to evaluate their teachers anonymously. Students present their opinion through review or comment from different aspects. For teacher rating, clarity, helpfulness, and difficulty are considered the most. While rating the courses and learning platform, students give comments considering different aspects such as academic institution reputation, education-related services offered, test and assessments, activities, and opportunities. "RateMyProfessors" (RMP) is a teacher review website where students can provide an open comment and express their emotions very transparently. RMC provides a simple way of sharing what students experience in a course and their professor's ratings. On this website, "ratings" refers to students' responses to a single survey question about overall professor quality that includes rating indicators, content knowledge, interest, clarity of lectures, etc.

In the proposed study, data of student feedback regarding teacher ratings are collected from the RMP website. The collected dataset considers comments indicating a review of several professors. A web scraping technique is used on RMP in the data collection process. The dataset represents only textual and numerical data, therefore of small dimensions.

B. Data Exploratory Analysis

In the system model, the data intuition is first created utilizing the word cloud. The entire dataset in the unstructured format is considered as a universal set (Ω) which consists of subsets of helpful comments (U_c) and non-useful comments (N_c) such as $U_c \subset \Omega$ and $N_c \subset \Omega$. Table I presents the sample view of the student feedback dataset.

Table I shows the data reading process from the dataset provided by ratemyprofessor.com. The first step in this data analysis phase is to observe the most common word in the comments or text specific to users and no useful comments. The dataset is labeled as class usefulness with two possible states {usefulness-state (U_c):1, non-usefulness (N_c):0}. The total number of samples (T_s) in the dataset is 562, whereas only 358 samples are applicable and 204 \in non-useful states. Therefore, the proportion of usefulness-state and non-usefulness state can be found using equations 1, 2 and 3, which are $x = 63.7\%$ and $y = 36.3\%$, respectively.

$$T_s = \sum(U_c, N_c) \tag{1}$$

$$x = \frac{100 \times U_c}{T_s} \tag{2}$$

$$y = \frac{100 \times N_c}{T_s} \tag{3}$$

To understand the distinct pattern between U_c and N_c , the mean length of the feedback comment text is computed using equations 4 and 5 for both U_c and N_c .

$$\mu_{U_c} = \frac{1}{n(U_c)} \sum_{i=1}^{n(U_c)} \sum_{j=1}^N U_{u_i}(w_j) \tag{4}$$

$$\mu_{N_c} = \frac{1}{n(N_c)} \sum_{i=1}^{n(N_c)} \sum_{j=1}^N N_c(w_j) \tag{5}$$

The mean (μ) length of each class of the comments computed is shown in Fig. 4. Computation of the mean value will offer a simplified way to understand the type of comment for further assisting in data analysis in upcoming operation steps. On an analysis as in Fig. 1, it is found that the average size of the U_c is 46.26 words, and the average length of the N_c is 26.59 words per comment. This numerical score offers a clear picture for the filtered formed of statements concerning the usefulness and non-usefulness state of the response.

The primary classification is possible even based on the word count. However, it may not be so in a real-time scenario, as sometimes or many times the average length of expression might be interchangeable. The study also presents text cloud to get more insight into both U_c (Fig. 5(a)) and N_c (Fig. 5(b)) as follows.

TABLE I. SAMPLE VIEW OF COMMENTS IN THE DATASET

Index	Comments	Label
0	He was boring and ruined psychology for me. No	Nc
1	challenging course. I thought I was go	Uc
2	Hard to understand at times. Tests are ok. Not.	Uc
3	SO glad to be the hell out of this class	Nc
4	great teacher and very smart, the class is very	Uc

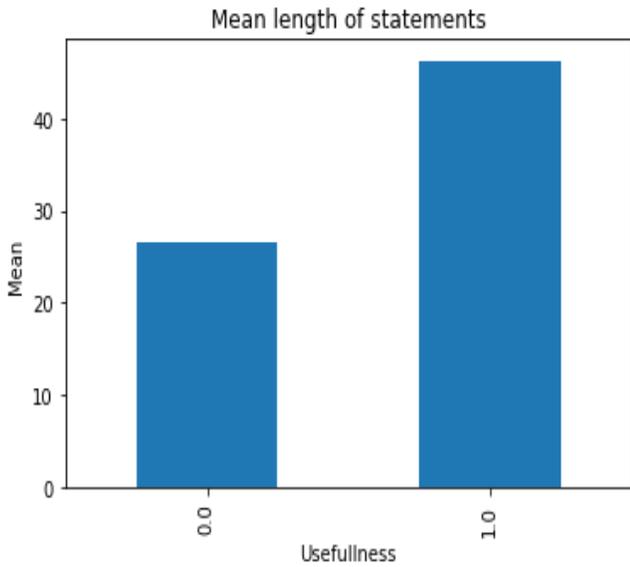


Fig. 4. Mean Length of Comment Text for Both U_c and N_c .

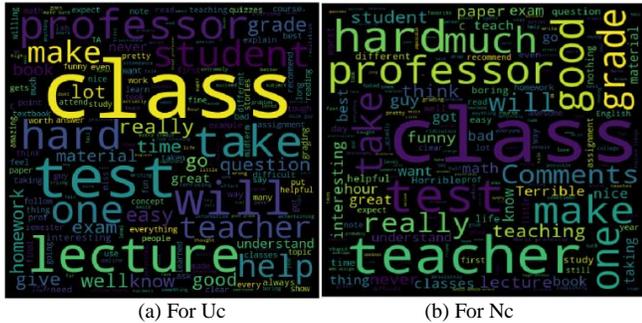


Fig. 5. Visualization of Text Cloud.

The study then checks for the most common words in the useful and non-useful categories. If the comments are insightful, it is considered useful, but the not constructive comments are not useful. The mapping of {useful, non-useful} → {1,0}. The short comments are also ignored. The text cloud is constructed with useful and non-useful. However, if the size of the word in the text cloud is big and bold then repeated, then it is more repeated, significant and smaller means less repeated.

The analysis obtained from text cloud Fig. 5(a) and Fig. 5(b) provides essential information that will help make the dataset suitable for the input to the model input by normalizing and discarding irrelevant and repetitive data. This process positively impacts the computational dependency of the model, i.e., it lessens the computational requirement in the feature representation and learning process. In this regard, the proposed exploratory analysis further explores the unique words in the U_c and N_c . A closer look indicates that many words stop words, so the next step is to remove the common and stop words. Fig. 6 highlights some stops words $\in U_c, N_c$.

i', 'me', 'my', 'myself', 'we', 'our', 'ours', 'ourselves', 'you', 'you're', 'you've", "you'll""you'd", 'your', 'yours', 'yourself', 'yourselves', 'he', 'him', 'his', 'himself', 'she', "she's", 'her', 'hers', 'herself', 'it', "it's", 'its', 'itself', 'they', 'them', 'their', 'theirs', 'themselves', 'what', 'which', 'who', 'whom', 'this', 'that', "that'll", 'these', 'those', 'am', 'is', 'are', 'was', 'were', 'be', 'been', 'being', 'have', 'has', 'had', 'having', 'do', 'does', 'did', 'doing', 'a', 'an', 'the', 'and', 'but', 'if', 'or', 'because', 'as', 'until', 'while', 'of', 'at', 'by', 'for', 'with', 'about', 'against', 'between', 'into', 'through', 'during', 'before', 'after', 'above', 'below', 'to', 'from', 'up', 'down', 'in', 'out', 'on', 'off', 'over', 'under', 'again', 'further', 'then', 'once', 'here', 'there', 'when', 'where', 'why', 'how', 'all', 'any', 'both', 'each', 'few', 'more', 'most', 'other', 'some', 'such', 'no', 'nor', 'not', 'only', 'own', 'same', 'so', 'than', 'too', 'very', 's', 't', 'can', 'will', 'just', 'don', "don't", 'should', "should've", 'now', 'd', 'll', 'm', 'o', 're', 've', 'y', 'ain', 'aren', "aren't", 'couldn', "couldn't", 'didn', "didn't", 'doesn', "doesn't", 'hadn', "hadn't", 'hasn', "hasn't", 'haven'

Fig. 6. Illustration of Some Stop Words.

The Stop words are the words that contain less information and are repetitive in the same line of comments as well as other lines of comments that $\in \{U_c, N_c\}$. The amount of information on a particular word is measured by entropy as described in equation 6 and equation 7 as follows:

$$H = -\sum p(x). \log(p(x)) \tag{6}$$

Where H denotes entropy of information reflected from particular words, $p(x)$ represents the probability of the word.

$$p(x) = \frac{\text{No.of time the word has been repeated}}{\text{Total number of words}} \tag{7}$$

If a word is most probable, it is closer to 1, and $\log(1)$ is zero, meaning it carries no information. However, it can be seen that a negative sign at the beginning of equation (6). Hence, the less repeated word carries more information since the value of $\log(p(x))$ is more. However, if a word is not appearing at all, then also it carries no information. In order to represent this, the $p(x)$ is multiplied to $\log(p(x))$.

Furthermore, when considering valuable comments, the punctuation cannot be ignored in the proposed study. People writing serious comments or helpful comments will not use punctuation marks like '!' or '?' or multiple dots. Hence, the words 'completed' and 'completed!!' give a very different meaning in the proposed study. The first word reflects the writer's seriousness, whereas the second word represents either excitement or frustration of the writer. When a professor or a teacher is being rated, such comments, which reflect emotion more than real criticism or appreciation, must be avoided. Therefore, the proposed study considers the only removal of stop words using preprocessing algorithm.

C. Data Preprocessing

The proposed system initiates a preprocessing operation to ensure better retention of data. Stop words commonly exist in all forms of text, and hence they should be first removed. Therefore, the preprocessing algorithm is designed to remove the stops words from the entire text corpus in this implementation phase.

The description of the algorithm is as follows:

1. Algorithm for Preprocessing

```

Input: Dataset (DS)
Output:Preprocessed feedback_texts
Start:
Load: DS → f1('DS')
        function: rmv_stop(text)
        for each non – useful comments df do
check: text(class == 0) do
W.join(rmv_stop('text') do
        join: non – useful → W
        for each useful comments df do
check: text(class == 1) do
W.join(rmv_stop('text') do
        join: useful → W
        Apply→text.split ( Words ∈ {Uc, Nc} )
        List useful comments & non useful comments
End
    
```

The algorithm has an inclusion of multiple parameters which are briefed as follow: i) *DS* is used as a dataset acting as input to proposed system, ii) *df* is used as non-useful comments which is required to be filtered out, iii) *W* is used as a useful comments which is considered for further analysis, iv) *U_c* and *N_c* is final matrix which restores useful and non-useful comments respectively. The algorithm takes all the textual feedback data and applies the *rmv_stop* function to remove stop words without scarifying the meaning of the sentences. The explicit function *rmv_stop* is used from the python library, representing all the stops words defined in the English language. Each sentence is passed into the functions, and all the stops' words are removed.

For each *N_c* in the text field of the dataset, a condition is evaluated that class of text is found to be 0 then remove stop word in the non-useful comments and joined to word vector *W*. Another condition gets evaluated to remove stop words from the valuable comments and further filtered helpful comments were appended to the *W*. Another function is then used, i.e., text. Split to separate the sequence of text and lists the word belonging to the *N_c* and *U_c*. Fig. 7 indicates the word cloud. The study explores to get insight on the common word contained in both *U_c* and *N_c*. Table II highlights common words extracted during analysis. A closer look into Table III and analysis of the word cloud shows some common words in *U_c* and *N_c*. Therefore, looking at the Venn diagram, only valuable words are considered, and common words are avoided.

Fig. 7 Venn diagram provides an analysis that words belong to both *U_c* and *N_c* such that: $U_c \cap N_c$ words are avoided. The familiar words are non-constructive, and only non-useful words are filtered. Those words will be considered if the phrase is uncommon in the helpful comment, and all the common words will be avoided. Similarly, uncommon words are selected for *N_c*, and common words are avoided. A frequency distribution plot is mentioned in Fig. 9 and Fig. 10 for unique words $\in \{U_c, N_c\}$.

The exploratory data analysis provided an understanding of data towards a better decision in the preprocessing, where only stops words and common words are removed. The study does not carry out any removal of punctuation as it has significant intent in the comments. The above processes provided a substantial analysis of the data, which positively impacted the feature reduction and training of the model.

From the visuals of Fig. 8, it is clear that the proposed system performs filtration of the words on the basis, thereby preprocessing the text.

TABLE II. SAMPLE OF COMMON WORDS

Rounds	Extracted Common Words
1	'extremely', 'difficult', 'course.', 'T', 'thought', 'T', 'was'
2	'going', 'to', 'have', 'to', 'retake', 'it', 'many', 'have', 'The'
3	'labs', 'are', 'hard', 'and', 'quite', 'time', 'and', 'the', 'pop'
4	'quizzes', 'are', 'T', 'think', 'the', 'tests', 'should', 'have'
5	'questions', 'but', 'be', 'If', 'you', '2', 'multiple', 'you'
6	'drop', 'a', 'grade.', 'this', 'course', 'is', 'VERY'
7	'Hard', 'to', 'understand', 'at', 'times.', 'Tests', 'are'
8	'Not', 'too', 'with', 'great', 'teacher', 'and', 'very'
9	'smart', ',', 'the', 'class', 'is'

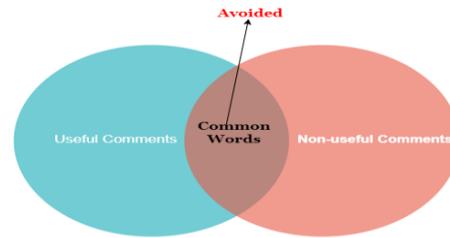


Fig. 7. Intersection of the *U_c* and *N_c* words is avoided



(a) Text cloud for *U_c* after removal of stops, words.



(b)Text cloud for *N_c* after removal of stop words.

Fig. 8. Text cloud analysis after removal of stop words.

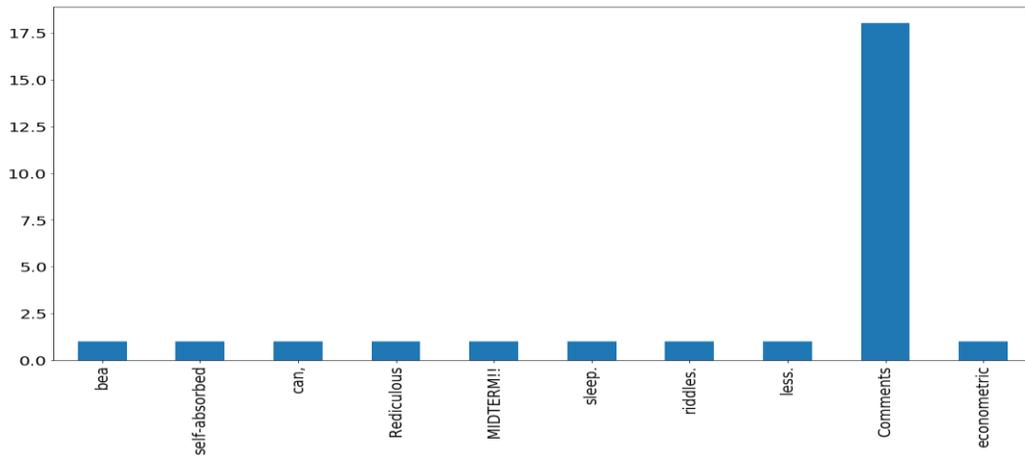


Fig. 9. Frequency Distribution of Words ∈ N_c.

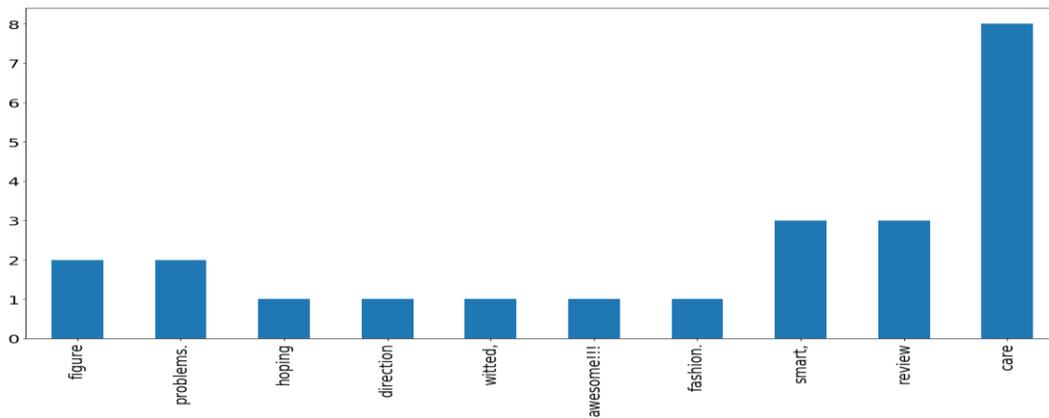


Fig. 10. Frequency Distribution of Words ∈ U_c.

The entire process discussed above is carried out phase-by-phase, providing effective feedback data modeling and preprocessing steps. The next step discusses the classification module, where the dataset split process is carried first, and different features are extracted using the BoW model. The algorithm for U_c and N_c classification is discussed as follows:

2. Algorithm for Classification

Input: Dataset DS
Output: Classified comment class (C1, C2)
Start:
Init DF → attri(DS)
For each text ∈ **DF**, **do**
Preprocessing: Use **Algorithm 1**
 Call **function:** rmv_stop(text)
Split DS → [Tr, Ts]
Extract Feature ← [Tr]
 Feat → []
 BoW → f2(Tr)
 Feat → Feat.append.Bow
Model Training → [Multinomial NB, Gaussian NB] **do**
 Training → model.train(Feat, Tr)
 Model Deployment: **do**
 Testing → model.test(Feat, Ts)
Testing done: **Evaluate** [Accuracy, F1 Score, Recall, Precision]
End

The algorithm takes the input dataset. After processing, it provides a classified class of comments. Initially, it loads the attributes of the dataset as a data frame. In the next step, the algorithm for the calls pre-processing operation is described in the first algorithm. In the next step, dataset split operation is carried out in terms of 80:20 ratio where 80% of the dataset is subjected to training set and 20% dataset as testing set.

Further feature extraction and vectorization are performed to make the training dataset a suitable input for the classification. The study uses the BoW model to extract features followed by the stemming and lemmatization process. In the proposed research, the probabilistic model, i.e., the Naive Bayes approach, is used to perform classification as it is free from extensive training data and capable of handling both discrete and continuous data. The Naive Bayes is based on the method of Bayes theorem numerically expressed in equation 6 as follows:

$$P(x|y) = \frac{P(x|y)P(x)}{P(x)} \quad (8)$$

In above equation(8), where (x) denotes the prior probability being true, P(x) refers to the probability of the data, P(x|y) is the probability of presumption x for the available data y, and P(x|y) denotes the probability of y given that presumption x is true. In the proposed work the study implements two types of Naive Bayes algorithm such as

i) Multinomial Naïve bayes, and ii) Gaussian Naïve bayes for performance analysis. The model is trained in a supervised manner using the function model. The train takes input argument of feature and training set. The performance evaluation model is carried out with multiple performance metrics.

D. Performance Metrics

This section discusses the performance metrics considered in the proposed system for model evaluation. Accuracy is the ratio of the number of correct predictions over a total number of predictions; it can be computed as follows:

$$\text{Accuracy} = \frac{\alpha + \alpha'}{\alpha + \alpha' + \gamma + \gamma'} \quad (9)$$

In above equation(9), the variable α represents true positive, α' is the true negative metric, γ indicates true negative and γ' represents false negative evaluation metric.

The precision metric is the ratio of correct predictions over a total number of predictions made to the current class. The numerical expression for precision is mentioned as shown in equation (10).

$$\text{Precision} = \frac{\alpha}{\alpha + \gamma} \quad (10)$$

Recall rate is the ratio of correctly predicted values over the number of values in that class. Recall rate can be numerically expressed as shown in equation (11):

$$\text{Recall rate} = \frac{\alpha}{\alpha + \gamma'} \quad (11)$$

F1 score is the weighted mean of precision and recall, which genuinely represents the system's performance. It can be computed as shown in equation (12):

$$\text{F1}_{\text{Score}} = 2 \left(\frac{\left(\frac{\alpha}{\alpha + \gamma} \right) \times \left(\frac{\alpha}{\alpha + \gamma'} \right)}{\left(\frac{\alpha}{\alpha + \gamma} \right) + \left(\frac{\alpha}{\alpha + \gamma'} \right)} \right) \quad (12)$$

V. RESULT ANALYSIS

In this section, the result and performance analysis of the proposed system is discussed. The proposed method for teacher rating based on valuable and non-useful comments is carried out in Python's numerical computing environment. Based on the probabilistic model, two supervised classifiers such as i) Multinomial Naïve Bayes and ii) Gaussian Naïve Bayes, are considered to classify helpful and non-useful comments. These classifiers are selected because they can handle large text datasets and are suitable for natural language processing tasks. Numerical outcomes are shown in Table III. The model training is carried out by 80 % of dataset text samples, i.e., 450 text samples out of 562 text samples, and model testing is carried out with 20% of text samples, i.e., 112 text samples. The performance of the proposed model is measured in terms of multiple performance metrics such as recall, F1-score, and accuracy rate. Fig. 10 shows the performance analysis of the proposed model based on the outcome achieved in terms of accuracy (%).

Fig. 11 compares the outcome achieved from the Gaussian probabilistic model and the multinomial probabilistic model. The graph trend exhibits that the Gaussian Naïve Bayes

outperforms the multinomial naïve byes classifier. The gaussian NB has achieved an 83.74% accuracy rate in the text class prediction, i.e., approximately 75 text samples were correctly predicted out of 112 text samples in the testing dataset. In the case of multi-nominal NB, only 71.15 % of the accuracy rate is achieved with the same training dataset. Total 63 text samples were correctly predicted as useful and non-useful by multi-nominal NB from the total 112 text samples in the testing dataset. The overall analysis suggests that the Gaussian Naïve Bayes classifier achieved a similar performance pattern concerning all metrics such as precision, recall, F1-score, and accuracy. Therefore, the Gaussian Naïve Bayes algorithm is most stable and suitable for comment classification. Apart from this, the proposed system is also assessed concerning processing time. Upon execution over a similar testbed, it is found that the Gaussian Naïve Bayes approach consumes less processing time than the Multinomial approach. The former method is appropriate for addressing prediction problems with multiple classes and hence they are ideal for the proposed study over the educational domain. From the numerical outcomes obtained in proposed analysis, it is seen that there are various rationale behind the improved outcomes of Gaussian Naïve Bayes approach in Machine learning in comparison to Multinomial Naïve Bayes approach. It is undeniable to state that Multinomial Naïve Bayes is one of the effective analytical approach used in natural language processing using probability concept; however, when this is exposed to larger set of dynamic data, irrespective of any domain of data, the prediction accuracy is usually lower in contrast to other schemes. Multinomial Naïve Bayes also computes the probability of all the tags in sample corpus with highest probability however, that is never satisfactory. Apart from this, it cannot be used for any regression and is restricted to forecast numerical value prediction. However, Gaussian Naïve Bayes, when exposed to proposed dataset, is witnessed to work in speedy manner and consumes less time. It is also found suitable for solving prediction of multi-class of data.

TABLE III. NUMERICAL OUTCOME

	Multinomial	Gaussian
Precision	0.726531	0.839381
Recall	0.771429	0.839286
F1-Score	0.715584	0.833227
Accuracy	0.715556	0.839286

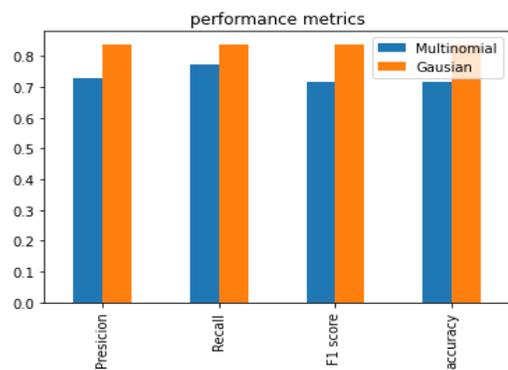


Fig. 11. Comparative Analysis.

VI. CONCLUSION

The study aims to understand feedback data from the teaching aspect, recognize its critical feature to classify comments as applicable and non-useful to score teachers, and lead to high student achievement. The proposed model performs exploratory analysis of the textual feedbacks and identifies unique and common words concerning contextual meaning. Further, the necessary data cleaning process is carried out to make the dataset suitable for comment classification two using the probabilistic model of the supervised learning approach. With a practical and phase-wise data modeling, the proposed model that does not suffer from high dimensional feature space provides a compelling analysis of student feedback that helps improve learning and teaching aspects in knowledge transfer as service platforms, like service MOOCs and e-learning education systems. The result indicated the effectiveness of the Gaussian Naïve Bayes classifier with a higher accuracy rate than the multi-nominal Naïve Bayes classifier.

REFERENCES

- [1] MM. Ghonge, R. Bag, A. Singh. Indian Education: Ancient, Medieval and Modern. In Education at the Intersection of Globalization and Technology 2020 Oct 27. IntechOpen.
- [2] J. Zinkina, A. Korotayev, A. Andreev. Mass primary education in the nineteenth century. In Globalistics and Globalization Studies: Global Transformations and Global Future, pp. 63-70, 2016.
- [3] A. A. Genlott, A. Grönlund, & O. Viberg, Disseminating digital innovation in school – leading second-order educational change. *Educ Inf Technol*, vol.24, pp.3021–3039, 2019.
- [4] J. Fraillon, J. Ainley., W. Schulz, T. Friedman, E. Gebhardt, Students' Use of and Engagement with ICT at Home and School. In: *Preparing for Life in a Digital Age*. Springer, Cham, 2014.
- [5] D. E. Fatumo and S. Ngwenya, "Online learning platforms and their roles in influencing pass rate in rural communities of South Africa: Massive Open Online Courses(MOOCs)," 2nd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2020, pp. 1-8, doi: 10.1109/IMITEC50163.2020.9334135.
- [6] A. Vaibhav and P. Gupta, "Gamification of MOOCs for increasing user engagement," 2014 IEEE International Conference on MOOC, Innovation, and Technology in Education (MITE), 2014, pp. 290-295.
- [7] K. Ingolfsdottir, "Impact of MOOCs and other forms of online education [point of view]," *Proceedings of the IEEE*, 16;102(11), pp.1639-43, 2014.
- [8] M. Alshehri, Alamri, A., Cristea, A.I et al. Towards Designing Profitable Courses: Predicting Student Purchasing Behaviour in MOOCs", Springer-International Journal of Artificial Intelligence in Education, vol.31, pp.215-233, 2021.
- [9] Okoye, K., Arrona-Palacios, A., Camacho-Zuñiga, C. et al. Impact of students evaluation of teaching: a text analysis of the teachers qualities by gender. *Int J Educ Technol High Educ* 17, 49 (2020).
- [10] Sangeetha, K., Prabha, D. Sentiment analysis of student feedback using multi-head attention fusion model of word and context embedding for LSTM. *J Ambient Intell Human*.
- [11] Rajput Q, Haider S, Ghani S. Lexicon-based sentiment analysis of teachers' evaluation. *Applied computational intelligence and soft computing*. 2016 Oct 1;2016.
- [12] Nasim, Zarmeen & Rajput, Quratulain & Haider, Sajjad. (2017). Sentiment analysis of student feedback using machine learning and lexicon based approaches. 1-6. 10.1109/ICRIIS.2017.8002475.
- [13] Tucker B. Student evaluation surveys: anonymous comments that offend or are unprofessional. *Higher Education*. 2014 Sep 1;68(3):347-58.
- [14] Boca GD. Factors Influencing Students' Behavior and Attitude towards Online Education during COVID-19. *Sustainability*. 2021 Jan;13(13):7469.
- [15] Wu XM, Dixon HR, Zhang LJ. Sustainable Development of Students' Learning Capabilities: The Case of University Students' Attitudes towards Teachers, Peers, and Themselves as Oral Feedback Sources in Learning English. *Sustainability*. 2021 Jan;13(9):5211.
- [16] Zughoul O, Momani F, Almasri OH, Zaidan AA, Zaidan BB, Alsalem MA, Albahri OS, Albahri AS, Hashim M. Comprehensive insights into the criteria of student performance in various educational domains. *IEEE Access*. 2018 Nov 14;6:73245-64.
- [17] Dhanalakshmi, V., Bino, D., & Saravanan, A. M. (2016). Opinion mining from student feedback data using supervised learning algorithms. In 2016 3rd MEC international conference on big data and smart city (ICBDSC) (pp. 1–5).
- [18] Nasim, Z., Rajput, Q., & Haider, S. (2017). Sentiment analysis of student feedback using machine learning and lexicon based approaches. In 2017 international conference on research and innovation in information systems (ICRIIS) (pp. 1–6).
- [19] Qi C, Liu S. Evaluating Online Courses via Reviews Mining. *IEEE Access*. 2021 Feb 24;9:35439-51.
- [20] Z. Liu, W. Zhang, J. Sun, H. N. H. Cheng, X. Peng, and S. Liu, "Emotion and associated topic detection for course comments in a MOOC platform," in Proc. Int. Conf. Educ. Innov. through Technol. (EITT), Sep. 2016, pp. 15–19.
- [21] J. Weng, W. Gan, G. Ding, Z. Tian, Y. Gao, and J. Qiu, "SESM: Emotional, social semantic and time series analysis of learners' comments," in Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC), Oct. 2020, pp. 20–28.
- [22] A. Koufakou, J. Gosselin, and D. Guo, "Using data mining to extract knowledge from student evaluation comments in undergraduate courses," in Proc. Int. Joint Conf. Neural Netw. (IJCNN), Jul. 2016, pp. 3138–3142.
- [23] C. K. Leong, Y. H. Lee, and W. K. Mak, "Mining sentiments in SMS texts for teaching evaluation," *Expert Systems with Applications*, vol. 39, no. 3, pp. 2584–2589, 2012.
- [24] A. Kumar and R. Jain, "Sentiment analysis and Feedback Evaluation," 2015 IEEE 3rd International Conference on MOOCs, Innovation, and Technology in Education (MITE), pp. 433–436, 2015.
- [25] Chethan G.S., Vinay S. (2019) Virtual Map-Based Approach to Optimize Storage and Perform Analytical Operation on Educational Big Data. In: Sridhar V., Padma M., Rao K. (eds) *Emerging Research in Electronics, Computer Science and Technology*. Lecture Notes in Electrical Engineering, vol 545. Springer, Singapore.
- [26] Kastrati, Z., Dalipi, F., Imran, A.S., Pireva Nuci, K., and Wani, M.A., 2021. Sentiment Analysis of Students' Feedback with NLP and Deep Learning: A Systematic Mapping Study. *Applied Sciences*, 11(9), p.3986.
- [27] Skedsmo G, Huber SG. Teacher evaluation: the need for valid measures and increased teacher involvement. *Educational Assessment, Evaluation, and Accountability*. 2018 Feb;30(1):1-5.
- [28] Zerihun Z, Beishuizen J, Van Os W. Student learning experience as an indicator of teaching quality. *Educational Assessment, Evaluation, and Accountability*. 2012 May;24(2):99-111.
- [29] Sindhu I, Daudpota SM, Badar K, Bakhtyar M, Baber J, Nurunnabi M. Aspect-based opinion mining on student's feedback for faculty teaching performance evaluation. *IEEE Access*. 2019 Jul 15;7:108729-41.

A Linguistic Analysis Metric in Detecting Ransomware Cyber-attacks

Diana Florea¹

Lucian Blaga University of Sibiu
10 Victoriei Bvd
Sibiu, 550024, Romania

Wayne Patterson²

Patterson and Associates
201 Massachusetts Ave NE, Suite 316
Washington, DC 20002 USA

Abstract—Originating and striking from anywhere, cyber-attacks have become ever more sophisticated in our modern society and users are forced to adopt increasingly good and vigilant practices to protect from them. Among these, ransomware remains a major cyber-attack whose major threat to end users (disrupted operations, restricted files, scrambled sensitive data, financial demands, etc.) does not particularly lie in number but in severity. In this study we explore the possibility of real-time detection of ransomware source through a linguistic analysis that examines machine translation relative to the Levenshtein Distance and may thereby provide important indications as to attacker's language of origin. Specifically, the aim of our research is to advance a metric to assist in determining whether an external ransom text is an indicator of either a human- or a machine-generated cyber-attack. Our proposed method works its argument on a set of Eastern European languages but is applicable to a large(r) range of languages and/or probabilistic patterns, being characterized by usage of limited resources and scalability properties.

Keywords—Cyber-security; cyber-attacks; machine translation; language; Levenshtein distance

I. INTRODUCTION

The recent COVID-19 pandemic has determined an upsurge of remote work that has increased both companies' and end users' exposure to various cyber-attacks. This has complicated an already existing landscape of risks associated with hacking and cyberattacks that the exponential advancement in technologies has brought about. Cyberattacks may be motivated by ideological, financial, or personal reasons and are directed at governments and institutions, businesses and private individuals engendering geopolitical, security, reputational and privacy concerns. While there is a wide literature on the typology, counter measures, policies and security information sharing across state and private sectors [1-8], for our practical purposes, we shall briefly refer in this section to ransomware and ways to address cybersecurity by means of linguistic approaches and instruments.

Ransomware represents a subset of cryptovirology malware that threatens to release and expose the victim's personal information or to permanently disable access to that data until a certain ransom is paid. Whereas some ransomware is designed to lock the system in such a way that it is easily reversible, more advanced malware employs techniques such as cryptoviral blackmail that encrypts the victim's data, rendering them unusable, and demands payment for their decryption [9].

Recovery of data without a decryption key is an uncontrollable problem in a cryptoviral extortion attack, one all the more difficult to trace as crypto currencies, such as Bitcoin, and Dark Web environments are used for completion of ransom payments.

What actually happens in the space between the human brain's complexity and the keyboard strokes on the computers' starred-out password field has been an object of constant inquiry for researchers coming from fields of cognitive sciences, including psychology, philosophy, logic, computer science, neuroscience, etc. In the world of cybersecurity, linguistics has also provided a wide array of approaches, methods and instruments to expose in particular the vulnerability of password creation by exploring various password strength metrics and creation strategies. Such approaches concern lexical patterns (word choices), structural preferences (in composition rules) and syntactic and semantic patterns (such as preference for semantic categories and/or their sequences). Thus, while areas concerning grammar and grammatical rules to crack passphrases [10], or general linguistic patterns in multi-word passphrase selection [11] have been investigated, other practical models and approaches, such as semantic segmentation frameworks of passwords based on Natural Language Processing algorithms [12], phrase generators for cracking pass-phrases [13], probabilistic context-free grammars [14] or predicting technologies [15, 16], represent as many functional models devised to assist in understanding password creation processes and ensuring users' protection in the cyberspace.

With ransomware, linguistic approaches have been either in the form of actual text-analyses (see [8]) or of ransomware detection devices and apps based on linguistic parsing [17]. Two types of linguistic analysis can be distinguished: one that examines the way the source code was written and another that examines the text that was used. While the former examines the code's style and compares it to other pieces of code discovered in malware samples, the latter is more concerned with the word choices made in user dialogues, code comments, input screens, and other user-visible displays. All ransomware includes ransom notes, however, unlike spam and phishing messages, where attackers must impersonate legitimate entities, ransom notes can conceal clues about the writer's proficiency in that language as well as his/her geographic location. Within efforts of linguists who have struggled with the question of attribution (2014 Sony breach, Coin Vault, Shadow Brokers and Guccifer 2.0), has been the infamous *WannaCry*

and *Petya* ransomware attacks, part of which a thorough linguistic and cultural review of ransom notes was conducted so as to determine the native tongue of the authors (Flashpoint 2017). The research found that almost all ransom notes were translated using Google Translate, three of which being likely to have been written by a human rather than machine translated. Further discovered within the same examination was the fact that machine translation into the other languages was performed by using the English note as the source text. Despite such spectacular results, the main attribute of such linguistic analyses as the above is that they try to shed light on the varying levels of language proficiency of attackers, which, in practice, can often obscure the very origin of a ransom attack. Thus, in order to mislead analysts, attackers frequently use red herrings, manipulate time stamps and/or deliberately implant false language clues and insert cultural references and phrases to instill confusion about either their backgrounds or their locations. This makes a linguist's effort a very complex yet an equally critical task. Nonetheless, linguistic examinations of ransom notes are all the more successful if they can be further combined with additional computer science evidence that points the way toward attribution.

This study is structured as follows: Section I includes some preliminary considerations concerning ransomware and a few linguistic approaches and instruments by means of which cybersecurity can be addressed. Section II describes the reason for using the English language (II-A) scope of our research relative to corpus (II-B) and the Levenshtein Distance metric (II-C) whereas Section III presents the research methodology, operations and emerging results. The final Section IV presents the conclusions and the implications of our study for further research in the field.

II. SCOPE OF RESEARCH

Internet access facilitates global outreach which is why a cyber-attack, launched to potentially target any location on Earth, is unconstrained by geography and/or distance. A variable vulnerability may represent the language of the attacker (and/or that) in the ransom notes however recent cases of malicious ransomware indicate that cyber-attackers have been able to develop additional language functionalities, such as the ability to issue ransom demands in as many as 30 languages¹, to enable them to more easily target their cyber-victims worldwide.

In previous studies [7, 8], we have analyzed ransomware external messaging via a mechanism that has involved six extensively used languages (French, Spanish, German, Russian, Chinese, and Hindi) and several round-trip translation (RTT) operations from target language into English using the Google Translate (GT) functionality. Our analysis was then conducted on a number of random quotations from popular culture and English literature and that finally allowed us to devise a procedure which could establish whether a perceived attack was initiated by a human writer with some knowledge of English, or alternatively, by a machine translation. An index

was further advanced to assist the cyber-defender in the profiling of potential human or machine cyber-attacks in which the attack message might have been originally written in a different language than English.

Starting from these assumptions and results, and looking to extend our analysis to other regional zones of interest, the scope of this research is to provide a methodology and a systematic metric to assist in detecting the possible origins (language/location-wise) of a remote cyber-attack potentially originating from the Southeast region of Europe. To conduct this analysis, we will use the GT functionality on a number of sampled texts analyzed in six Southeast European languages (Macedonian, Romanian, Albanian, Bulgarian, Greek and Serbian) through a RTT process (a back and forth translation hereafter referred to as ABA). Additionally, while the effectiveness of GT is under scrutiny as well, several comparisons between the earlier data [7] and the languages that now form the basis of our approach will afford a better grasp of the method we are proposing relative to its general use and scalability properties.

A. The Medium: The English Language Rationale

There are a variety of reasons why a cyber-attack launched from any location on the planet may include text or instructions to the target written in the English language. For one reason, cyber-attackers might perceive that potentially more lucrative targets might be easier to find in the English-speaking world. A second reason may well be that there is a far greater usage of the English language throughout the Internet, which from its very inception tended to be far easier to use than compared to any other language based for example on logograms (Chinese) or the Cyrillic writing system (Bulgarian, Macedonian, Serbian, Russian, etc.). Thirdly, as experience has often shown, non-English language speakers are very likely to use English in their Internet communication and resort to GT whenever cyber-attackers are not proficient in English.

To push the argument further, for any analysis of cyber-attacks involving exclusively the languages of the South Eastern European countries, it would be also reasonable to ask why any measurements of translation effectiveness should use English at all, since there are currently 24 official languages spoken within the Member States of the EU. Being the world's lingua franca, English is spoken by nearly 360 million native speakers worldwide, with slightly less than 60 million of them residing in Europe. It is the most spoken language in the EU (44%) and the most spoken second language by roughly half European language speakers within the 15- 35 age group who can communicate in English. More recent studies [18] assume that English still remains the EU's most spoken language post-Brexit and that the English figure is in reality much higher as English proficiency has recently increased rapidly among young people across the continent.

B. The Corpus: Southeastern European Languages Medium

The Southeastern European countries represent particular zones of interest for cybersecurity issues due to their increasing reputation on digital skills and education, internet usage (Table I), strengthened national cybersecurity capabilities, IT savviness, and increasing number of successful technology companies. In particular, Romania is home to the European

¹For more, see: <https://www.zdnet.com/article/locky-ransomware-how-this-malware-menace-evolved-in-just-12-months/>;
<https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/>

Cybersecurity Competence Center, has a high performance in broadband internet speed and its talent pool in IT is ranked among the best in Europe.

TABLE I. INTERNET USAGE IN THE EASTERN EUROPEAN REGION
SOURCE:(INFO COMPILED BY AUTHORS)

Country	World pop. rank	World population	Internet users	Internet user %	World rank of internet users
North Macedonia	124	2,083,160	1,589,659	76.3%	72
Albania	117	2,930,187	2,105,339	71.8%	81
Greece	58	11,159,773	7,923,438	71.0%	83
Serbia	75	8,790,574	6,182,411	70.3%	85
Romania	45	19,679,306	12,545,558	63.8%	105
Bulgaria	88	7,084,571	4,492,326	63.4%	106

The geographical area of the South Eastern European region and the prevalence of languages throughout this region are the very basis for our examination of cybersecurity issues in this study. The six corpus languages are Albanian, Bulgarian, Greek, Macedonian, Romanian, and Serbian which are spoken by a population of approximately 66 million people (Table II). The area of this study has a population of 51,727,571, which, if it were a single country, would rank 28th in the world by population.

TABLE II. PREVALENCE OF LANGUAGES UNDER CONSIDERATION IN THIS STUDY SOURCE: (INFO COMPILED BY AUTHORS)

Language	Approximate number of speakers in Millions (M)
Romanian	24.3 M
Greek	13.1 M
Serbian	11 M
Bulgarian	8 M
Albanian	6 M
Macedonian	3.5 M

C. The Metric: The Levenshtein Distance

Levenshtein distance is a string metric used in information theory to quantify the difference between two sequences [19]. The Levenshtein distance established between two units/words is the least possible number of single-character modifications required to convert one to the other. The Levenshtein distance (MLD) was modified to elucidate the fact that certain languages swap the positions of parts of speech when performing an ABA translation. Strings are compared until no characters match. Then proceeding forward, the number of mismatched characters are counted until another match is met. Processing is continued until the example ends. MLD is the sum of mismatched pairs. These three examples demonstrate the process.

1) *ERE English-Romanian-English*: Romanian: Dintre toate articulațiile de gin din toate orașele din întreaga lume, ea intră în a mea.

Of all the gin joints in / all the towns / in all / the world, she
Of all the gin joints in / every city /around / the world, she
/ store 9 ↑ store 6 ↑

/ walks into / mine.

/ enters / mine.

/ store 9 ↑

Thus MLD = 9 + 6 + 9 = 24.

2) *EBE English-Bulgarian-English*:Bulgarian: Лъжата се разпростира на половината земя, преди истината да има шанса да си сложи гащите.

A /lie /gets / half / way around / the earth before the

The / lie / spreads to / half / / the earth before the

Store 3↑ store 9↑ / store 9↑

truth has a chance to / get / its pants on.

truth has a chance to / put on / its pants.

/ store 6 ↑

Thus MLD = 3 + 9 + 9 +6 = 27.

3) *EGE English-Greek-English*: Greek: Ένα ψέμα φτάνειστα μισάτηςης πριν η αλήθεια έχειτηνευκαιρία να φορέσειτο παντελόνιτης.

A lie / gets / half / way / around the earth before the truth

A lie /reaches / half / / around the earth before the truth

/ store7 ↑ / store 3 ↑

has a chance to / get its/ pants on.

has a chance to / put on/ her pants.

/ store 6 ↑ store 8↑

Thus MLD = 7 + 3 + 6 + 8 = 24.

III. RESEARCH METHODOLOGY

The goal of this research is to construct a metric that may be used to ascertain the probability that a text retrieved from an external source is representative of a cyberattack, whether human- or machine-initiated. We can capture the text in order to establish a profile against which an unrecognized text can be checked and subject it to the ABA test mentioned above in order to ascertain the original language of the probable cyberattack. We created a sequence of twenty English quotations, half of which are quotations from English literature (Q), Table III and the other half from English popular culture, specifically movies (F). Each text sample was exposed to the ABA procedure in each of the six languages mentioned above.

One can reasonably inquire why familiar English language phrases and film or television dialogue should be employed as a test bed. The rationale is that recognized quotations are more likely to adhere to proper English grammar and syntax, whereas cinema dialogue is frequently intended to emulate actual English conversation, being thus more likely to adhere to the conventions of everyday speech.

TABLE III. TEST QUOTATIONS FROM ENGLISH LITERATURE AND FILM SCRIPTS

No.	Category	Quotation	Length (no. of chars)
T1	F	"I'm as mad as hell, and I'm not going to take this anymore!"	60
T2	Q	When a person suffers from delirium, we speak of madness. When many people are delirious, we talk about religion.	113
T3	F	Of all the gin joints in all the towns in all the world, she walks into mine.	77
T4	F	Open the pod bay doors, please, HAL.	36
T5	F	Mrs. Robinson, you're trying to seduce me. Aren't you?	54
T6	F	Keep your friends close, but your enemies closer.	49
T7	F	If you build it, he will come.	30
T8	Q	A lie gets halfway around the earth before the truth has a chance to get its pants on.	86
T9	F	I have always depended on the kindness of strangers.	52
T10	Q	Sex and divinity are closer to each other than either might prefer.	67
T11	Q	Political correctness is despotism with manners.	48
T12	Q	The only way to get rid of a desire is to yield to it.	54
T13	Q	Whether you think that you can, or that you can't, you are usually right.	73
T14	Q	There are no facts, only connotations.	38
T15	Q	I'm living so far beyond my income that we may almost be said to be living apart.	81
T16	Q	People demand freedom of speech to make up for the freedom of conviction which they avoid.	90
T17	F	Tell'em to go out there with all they got and win just one for the Gipper.	75
T18	F	Round up the usual suspects.	28
T19	F	Love means never having to say you're sorry.	44
T20	Q	The greatest glory in living lies not in never falling but in rising every time we fall."	89
		TOTAL CHARACTERS	1244

The average MLD values, emerging from the translation into one of the available languages and then back to English for each of the test sentences, are provided in Table IV. The sources for the quotations can be found at [8].

This examination is intended to ascertain the cyberattack's original source language. If the other language could be limited to the six instances, the attacked party would be able to condense the spectrum range of probable assault sources. Additional analyses to ascertain the translated material's validity are used.

A. Comparing Literary Quotes (Q) and Film Dialog (F)

Half of the text quotes were taken from Q examples and half from F examples, on the presumption that the majority of writers quoted in literature observe strict grammatical rules and that screenwriters may be more prone to deviate from grammatical norms for achievement of dramatic effect. As a result, we compared the two subsets of Q and F in order to

determine whether translation systems were more accurate in terms of MLD (Table V).

TABLE IV. VALUE OF MODIFIED LEVENSHTAIN DISTANCE (MLD) FOR LANGUAGE PAIRS

ABA Example	Code for Translation	MLD Value Averaged Over All Test Entries
English-Romanian-English	ERE	29.0%
English-Bulgarian-English	EBE	25.1%
English-Macedonian-English	EME	30.2%
English-Greek-English	EGE	30.5%
English-Serbian-English	ESE	26.5%
English Albanian-English	EAE	28.5%
English-French-English	EFE	15.5%
English Spanish-English	ESpE	17.0%
English-German-English	EGeE	20.7%
English-Russian-English	ERuE	32.6%
English-Chinese-English	ECE	35.5%
English-Hindi-English	EHE	30.0%

These findings appear to imply that the translation program works similarly across all sets of cases, regardless of the translation type.

B. Comparing the Most and Least Accurate MLD Measures

The MLD was compared for each language's test bed of twenty items, T1-T20. In terms of accuracy, the six languages under examination fell into two categories (of three languages each): Bulgarian, Serbian, and Albanian, and Greek, Macedonian, and Romanian. Across the entire range of quotes, those for which the MLDs were minimal were found in Table VI.

The identification of specific test items and the MLD values aid in the refinement of the type of test bed that will provide a more precise characterization of the test item. For instance, the T7 test item translation is 94 percent accurate across all ABA language translations chosen. Thus, the T7 is unlikely to be a strong option for determining the source language of a potential hacker. Additionally, Table VII demonstrates the usefulness of the translation type and the test quote. For example, the MLD is zero in six of the test instances T1-T20, indicating that these items are useless for identifying malicious cyberattacks. This is also true for T11 and T14 which correspond to flawless translations in four of our six language pairs.

TABLE V. MLD SCORES ON FILM DIALOGUE (F) AND LITERARY QUOTES (Q)

Language Pair	MLD F Score	MLD Q Score	Total MLD Score	% Difference
English – Romanian	25.54%	20.97%	22.83%	4.57%
English – Bulgarian	17.23%	21.38%	19.69%	4.15%
English – Macedonian	23.17%	24.09%	23.71%	0.92%
English – Greek	22.57%	24.90%	23.95%	2.33%
English – Serbian	21.39%	20.43%	20.82%	0.96%
English – Albanian	21.39%	23.55%	22.67%	2.16%

TABLE VI. QUOTATIONS AMONG T1-T20 WITH MINIMAL AND MAXIMAL MLD VALUES

Minimal MLD Case	Film (F) or Quotation (Q)	MLD Value	Max. MLD Case	Film (F) or Quotation (Q)	MLD Value
T9	F	0.7	T15	Q	30.8
T7	F	2.0	T3	F	27.0
T14	Q	3.3	T8	Q	24.3
T6	F	3.7	T2	Q	23.8
T11	Q	5.3	T16	Q	23.7
T19	F	6.0	T17	F	21.3
T4	F	9.5	T20	Q	21.2
T18	F	9.5	T1	F	19.0
T12	Q	10.8	T10	Q	12.0
T13	Q	11.3	T5	F	11.8

C. Alternative Test to Further Distinguish Eastern European Region Languages

Comparisons are made in this study among the six chosen Eastern European region nations, but the linguistic differences among these nations and their natural languages are somewhat obscured when analyzed in the context of these languages compared to other world languages where the linguistic structures are so different. For example, in an earlier paper [8] we considered more closely related European-based languages compared to Hindi, Russian and Chinese. In order to draw greater distinctions between the set of languages in this study, we used the same test bed (T1-T20) of well-known English language text, and sought to find a subset of the test items that would provide a greater discrimination between the Eastern European languages in the study. One approach to doing this could be to consider subsets of the test items to see if the differences in results applied only to the Eastern European languages would be more pronounced when only a subset of the test items is considered.

To measure the difference in the results for only our six Eastern European countries in consideration, we compute the following. Consider the differences of the results for each pair of languages. In order to ensure that we can eliminate positive and negative differences, we square each comparison of values. For these six languages, there are $(6 \times 5)/2 = 15$ pairs for comparison (Table VIII).

TABLE VIII. CHARACTERS CHANGED IN TRANSLATION FOR EACH LANGUAGE PAIR USING ALL QUOTES T1-T20

	Albanian	Bulgarian	Greek	Macedonia	Romanian	Serbian
Chars changed in translation	282	245	298	295	284	259
Albanian		1369	256	169	4	529
Bulgarian			2809	2500	1521	196
Greek				9	196	1521
Macedonia					121	1296
Romanian						625
Serbian						
Column sum		1369	3065	2678	1842	4167
% of total chars squared		$8936/207025 =$.0043163 (see below)			8936

Calculate the squares of the differences for each of the 15 pairs. For example: Albanian – Bulgarian: $(282 - 245)^2 - 37^2 = 1369$; Macedonia – Romanian: $(295 - 284)^2 = 11^2 = 121$.

Express each term as a fraction of the square of the overall number of comparisons, $N = 1244$ (see page 4). Thus $N^2 = 1547536$. Thus, the Albanian – Bulgarian ratio is $1369/1547536 = 0.00088463$. Averaging all the difference for the 15 comparisons gives a separation factor related to the specific quotation differences, in this case 0.0043163.

In order to be able to distinguish GT for the translation, we look for a subset of the test items where the separation factor is greatest. In that way, we can more easily distinguish which languages were used through the average magnitude of the separation factor. To give a more distinct separation, we choose the following subset of test items, {T1, T3, T13, T15, T17, T20}. Constructing the same table as before, one obtains (Table IX).

Calculate the squares of the differences for each of the 15 pairs. For example: Albanian – Bulgarian: $(120 - 108)^2 - 12^2 = 144$; Macedonian – Romanian: $(155 - 139)^2 = 16^2 = 256$. Express each term as a fraction of the square of the overall number of comparisons, $N = 455$. Thus $N^2 = 207025$. Thus, the Albanian – Bulgarian ratio is $144/207025 = 0.00069556$. Averaging all the difference for the 15 comparisons gives a separation factor related to the specific quotation differences, in this case 0.043163. Thus, the separation ratio is multiplied by approximately 5 between the values calculated (0.043163 vs. 0.00847) for the selected test items { T1, T3, T13, T15, T17, T20 } as compared to all 20 test items T1-T20.

TABLE VII. FONT SIZES OF HEADINGS

Translation Type	No. of Exact Translations (of 20)	Test Quotation (T or Q)	No. of Exact Translations
EBE	5	T9 (F),	5
ERE	4	T11 (Q), T14 (Q)	4
EME, ESE	3	T6 (F)	3
EAE	2	T4 (F)	2
EGE	1		

TABLE IX. CHARACTERS CHANGED IN TRANSLATION FOR EACH LANGUAGE PAIR USING 6 INDICATED QUOTES

	Albanian	Bulgarian	Greek	Macedonia	Romanian	Serbian
Chars changed in translation of subset	120	108	141	155	139	121
Albanian		144	441	1225	361	1
Bulgarian			1089	2209	961	169
Greek				196	4	400
Macedonia					256	1156
Romanian						324
Serbian						
Column sum		144	1530	3630	1582	2050
% of total chars squared			.00847864			8936

IV. CONCLUSION

Despite the fact that the information gathered from the given data set of quotations and language translation methods is to a certain extent limited, the study may be a valuable strategy in real-time detection of ransomware and other cyberattacks because it can narrow the field of suspects of an attack. For instance, if the language used in a suspected attack is exposed to the methods given in this paper, the approaches presented herein may yield critical information on the language of origin used by the attacker. The metric we have presented above is applicable to a large range of languages and is characterized by sustainability, usage of limited resources and scalability properties.

ACKNOWLEDGMENT

The authors are grateful for the contributions and assistance provided by Professor Silvia Florea of the Lucian Blaga University of Sibiu, Romania.

REFERENCES

[1] Ablon, Lillian, Martin C. Libicki and Andrea A. Golay. *Markets for Cybercrime Tools and Stolen Data*. RAND Corporation. 2014.

[2] Carr, Madeline. *Public-private Partnerships in National Cyber-security Strategies*. Chatham House, January 2016.

[3] Deibert, Ron. *Bounding Cyber Power: Escalation and Restraint in Global Cyberspace. Internet Governance Papers: Paper No. 6*. Center for International Governance Innovation. 2013.

[4] Deibert, Ron. *The Geopolitics of Cyberspace After Snowden. Current History* 114, no. 768. 2015, pp 9–15.

[5] Libicki, Martin C., Lillian Ablon, Timm Webb. *The Defender's Dilemma: Charting a Course Toward Cybersecurity*. RAND Corporation. 2016.

[6] Meyer, Paul. *Outer Space and cyberspace: A Tale of Two Security Realms*. In *International Cyber Norms: Legal, Policy & Industry Perspectives* edited by Anna-Maria Osula and Henry Røigas, NATO CCD COE Publication, Tallinn, 2016.

[7] Patterson, Wayne and Cynthia Winston-Proctor, *Behavioral Cybersecurity*, CRC Press, 2018, pp 178.

[8] Patterson, Wayne, Acklyn Murray and Lorraine Fleming, *Distinguishing a Human or Machine Cyberattacker*, Proceedings of the 3rd Annual Conference on Intelligent Human Systems Integration, Modena, Italy, February 2020, pp. 335–340.

[9] Young, A. and Moti Yung. *Malicious Cryptography: Exposing Cryptovirology*. Wiley, 2004.

[10] Rao, A., B Jha G Kini. *Effect of Grammar on Security of Long Passwords*. Proceedings of the 3rd ACM Conference on Data and Application Security and Privacy, Ser. CODASPY '13. New York, NY, USA: ACM, 2013, pp. 317–324.

[11] Bonneau, Joseph, Ekaterina Shutova. *Linguistic Properties of Multi-Word Passphrases*. Proceedings BS12 of USEC '12: Workshop on Usable Security, March 2012.

[12] Veras, R., C Collins, J Thorpe. *On the Semantic Patterns of Passwords and Their Security Impact*. NDSS. Internet Society, 2014.

[13] Sparell, Peder, Mikael Simovits. *Linguistic Cracking of Passphrases Using Markov Chains*. Cryptology ePrint Archive, Report 2016/246.

[14] Weir, M., Aggarwal, S., Medeiros, B. D., and B. Glodek. *Password Cracking Using Probabilistic Context-Free Grammars*. Proceedings of the IEEE Symposium on Security and Privacy, 2009, pp 391–405.

[15] Ur, Blasé et al. *The Art of Password Creation*. *34th IEEE Symposium on Security and Privacy, SP '13, IEEE*, May 2013. <http://passwordresearch.com/papers/paper442.html>

[16] Komanduri, Saranga et al. *Telepathwords: Preventing Weak Passwords by Reading Users' Minds*. Proceedings of the 23rd USENIX Security Symposium. August 20–22, 2014. San Diego, CA.

[17] Alzahrani, A., Alshehri, A., Alshahrani, H., Alharthi, R., Fu, H., Liu, A., & Zhu, Y. *RanDroid: Structural Similarity Approach for Detecting Ransomware Applications in Android Platform*. 2018 IEEE International Conference on Electro/Information Technology (EIT), 2018, pp 0892–0897.

[18] Keating, Dave. "Despite Brexit, English Remains The EU's Most Spoken Language By Far". *Forbes*. Retrieved 7 February 2020.

[19] Levenshtein, Vladimir I. *Binary codes capable of correcting deletions, insertions, and reversals. Soviet Physics Doklady*. February 1966, 10 (8): pp. 707–710.

ONLINE SOURCES

<https://www.flashpoint-intel.com/blog/linguistic-analysis-wannacry-ransomware/>

<https://www.theguardian.com/technology/2017/may/17/hackers-shadow-brokers-threatens-issue-more-leaks-hacking-tools-ransomware>

<https://www.vice.com/en/article/d7ydwy/why-does-dnc-hacker-guccifer-20-talk-like-this>

https://www.theregister.com/2015/09/18/coinvault_ransomware_arrests_dutch_netherlands/

<https://www.bbc.com/news/business-34589710>

<https://www.zdnet.com/article/locky-ransomware-how-this-malware-menace-evolved-in-just-12-months/>

<https://www.zdnet.com/article/ransomware-an-executive-guide-to-one-of-the-biggest-menaces-on-the-web/>

Design and Implementation of Dynamic Packet Scheduling with Waiting Time Aware: DPSW2A

K Raghavendra Rao¹

Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation
Vaddeswaram-522502, Guntur, Andhra Pradesh, India

B N Jagadesh²

Professor, Department of CSE
Srinivasa Institute of Engineering & Technology
Amalapuram, Andhra Pradesh, India

Abstract—One of the principal goals of 5G is to enhance performance in connection with speed and delay curtailment. To accomplish this, IETF has proposed Multipath TCP to utilize the accessible interface for communication. The demand for mobile communication is escalating day by day. The predominant communication option for people is mobile. For giving better service for users, nodes are fitted out with multiple interfaces. Multiple interfaces are as well one of the benefits of 5G. Multi path protocols are used to load balancing and resilience to failure. When communicating with asymmetric interfaces, latency is an imperative factor. To attain low latency is hard when asymmetric interfaces are used. When communication happens using multiple interfaces, the scheduler plays a central role since it decides which interface needs to be used for the packet. In this article we spotlight on scheduling algorithms, how this schedule will play a vital role to transfer data to receiver nodes with low latency. In this paper, we emphasize on the Scheduler named DPSWWA with the objective of minimizing delay and effective usage of interfaces.

Keywords—MPTCP; scheduler; latency; delay; transport protocol; waiting time

I. INTRODUCTION

Mobile devices are one of the predominant communication devices to users. Mobile devices are steadily increasing day by day. Mobile devices are equipped with multiple interfaces like 3G and Wi-Fi interface for better communication. Many researchers are developing algorithms for multipath communication. Multipath TCP provides resilience to failure and better communication [1]. When compared to single path TCP, MPTCP will give better performance [2]. Mainly multipath TCP is useful in one of the scenarios is data centers [3]. Latency is more important for sensitive applications [4]. Latency is very important when the interfaces are asymmetric [28]. This paper mainly focused on scheduling data packets using MPTCP protocol to multiple interfaces of type asymmetric. Here we mentioned some of the widely used state-of-the-art MPTCP schedulers. Most of the schedulers are not effectively utilizing and reaching the goal of MPTCP in terms of using all interfaces. In this paper we propose an algorithm Dynamic Packet scheduling with Waiting time Aware (DPSWWA). We mainly focused on how to effectively utilize the interface and schedule the packets not to occur late at the receiver end. This paper covers both the implementation and the design of scheduling techniques in the Linux kernel. The result shows that DPSWWA fulfill its design goals.

Compared to existing default MPTCP schedulers DPSWWA is increasing the speed of communication between nodes.

This article is structured as follows: Section II presents background; Section III presents the state-of-the-art-of-the MPTCP scheduler, Section IV presents the state-of-the-art-of-the schedulers, Section V discussed about DPSWWA, Section VI evaluated through experiments with the goal of less latency. Throughout this scenario we use web traffic. In Section VII, we present an evaluation report. In Section VIII, we present conclusion and in Section IX is presented the future enhancement.

II. PARALLEL RESEARCH WORK

Smart phones are equipped with multiple interfaces. The advantage of multiple interfaces is easy to handover from one interface to another interface when a problem occurs. This advantage is given to mobile devices to grow like anything and make it the people predominant communication device. MPTCP was designed as an alternative to TCP for working on multiple interfaces at the same time. The available Transport protocols are not supported to multiple interfaces used at the same time. So we need new protocols to support multiple interfaces at the same time. IETF is standardized by MPTCP in RFC 6824[5]. There are commercial applications that use MPTCP; one of the MPTCP used is Apple Siri [6]. Fig. 1 shows how the MPTCP can transfer the data to multiple sub-flows, once it receives data from the application layer.

Fig. 1 shows how data is delivered from sender application layer to receiver network layer via MPTCP sub layer. Once data is available to the application layer it can send the data to the transport layer. Here MPTCP protocol comes into picture, by taking data from the upper layer it sends the packets to all available flows. MPTCP considers all the factors before sending the packet to sub-flow. Like RTT, when MPTCP contains more than one sub flow, then the scheduler will decide which sub-flow should send packets. Which sub-flow has lowest round trip time. The scheduler will select that sub-flow with consideration of the network properties.

Fig. 2 represents the MPTCP connection establishment from client to server or node/node. Connection establishment of MPTCP is same as to TCP. Here MPTCP can create a one connection first then he will establish another connection to server. Initially client sends a request packet to server, then server will accept that request and sends the acknowledgment. Once the client has received the acknowledgment it is send to

server segment. Once the first flow connection establishment is over then client can create another flow connection from client to server. In this manner a client can create multiple flow form client to server. The diagram clearly represents the connection establishment flow from source to destination or client to server or one node to another node. The comprehensive connection establishment is also known as MPTCP 3-way handshake.

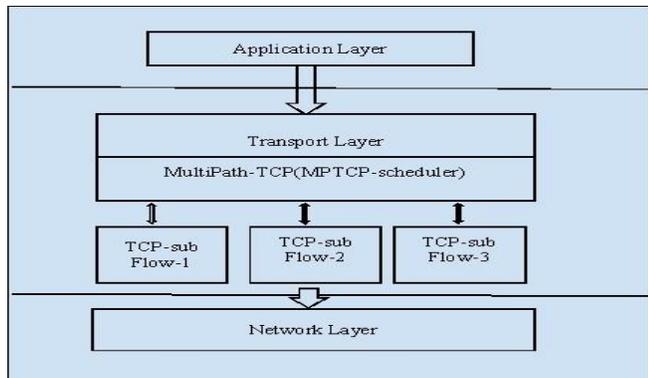


Fig. 1. Data flow from Application to Network via MPTCP.

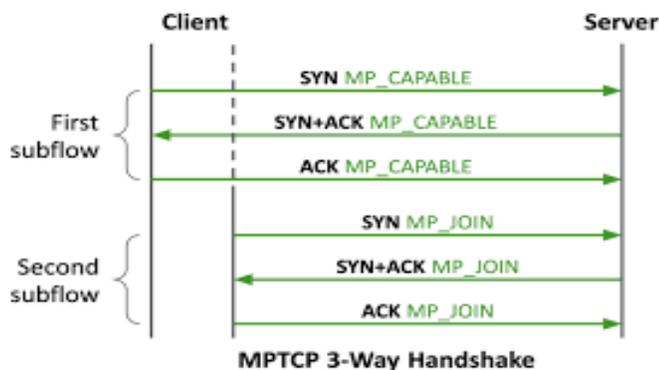


Fig. 2. MPTCP Connection Establishment.

Fig. 3 represents the connections/flows from sender to receiver or client to server or client host to server host. The above picture shows two flows from client to server. Here one flow is from Wi-Fi and another flow is 3G/4G/LTE connection. The above two flows are simultaneously used to transfer the data from client to server.

available flow. When the MPTCP buffer received the data from upper layer, then it can check all available resources like path characteristics and send the packet to flows. The above diagram represents two flows from sender to receiver. One flow is named as sub-flow-1 and another flow is named as sub-flow-2. The characteristics of flows are flow-1 rtt time is 10ms, cwnd is 30 bytes and flow-2 rtt is 30 ms and cwnd is 30 bytes.

Most of the communications requires data in the same order as what the sender sends. Multipath protocol splits data to different flows, so chances are there to receive the packets out of order on the receiver side. When data arrives out of order many problems may occur. Some of the well-known problems are discussed in [7].

Fig. 6 explains problems of transmitting data over asymmetric paths.

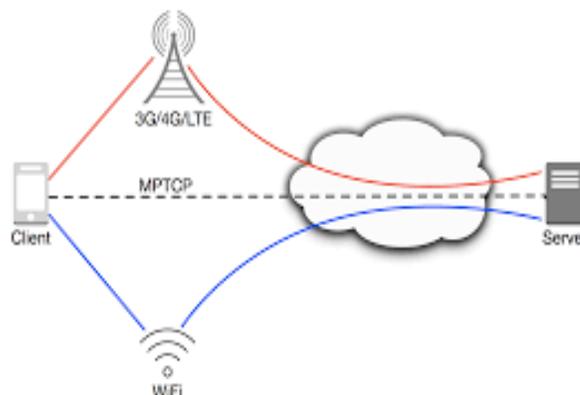


Fig. 3. MPTCP Connection Representation from Sender to Receiver.

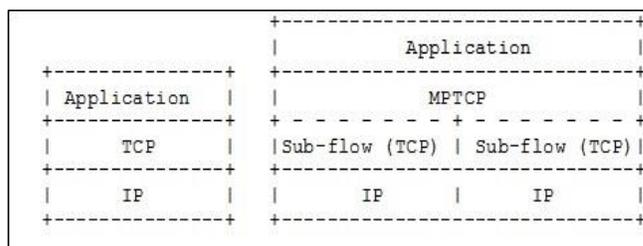


Fig. 4. Comparison of Standard TCP and MPTCP Protocol Stacks.

Fig. 4 presents protocol stack of TCP and MPTCP. In TCP we can make use of only one interface communication whereas MPTCP can use multiple interfaces at the same time using multiple interfaces. MPTCP have multiple interfaces to transfer the data from client to server / node to node.

Fig. 5 represents the functional flow from sender application layer to receiver buffer. Here data flow will start from multiple flows. More exactly once data is available from application layer to MPTCP send buffer, then MPTCP send buffer will apply scheduling algorithm to schedule the segments to available flows not to occur HOL problem, receiver buffer problem and out-of-order packets problem. Here scheduler plays a vital role to schedule the segments to

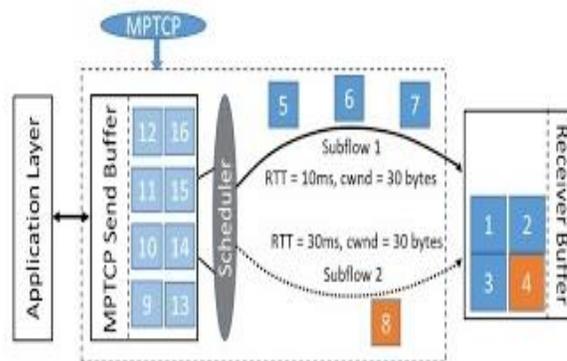


Fig. 5. Data flow from Sender Application Layer to Receiver Buffer.

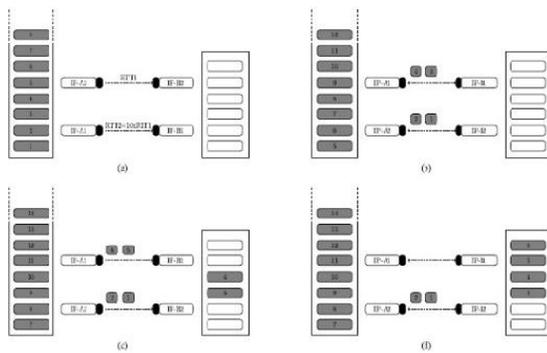


Fig. 6. Represents the Work Flow of Sender and Receiver, how the HOL Problem Occurs.

Here two nodes are communicating using two paths to share information. In the two paths path one has the RTT 10 times larger than the path two. Segments are transferred to 1, 2 using slow path and 3,4 using fact path Fig. 6b. Fig. 6c represents a well-known problem of HOL. Where 3 and 4 received and kept buffered until received 1,2. So it introduces delay in delivering data to applications explained in Fig. 6d. If the receiver buffer is filled with unordered packets then the sender will block them from sending. Then will face reduced throughput and increased delay. So to address this issue, we are very careful while selecting interfaces to use segment segments using multipath protocols. For work explained in this article, the Linux Kernel implementation. Some variants are available LowRTT [8]. Now take one example to send 15 packets using MPTCP. One flow is using 3G and another flow is used with WLAN. One of the interfaces is WLAN having RTT 10ms and another one having 100 ms in 3G of RTT. Now if we apply LRTT it immediately uses 10ms flow instead of 100ms flow. Initial congestion window will take 10 segments. First 10 will send in fast flow remaining 5 segments will send in slow sub flow. To address the buffer problem many researchers have put forward schedulers for MPTCP. The four state-of-the-art-of-the schedulers DAPS, ECF, OTIAS, BLEST will be explained in the next section.

S. Habib, [13] present a report on the need for a single path to multipath TCP. They offer multiple features like load balancing and reduced delay.

Y.-C. Chen [14] mentioned the advantages of multipath over single path; flow capacity and how scheduling will affect the performance.

M. Baerts, [15] has identified the gap between TCP and MPTCP; he implemented the MPTCP in android smartphones to understand the performance of heavy applications.

L. Ji, [16] studied multipath TCP; he mentioned the advantages of multipath TCP in mobile communication and gained less delay by considering the low rtt flows.

B. Briscoe [17] specifies the sources of reducing performance of multipath tcp in terms of latency and throughput.

S. Ferlin [4] finds the results of asymmetric links do not make MPTCP performance better than TCP.

A. Barnstorm, [18] mentioned his report on cloud based multipath mobile communication he mentioned how the latency has decreased and improved the performance of cloud based communication.

M. Wang [19] assessed the MPTCP in high quality video streaming, he assessed the video streaming with multiple interfaces facing issues. He mentioned data retransmission also.

A. Gurney, [20] specifies that low latency is not achieved by using multiple paths, but we can achieve low latency by using a good scheduler. He mentioned that scheduling plays a vital role in the MPTCP packet scheduling when having multiple interfaces.

S. Alfred son, [21], specifies that Network delay and latency plays a very important role in cellular networks. He studied a detailed report on delay in respect to network, application and transport application perspective.

J. Huang, [22], specifies that lower latency and higher bandwidth is attracting many users. He discovered various limitations in TCP over LTE. He proposed a novel and light weight algorithm to estimation of bandwidth. Based on his observation many tcp connections are under utilizing the available bandwidth.

J. Vehkaperä, [23], specifies the optimized scheduling based on the traffic. He suggests that for scheduling on different types of traffic different types of mechanism is needed. Making network aware applications play a vital role in scheduling segments.

G. Texier, [24], online video services are sensitive to overall quality of video stream and a more important factor is latency between video generation and video playback. He addresses some of the problems in video streaming. He proposed an implementation of multipath video delivery at the application level.

A. Alheid, [25] specifies that multipath TCP achieves higher bandwidth and higher resilience against network path failures. He mentioned how out-of-order packets affect the communication. He specifies how best we can re-order the packet technique.

N. Kuhn, [26] specifies that the increasing heterogeneity and asymmetry in network communication makes delay and quality of service to be a challenging task. He proposed a novel scheduling algorithm to reduce the receiver buffer blocking problem.

J. Rexford, [27], points out delay sensitive applications like video streaming, voice over IP and live streaming requires low end-to end delay. Recent year's popularity of low delay applications has increased. He proposed an algorithm that minimizes the end-to-end delay experienced by inelastic traffic.

III. STATE-OF -THE-ART-OF-THE MPTCP SCHEDULER

MPTCP default scheduler will allocate packets to the facts path by considering the congestion window with low RTT [8].

This will work fine in symmetric paths but not in asymmetric paths like 3G and WLAN.

1) *Delay aware packet scheduling*: The main goal of this scheduler is to send segments to the receiver in order. DAPS [9] can send segments to the receiver by considering only “not to block the receiver buffer”. It can send the data to sub flows. First it selects which sub-flow to use then it determines which segment to send which sub-flow and last it sends data segments according to the selected sub-flow.

2) *Out-of-order-transmission-for-in-order-arrival*: TIAS [10] sends the packets based on the low RTT. It uses simplification of $RTT/2$. Here with, it considers the one way delay. OTIAS differs from LRTT and DAPS. Every time OTIAS calculates the transfer time for every packet then it selects the flow which has very less transfer time flow.

3) *Earliest completion first*: ECF [11] addresses the issue of performance degradation problems that come from path asymmetric. It minimizes the fast path waiting time. ECF can consider the parameters $CWND$, RTT A and data available to send. By considering the factors ECF schedules the packets to sub-flow. ECF can wait and send data to the fast path.

4) *Block estimation scheduler*: BLEST [12], which aims to, reduce the buffer blocking of receiver buffers in heterogeneous networks. By increasing throughput and reducing spurious retransmission. It increases the good-put also.

IV. START-OF-THE-ART-OF-THE SCHEDULER EVALUATION AND DISCUSSION

For WLAN/3G, we observe the OTIAS is similar to LRF and DAPS, ECF worse than LRF. BLEST gives better performance compared to DAPS.

Fig. 7 is the functional flow diagram of default RTT algorithm and Fig. 8 is the proposed algorithm functional flow. Fig. 9 shows the good put of WLAN/3G.

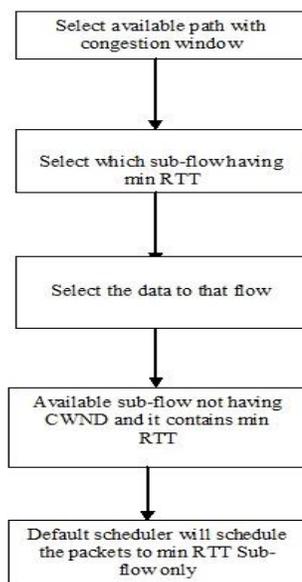


Fig. 7. Functional flow Diagram for Default Min-RTT Scheduler.

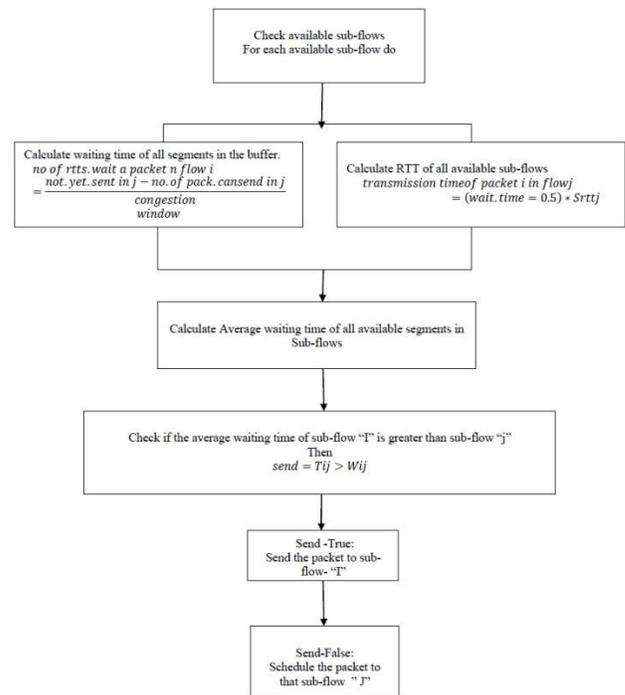


Fig. 8. Functional flow Diagram for Proposed DPSWWA Scheduler.

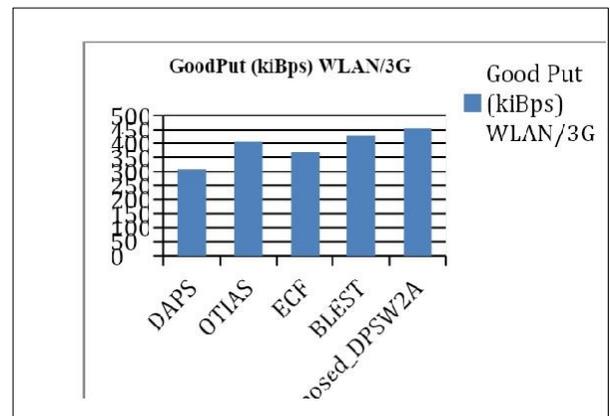


Fig. 9. Illustrates the Performance of State-of-the-art-of-the Scheduler using Bulk Transfer; we Consider the Good-put as a Metric.

V. PROPOSED METHODOLOGY

Waiting-Aware MPTCP-Scheduler: Design and Implementation.

Asymmetric interfaces flow, to avoid out-of-order delivery, delay can be reduced. However, state-of-the-art-of-the schedulers do not completely address this issue. To address this issue, we introduce the new scheduling algorithm: DPSWWA.

A. DPSWWA

The main idea of DPSWWA is to utilize all the available sub flows and reduce the delay in segment delivery to the receiver. Here we explained the design of DPSWWA, new metric to estimate the waiting time of sub flow that might result from scheduling the segment on an available flow. The DPSWWA algorithm 1 is present in

Algorithm 1: Proposed Algorithm: DPSW2A

Step1: Schedule the packet
Step2: Calculate waiting time of flow
Step3: waiting=RTT of fast path /2
Step4: if Fast path waiting time >= Waiting
Step5: then calculate the packet Arrival Time
Step6: if packet arrival time is equal to slow path of RTT/2
Step7: then
Step8: send the packet into available flow J else
Step9: Select the another path of available cwnd with min rtt to send
Step10: Calculate arrival time of the packet
Step11: Do

To address the issue of not utilizing all sub flows, we present a dynamic scheduling algorithm with waiting time awareness. MPTCP maintains the send window on connection level for each connection, which is necessary for multiplexing the data. DPSWWA assumes that the provided segment will occupy the space in the MPTCP window. We infer all packets in the window will wait at the same time.

We estimate the data that will send on flow during one RTT. For every RTT we increase by 1segment of the congestion window.

$$rtts=RTTSRTTF \tag{1}$$

$$x=MSSF(CWND+(rtts-1)2)*rtts \tag{2}$$

1) *Functional comparison of LRF and DPSWWA*: We will show how scheduling decisions are made by LRF and DPSWWA. The data shown in Fig. 4 was collected from emulation experiments using Linux with an enabled MPTCP kernel. We show how the scheduler act when a burst of 15 segments are sent by an application using tow flows. Paths RTT are p1=10ms and p2=100ms, the availability capacity for both paths have taken (0.5Gbits/s) and congestion window capacity is 10 segments.

First we consider the LRF scheduler 4a when scheduling first 6 packets are selected path p1 having 10ms of rtt. Then 6.7 are selected to 100ms flow. We allocate segments to all flows because of TSQ mechanism. After the two segments are scheduled to slow path, then remaining packets are scheduled to fast path, after the window full of fast flow schedulers schedule the packets to slow path.

The scheduling decision of DPSWWA is made with waiting time of flows. DPSWWA schedule the packets to fast flow once the window is full, then it moves to slow path equation taken from [10].

$$RTTOWAITJI=(NOTYETSENTJ-PACKCANSENDJCWNDJ)$$

Packets are scheduled based on the waiting time of fast path, then the scheduler will schedule the packets to slow path.

VI. EVALUATING DPSWWA

To assess the blocking and overuse of fast flow, we performed controlled experiments comparing the performance of LRF and DPSWWA. We evaluated latency and throughput

of the scheduler. The scheduler is evaluated in Linux kernel implementation and the results are reported in section

VII. EXPERIMENTAL SETUP

We implemented this experiment in Linux Kernel and NS-3 Implementation; setup is consisting of two machines. A client, two Wireless access points (WLAN/3G), a server accessing router equipped with two interfaces. We used Experiment, throughput and latency. Table mentioned the parameters used in the experiments.

To enable MPTCP communication between two nodes, the nodes were equipped with the MPTCP-enabled Linux kernel. The client used the MPTCP kernel and a server equipped with a modified DPSWWA MPTCP Linux kernel. For experiment, MPTCP was configured to use path one as the primary path. Table I has Network Parameters.

A. Throughput and Latency

We assess the scheduler’s latency and throughput; we compare transmission of two paths. (Path one has 10 to 50 ms and path 2 having 10 to 50ms).

Below Diagram shows the results of the experiment, the y-axis shows the transmission time from sender to receiver. X-axis shows the size of the segment to transfer the sender to receiver.

Fig. 10 will shows the transmission time of all algorithms, Fig. 11 has mentioned the page load time of algorithms with page load time. Table II has site information, objects size and size. Fig. 12 shows the path sharing of WLAN and 3G.

The difference among the scheduler, LRF scheduler with approximately 67% of the traffic over WLAN, BLEST a little more 72 % of traffic will use WLAN and DPSWWA is 79% of traffic use WLAN.

TABLE I. NETWORK CHARACTERISTICS, LATENCY AND THROUGHPUT EXPERIMENT

Path/Parameter	Latency and Throughput	
	Path-1	Path-2
Capacity [Mbps]	100	100
Delay[ms]	10...50	10...50
Loss[%]	0	0

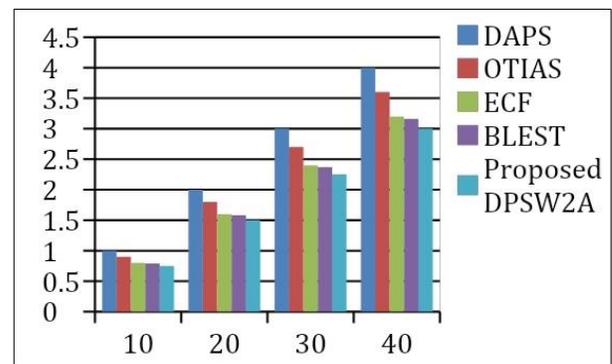


Fig. 10. Average Transmission Time for Burst of different Sizes over Sub-flows with Asymmetric Paths.

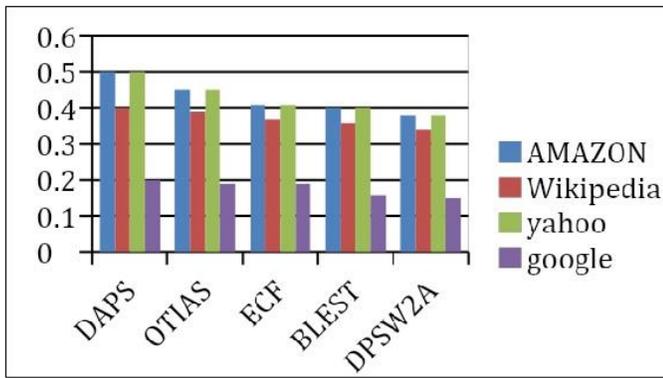


Fig. 11. Represent the Page Load Time of different Site of Schedulers.

TABLE II. WEB SITES USED IN THE EVALUATION

Web Site	Objects	Total Size[Kbits]
Amazon	10	300
Google	15	120
Wikipedia	19	40
Yahoo	22	250

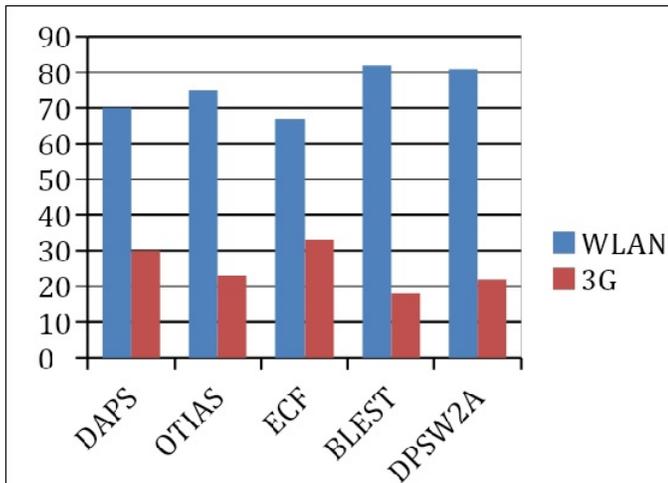


Fig. 12. Represents the Path Load Share between WLAN and 3G for Real Experiment.

VIII. CONCLUSION

The present-day devices are outfitted with multiple interfaces. Networks are often multipath. A node can extend to another node by utilizing multiple paths. For example, mobile phones have multiple interfaces and data centers having redundant paths to transfer the data. It has been shown to increase delay and throughput/output when using asymmetric interfaces. The rationale for poor performance can be encountered with the scheduler. If the scheduler will react dynamically to schedule the packet, then we achieve less delay and more throughputs. This paper provides in-depth analysis of state-of-the-art-of-the scheduler (DAPS, ECF, OTIAS, BLEST) for MPTCP to problems of asymmetric. DPSWWA is schedule the packet and reduce the delay and increase more throughputs with using all available paths.

IX. FUTURE ENHANCEMENT

Future work includes refinement of the DPSWWA to schedule packets in more network changes.

REFERENCES

- [1] Paasch, Christoph, and Olivier Bonaventure. "Multipath tcp." *Communications of the ACM* 57.4 (2014): 51-57.
- [2] Wischik, Damon, et al. "Design, Implementation and Evaluation of Congestion Control for Multipath TCP." *NSDI*. Vol. 11. 2011.
- [3] Raiciu, Costin, et al. "Improving datacenter performance and robustness with multipath TCP." *ACM SIGCOMM Computer Communication Review* 41.4 (2011): 266-277.
- [4] Ferlin, Simone, Thomas Dreiholz, and Özgü Alay. "Multi-path transport over heterogeneous wireless networks: Does it really pay off?." *2014 IEEE Global Communications Conference*. IEEE, 2014.
- [5] Ford, Alan, et al. "TCP extensions for multipath operation with multiple addresses." (2013).
- [6] "Advances in Networking" (WWDC), <https://developer.apple.com/videos/wwdc2017>.
- [7] Yedugundla, Kiran, et al. "Is multi-path transport suitable for latency sensitive traffic?" *Computer Networks* 105 (2016): 1-21.
- [8] Paasch, Christoph, et al. "Experimental evaluation of multipath TCP schedulers." *Proceedings of the 2014 ACM SIGCOMM workshop on Capacity sharing workshop*. 2014.
- [9] Sarwar, Golam, et al. "Mitigating receiver's buffer blocking by delay aware packet scheduling in multipath data transfer." *2013 27th international conference on advanced information networking and applications workshops*. IEEE, 2013.
- [10] Yang, Fan, Qi Wang, and Paul D. Amer. "Out-of-order transmission for in-order arrival scheduling for multipath TCP." *2014 28th international conference on advanced information networking and applications workshops*. IEEE, 2014.
- [11] Lim, Yeon-sup, et al. "ECF: An MPTCP path scheduler to manage heterogeneous paths." *Proceedings of the 13th international conference on emerging networking experiments and technologies*. 2017.
- [12] S. Ferlin and C. Paasch. (2017). MPTCP BLEST Linux Kernel Implementation.
- [13] Habib, Sana, et al. "The past, present, and future of transport-layer multipath." *Journal of Network and Computer Applications* 75 (2016): 236-258.
- [14] Chen, Yung-Chih, et al. "A measurement-based study of multipath tcp performance over wireless networks".
- [15] De Coninck, Quentin, et al. "Observing real smartphone applications over multipath TCP." *IEEE Communications Magazine* 54.3 (2016): 88-93.
- [16] Han, Bo, et al. "An anatomy of mobile web performance over multipath TCP." *Proceedings of the 11th ACM Conference on Emerging Networking Experiments and Technologies*. 2015.
- [17] Briscoe, Bob, et al. "Reducing internet latency: A survey of techniques and their merits." *IEEE Communications Surveys & Tutorials* 18.3 (2014): 2149-2196.
- [18] Grinnemo, Karl-Johan, and Anna Brunstrom. "A first study on using MPTCP to reduce latency for cloud based mobile applications." *2015 IEEE Symposium on Computers and Communication (ISCC)*. IEEE, 2015.
- [19] Wu, Jiyan, et al. "Streaming high-quality mobile video with multipath TCP in heterogeneous wireless networks." *IEEE Transactions on Mobile Computing* 15.9 (2015): 2345-2361.
- [20] Arzani, Behnaz, et al. "Impact of path characteristics and scheduling policies on MPTCP performance." *2014 28th International Conference on Advanced Information Networking and Applications Workshops*. IEEE, 2014.
- [21] Garcia, J., Alfredsson, S., & Brunstrom, A. (2015, June). Delay metrics and delay characteristics: A study of four Swedish HSDPA+ and LTE networks. In *2015 European Conference on Networks and Communications (EuCNC)* (pp. 234-238). IEEE.

- [22] Huang, Junxian, et al. "An in-depth study of LTE: Effect of network protocol and application behavior on performance." *ACM SIGCOMM Computer Communication Review* 43.4 (2013): 363-374.
- [23] Ojanperä, Tiia, and Janne Vehkaperä. "Network-assisted multipath DASH using the distributed decision engine." *2016 International Conference on Computing, Networking and Communications (ICNC)*. IEEE, 2016.
- [24] Houze, Patrice, et al. "Applicative-layer multipath for low-latency adaptive live streaming." *2016 IEEE International Conference on Communications (ICC)*. IEEE, 2016.
- [25] Alheid, Amani, Angela Doufexi, and Dritan Kaleshi. "A study on MPTCP for tolerating packet reordering and path heterogeneity in wireless networks." *2016 Wireless Days (WD)*. IEEE, 2016.
- [26] Kuhn, Nicolas, et al. "DAPS: Intelligent delay-aware packet scheduling for multipath transport." *2014 IEEE International Conference on Communications (ICC)*. IEEE, 2014.
- [27] Javed, Umar, et al. "Multipath protocol for delay-sensitive traffic." *2009 First International Communication Systems and Networks and Workshops*. IEEE, 2009.
- [28] Hurtig, Per, et al. "Low-latency scheduling in MPTCP." *IEEE/ACM Transactions on Networking* 27.1 (2018): 302-315.

Evaluating Domain Knowledge and Time Series Features for Automated Detection of Schizophrenia from EEG Signals

Saqib Hussain¹, Nasrullah Pirzada², Erum Saba³, Muhammad Aamir Panhwar⁴, Tanveer Ahmed⁵

Department of Telecommunication Engineering^{1, 2, 5}
Information Technology Centre³

Department of Bio-Medical Engineering⁴
Mehran University of Engineering & Technology, Jamshoro, Sindh, Pakistan^{2, 4, 5}
Sindh Agriculture University Tandojam, Sindh, Pakistan³

Abstract—Over the recent years, Schizophrenia has become a serious mental disorder that is affecting almost 21 million people globally. There are different symptoms to recognize schizophrenia from healthy people. It can affect the thinking pattern of the brain. Delusions, hallucinations, and disorganized speech are the common symptoms of Schizophrenia. In this study, we have used electroencephalography (EEG) signals to analyze and diagnose Schizophrenia using machine learning algorithms and found that temporal features performed well as compared to statistical features. EEG signals are the best way to analyze this disorder as they are intimately linked with human thinking patterns and provide information about brain activities. The present work proposes a Machine Learning (ML) model based on Logistic Regression (LR) along with two feature extraction libraries Time Series Feature Extraction Library (TSFEL) and MNE Python toolkit to diagnose Schizophrenia from EEG signals. The results are analyzed based on 5 different sampling techniques. The dataset was cross-validated using leave one subject out cross-validation (LOSOCV) using Scikit learn and achieve greater accuracy, sensitivity, specificity, macro average recall, and macro f1 score on temporal features respectively.

Keywords—Artificial intelligence (AI); Logistic Regression (LR); smote-class weight (S-CW); borderline smote-class weight (BS-CW); electroencephalography; Time Series Feature Extraction Library (TSFEL)

I. INTRODUCTION

Schizophrenia is one of the most common and severe mental disorders which is affecting more than 21 million people around the globe [1] and almost 50% of the total population of men [2] are suffering from this mental disease than women. This mental disorder directly affects the thinking pattern of human beings if it is not treated properly and can cause discrimination, stigmatization, and disobedience of human rights [3], [4].

Delusions, hallucinations, and disorganized speech [5] are the most common examples of this severe psychotic disorder. Hallucinations are sensory illusions that appear to be real [6] but are generated by your mind. Delusions are false beliefs that contradict reality and are not true. One cannot distinguish between what is real and what is imagined [7]. The patients

having this psychotic disorder have a relative life expectancy is between 10 to 15 years and it also increases the risk of suicide to 10% which is not a great sign for human beings [8].

The diagnosis and analysis of schizophrenic patients can be done through the use of electroencephalogram (EEG) signals [9], [10]. The EEG signals have unique characteristics, variability, and dimensionality [11] as they can provide information about the electrical activities of a human brain [12], [13], and also they have the great potential to predict whether a person is a healthy control or schizophrenic [14]–[16]. In the medical field, EEG signals have vast applications like it can be used to detect epilepsy, comma, clinical death, and schizophrenia [17]. The scalp-based activity of EEG signals exhibits oscillations at different frequencies [18]. The main advantage of using EEG signal is that it is non-invasive, cheap, and possesses a high temporal resolution which gives a clear advantage over other techniques being used to diagnose schizophrenia [19].

According to researchers, there are five types of frequencies emitted by the human brain. Based on their frequency bands and locations they are categorized into delta (δ), theta (θ), alpha (α), beta (β), and gamma (γ) respectively which is shown in Table I [20].

Schizophrenia is classified into five categories according to the Diagnostic and Statistical Manual of Mental Disorders, 4th edition DSM-IV [21], [22]. The well-known five categories are further classified into positive and negative symptoms. Delusions and hallucinations are positive symptoms while avolition, alogia, and anhedonia are negative symptoms [23], [24].

TABLE I. EEG SIGNAL FREQUENCY BANDS

ACTIVITY	FREQUENCIES (KHz)	SIGNAL CHARACTERISTICS	BEHAVIOR
Delta	0.005-0.004	Lowest Frequency	Sleeping
Theta	0.004-0.008	Low Frequency	Drowsy
Alpha	0.008-0.013	High Frequency	Relaxing
Beta	0.013-0.03	High Frequency	Busy
Gamma	0.03-0.04	Highest Frequency	Concentration

Several techniques and methods have been employed to diagnose schizophrenia with the help of electroencephalography. In [25] the authors have used a thirteen (13) layers Convolutional Neural Network model to diagnose practical, normal, and seizure classes. In [26] they have used a deep learning algorithm such as CNN with random forest. They have implemented a voting layer to differentiate between those individuals who are at high-risk with schizophrenia and healthy controls. In [27] authors have used a CNN model to diagnose and evaluate different partitions of EEG to visualize unusual brain activities. In [28] authors have used EEG signals to compare real and imaginary music and classified them using CNN. In [29] have used a cross trail encoding technique with the aid of convolutional autoencoders and used EEG signals. The dataset used in the training was very small. In [30] have utilized a single electrode approach to classify and diagnose schizophrenia from EEG recordings. They have used the time-frequency technique to differentiate between schizophrenia and healthy controls. The authors have proposed a state-of-the-art model to recognize Alzheimer's disease with the help of logistic regression and achieved higher accuracy as compared to the domain knowledge-based handcrafted features [31].

The motivation behind this research is to evaluate the performance of different sampling techniques with the help of EEG signals for the diagnosis of schizophrenia and also to assist and verify the psychiatrist's decision because the diagnosis takes around 6-12 months as it is based on the questionnaire surveys.

The objective of this research is to develop a Machine Learning (ML) model and to compare the effect of different sampling techniques on the mentioned dataset that can validate the doctor's decision and quickly diagnose this severe mental disorder.

The following is the structure of this research paper. The introduction is included in Section I. Section II explains the methodology and different python toolkits used in the experiment. Section III includes the results on three different techniques with filtered, no Z score, and no filter and unfiltered datasets. Section IV concludes the conclusion and how this study can be useful to diagnose Schizophrenia with the help of machine learning algorithms. Section V explains the future work.

II. METHODOLOGY

A. EEG Dataset and Preprocessing

The raw EEG data of fourteen (14) patients having schizophrenia, comprised of seven (7) males and seven (7) females with their average ages of 27.9 ± 3.3 and 28.3 ± 4.1 years, respectively. The experiment was carried out at the Institute of Psychiatry and Neurology in Warsaw, Poland [32]. Similarly, fourteen (14) healthy patients having no major disease were recruited of the same gender and same age group with seven (7) males and (7) females, respectively. The raw data were collected with the consent of all the participants.

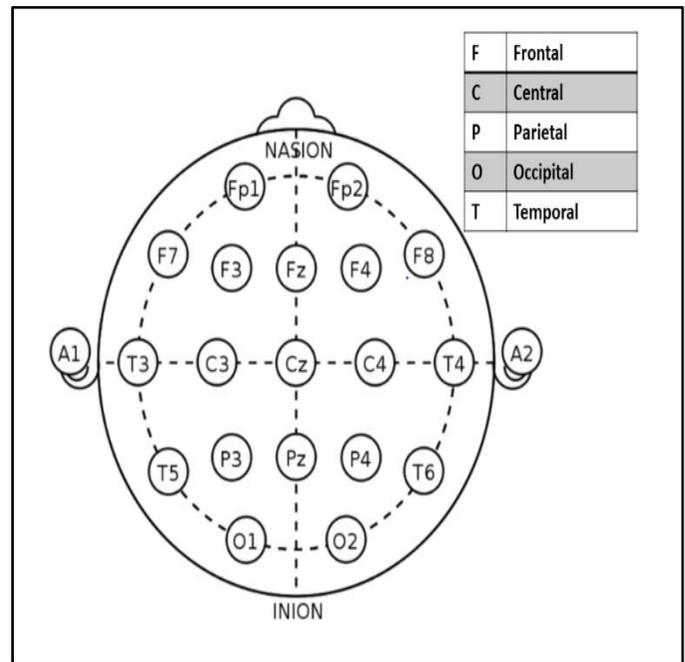


Fig. 1. International 10-20 System Electrode Placement Method [33].

Data were collected at a sample rate of 250 Hz using the International 10-20 system [33] as depicted in Fig. 1. Raw data were obtained when the patients were in a relaxed state with their eyes closed. The channels utilized to collect data were Fp1, Fp2, F7, F3, Fz, F4, F8, T3, C3, Cz, C4, T4, T5, P3, Pz, P4, T6, O1, and O2 respectively. The acquired EEG data was partitioned into different partitions and are considered stationary signals. Each segment had a window duration of 25 seconds (6250 samples). There were 1142 EEG segments in total, with each segment containing 6250×19 sample points and were normalized with Z-score before being sent to the logistic regression (LR).

B. Research Toolkits

1) *Time Series Feature Extraction Library (TSFEL)*: TSFEL is one of the most effective available libraries of python to compute the extracted features of EEG signals. It helps the data scientist to evaluate a variety of domain knowledge features as well as handcrafted features. It can compute 60 distinct features which are extracted from statistical, temporal, and spectral domains [34].

2) *MNE tool python*: MNE Python toolkit [35] is an open-source python package used to evaluate and analyze human neurophysiological data such as EEG, MEG, sEEG, ECoG, NIRS, and many more. This toolkit is very helpful to visualize EEG signals. It can compute 28 univariate features and 6 bivariate features.

C. Proposed Methodology

The raw EEG data of schizophrenia was downloaded from the Repository of Open Data (RepOD), Department of Methods of Brain Imaging and Functional Research of Nervous System[36]. A bandpass filter of 0.1 Hz to 45 Hz was applied to remove the unwanted frequencies and data

segmentation was done in the first phase. After data segmentation different features were extracted with the help of feature extraction libraries such as Time Series Feature Extraction Library (TSFEL) and MNE Python toolkit. Logistic Regression (LR) was utilized for classification and to differentiate the schizophrenic and healthy control patients depicted in Fig. 2.

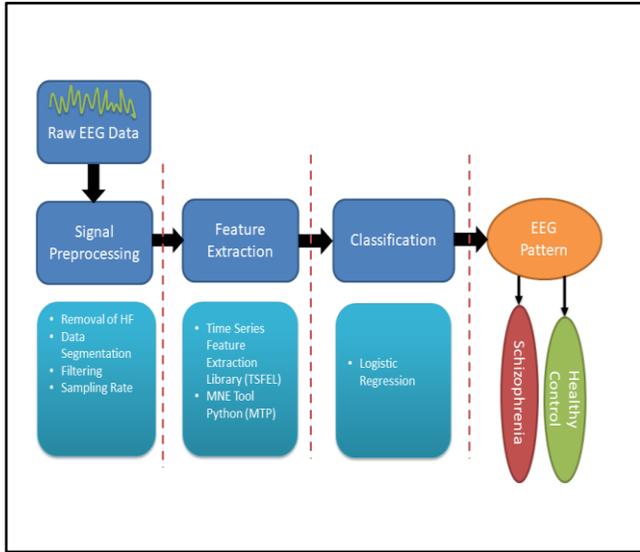


Fig. 2. Proposed Model for Automated Recognition of Schizophrenia.

III. EXPERIMENTAL RESULT

In the experimental phase, two feature extraction libraries are used such as TSFEL and MNE Python toolkit. The experimental results are divided into three phases. First, we have analyzed results by applying Z score normalization (Filtered), No Z score normalization and no filter in the second phase, and unfiltered data in the third phase. For the classification purpose, Logistic Regression (LR) was employed as a machine learning algorithm.

1) *Logistic regression on TSFEL filtered data:* LR was implemented on the TSFEL library with Z score normalization and applied five different sampling techniques such as Synthetic Minority Oversampling Technique (SMOTE) with Class Weight abbreviated as S-CW, Borderline SMOTE Class Weight (BS-CW), Random Oversampling Class Weight (ROS-CW), None-Class Weight (N-CW) and None-None (N-N). It is found that S-CW and ROS-CW achieved an accuracy of 77.90% which is quite good when we have a smaller data size as shown in Table II and Fig. 3.

TABLE II. SUMMARY OF LR ON TSFEL FILTERED DATA

Channels	Sampling Technique	Macro-recall	Macro F1 score	Sens.	Spec.	Acc.
All	S-CW	78.07	77.89	75.34	80.81	77.90
All	BS-CW	77.77	77.62	75.51	80.03	77.63
All	ROS-CW	78.10	77.90	75	81.20	77.90
All	N-CW	77.37	77.37	78.59	76.16	77.45
All	N-N	77.70	77.53	75.17	80.23	77.54

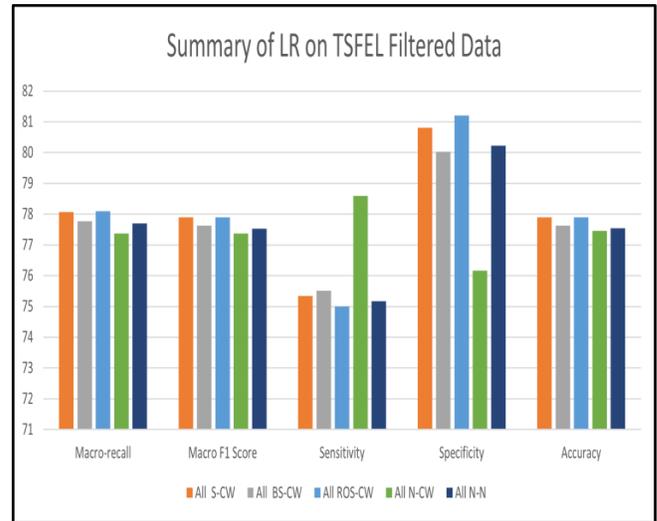


Fig. 3. Summary of LR on TSFEL Filtered Data.

2) *Logistic regression on TSFEL with No Z score & no filtered data:* In Table III, S-CW AND BS-CW achieved the higher accuracy of 82.27% and 82.72%, respectively when filtering and normalization was not implemented shown in Fig. 4.

TABLE III. SUMMARY OF LR ON TSFEL NO Z SCORE AND NO FILTERED DATA

Channels	Sampling Technique	Macro-recall	Macro F1 score	Sens.	Spec.	Acc.
All	S-CW	82.36	82.25	80.82	83.91	82.27
All	BS-CW	82.88	82.71	80.30	85.46	82.72
All	ROS-CW	82.27	81.80	74.82	89.72	81.81
All	N-CW	82.19	81.71	74.65	89.72	81.72
All	N-N	81.58	81.50	80.99	82.17	81.54

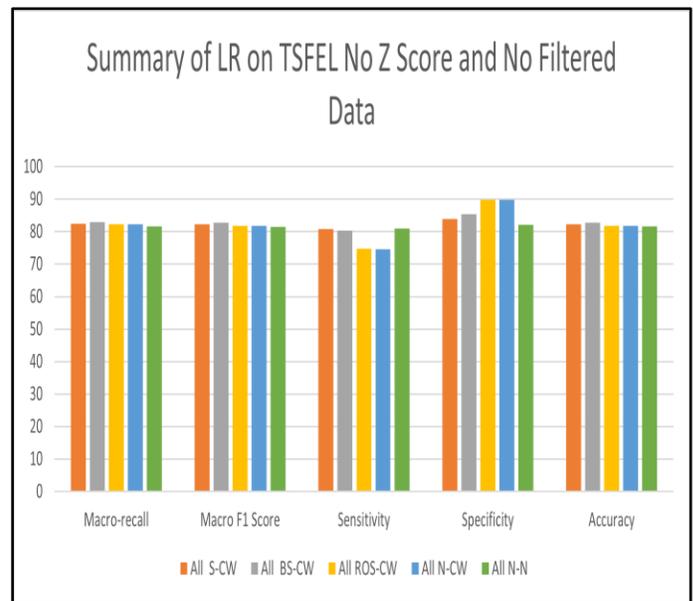


Fig. 4. Summary of LR on TSFEL No Z Score and No Filtered Data.

3) *Logistic regression on TSFEL unfiltered data:* In Table IV. LR was implemented on unfiltered data and interestingly the accuracy of N-CW was 79.36 which was very good as compared to other sampling techniques shown in Fig. 5.

TABLE IV. SUMMARY OF LR ON TSFEL UNFILTERED DATA

Channels	Sampling Technique	Macro-recall	Macro F1 score	Sens.	Spec.	Acc.
All	S-CW	79.17	78.90	74.82	83.52	78.90
All	BS-CW	78.25	78.15	77.05	79.45	78.18
All	ROS-CW	79.41	79.17	75.68	83.13	79.18
All	N-CW	79.60	79.36	75.68	83.25	79.36
All	N-N	78.25	78.15	77.05	79.45	78.18

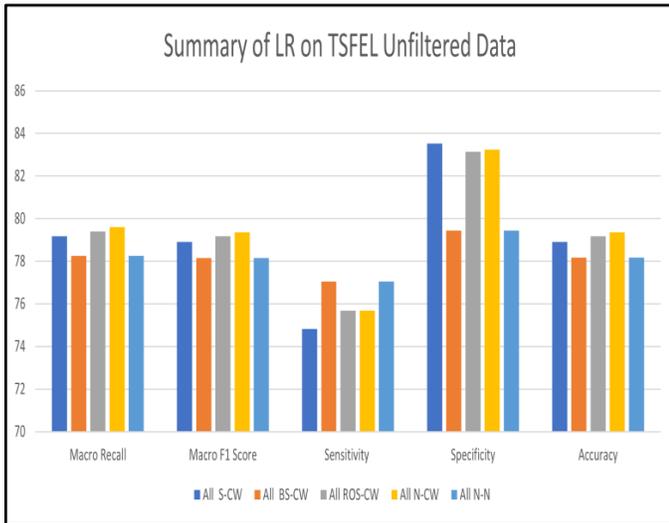


Fig. 5. Summary of LR on TSFEL Unfiltered Data.

4) *Logistic regression on MNE filtered data:* In Table V, MNE-Python toolkit was used on Filtered data with Z score normalization and BS-CW accuracy was 77.45% as compared to other sampling techniques used in the experiment shown in Fig. 6.

5) *Logistic regression on MNE with no Z score and no filter data:* In Table VI, LR was used with MNE, and No Z Score, and No Filtered data, and S-CW performed better than other oversampling techniques. S-CW achieved an accuracy of 91.63% which is very good as shown in Fig. 7.

TABLE V. SUMMARY OF LR ON MNE FILTERED DATA

Channels	Sampling Technique	Macro-recall	Macro F1 score	Sens.	Spec.	Acc.
All	S-CW	77.13	76.98	75	79.26	77
All	BS-CW	77.61	77.44	75	80.23	77.45
All	ROS-CW	76.86	76.71	74.65	79.06	76.72
All	N-CW	77.03	76.89	75	79.06	76.90
All	N-N	76.57	76.43	74.65	78.48	76.45

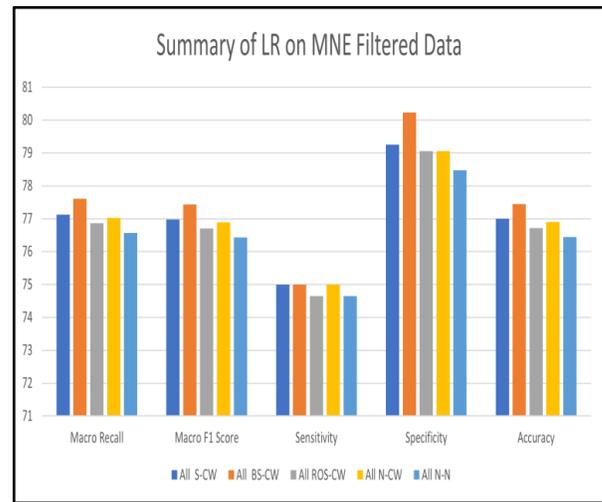


Fig. 6. Summary of LR on MNE Filtered Data.

TABLE VI. SUMMARY OF LR ON MNE NO Z SCORE & NO FILTER DATA

Channels	Sampling Technique	Macro-recall	Macro F1 score	Sens.	Spec.	Acc.
All	S-CW	80.02	79.52	72.26	87.79	91.63
All	BS-CW	79.87	79.34	71.57	88.17	79.36
All	ROS-CW	80.31	79.79	72.26	88.37	79.81
All	N-CW	80.49	79.98	72.43	88.56	80
All	N-N	80.18	79.71	72.77	87.59	79.72

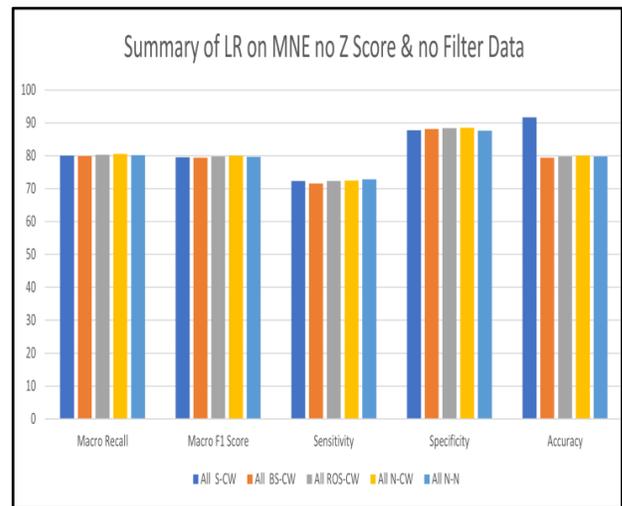


Fig. 7. Summary of LR on MNE no Z Score & no Filter Data.

6) *Logistic regression on MNE unfiltered data:* In Table VII, LR was used on the unfiltered data and S-CW and N-CW performed better and achieved the accuracies of 79.45% each shown in Fig. 8.

7) *Comparison of logistic regression on TSFEL:* After applying LR on three different datasets such as filtered, no z score, and no filter and unfiltered data we found that BS-CW has the highest unweighted macro recall value of 82.88 on no z score and no filter data as shown in Table VIII.

8) Comparison of logistic regression on MNE python:

Similarly, we have applied LR on the MNE Python toolkit to observe the performance of three different datasets and we have analyzed that N-CW has achieved the highest unweighted macro recall value of 80.49 as compared to others as shown in Table IX.

TABLE VII. SUMMARY OF LR ON MNE UNFILTERED DATA

Channels	Sampling Technique	Macro-recall	Macro F1 score	Sens.	Spec.	Acc.
All	S-CW	79.37	79.37	80.65	78.10	79.45
All	BS-CW	79.29	79.28	80.47	78.10	79.36
All	ROS-CW	78.73	78.73	80.13	77.32	78.81
All	N-CW	79.38	79.38	80.47	78.29	79.45
All	N-N	78.68	78.71	80.82	76.55	78.81

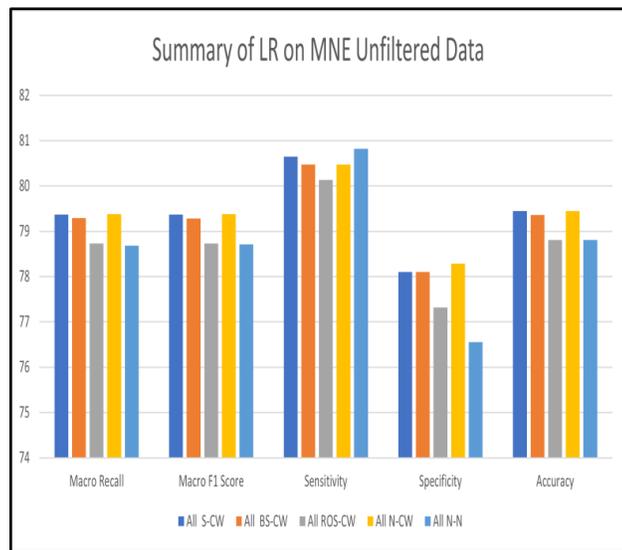


Fig. 8. Summary of LR on MNE Unfiltered Data

TABLE VIII. SUMMARY OF LR ON MNE UNFILTERED DATA

Sampling Techniques	Filtered	No Z Score No Filter	Unfiltered
S-CW	78.07	82.36	79.17
BS-CW	77.07	82.88	78.25
ROS-CW	78.10	82.27	79.41
N-CW	77.37	82.19	79.60
N-N	77.70	81.58	78.25

TABLE IX. SUMMARY OF LR ON MNE UNFILTERED DATA

Sampling Techniques	Filtered	No Z Score No Filter	Unfiltered
S-CW	77.13	80.02	79.37
BS-CW	77.61	79.87	79.29
ROS-CW	76.86	80.31	78.73
N-CW	77.03	80.49	79.38
N-N	76.57	80.18	78.68

IV. CONCLUSION

In this paper, a deep learning model is proposed to diagnose schizophrenia from EEG signals as they contain information about the electrical activities of the human brain. We have proposed a machine learning model that can diagnose Schizophrenia from EEG signals. According to World Health Organization (WHO), it is affecting almost 21 million people worldwide and it is very hard to diagnose Schizophrenia as the treatment can take from 6 months to 1 year because doctors ask several questionnaires and take the survey from the patients. Different studies suggest that it can be found more in men than women. So, we need to take help from machine learning algorithms to diagnose this chronic mental disorder as quickly as possible. In our proposed model, we have used Logistic Regression (LR) as a classifier because it provides very good results when we have smaller datasets. We have evaluated the results in three different domains. First filtered data with Z score normalization, then without Z score normalization, and finally on the unfiltered data. We have used 5 different sampling techniques like SMOTE Class Weight (S-CW), Borderline SMOTE Class Weight (BS-CW), Random oversampling Class Weight (ROS-CW), None Class Weight (N-CW), and None-None (N-N), respectively. From our observation we have analyzed that the results achieved with no z score and no filter have the highest unweighted macro recall value it is due to the EEG recordings obtained from 14 SZ and 14 HC people does not have artifacts. It is also observed that when we have applied some filtering techniques so the ML model performance significantly decreased.

For cross-validation of ML model the leave-one-subject-out cross-validation technique using Scikit Learn has been utilized to validate the results in the form of evaluations parameters macro recall, macro f1 score, sensitivity, specificity, and accuracy, respectively.

V. FUTURE WORK

This research has still some limitations as the proposed model can predict and diagnose schizophrenic patients (SP) and the healthy control (HC) from the EEG signals. It cannot predict the disease severity. Also, this experiment has been done on the smaller dataset, but it can be carried out on the larger datasets as well to verify the model's accuracy.

ACKNOWLEDGMENT

We would like to express our gratitude to Syed Zafi Sherhan Shah for his helpful, constructive talks and support to carry out the related experiments.

REFERENCES

- [1] C. A. T. Naira and C. J. L. Del Alamo, "Classification of people who suffer schizophrenia and healthy people by EEG signals using deep learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 10, pp. 511–516, 2019.
- [2] S. L. James et al., "Global, regional, and national incidence, prevalence, and years lived with disability for 354 Diseases and Injuries for 195 countries and territories, 1990-2017: A systematic analysis for the Global Burden of Disease Study 2017," *Lancet*, vol. 392, no. 10159, pp. 1789–1858, 2018.

- [3] C. S. Haller, J. L. Padmanabhan, P. Lizano, J. Torous, and M. Keshavan, "Recent advances in understanding schizophrenia," *F1000Prime Rep.*, vol. 6, no. July, pp. 1–11, 2014.
- [4] C. Pelta, "Emotional Cascade Model and Deep Learning," *Int. J. Adv. Comput. Sci. Appl.*, vol. 12, no. 8, pp. 363–367, 2021.
- [5] J. F. Rodríguez-Testal, C. Senín-Calderón, and R. Moreno, "Hallucinations and Delusions as Low-Quality Attributions: Influencing Factors and Proposal for Their Analysis," *Front. Psychol.*, vol. 12, no. July, pp. 1–9, 2021.
- [6] A. Sarré et al., "Verbal hallucinations in deaf schizophrenia patients," *Schizophr. Res.*, vol. 232, pp. 31–32, 2021.
- [7] R. A. Adams, P. Vincent, D. Benrimoh, K. J. Friston, and T. Parr, "Everything is connected: Inference and attractors in delusions," *Schizophr. Res.*, no. March, 2021.
- [8] L. Henco et al., "Aberrant computational mechanisms of social learning and decision-making in schizophrenia and borderline personality disorder," *PLoS Comput. Biol.*, vol. 16, no. 9, pp. 1–22, 2020.
- [9] Y. Ren and Y. Wu, "Convolutional deep belief networks for feature extraction of EEG signal," *Proc. Int. Jt. Conf. Neural Networks*, pp. 2850–2853, 2014.
- [10] L. J.-S. Moon, Seong-Eun, Jang Soobeom, "Convolutional Neural Network Approach for EEG-Based Emotion Recognition using Brain Connectivity and its Spatial Information Seong-Eun Moon Soobeom Jang Jong-Seok Lee Republic of Korea," 2018 IEEE Int. Conf. Acoust. Speech Signal Process., pp. 2556–2560, 2018.
- [11] R. Akhter, K. Lawal, M. T. Rahman, and S. A. Mazumder, "Classification of Common and Uncommon Tones by P300 Feature Extraction and Identification of Accurate P300 Wave by Machine Learning Algorithms," *Int. J. Adv. Comput. Sci. Appl.*, vol. 11, no. 10, pp. 646–652, 2020.
- [12] B. J. Vorderwülbecke, A. G. Baroumand, L. Spinelli, M. Seeck, P. van Mierlo, and S. Vulliémoz, "Automated interictal source localisation based on high-density EEG," *Seizure*, vol. 92, no. October, pp. 244–251, 2021.
- [13] M. Saes, C. G. M. Meskers, A. Daffertshofer, E. E. H. van Wegen, and G. Kwakkel, "Are early measured resting-state EEG parameters predictive for upper limb motor impairment six months poststroke?," *Clin. Neurophysiol.*, vol. 132, no. 1, pp. 56–62, 2021.
- [14] A. Craik, Y. He, and J. L. Contreras-Vidal, "Deep learning for electroencephalogram (EEG) classification tasks: A review," *J. Neural Eng.*, vol. 16, no. 3, 2019.
- [15] H. U. Amin, W. Mumtaz, A. R. Subhani, M. N. M. Saad, and A. S. Malik, "Classification of EEG signals based on pattern recognition approach," *Front. Comput. Neurosci.*, vol. 11, no. November, pp. 1–12, 2017.
- [16] R. T. Schirmer et al., "Deep learning with convolutional neural networks for EEG decoding and visualization," *Hum. Brain Mapp.*, vol. 38, no. 11, pp. 5391–5420, 2017.
- [17] T. Bose, S. D. Sivakumar, and B. Kesavamurthy, "Identification of Schizophrenia Using EEG Alpha Band Power During Hyperventilation and Post-hyperventilation," *J. Med. Biol. Eng.*, vol. 36, no. 6, pp. 901–911, 2016.
- [18] B. Kaliappan, K. Rajamanickam, and S. Jayapal, "A Novel Classifier Algorithm for EEG Signal Based Person Authentication from Cz Channel with 2D-Wavelet Compression for the Online Voting System Using Touch Panel," *Aust. J. Basic Appl. Sci.*, vol. 8, no. 5, pp. 399–409, 2014.
- [19] R. De Filippis et al., "Machine learning techniques in a structural and functional MRI diagnostic approach in schizophrenia: A systematic review," *Neuropsychiatr. Dis. Treat.*, vol. 15, pp. 1605–1627, 2019, doi: 10.2147/NDT.S202418.
- [20] W. Liang, L. Cheng, and M. Tang, "Identity Recognition Using Biological Electroencephalogram Sensors," *J. Sensors*, vol. 2016, 2016.
- [21] D. McLean et al., "DSM-IV 'criterion A' schizophrenia symptoms across ethnically different populations: evidence for differing psychotic symptom content or structural organization?," *Cult. Med. Psychiatry*, vol. 38, no. 3, pp. 408–426, 2014.
- [22] R. Jardri et al., "Hallucination Research: Into the Future, and beyond," *Schizophr. Bull.*, vol. 45, no. 1, pp. S1–S4, 2019.
- [23] R. Tandon et al., "Definition and description of schizophrenia in the DSM-5," *Schizophr. Res.*, vol. 150, no. 1, pp. 3–10, 2013.
- [24] M. F. Green and P. D. Harvey, "Cognition in schizophrenia: Past, present, and future," *Schizophr. Res. Cogn.*, vol. 1, no. 1, pp. e1–e9, 2014.
- [25] U. R. Acharya, S. L. Oh, Y. Hagiwara, J. H. Tan, and H. Adeli, "Deep convolutional neural network for the automated detection and diagnosis of seizure using EEG signals," *Comput. Biol. Med.*, vol. 100, pp. 270–278, 2018.
- [26] L. Chu, R. Qiu, H. Liu, Z. Ling, T. Zhang, and J. Wang, "Individual Recognition in Schizophrenia using Deep Learning Methods with Random Forest and Voting Classifiers: Insights from Resting State EEG Streams," pp. 1–7, 2017, [Online]. Available: <http://arxiv.org/abs/1707.03467>.
- [27] S. L. Oh, J. Vicnesh, E. J. Ciaccio, R. Yuvaraj, and U. R. Acharya, "Deep Convolutional Neural Network Model for Automated Diagnosis of Schizophrenia Using EEG Signals," *Appl. Sci.*, vol. 9, no. 14, p. 2870, 2019.
- [28] S. Sarkar, K. K. Reddy, A. Dorgan, C. Fidopiastis, and M. Giering, "Wearable EEG-based activity recognition in PHM-related service environment via deep learning," *Int. J. Progn. Heal. Manag.*, vol. 7, no. Special Issue 6, 2016.
- [29] S. Stober, A. Sternin, A. M. Owen, and J. A. Grahn, "Deep Feature Learning for EEG Recordings," *Arxiv*, vol. abs/1511.0, 2015, [Online]. Available: <http://arxiv.org/abs/1511.04306>.
- [30] Z. Dvey-Aharon, N. Fogelson, A. Peled, and N. Intrator, "Schizophrenia detection and classification by advanced analysis of EEG recordings using a single electrode approach," *PLoS One*, vol. 10, no. 4, pp. 1–12, 2015.
- [31] M. Lech and E. Pirogova, "Automated Recognition of Alzheimer's Dementia Using Bag-of-Deep-Features and Model Ensembling," *IEEE Access*, vol. 9, pp. 88377–88390, 2021.
- [32] S. L. Oh, J. Vicnesh, E. J. Ciaccio, R. Yuvaraj, and U. R. Acharya, "Deep convolutional neural network model for automated diagnosis of Schizophrenia using EEG signals," *Appl. Sci.*, vol. 9, no. 14, 2019.
- [33] G. M. Rojas, C. Alvarez, C. E. Montoya, M. de la Iglesia-Vayá, J. E. Cisternas, and M. Gálvez, "Study of resting-state functional connectivity networks using EEG electrodes position as seed," *Front. Neurosci.*, vol. 12, no. APR, pp. 1–12, 2018.
- [34] M. Barandas et al., "TSFEL: Time Series Feature Extraction Library," *SoftwareX*, vol. 11, p. 100456, 2020.
- [35] A. Gramfort et al., "MEG and EEG data analysis with MNE-Python," *Front. Neurosci.*, vol. 7, no. 7 DEC, pp. 1–13, 2013.
- [36] W. Olejarczyk, Elzbieta and Jernajczyk, "EEG in schizophrenia," *RepOD*, 2017, [Online]. Available: <https://reprod.icm.edu.pl/dataset.xhtml?persistentId=doi:10.18150/reprod.0107441>.

Long Term Solar Power Generation Prediction using Adaboost as a Hybrid of Linear and Non-linear Machine Learning Model

Sana Mohsin Babbar, Chee Yong Lau, Ka Fei Thang

School of Engineering, Asia Pacific University of Technology and Innovation (APU)
Kuala Lumpur 57000, Malaysia

Abstract—The usage of renewable energy sources has increased manifolds in terms of electric utilities. From other non-conventional sources, solar energy has been seen as a promising and convenient source used around the globe. In terms of meeting the daily requirements, solar energy has huge potential to fulfil the world's demand. However, firstly the characteristic of solar energy is very unpredictable and intermittent due to variation of weather. Secondly, the optimization and the planning of smart grid effect the operation of PV system. Thus, prediction on the long horizon is needed to address this problem. Nevertheless, long term forecasting of solar power generation is deliberated as a challenging problem. Therefore, this paper proposes a 10 day ahead solar power forecasting using combination of linear and non-linear machine learning models. At first, the outputs are generated from Recurrent Neural Network (RNN), Support Vector Machine (SVM) and Autoregressive with exogenous variable (ARX). Later on, these three outputs are combined and are made as a strong classifier with the Adaptive boost (Adaboost) algorithm. The simulations were conducted on the data obtained from real PV plant. By the experimental results and discussion, it was endogenously concluded that the combination of all techniques with the Adaboost have increased the performances and showing the high accuracy as compare to the individual machine learning models. The hybrid Adaboost shows %MAPE 8.88, which proven high accuracy. While on the other hand, for the individual technique, RNN shows 10.88, SVM reveals 11.78 and ARX gives 13.00 of percentage MAPE. The improvement proves that combination of techniques performs better than individual models and proclaims the high accuracy.

Keywords—Recurrent neural network (RNN); support vector machine (SVM); autoregressive with exogenous variable (ARX); adaptive boosting (Adaboost) and photovoltaic system (PV)

I. INTRODUCTION

In recent years, the attention has been drawn towards the renewable energies. The importance of wind and solar energies are at glance around the globe. Development of clean and green energy is highly considered by the researches in the present-day [1]. Wind turbines and photovoltaic array (PV) are vital technologies for harvesting energy from solar irradiance, module temperature and wind speed etc. Due to the rapid increase in population and the economy, the demand of electricity has been raised up in the past decade. Consequently, solar power systems and other renewable energy sources are widely used as a solution [2]. The solar

energy is eco-friendly non-conventional sources which is why it is adopted widely. Industrial, commercial and residential applications can be operated by the solar energy sufficiently [3]. While contrastingly, the nature of solar energy is sporadic and unpredictable due to which errors can be caused to the power grid. It can greatly limits the large-scale integration of PV power generation system to the power or smart grid. Forecasting on the large horizon is most promising key solution to the problems of intermittency and volatility. Forecasting energy is used for mitigating the unresolved challenges in the resources. In the research community, solar power forecasting is growing rapidly.

The collection of solar power data is itself a field. The nature of the solar power data set depends upon the model from which it has been collected. Solar power production has become the limelight of sustainability and planning of electricity generation and there are few models of energy generation of PV system. The observed values of solar power or other renewable energies are usually fetched from physical or statistical model. Generally in the past researches, forecasting is done by three models. First one and extensively used are physical models. Physical models usually contain the natural parameters from Numerical Weather Prediction (NWP) models. The forecasted data conventionally is solar irradiance, wind speed, orography, humidity, wind power and solar power, etc. [4]. The second one is statistical model which contains the historical data. And the third one is hybrid model, which is the ensemble of physical and statistical model [5]. In this paper, the input data is taken from physical model.

On the other side, forecasting also depends upon the time horizon and the usage of source. There are three types of forecasting based on the range of time period: (1) Short term forecasting (2) Medium-term forecasting and (3) long term-forecasting. Numerous studies have been carried out for short and medium forecasting which ranges from 3 to 72 hour ahead [6]. Less amount of work has been done for having a long term forecasting. The maximum range of prediction is days ahead. This paper aims to bring originality and predicts 10 days ahead solar power generation. This research also highlights the usefulness of solar power forecasting for the integration of electricity generation. In actual fact, if the prediction is done accurately, the integration and utilization of electricity can be of better service.

The paper is organized in a way that summarizes all aspects of the originality of this research work. The paper is structured as follows: in Sections 2 and 3 brief review of the machine learning models and problem statement has been discussed. In Section 4, proposed methodology is described step by step. In Section 5, the proposed models with implementations are discussed extensively. Whereas, Section 6 shows the 10 days ahead solar power generation prediction using different machine learning algorithms, in terms of root mean square error, mean absolute error and mean absolute percentage error. Furthermore, Section 6 also compares and analyze the precision of all proposed models. In the end, conclusion and future work are stated.

II. LITERATURE REVIEW

Over the few decades, machine learning techniques are substantially used for prediction, forecasting, classification, image and pattern recognition etc. Machine learning and Artificial Intelligence (AI) plays a vital role in forecasting of solar power. Neural networks and various kinds are popular for prediction purposes. Feed-forward Neural Network (FFNN), Multi-layer perceptron (MLP), Recurrent Neural Network (RNN) and Elman Neural Networks are always in demand of researches and studies. Recently, Artificial Neural Networks (ANN) is widely chosen for electricity demand forecasting field [7-8]. On the other hand, Support Vector Machine (SVM) and related regression techniques are also performing well in the field of forecasting. Aforementioned studies showed that SVM performs equally and greater than neural networks and other statistical models [9]. SVM has non-linear features with fitting ability and it can easily predict solar radiation at its fine [10]. While on the other hand, linear models like regression model, Autoregressive model (AR), Autoregressive with exogenous variable (ARX), and Autoregressive integrated moving average (ARIMA) are also widely used for prediction purpose for its time-series analysis with variable co-efficient [11].

There always been a comparison in linear and non-linear models with respect to prediction. It has been seen from the past studies that linear models mostly need time-series data for prediction while non-linear models like ANN, SVM and fuzzy logics does not depend on the historical data. They are usually depend upon the machine learning algorithms to maintain and create a relationship between Numerical Weather Prediction (NWP) data and solar power generation [12]. In [13], a new way of RNN has been proposed for short term solar forecasting. Non-linear features were extracted from data set and then RNN was applied. Previous PV data was taken as input data. Later on, output was compared with persistence model and other machine learning techniques. RNN proved to be better performer in terms of accuracy. RNN is very well known for solving the complex networks and architecture. It is also keenly observed in past studies that was using long-short term memory recurrent neural network (LSTM-RNN) for forecasting can also be applicable for efficacy. This study was evaluated using hourly dataset of almost one year. The results were compared with three PV forecasting methods and showed accurate and precise output. It was also concluded that this propose model is effective tool for controlling and planning of PV grid system [14] while SVM is also a very

promising technique in terms of classification and regression. In [15], SVM with least square has been applied to the historical data. The predicted output was atmospheric transmissivity and then it was converted into short term solar power. By the results, it was observed that SVM flaunted more refined outputs as compare to the conventional AR model and radial base neural network function. Using satellite's image data to predict solar power with the help of SVM has shown remarkable results and then the proposed model was compared with ANN and time-series model to observe the accuracy [16]. Contradictory to the non-linear model, linear models have got their own specifications and characteristics. ARX and ARIMA have been extensively used over the past few years. ARX works best on the time series data and historical data as well. A piece of research showed that ARX as compare to the persistence models can be useful for 24 hour ahead prediction and it can be fully improved in terms of forecasting precision [17]. Solar power were predicted using Gaussian Conditional Random fields (GCRF). After obtaining the results, the final solar power was compared with persistence and ARX model after several experiments with and without pre-processing of data. It was concluded by the RMSE that GCRF has attained the forecasting estimation accurately as compare to persistence and ARX [18].

According to the data type, the good predictive models are selected and then trained to have precise results. Ensemble approaches are gaining popularity in terms of best performance. In the past research, it has been seen at a higher rate that hybrid approach of linear or non-linear models brings the better accuracy and performance. The combination and contrast of linear and non-linear models brings explicit results [19]. Numerous works has been done in the hybrid machine learning approaches. A research showed well-refined results using combination of different linear and non-linear models. A data of wind speed was taken from NWP and then employed to the Feed-forward Neural Network (FFNN), SVM and regression model. 72 hour ahead prediction was made into the consideration. Quantifying measures showed that ensemble approaches of different algorithms can perform much better as compare to the individual ones [20]. In [21], different training models i.e. Levenberg-Marquardt (LM) and Bayesian Regularization (BR) embedded in neural networks are used for solar power forecasting. It was observed that BR outperformed and brought significant results. Hybrid approaches using machine learning tools are attractive proposed methodologies with respect to the performance. Different kind of adaptive boosting techniques have been used in the past. Adaboost is best known for its combination with the weak classifier to form a strong classifier. In [22], ensemble approach of sparse Adaboost with Echo State Network (ECN) has been implemented on the electrical consumption in the Hubei, China. Aforementioned studies depicts that ensemble approach is a good choice for Industrial Electrical Consumption (IEC) planning and controlling.

Lots of review studies have been executed for analyzing the hybrid behavior. Ensemble approaches are categorized into two main categories: (1) Competitive ensemble forecasting and (2) Cooperative ensemble forecasting. Competitive

ensemble forecast is about training the different kinds of predictor with same or different datasets while cooperative divides the task to the different predictors and finally sums up the outputs [23]. In this paper, competitive ensemble approach has been adopted due to the parameters diversity.

In this work, linear and non-linear models are combined with each other using Adaboost algorithm. It makes use of different inputs obtained by the physical model i.e. solar irradiance, module temperature and solar power with per minute resolution. Non-linear models like RNN and SVM, while linear models like ARX are employed to the input data individually. Later on, the output obtained from the individual models are trained and combined with the assistance of Adaboost to form a strong classifier. They are trained with accurate ratio of training and testing to have best forecast accuracy with minimal error.

III. PROBLEM STATEMENT

Due to higher rate of fluctuations and intermittency in solar energy, there is always a need of accurate predictive model. In this regard, this paper provides an extensive comparison and combination of different machine learning approaches. The predictive models used in this study are RNN, SVM and ARX. Later then, the outputs from these predictive models are fed to Adaboost. This boosting technique is used in this research as an ensemble approach. In context of combining the techniques, several problems have been noticed in the past research. Firstly, lack of quality data and pre-processing of data. Secondly, choosing the right parameters for predictive models chosen. Lastly, the capability of churning the load of bid data sets. These are the key problems which usually researchers face while making combining the different machine learning models [24]. Therefore, Adaboost is chosen as combination of RNN, SVM and ARX for addressing these problems related to the data set because this combiner understands how to resist from over-fitting which makes a better hybrid approach [25].

Major contributions of the solar power prediction generation differ from other methods shown in the literature review, are listed down in the following aspect:

1) A new approach of combination of linear and non-linear models with different inputs are considered. Hybrid approach is contemplated with Adaboost, which has brought originality in the work done. Adaboost has chosen for combining the techniques because it efficiently increases the accuracy of predictors. It constructs the strong classifier by combining all weak classifiers with the poor performance and help them to achieve high accuracy.

2) Long term solar power prediction is proposed with the ensemble approach. Least amount of work has been carried out in the past for the long term forecasting. The main objective was to predict 10 day ahead solar power for combating the problem of variation of weather climate. Trading of electric supply to the smart grid shows errors sometimes due to intermittent nature of solar energy. For combating this issue in controlling and planning, a system is designed and implemented.

By the literature review and several experiments, it has been observed keenly that individual model would not be enough to have sharp accuracy. It was a great challenge to foster the precision with individual models. For the sake of having precision, amalgamation of different machine learning models has been proposed.

IV. PROPOSED METHODOLOGY

The multi-stage solar power forecasting techniques are generically comprises of three main stages. Firstly, data set is obtained from physical model and is molded and sifted according to the desired output then the predictive models are picked as stated in the past researches. Secondly, the outputs taken from linear and non-models are taken as an input for the ensemble model. Lastly, the hybrid model is trained and exhibits the final predicted output. The block diagram is shown in Fig. 1, which demonstrates the long term solar power forecasting using amalgamation of different machine learning algorithms with Adaboost model. Each stage is described below briefly:

Stage 1: First and foremost step is to analyse the data set. The availability of data set is very important for training the predictive model. The data was obtained from a physical model. The data set contains solar power (MW), solar irradiance (W/m^2) and module temperature and these parameters are the inputs of the RNN, SVM and ARX model. The division of data set is decided by the hit and trail rule, 70% of the data is set for the training purpose while 30% for the testing and validation. For the training purpose, the data is divided into months and 12283 samples are taken per month.

Stage 2: After sifting the data according to the nature of predictive models, the input data (12283×3) is fed to the RNN model first. The same input data is designated to SVM and then ARX. Every model shows us the solar power as their outputs. These outputs are now taken as an input to the ensemble approach proposed in this methodology. The process of how each model has performed is shown in Fig. 2.

Stage 3: The outputs taken from RNN, SVM and ARX are actually serving as an input to the Adaboost algorithm. All the predictive tools used in the proposed model are the weak classifiers and they are trained again with new and updated weights. After having new weights, strong classifier is formed by applying signum function as shown in the Fig. 3. In the end, the strong classifier shows the final predicted solar power with precision and accuracy.

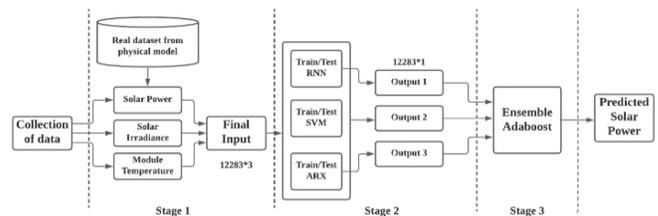


Fig. 1. Block Diagram of Proposed Methodology.

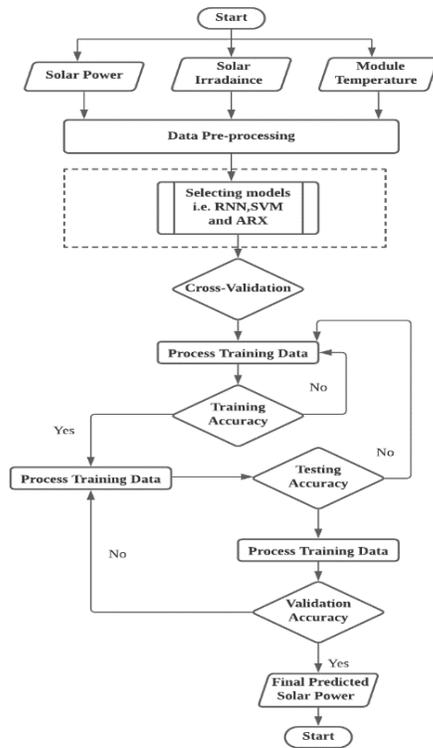


Fig. 2. Flow Chart of Performance of Stage 2 in Proposed Model.

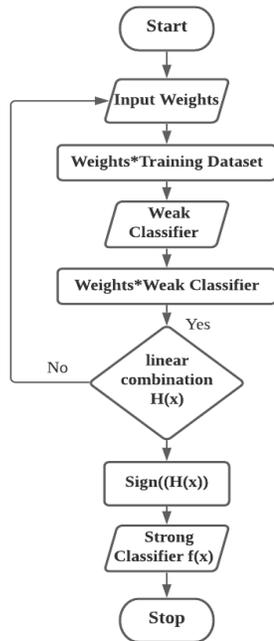


Fig. 3. Process of Adaboost Algorithm.

V. APPLICATIONS OF MODEL USED

The implementation and design of solar power forecasting has been enhanced with the methodology proposed in this paper. This research aims to determine the efficient use of solar power forecasting in terms of solar energy trading and management of electricity grid. It also emphasize in the planning and controlling of the PV power system. Due to the

variation in climate, difficulties occur in the generation of energy and trading the electrical energy to the power grid. Therefore, a multi-stage long term solar power generation has been predicted with the use of ensemble machine learning approaches [26].

Observations has been made by the past researches that combining models can bring efficacy in the predicted output. There are ample of advantages of using ensemble approaches. Combination of models brings more refined results as compare to the individual models. It also reveals good results with small datasets, as it removes all necessary outliers due to several iterations. Ensemble approach can easily be applicable to other domain of energy management systems. As described in the proposed methodology, RNN, SVM and ARX are the input generators for the hybrid approach used in this research. In this section, all the machine learning approaches are explained briefly with their working schematics. All the proposed models are using three basic parameters as an input i.e. solar power (MW), solar irradiance (W/m^2) and model temperature (K). In terms of predicting solar power, solar irradiance and power plays a vital role. Accurate solar power forecasting can help the grid operations to be optimized the electricity production.

A. Implementation of RNN

RNN is a different type of neural network with deals with a complex structure and data sets. It can deal with multiple hidden layers with a back propagation function. The training model used in this neural network is Levenberg-Marquadt (LM). LM is highly adaptive training model used in the neural networks. It has significant number of adaptive weights with respect to the training. It is also very well-known about its memory and operations [27]. RNN are also known as traditional kind of Elman neural networks. The output summation of RNN is stated in Equation 1.

$$v(t) = f(h(t - 1), x(t); b) \quad (1)$$

Where $v(t)$ denotes the output obtained after training. While $h(t)$ operates as a function which deals with the past sequence with respect to the input $x(t)$ and b shows the parameters chosen in the study. Now $v(t)$ is transferred through an activation function shown below in Equation 2.

$$y(t) = \emptyset(v(t)) \quad (2)$$

The reason that solar power generation being a positive number, sigmoid activation is considered for boosting up the training. It's a connection between output and hidden layer shown in Equation 3.

$$\emptyset = \frac{1}{(1 + \exp(-az))} \quad (3)$$

Where a is the slope and z is an input of activation function.

For having the optimal solution, the right parameters and the values should be chosen accordingly. Hit and trial method is always adopted to find out the number of hidden layers between input and output. After several trials, 30 layers were chosen to quantify the output. Supervised machine learning technique is introduced for input and output pairing. Main

objective of training the model is to minimize the biases and errors at its best. The process of having solar power as an output is shown in Fig. 4 with the assistance of flow chart.

B. Implementation of SVM

SVM is a popular supervised machine learning model which is a leading classifier [28]. By the past researches, SVM has gained the attention due to its high accuracy. Every so often, it shows accuracy more than any neural network and sometimes gives equal to it [29]. For forecasting purpose, SVM trains the response values at low-dimensions and shows good results. In SVM, the data is separated by hyper plane and defines classes. More the data is closed to the hyper plane, more it is incline towards high accuracy [30]. The expression of the SVM is given below in Equation 4.

$$y = \sum_{i=1}^n w K(\cdot) + b_0 + \varepsilon \quad (4)$$

Where y is the corresponding output, n is the training samples, w is the value of weights, $K(\cdot)$ is the kernel function, b_0 is the bias while ε is the error.

There are several types of kernel function used in the past studies. It is very critical to choose kernel function which should be operational to both linear and non-linear models. Radial base kernel function has been chosen for this paper. This function is also selected after several trials. The main reason behind choosing Radial base kernel function is to minimize the distance and ranges between input points and the hyper-plane. Appropriate kernel function is always obtained after the continuous iterative process until the square of the error gets decrease [31].

The process of working of SVM in this study is illustrated in Fig. 5. The operation shows that after selecting the input parameters i.e. solar power, solar irradiance and module temperature; the functional parameters are set for training the SVM model. After successive training, converging fitness model is calculated for model's accuracy. If solar power is achieved with minimal percentage error as output then SVM model will get stop else it will again select the weights, kernel function and train itself again.

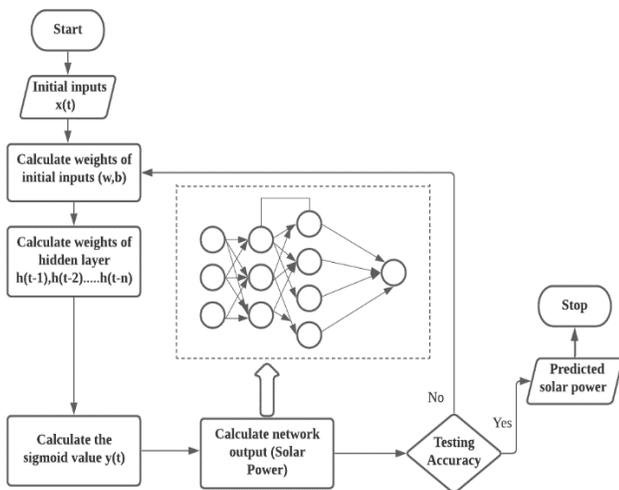


Fig. 4. Flow Chart showing Process of RNN.

C. Implementation of ARX

ARX is used as a linear machine learning model in the proposed method. ARX is one of the widely adopted linear technique in the past studies [32]. ARX is basically a time-series linear model which creates a relationship between dependent and independent variable. The basic criterion in ARX is choosing the exogenous variable based on priori analysis. In this study, module temperature and solar irradiance are the dependent variables for having the solar power at the output [33]. Accuracy of the model is calculated based on the co-efficient and training phase. The ARX model is demonstrated in the Equation 5 below [34]:

$$A(z)y(t) = B(z)x(t) + e(t) \quad (5)$$

Where $y(t)$ is the desired output i.e. solar power (MW), $x(t)$ is an input, $e(t)$ is the white noise produced in the system. While $A(z)$ and $B(z)$ are the coefficients varies with the time delay. Fig. 6 shows the process of ARX model which is implemented in this study. Operation of ARX model is started with initializing input i.e. solar power (MW). After introducing the input, the estimator is chosen according to the complexity of dataset. Cascaded feed-forward neural network is selected with 20 hidden layers to have better accuracy. Later then, ARX model is applied with a delay of 0.2 seconds with coefficients $A(z)$ and $B(z)$. In this model, forecasting is estimated with the help of Mean Square Error (MSE). Uncertainly, if model is giving good accuracy then ARX model is ready to show the predicted solar power (MW). Otherwise, again the estimator is selected and training will be held.

In past researches, ARX is constructed for predicting the solar power with good accuracy. It was also observed that ARX model or other regression techniques gives more accuracy when combine with other machine learning techniques [35].

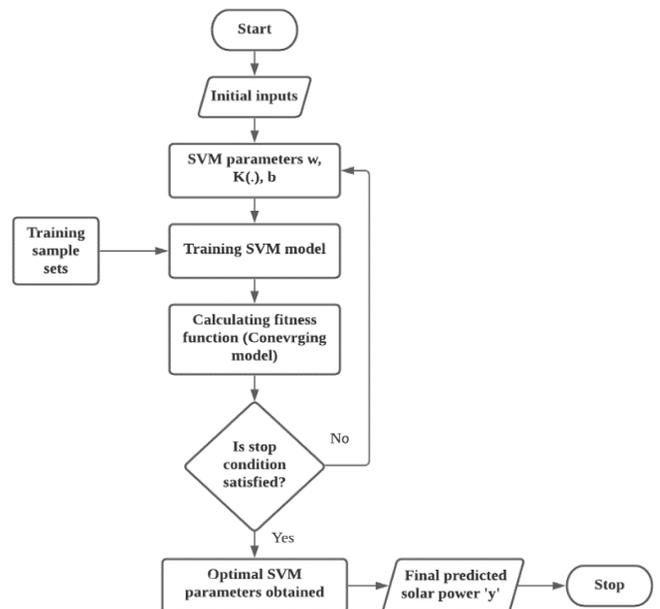


Fig. 5. Flow Chart showing the Process of SVM.

D. Hybrid of all Models using AdaBoost

In this study, the predictive models are combined by the Adaboost technique. Adaboost plays an important and vital role in this research. The main purpose of Adaboost is to ensemble machine learning models and improves the accuracy and precision. Adaboost has been extensively adopted in the recent years [36]. In the mechanism of this model, weights are generated at each step of algorithm for better classification and prediction. In this paper, outputs taken from RNN, SVM and ARX are fed to Adaboost to form a strong classifier as shown in Fig. 7 [37].

The figure shows the generic schematics of Adaboost model. The expression below depicts the function of n=3 variables used as an input.

$$f(x_1, x_2, x_3) = y \tag{6}$$

Where x_1, x_2, x_3 are the outputs taken from the RNN, SVM and ARX while y is the final predicted solar power.

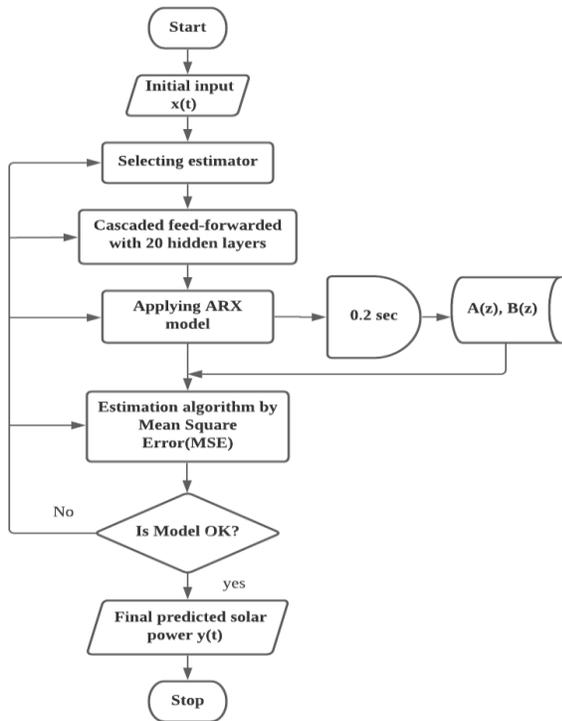


Fig. 6. Flowchart showing the Process of ARX.

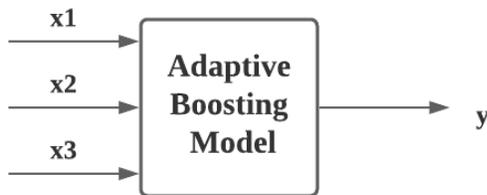


Fig. 7. Block Diagram of Output Fed to the Adaboost.

There are mainly two parts consists in the Adaptive boosting technique: First is step-by-step forward model and second is additional model [38]. In this paper, additional model is adopted for the linear combination of weak classifiers. The algorithm prepared for this research is demonstrated below in the Table I. The Pseudo code below describes well the whole process of Adaboost. In this paper, additional model Adaboost type is used. The expression of additional model is shown below in the Equation 7:

$$H(x) = \sum_{t=1}^T a_t h_t(x) \tag{7}$$

In the above equation, $H(x)$ shows the linear combination of weak classifier, whereas $h(x)$ is a weak classifier itself with a product of at weights generated of every step. On the other hand, there is also an expression found to calculate the weighted strategy, which is depicted below in Equation 8:

$$a_t = 0.5 \ln \left(\frac{1 - \text{total error}}{\text{total error}} \right) \tag{8}$$

Where total error is the classification error at the nth iteration while training. Lastly, the strong classifier is formed by the linear combination of weak classifier with the assistance of signum function as shown in Equation 9:

$$f(x) = \text{sign}(H(x)) \tag{9}$$

However, sign function is a symbolic function which converts the prediction results into the desired output. The block diagram of strong classifier is demonstrated in the Fig. 8.

TABLE I. ALGORITHM OF ADAPTIVE BOOSTING LEARNING MODEL

Pseudo code of the Adaptive boost algorithm
Input: The data A; The number of weak classifier T
Output: The strong classifier $f(x)$
1: Initializing sample weights a_1, a_2, \dots, a_t
2: for $t=1; t < T; t++$ do
3: Training weak classifier h_t based on a_t and A.
4: Calculating the total classification error
5: Calculating the weight a_t of the weak classifier h_t , $a_t = 0.5 \ln(1 - \text{total error} / \text{total error})$
6: Updating new sample weights = $w_t * e^{a_t}$
7: Forming a linear combination of weak classifiers, $H(x) = \sum_{t=1}^T a_t h_t(x)$
8: end for
9: Forming a strong classifier, $f(x) = \text{sign}(H(x))$
10: return $f(x)$

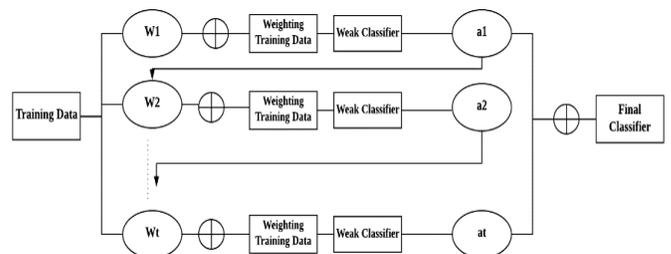


Fig. 8. The Schematics of Adaptive Boost Model.

VI. RESULT AND DISCUSSION

Training period of data set is 9 months from July-2019 to Mar-2020, solar power and solar irradiance varies according to the weather changes. Noticeably, the data set was maintained in per minute resolution according to each day. Solar irradiance plays an important role in solar power forecasting. For having a smooth power supply and balance in energy trading, it is necessary to have predicted solar power along solar irradiance. The nature of solar energy is sporadic in nature due to so many climate variations and deviation in the solar radiation. The solar power can be varied minute to minute as shown in Fig. 9. The characteristic of solar power below in the plot shows the behaviour of solar power from 8:00 am to 5:30 pm respectively. It can be observed easily that every day, every minute even every second matters in terms of forecasting. Therefore, an effective method of prediction is proposed to address this issue for generating solar power using different machine learning techniques.

In this section, individual and combined behaviour of all proposed model is discussed briefly in order. Comparison of all the models is also performed with the Adaboost to observe the performance of each technique with the performance indices. There are different kind of quantifying measures used in the past researches for observing the accuracy and precision. In this paper, Root Mean Square Error (RMSE), Mean Absolute Error (MAE) and Percentage Mean Absolute Error (%MAPE) are chosen as performance evaluators and are expressed below:

$$RMSE = \frac{\sqrt{\sum_{i=1}^N (y - y')^2}}{N} \tag{10}$$

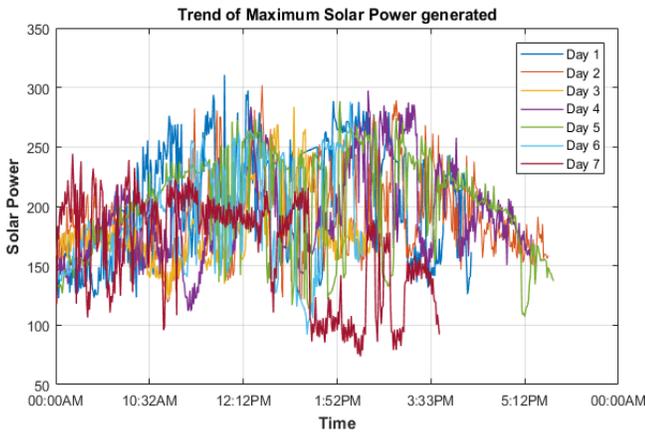


Fig. 9. Trend of Solar Power.

$$\%MAPE = \frac{1}{N} \sum_{i=0}^n \left| \frac{y - y'}{y} \right| \times 100 \tag{11}$$

$$MAE = \frac{\sum_{i=0}^n |y - y'|}{N} \tag{12}$$

Where y is the observed value and y' is the predicted value. For a comparative analysis, these values are contrasted with each model to check the efficacy and precision. While on the other hand, the ranges of good and worst accuracy have also been setup by checking percentage MAPE. Table II shows the estimation of accurate forecasting.

TABLE II. ESTIMATION OF FORECASTING ACCURACY BY THE %MAPE CRITERION

%MAPE	Forecasting Evaluation
≤ 10%	High accuracy
% 10 to 20%	Good accuracy
20% to 50%	Reasonable accuracy
≥ 50%	Inaccurate accuracy

A. Comparison of RNN, SVM and ARX

In the first stage, the outputs are taken from RNN, SVM and ARX individually. The outputs are matched with the response taken as a catalyst in the proposed predictive models. Each model is trained separately with the data set of different months. The process of obtaining output is already shown in Fig. 4.

Firstly, RNN was trained and the output was validated until it shows a refine output with minimal errors as shown in the Fig. 10. In all the figures discussed in this section represents time on the horizontal axis while solar power (MW) on the vertical axis. The trend between output and response is plotted in the graph. The blue colored segment illustrates the predicted solar power obtained from RNN while red trend shows the target chosen for training purpose. The plot is constructed on the test indices. The solar power characteristic illustrates that there is serrated relation between output and the target. It is seen that the RMSE, MAE and %MAPE by the RNN model for the month of August, 2019 is 30.18, 37.40 and & 11.29%, respectively. According to the Table II, the %MAPE lies in the category of good accuracy. It is also concluded that RNN removes up to 70 percent of the errors between actual and predicted values.

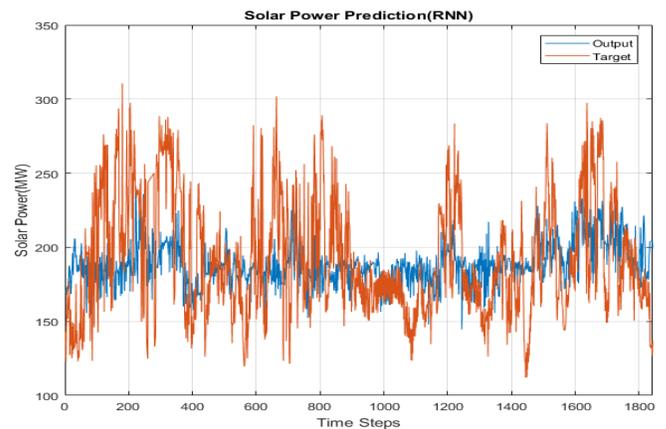


Fig. 10. Solar Power Characteristic Obtained by RNN.

After the training of RNN, same dataset is applied to the SVM for the same purpose. In the past studies, it was seen that SVM outperforms better than any other neural network [39]. In this proposed methodology, RNN and SVM performed approximately equal to each other with a minor difference. According to the performance indicators, SVM has attained 32.25 of RMSE, 40.55 of MAE while 11.77 percent of %MAPE. The output gained by the SVM is demonstrated in the Fig. 11. In the mentioned figure below, the red peaks

shows target while the blue highlights the output i.e. solar power (MW). The relationship between target and the output attained by the SVM is quite level-headed. By the criterion of percentage MAPE, SVM has showed good accuracy slightly equal as compare to the RNN.

In line with, the implementation of non-linear model is more adaptive as compare to the linear models in aforementioned studies. It depends on the data set that which model is working well. In the perspective of statistical analysis, regression models like ARX, ARMA and ARIMA performs well on the skewed and historical data while non-linear predictive tools such as neural networks, support vector machines and fuzzy logics performs excellent on the real data [40].

Together with non-linear models, ARX is applied to the same data set as this research heads to competitive ensemble approach. As the data used in this study was real data, ARX showed good accuracy as depicted in Fig. 12. In the graph below, the blue crests and troughs shows target while red ones are showing the output obtained after the training by ARX. It attained good accuracy with respect to the MAPE criterion showing 13.81 percentage MAPE. While on the other hand, ARX obtained 35.09 of RMSE and 44.29 of MAE. Conclusively, it is observed that RNN outperformed well as compare to the SVM and ARX in this research. The order of the performance is shown below in the expression:

$$RNN > SVM > ARX$$

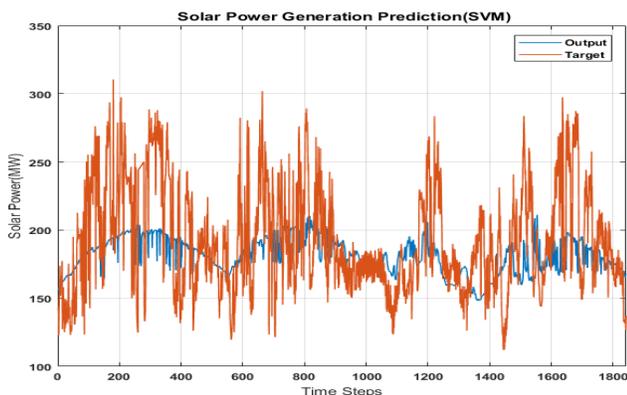


Fig. 11. The Solar Power Characteristic Obtained by SVM.

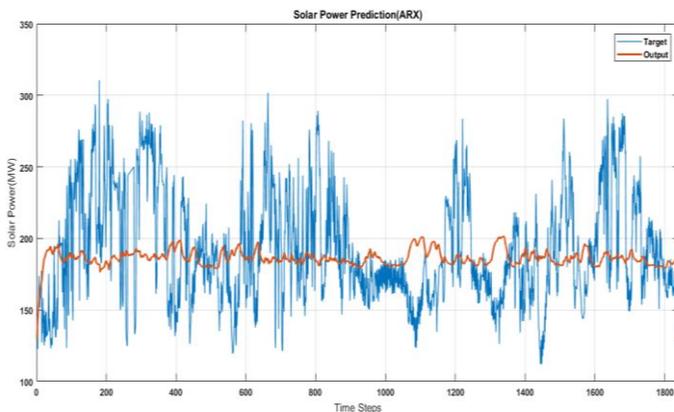


Fig. 12. The Solar Power Characteristic Obtained by ARX.

B. Comparison of Techniques with Adaboost

Adaptive boosting algorithm has been seen as a hallmark in terms of combining classifiers [41]. In terms of prediction and forecasting, any kind of boosting technique would perform well and gives suitable accuracy and precision as compare to other individual machine learning techniques [42]. In this paper, RNN, SVM and ARX are combined together and formed a strong classifier with the help of Adaboost algorithm. By the results and simulations, it was keenly observed that Adaboost is showing some major decrease in the performance indicators as shown in Table III. The statistical figures in the table depicts that Adaboost has served as strong classifier and has obtained the high performance among all other models proposed. By looking at the Table III, it is obvious that hybrid of linear and non-linear models showed up with high accuracy of forecasting. Almost in all months from August 2019 to March 2020, the results are quite same but there are fluctuations and disparities due to the weather changes.

C. Comparison of all Models used

By the brief analysis of results and simulations, it was concluded that all linear and non-linear models used in the proposed method are showing good accuracy while Adaboost is attaining high accuracy by the combination of RNN, SVM and ARX. Fig. 13 demonstrates the performance of each model and showing that Adaboost has lowest %MAPE well as compare to the other machine learning models. In Fig. 14, it is depicted that Adaboost outperforms well than RNN, SVM and ARX by the means of quantifying measures as shown in the expression below.

$$Adaboost > RNN > SVM > ARX$$

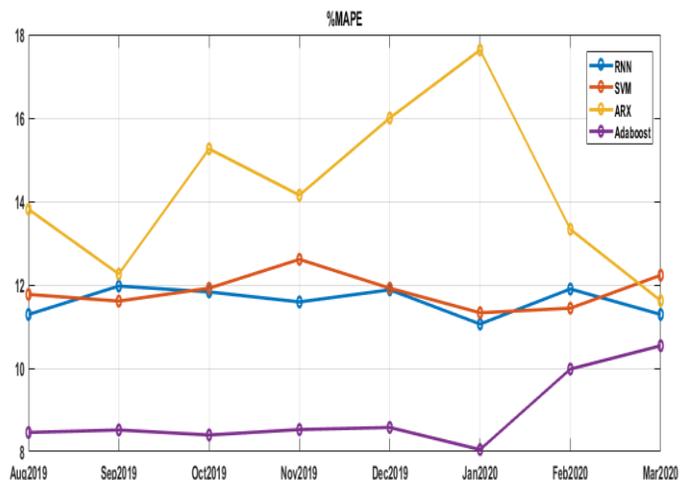


Fig. 13. %MAPE of Proposed Models.

In the aforementioned studies, the performance of ensemble approach is always better than individual models. Latently, the data set went through lots of variant processes and training sessions which finally show the precision in the prediction. In [26], simple neural networks are used and %MAPE has been calculated. It has bought 9.97% accuracy. On the other hand, the proposed model in this research has

shown more precision till 8.05. In this study also, the combination of techniques forming Adaboost gives major goals of attaining high accuracy and led to successful long term solar power generation prediction. Hence, it shows the combination of technique can achieve high accuracy and brings effective results.

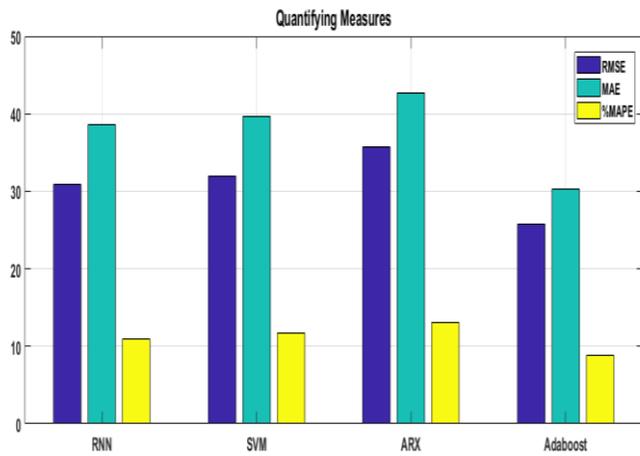


Fig. 14. Performance Indicator of Proposed Model.

TABLE III. QUANTIFYING MEASURES OBTAINED BY THE PROPOSED METHOD

Months	Errors	RNN	SVM	ARX	Adaboost
August 2019	RMSE	30.18	32.45	35.09	25.25
	MAE	37.40	40.35	44.29	29.56
	%MAPE	11.29	11.77	13.81	8.46
September 2019	RMSE	31.54	31.79	31.57	25.26
	MAE	39.22	39.10	37.03	29.6
	%MAPE	11.97	11.61	12.26	8.52
October 2019	RMSE	31.47	32.6	35.9	25.27
	MAE	39.18	40.72	43.06	29.7
	%MAPE	11.83	11.92	15.26	8.40
November 2019	RMSE	30.8	32.42	34.12	25.3
	MAE	38.2	40.36	40.25	29.5
	%MAPE	11.59	12.16	14.15	8.53
December 2019	RMSE	31.39	32.28	41.00	25.23
	MAE	39.5	40.48	38.88	29.6
	%MAPE	11.88	11.92	6.00	8.58
January 2020	RMSE	29.87	31.20	44.00	24.22
	MAE	39.6	41.32	57.20	28.4
	%MAPE	6.06	11.33	17.63	8.05
February 2020	RMSE	31.38	31.31	34.14	27.15
	MAE	38.6	37.89	44.24	31.86
	%MAPE	11.90	11.44	13.33	9.98
March 2020	RMSE	30.19	31.97	30.30	28.48
	MAE	37.40	36.5	36.40	34.03
	%MAPE	11.29	12.23	11.62	10.54

VII. CONCLUSION AND FUTURE WORK

The importance of renewable energy has been taken into the consideration since last two decades. Economic dispatch, integration to the power grid and mismanagement in the power management system due to the variability in the solar energy are the key issues to address. Therefore, to resolve these problems, an effective model is proposed to predict the

solar power generation for 10 days ahead using the hybrid approach. The ensemble technique utilizing RNN, SVM and ARX with the adaptive boosting classifier is presented in this paper. The results and discussion brought a significance stance that using adaptive boosting algorithm for combination of linear and non-linear models produces good results and shows high accuracy. From the output, it was seen that percentage MAPE of solar power characteristic lies between the ranges of 8 to 10 percent, which is a high accuracy for forecasting estimation. On the other hand, hybrid approach has obtained 25.77 of RMSE and 30.28 of MAE respectively. It is noteworthy that the optimizations and improvement brought in solar power generation prediction using combination of RNN, SVM and ARX with the Adaboost is significant and applicable.

REFERENCES

- [1] Nema, P., Nema, R. K., and Rangnekar, S. (2009) A current and future state of art development of hybrid energy system using wind and PV-solar: A review. *Renewable and Sustainable Energy Reviews*, 13(8), 2096-2103.
- [2] Perera, K. S., Aung, Z., and Woon, W. L. (2014) Machine learning techniques for supporting renewable energy generation and integration: a survey. In *International Workshop on Data Analytics for Renewable Energy Integration* (pp. 81-96). Springer, Cham.
- [3] Shaikh, M. R. S (2017). A review paper on electricity generation from solar energy.
- [4] Sun, X., and Zhang, T. Solar power prediction in smart grid based on NWP data and an improved boosting method (2017). In *2017 IEEE International Conference on Energy Internet (ICEI)* (pp. 89-94). IEEE.
- [5] Ozkan, M. B., and Karagoz, P. (2015) A novel wind power forecast model: Statistical hybrid wind power forecast technique (SHWIP). *IEEE Transactions on industrial informatics*, 11(2), 375-387.
- [6] Abdel-Nasser, M., and Mahmoud, K. (2019) Accurate photovoltaic power forecasting models using deep LSTM-RNN. *Neural Computing and Applications*, 31(7), 2727-2740.
- [7] Abuella, M., and Chowdhury, B.(2015) Solar power forecasting using artificial neural networks. In *2015 North American Power Symposium (NAPS)* (pp. 1-5). IEEE.
- [8] Mohsin, S., Ramli, S.N. and Imdad, M., (2021) Medium-Term Wind Speed Prediction using Bayesian Neural Network (BNN). *International Journal of Systematic Innovation*, 6(5), pp.11-20.
- [9] Buwei, W., Jianfeng, C., Bo, W., and Shuanglei, F. (2018) A solar power prediction using support vector machines based on multi-source data fusion. In *2018 International Conference on Power System Technology (POWERCON)* (pp. 4573-4577). IEEE.
- [10] Antonanzas, J., Osorio, N., Escobar, R., Urraca, R., Martinez-de-Pison, F. J., and Antonanzas-Torres, F. (2016) Review of photovoltaic power forecasting. *Solar Energy*, 136, 78-111.
- [11] Yang, C., and Xie. (2012) A novel ARX-based multi-scale spatio-temporal solar power forecast model. In *2012 North American Power Symposium (NAPS)* (pp. 1-6). IEEE.
- [12] Aggarwal, S. K., and Saini, L. M. (2014) Solar energy prediction using linear and non-linear regularization models: A study on AMS (American Meteorological Society) 2013–14 Solar Energy Prediction Contest. *Energy*, 78, 247-256.
- [13] Li, G., Wang, H., Zhang, S., Xin, J., and Liu, H. (2019) Recurrent neural networks based photovoltaic power forecasting approach. *Energies*, 12(13), 2538.
- [14] Lee, D., and Kim, K. (2019) Recurrent neural network-based hourly prediction of photovoltaic power output using meteorological information. *Energies*, 12(2), 215.
- [15] Zeng, J., and Qiao, W. (2013) Short-term solar power prediction using a support vector machine. *Renewable Energy*, 52, 118-127.

- [16] Jang, H. S., Bae, K. Y., Park, H. S., and Sung, D. K. (2016) Solar power prediction based on satellite images and support vector machine. *IEEE Transactions on Sustainable Energy*, 7(3), 1255-1263.
- [17] Duran, M. J., Cros, D., and Riquelme, J. (2007) Short-term wind power forecast based on ARX models. *Journal of Energy Engineering*, 133(3), 172-180.
- [18] Zhang, B., Dehghanian, P., and Kezunovic, M. (2016) Spatial-temporal solar power forecast through use of Gaussian conditional random fields. In 2016 IEEE Power and Energy Society General Meeting (PESGM) (pp. 1-5). IEEE.
- [19] AlKandari, M., and Ahmad, I. (2020) Solar power generation forecasting using ensemble approach based on deep learning and statistical methods. *Applied Computing and Informatics*.
- [20] BABBAR, S. M., and LAU, C. Y. (2020) Medium Term Wind Speed Forecasting using Combination of Linear and Nonlinear Models. *Solid State Technology*, 63(1s), 874-882.
- [21] Younis, O., (2018). A predictive model for solar photovoltaic power using the Levenberg-Marquardt and Bayesian regularization algorithms and real-time weather data. *International Journal of Advanced Computer Science and Applications*, 9(1).
- [22] Wang, L., Lv, S. X., and Zeng, Y. R. (2018) Effective sparse adaboost method with ESN and FOA for industrial electricity consumption forecasting in China. *Energy*, 155, 1013-1031.
- [23] Ren, Y., Suganthan, P. N., and Srikanth, N. (2015) Ensemble methods for wind and solar power forecasting—A state-of-the-art review. *Renewable and Sustainable Energy Reviews*, 50, 82-91.
- [24] Schleder, G. R., Padilha, A. C., Acosta, C. M., Costa, M., and Fazzio, A. (2019) From DFT to machine learning: recent approaches to materials science—a review. *Journal of Physics: Materials*, 2(3), 032001.
- [25] Wang, F., Li, Z., He, F., Wang, R., Yu, W., and Nie, F. (2019) Feature learning viewpoint of AdaBoost and a new algorithm. *IEEE Access*, 7, 149890-149899.
- [26] Alanazi, M., Alanazi, A., and Khodaei, A. (2016) Long-term solar generation forecasting. In 2016 IEEE/PES transmission and distribution conference and exposition (T&D) (pp. 1-5). IEEE.
- [27] Lera, G., and Pinzolas, M. (2002) Neighborhood based Levenberg-Marquardt algorithm for neural network training. *IEEE transactions on neural networks*, 13(5), 1200-1203.
- [28] Cervantes, J., Garcia-Lamont, F., Rodríguez-Mazahua, L., and Lopez, A. (2020) A comprehensive survey on support vector machine classification: Applications, challenges and trends. *Neurocomputing*, 408, 189-215.
- [29] Zhang, Y. (2012) Support vector machine classification algorithm and its application. In *International Conference on Information Computing and Applications* (pp. 179-186). Springer, Berlin, Heidelberg.
- [30] Eseye, A. T., Zhang, J., and Zheng, D. (2018) Short-term photovoltaic solar power forecasting using a hybrid Wavelet-PSO-SVM model based on SCADA and Meteorological information. *Renewable Energy*, 118, 357-367.
- [31] Hsu, C. W., Chang, C. C., and Lin, C. J. (2003) A practical guide to support vector classification.
- [32] Guo, Y., Nazarian, E., Ko, J., and Rajurkar, K. (2014) Hourly cooling load forecasting using time-indexed ARX models with two-stage weighted least squares regression. *Energy Conversion and Management*, 80, 46-53.
- [33] Mechaqrane, A., and Zouak, M. (2004) A comparison of linear and neural network ARX models applied to a prediction of the indoor temperature of a building. *Neural Computing & Applications*, 13(1), 32-37.
- [34] Shadab, A., Ahmad, S., and Said, S. (2020) Spatial forecasting of solar radiation using ARIMA model. *Remote Sensing Applications: Society and Environment*, 20, 100427.
- [35] Brownlee, J. (2016) A Gentle Introduction to the Gradient Boosting Algorithm for Machine Learning.
- [36] Potočník, P., Vidrih, B., Kitanovski, A., and Govekar, E. (2019) Neural network, ARX, and extreme learning machine models for the short-term prediction of temperature in buildings. In *Building Simulation* (Vol. 12, No. 6, pp. 1077-1093). Tsinghua University Press.
- [37] Tang, D., Tang, L., Dai, R., Chen, J., Li, X., and Rodrigues, J. J. (2020) MF-Adaboost: LDoS attack detection based on multi-features and improved Adaboost. *Future Generation Computer Systems*, 106, 347-359.
- [38] Javed, A., Kasi, B. K., and Khan, F. A. (2019) Predicting Solar Irradiance Using Machine Learning Techniques. In 2019 15th International Wireless Communications & Mobile Computing Conference (IWCMC) (pp. 1458-1462). IEEE.
- [39] Al-Smadi, M., Qawasmeh, O., Al-Ayyoub, M., Jararweh, Y., and Gupta, B. (2018) Deep Recurrent neural network vs. support vector machine for aspect-based sentiment analysis of Arabic hotels' reviews. *Journal of computational science*, 27, 386-393.
- [40] Lydia, M., Kumar, S. S., Selvakumar, A. I., and Kumar, G. E. P. (2016) Linear and non-linear autoregressive models for short-term wind speed forecasting. *Energy conversion and management*, 112, 115-124.
- [41] Ferreira, J. M., Pires, I. M., Marques, G., Garcia, N. M., Zdravevski, E., Lameski, P., and Spinsante, S. (2020) Identification of daily activities and environments based on the adaboost method using mobile device data: A systematic review. *Electronics*, 9(1), 192.
- [42] Kamalasri, D., Prasath, J. A., and Prabu, R. T. (2015) Solar Radiation Prediction using Adaboost Algorithm.

HORAM: Hybrid Oblivious Random Access Memory Scheme for Secure Path Hiding in Distributed Environment

Snehalata Funde^{1*}, Gandharba Swain²

Department of Computer Science and Engineering
Koneru Lakshmaiah Education Foundation, Vaddeswaram-522502, Guntur, Andhra Pradesh, India

Abstract—Now-a-days in most of the sectors digitization has taken place to store data and process it easily with enhanced techniques. Online transactions produce very huge data daily in various sectors like health care, military, government office. To store huge data many firms, take the help of third-party organizations and store data on machines provided by them which creates new security issues. While performing operations on the data or accessing data metadata leakage may happen due to untrustworthy systems. This paper proposed hybrid oblivious random-access memory (HORAM) offers users to access their data from untrusted storage devices without sharing any information about their access patterns or techniques. Here random data block shuffling approach is used which helps in hiding storage policies about the user data blocks placement and preserving privacy of data. HORAM techniques perform pull-push operations on data in a parallel manner which in turn minimizes network overhead and reduces the execution time of operation. An extensive experimental analysis of the proposed system produces better results than weak and strong Federated oblivious random access memory (FEDORAM) respectively. The method is faster than weak FEDORAM and strong FEDORAM as it takes 0.96 seconds for communication with 5 servers whereas weak and strong FEDORAM takes 1.5 and 2 seconds respectively for reading and writing data.

Keywords—HORAM; metadata; data blocks; privacy; block shuffling

I. INTRODUCTION

Big data analytics is becoming very easy with the evolving techniques in big data management and cloud storage. Nonetheless, placing information on untrusted servers raises security concerns. Nowadays privacy is required in every sector as everything is becoming digital [1]. Every system is getting transformed from offline form to online as it can be accessed from anywhere. Many of the people are giving priority to online system instead of offline system. In the current situation of corona pandemic most of the systems like government offices, educational systems, healthcare systems as well as private sectors put everything online to make it easy to people. Online platform opens easy entrance to security threats to enter in the database systems and obtain the information easily [1][4]. Especially if the information is extremely sensitive it becomes very harmful and owner may need to pay high cost for it if it gets stolen by third party.

If for example a health care system is considered with a database of patient records, specific record denotes each patient information, and columns reflect various characteristics. By executing queries on a particular attribute, a health care system may obtain details of the patient. For example, a point query will return results for people aged 30, while a range query would provide data for those aged between 19 and 30. Outsourcing such information to a user is a common practice that allows for efficient querying [2]. While executing queries encryption is employed because a user could always be trusted with critical information. To query the leased database effectively, system creates a key and encrypts it together with a data encryption structure, balancing system security and reliability. There are many existing techniques like encryption to protect data but it's not much efficient as data is exponentially growing. With existing cryptographic technique data can be secured but metadata about data can't be secured because it is created daily with the various web activities hosted by web server in many organizations [2][4]. Only encryption cannot secure dataset completely.

Applying encryption algorithm to user message may give information privacy, however it isn't adequate to address metadata concerns. Specifically, if information regarding access pattern get disclosed then it is going to damage whole record. By guessing access pattern attacker can get access directly to the private data. There is scope for cloud as well as other attacker for catching the leaked access pattern and misuse it [3]. Everyday internet thefts are finding new tricks to access data for the financial advantage. Thus, there is need Oblivious Random Access Machine (ORAM) is a strategy that allows customer to retrieve encrypted data from the cloud servers in secret way without disclosing path of data retrieval. Path of physical location is different from actual data access by user in ORAM. Basically to accomplish the motive of ORAM many researchers have contributed. Researchers have updated basic model of ORAM to improve performance of ORAM. As ORAM is limited in terms of complexity researchers tried to reduce it so that it will be more functional [5] to have dynamic strategy to deal with these security risks to sensitive information [4]. The Path ORAM techniques are used for security in recent years, initially anticipated by Stefanov et al. [5]. Path ORAM works to store the data blocks into the binary tree structure, including multiple leaf nodes such as buckets. Every bucket of a tree having a specific constant number of blocks which is denoted as z . When the tree has initialized, the

*Corresponding Author.

leaf bucket is defined as 0 to N-1, while each block has a random tag or position from range 0 to N [5]. Moreover, it contains a single small stash region that holds numerous blocks temporarily. If a block contains tag p, it will reside in the cache or some along the route from the base of the plant to the pth leaf node, according to the tree's constant.

A fully functional Oblivious RAM [6], sometimes abbreviated as ORAM, is fundamental that obscures the device's access privileges to a repository such as DRAM. In contrast, an attacker cannot learn very little about the data transmitted by watching the main memory trends. The ORAM interface converts the user's program accessing sequencing into a series of ORAM visits to seemingly random address information. Because the opponent is aware of the actual locations getting accessed, the ORAM implementation of global that the physical and logical sequence is autonomous of the proper access sequence, ensuring that the user's access sequences are not disclosed. Moreover, information stored inside database is secured using stochastic encryption to hide the captured data. Some security problem arises in hardware, software, and application levels. Several recent studies have taken use of the growing availability of trustworthy equipment for database systems.

Bajaj et al. [7] introduced TrustedDB which implements tamper-proof data aggregation using IBM 4758 PCI [8]. CryptSQLite encases the SQLite processor in an Intel SGX compartment to provide secrecy with a bit of efficiency hit [9]. OblIDB, a more recent study, improves point query speed to 722x quicker than current encrypted communication oblivious databases [10]. Access pattern threats in untrustworthy storage are identified by StealthDB and EnclaveDB which offer cryptographic solutions based on protected hardware [11] [12]. They are distinct from their ProDB regarding security border, access pattern depreciation, and high connectivity adjustments with hardware enclave, ORAM, and disk space. Hardware enclaves are used to solve database problems or build data structures with particular usage [13] [14].

ZeroTrace uses a new components library in its suggested ORAM microcontroller to offer extra protection against application attacks are launched on the SGX enclave, i.e., the oblivious positioning map access [15]. Even with processor enclaves, Oblix and OblIDB recognize the presence of access pattern leaking of the insight of database table employed in index searches and provide more effective performance than the naive worst-case buffer [16] [17]. Pro-ORAM increases system performance by utilizing the number of co Shuffle with SGX enclaves. Even though many researchers put efforts in providing security to metadata it is very difficult to fill the gap between security and practical usability of system [18].

Even though there are many ORAM techniques as mentioned above to secure metadata in online transaction they have some limitations as mentioned below.

- Traditional ORAM techniques suffer from more complexity in model construction.
- Many of the existing techniques are able to provide obliviousness to metadata but failed to improve performance with increasing data.

- As more number of users increases response time decreases.
- Existing system are unable to maintain balance between security and performance.

By considering previous works main inspiration of this paper is to seek out solution which can provide combined solution with maintaining privacy and improving performance of existing ORAM technique.

Our Contribution:

We design our system to achieve main three goals: 1) To reduce complexity and response time 2) To secure metadata with active adversary attacks 3) To improve performance of overall system with increase in number of users.

The proposed system focuses on providing security to metadata in online transactions. As previous ORAM technique strong FEDORAM [28] faces problem of high response time for communication in between client and server, our proposed system tries to reduce the execution time for pull-push operations by making the system work in parallel manner. Parallelizing tasks will optimize the ORAM system in turn reducing response time and will improve performance of overall system. As we observed weak FEDORAM suffers from sensitive data leakage problem in active adversary attacks, our proposed system focuses on protecting data from various attacks like collusion attack, session hijacking, bypass authentication, sink hole and warn hole attacks with designing an XOR-based lightweight cryptographic technique for data encryption as well as decryption during the communication.

Moreover, the further sections of the paper are divided as follows: Section II describes related work done by previous researchers. In Section III describes the algorithm for proposed implementation. The Section IV describes the experimental setup for evaluating the proposed work and results achieved with our methodology and comparative analysis with various state-of-art methods. Section V concludes the proposed work and provides future work guidelines.

II. RELATED WORK

Yanyu Huang et al. [19] proposed real-time oblivious data exchange into the Fog Computing. This approach can eliminate the complex execution process of the client-side and requires low communication cost, including the minimum response time, and it reduces to computation up to 2x than state-of-art methods. The Edge computing environment has been deployed, and all transactions are performed on the edge node. This system depicts an extensive experiment analysis, and it achieves low network bandwidth utilization, fixed data storage on the client machine, and minimum network overhead. The new approach of path oblivious random-access memory is called as R-Path ORAM with large root basket dimensions including the small constant size of remaining buckets in the tree [20]. A thorough examination of the root bucket capacity is carried out in order to arrive at a restricted solution for such necessary root buckets size with a minimal error possibility. Using a common platform, the effectiveness of the R-Path ORAM is assessed to that of the conventional Path ORAM. The results of the tests indicate that R-Path ORAM offers

much less server bandwidth and time taken than the original Path ORAM. This is also a hidden eviction method for reducing the size of the bottom bucket and preventing system failure.

Cao et al. [21] proposed an approach string ORAM access using spatial and temporal optimization techniques. This approach can improve the string ORAM access by using temporal and spatial optimization methodologies. Initially it recognizes dummy data blocks with significantly waste storage space and defines the optimized ORAM scheme that reduces high time computation and effective scheduling. The outcome of this approach reduces the 30% execution time complexity, thus a 40% reduction of memory utilization during the execution. A similar approach of fast and secure ring data retrieval techniques has been proposed by Yeuzhi che et al. [22]. According to Fletcher et al. [23] secure processors have a quality and speed inefficiency of more than 50%. Fletcher et al. [23] suggested a dynamic system with a limited amount of emission allowed.

The first Path ORAM implementations on hardware were presented by Maas et al. [24]. Parallel Computing techniques have been used with implementing the super demon during the process of read and write execution. In demon, two methods were employed to improve Path ORAM's effectiveness. Treetop caching is the first method. Treetop caching saves the first coefficient of determination of the tree in the cache because only the bottom layers are changed while reading and writing to the ORAM, decreasing latency and complexity. The Phantom is the second method. The second Phantom method is min-heap evictions, which stores the cache as a min-heap and evicts the blocks that have been utilized the least in the past initially.

In addition, Fork Path ORAM was introduced by Zhang et al. [25]. Fork Path ORAM combines two successive ORAM applications. Researchers highlighted two consecutive queries could have containers in their routes which are overlapped. As a result, they recommended when a noticed request is made and the entire pathway of the requested data block is received from the servers and put into the stash, the rewriting back of the whole route be postponed until the subsequent request is made. The buckets that intersect in the two ways are not written back in the given details, and only the containers in the first request's path are published back. Furthermore, only the elements in the second route that do not overlap with the direction of the first demand were read into the cache to execute the new request. The procedure is then repeated with the second and third requests, and so on. Researchers also recommended postponing any outstanding ORAM requests. Even though all of their studies were done using the safe processor option, Sanchez [26] found that the advantage of combining the requests is negligible. Sanchez demonstrated that combining queries of size two may save one bucket. Fletcher et al. [27] proposes an optimization that uses a large group counter and many tiny individual numbers per Position Map block to condense these markers to a manageable amount.

Pujol et al. [29] presented FEDORAM. Weak and strong FEDORAM tried to tradeoff between security and performance in the instance messaging. Weak FEDORAM focused on

performance of system while strong FEDORAM focused on security of the system. Weak FEDORAM suffers sensitive data leakage problem while strong FEDORAM suffers from increasing response time with increase in number of users.

Apart from the access cost imposed by ORAM procedures, contemporary ORAM architectures ignore the current computer system's extensive memory and processing hierarchy. According to [28], if the data size is higher than actual memory capacity, it directly enhances the leaf nodes of storage in the background illustrated in Fig. 1(a). Although most layers will be in the high-speed memory area, the tree-top caching has a simple design. On the other hand, each path access is converted into a series of rapid memory locations and sluggish I/O accesses. Due to the general poor locality, alternative caching methods find it difficult to adapt the tree-type structure. Such a design is improvident in terms of I/O frequency cost due to the design difference between storage and I/O access, as well as the disparity of storage and I/O use.

In FEDORAM and Multi-User Oblivious Storage via Secure Enclaves (MOSE), both techniques emphasize on reducing the input-output overhead because they extract single block data during the transaction from backend storage which is demonstrated in Fig. 1(b) and Fig. 1(c). Furthermore, the flat memory structure enables effective top-layer buffering. On the other hand, the shuffling procedure must be done often, and the whole storage must wait for such shuffled to finish before proceeding to another ORAM process. It adds extra waiting time to the process resulting in delayed output [29] [30].

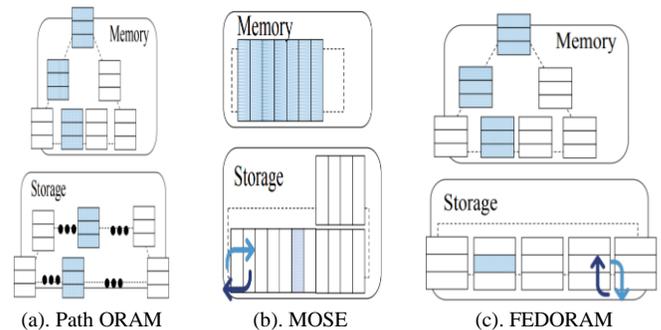


Fig. 1. Various ORAM Techniques for Efficient Input and Output Data Access.

III. PROPOSED SYSTEM DESIGN

A. System Architecture

In the proposed system client server architecture is considered. Fig. 2 shows architecture of proposed HORAM. Initially if client Cl_1 wants to send message to client Cl_2 from server destination list (Ser_{dest} list), then the client Cl_1 generates the message according to below equation 1.

$$M = \{M, Rd_l\} \quad (1)$$

Here Rd_l is the random dummy leaf of destination node list. The Cl_1 establishes connection with entry server S_E and S_E establishes connection to root server S_R to forward M to S_R . The S_R established parallel connection with Rd_l candidate servers such as distributed environment. The all-candidate servers perform the decrypt operation with given M ,

and if it is accurate with server id then it is destination server selected by Cl_1 . The same time data has been stored in internal tree structure by particular S_D . S_R stores positionMap[id] and OTMap[id] in which the positionMap[id] describes each leaf node information while OTMap[id] gives the information of message identifier of encrypted text.

In the system architecture four terms are more important.

- 1) Client
- 2) Entry Server
- 3) Root Server
- 4) Destination Server

In this architecture direct connection between client and destination server is avoided. Instead two entities are added in between client and destination server for secure communication.

In data storage algorithm initially client generates a message to Entry server S_E . Then S_E establishes connection with root server S_R which keeps virtual id of all real and dummy messages received from entry server to destination server. Then encrypted message will be sent to all servers in the federation to get reply from actual destination server in parallel manner. The server who has authority to decrypt the message will get back to root server by decrypting message with its keys. Sending message in parallel manner saves communication time instead of sending it in parallel manner. After that root server makes entry about the current transaction id, user id and server id in its position map for further reference.

In data access algorithm, step 1 to step 3 states about connection establishment from user to root server through entry server. After establishment of connection to root server current server id for transaction is fetched and data will be extracted from specific server. After that for securing metadata and hiding path of current access to destination server current destination id will be replaced with new destination server id. Then entry for current sever id will get deleted and root server will be updated with new server id. In this way metadata privacy preserving access can be performed using the HORAM data access algorithm with employing parallelism in architecture to reduce overall response time of system.

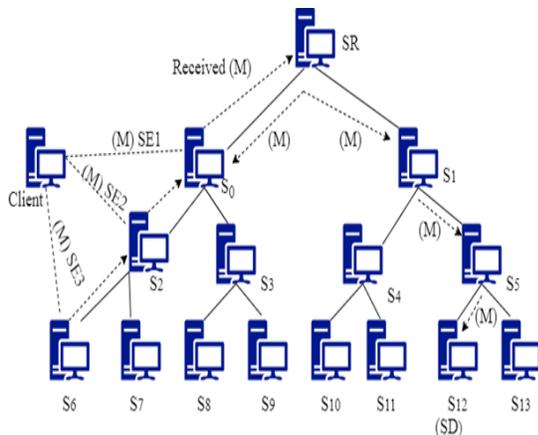


Fig. 2. Architecture of Proposed HORAM.

In data access algorithm we describe the pull activity perform by client Cl_1 . Once data has been extracted it decrypts outside of ORAM, and perform the eviction function for update the repository of access patterns.

B. Algorithm Design

Some basic data structures have been used for implementation for proposed system. Basic ORAM tree is a binary tree of encoded text. Every node of tree contains certain number of data blocks. In the below section we describe data structure used for proposed hybrid ORAM during the execution.

TABLE I. SYMBOLS USED IN PROPOSED HORAM

Symbol	Operation
M	Generated message block
$S(id)$	server id
U_{id}	Current session user identity
T_{id}	Database transaction identity
$random(n, m)$	Random function for selection from n to m
$S_{current}(id)$	Current utilized server
$S_{new}(id)$	Selected new server
positionMap	Positional map
Stash	Temporary buffer memory
R & W	Read and write operation representation
S_D	Destination server
msg	Message
S_E	Entry server

Data storage algorithm (Push):

1: Initially client generates a message using below equation to send to entry server S_E , Message is the random text data.

$$M \leftarrow \text{Generate_Message_Block}(\text{msg}, S_D) \quad (2)$$

2: Send message M to entry server S_E .

3: Once entry server receives message from client then S_E creates connection to S_R .

Now, S_R establishes concurrent online transactions with all m servers.

$$S(id) = \sum_{D=1}^m (\text{ReadNextServer}(D, m)) \quad (3)$$

4: Once server connection has done, according to decryption process only one server who can decrypt the data will return data. The data has forwarded to push function in the form of Push ($M, S(id), U_{id}$).

5: Then root server generates transaction id for further transaction and add entry into the positional map with encrypted data like below.

Function- Add_positionMap($T_{id}, U_{id}, S(id)$)

TABLE II. POSITION MAP

T _{id}	U _{id}	S _(id)
T454565	U343	SS203
T454568	U345	SS204
T454575	U347	SS201
T454589	U349	SS203

6: Commit transaction

Data access algorithm (Pull):

1: Client sends message to Entry server as below:

$M \leftarrow \text{requestMessage}(\text{Msg}, U_{id})$ (4)

2: Entry server gives request to root server to get allocated server with $\text{get_Server_info}(U_{id})$ and detect the allocated server for specific user.

$$S_{\text{current}}(\text{id}) = \sum_{n=1}^m (\text{getServer}(\text{Msg}, \text{id})) \quad (5)$$

3: Establish connection with $S(\text{id})$ from entry server and extract data from

$$D_{\text{set}} \leftarrow \text{getData}(S_{\text{current}}(\text{id}), \text{Msg}) \quad (6)$$

4: Now, select server from set of servers by entry server

$$S_{\text{new}}(\text{id}) = \sum_{n=1}^m (\text{random}(n, m)) \quad (7)$$

5: Once server selection has done, forward data to alter function given as $\text{Alter}(M, S_{\text{new}}(\text{id}), U_{id})$.

6: Entry server generates transaction id for further transaction and update the positional map on root party server like below step 7 and step 8.

7: Delete $(S_{\text{current}}(\text{id}), M)$

8: Update $\text{positionMap}(T_{id}, U_{id}, S_{(id)})$

Here, Table I shows symbols used in the algorithm of proposed HORAM technique and Table II shows entries of position map for particular transaction along with user id and server id.

IV. DISCUSSION

A. Environmental Setup

The proposed implementation is an open-source java environment with 10 data servers in parallel computation for HORAM. In the configuration setup, all are homogeneous with a single client. In all servers there should be a single entry server and single root server, and one destination server in the remaining servers.

B. HORAM Performance

1) *Response time*: Fig. 6 depicts the average response time for the system when 100 messages sent over the network. It shows better result than existing strong FEDORAM as it took less time than strong FEDORAM with increase in number of users. It took little less time than weak FEDORAM. For 300 users it takes average 5 seconds for strong FEDORAM, 2.6

seconds for weak FEDORAM and 3.2 seconds for HORAM. It is observed with the experiment that our technique takes less response time with increase in number of servers. It takes 1.4 seconds for weak FEDORAM, 2 seconds for strong FEDORAM while 0.9 seconds for HORAM.

2) *Complexity*: Table III illustrates our innovations and compares our system to some of the most cutting-edge ORAM structures, as seen above. Where N denotes the total number of messages stored in the whole oblivious system. Because our HORAM's client-to-server connection is based on the RAM, they have similar client-to-server bandwidth and device storage complexity. The federation's communication channels and server computation are both linear.

TABLE III. PROPOSED ORAM AND EXISTING ORAM COMPLEXITY COMPARATIVE ANALYSIS

Scheme	Bandwidth cost	Client storage	Server storage
Weak FEDORAM	$O(N \log N)$	$O(N)$	$O(N)$
Strong FEDORAM	$O(N \log N)$	$O(N)$	$O(N)$
HORAM (Proposed)	$O(N \log N)$	$O(N \log N)$	$O(N \log N)$

C. Security Analysis

The proposed approach provides how it achieves higher security and eliminate the metadata leakage problem during communication.

- **Data Generation**: The client generates random message, and encrypt with proposed XOR operation techniques with the help of receiver's token id. The encryption works like one-way hash function, due to no existence of both encryption and decryption key in message generation and transmission. The encrypted data could transfer to S_E and S_R respectively. Moreover if S_E or S_R compromised with attacker even though attacker can't extract the decrypted text, due to dependency of receiver's token.
- **Data Forwarding**: The S_E and S_R can forward data to next hops or servers. Initially S_E receives the M and he knows the client as well as S_R . The S_E forward similar data to S_R and generate positionMap and OTMap respectively. The $\text{positionMap}[\text{id}]$ describes each leaf node information while $\text{OTMap}[\text{id}]$ gives the information of message identifier of encrypted text, this information stored on root server. The S_R securely keeps both records in ciphertext format that eliminates the possibility of internal or external attacks. The defined ciphertext works like a one-way hash function, which requires a negligible cost to operate; it also does not require significant dependency for encryption and decryption. Moreover, worst case, we consider root server compromised with any attacker even then they are not able to extract actual plain text due to this lightweight cryptographic policy.

- **Data Extraction:** When any client wants to extract the data, it gives a request to entry server S_E and S_E forward to S_R . The message extracted from positionMap with its server information and similar requests were forwarded to SD from S_R and downloaded the plain text. Once the user extracts data properly, the proposed algorithm works to provide additional security to stored information. It first erases the current record from positionMap and selects any random server from the available server set. When the user extract data from S_R holds that decrypted plain text in cache memory. The selected new server and current plain encrypt again by cryptography function and generate a new entry into the positionMap. Once a new transaction is successfully committed, it erases the previous entry of duplicate data.

In proposed architecture, it can be observed that the last transaction has changed on root server into the positional map. This activity can change every time when similar frequent access request has generated by client. The stash memory auto release when time complexity generates such $2N$ for N data blocks. This functionality provides eliminate the dummy blocks and reduce the time as well as space complexity respectively. This algorithm automatically erases the previous entry of a particular transaction with location details from the position map when the user has performed a data pool operation. It generates and stores the new entry into the position map. The significant advantage of this functionality traitor never identifies the background knowledge extracted data source as well as the location of data source.

V. RESULTS

Fig. 3 describes the time required in seconds for data encryption as well as decryption. Based on this experiment, the decryption could take high time than the encryption process.

The two-way encryption techniques are also carried out to achieve security to data during transmission and dynamic decryption at the selection of the destination server. The below table we demonstrate the complexity of proposed and existing systems.

According to above Fig. 4, the data uploading and downloading time required for the client-server in the proposed HORAM. The time required based on the proposed configuration could be flexible when the operating environment has changed. Fig. 5 shows network utilization in communication with number of servers.

The performance evaluation of the proposed evaluation is based on the communication cost required for data push and pull events. When a data push event has been generated, all n receiver data nodes are utilized for communication. Furthermore, the network capacity is handled to 10kb data in a single M. The message size could be changed when the client updates the information or generate a new message. The below Fig. 5 describes a network utilization in MB during data transmission.

In another experiment, we evaluated the communication cost required for data push and pop event from S_R to S_D .

According to FEDORAM, it describes one-to-one communication between all servers, which may produce high communication costs [29]. The proposed module generates a parallel connection between S_R to all available sets of servers S .

Fig. 6 and Fig. 7 depict response with number of servers and number of users and how proposed approach reduces the computation cost than state of the art methods.

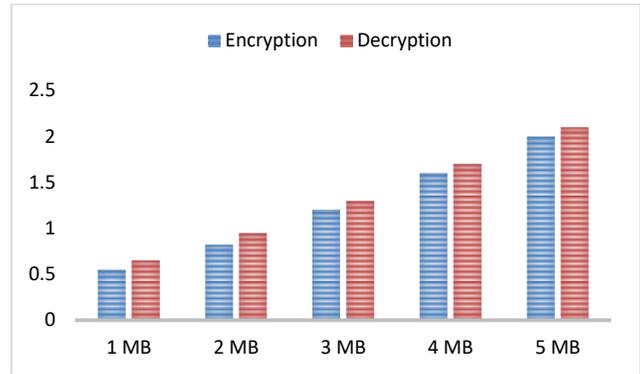


Fig. 3. Time Required in Seconds for Data Encryption and Decryption.



Fig. 4. Time Required in Seconds for Data Push and Pop Operation with all (10) Servers.

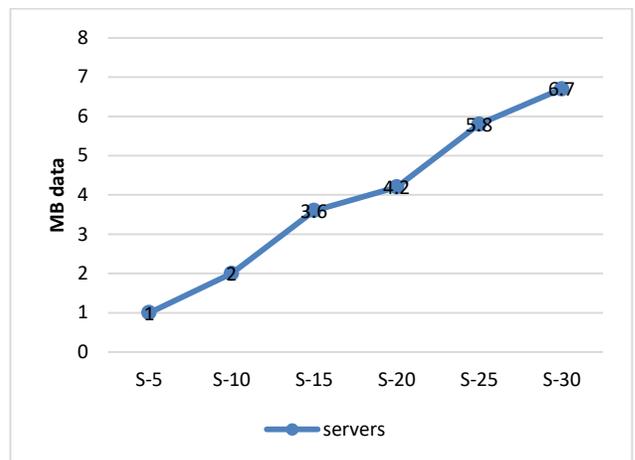


Fig. 5. Network Utilization (MB) with Number of Servers.

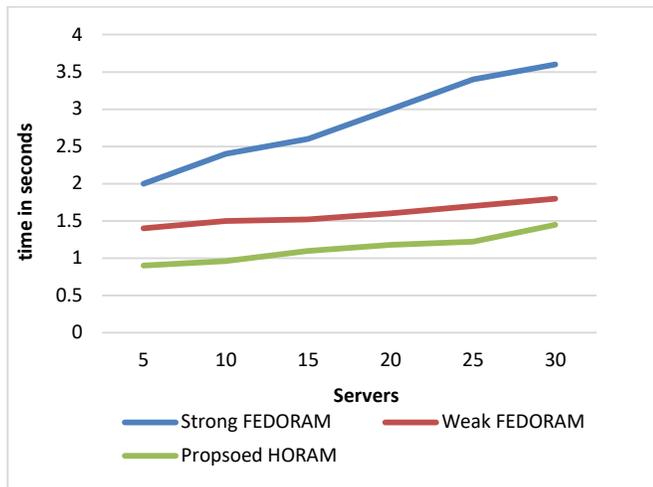


Fig. 6. Average Response Time with Number of Servers.

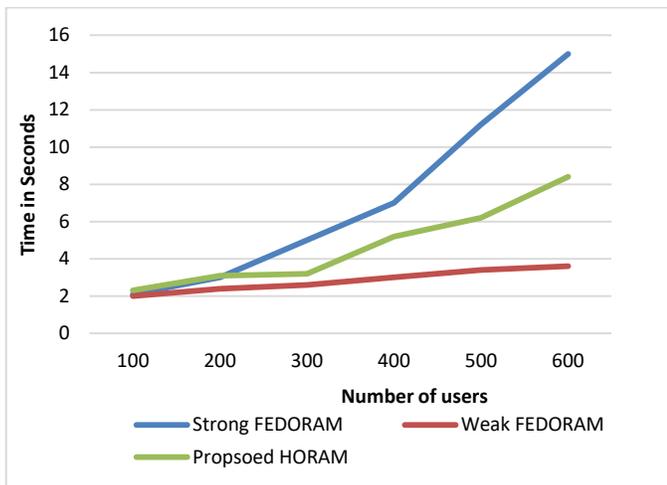


Fig. 7. Average Response Time with Number of Users.

Table IV compares different existing techniques with HORAM for response time taken in data communication.

The proposed approach has evaluated with number of users and number of servers for communication cost, based on both results our system is efficient than [29] in both experiments.

TABLE IV. AVERAGE RESPONSE TIME REQUIRED FOR HORAM AND EXISTING TECHNIQUES

Sr. No.	Techniques	Response time with number of servers in seconds			Response time with number of users in seconds		
		$N=5$	$N=10$	$N=30$	$N=100$	$N=200$	$N=300$
1	Weak FEDORAM	1.4	1.5	1.8	2	2.4	2.6
2	Strong FEDORAM	2	2.4	3.6	2.1	3	5
3	HORAM	0.9	0.96	1.45	2.3	3.1	3.2

VI. CONCLUSION

The proposed HORAM, an innovative ORAM approach achieves high level data privacy and low time computation in distributed environment with untrusted memory. The proposed parallel distribution HORAM provides low computation for database transaction such as push and pull respectively. Experimental analysis shows that the HORAM gives better results in terms of computation time. The method is faster than weak FEDORAM and strong FEDORAM as it takes 0.96 seconds for communication with 5 servers whereas weak and strong FEDORAM takes 1.5 and 2 seconds respectively for reading and writing operation. It improves security in comparison with weak FEDORAM by avoiding direct contact of user with destination server and provides more privacy to metadata with data shuffling and XOR based lightweight cryptographic technique. To enhance this system with large data processing environment for achieving security and privacy of data will be addressed in future work. In future work emphasis will be on reducing complexity of encryption and decryption of extensive data.

REFERENCES

- [1] M. Suresh Babu, K. Bhavana Raj, and D. Asha Devi, "Data Security and Sensitive Data Protection using Privacy by Design Technique", 2nd EAI International Conference on Big Data Innovation for Sustainable Cognitive Computing, 2021, ISBN : 978-3-030-47559-8.
- [2] N. B. Gayathri, G. Thumbur, P. Rajesh Kumar, M. Z. U. Rahman, P. V. Reddy, and A. Lay-Ekuakille, "Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks", IEEE Internet of Things Journal, vol. 6, no. 5, pp. 9064-9075, Oct. 2019, doi: 10.1109/JIOT.2019.2927089.
- [3] A. Tarannum, Z. U. Rahman, L. K. Rao, T. Srinivasulu, and A. Lay-Ekuakille, "An Efficient Multi-Modal Biometric Sensing and Authentication Framework for Distributed Applications", IEEE Sensors Journal, vol. 20, no. 24, pp. 15014-15025, Dec.15, 2020, doi: 10.1109/JSEN.2020.3012536.
- [4] R. Nellutla and Moulana Mohammed, "Survey: A Comparative Study of Different Security Issues in Big Data", Emerging Research in Data Engineering Systems and Computer Communications, Vol. 1054, 2020, ISBN: 978-981-15-0134-0.
- [5] E. Stefanov, M. V. Dijk, E. Shi, C. W. Fletcher, L. Ren, X. Yu, and S. Devadas, "Path ORAM: an extremely simple oblivious RAM protocol", Journal of the ACM, vol. 65, no. 4, pp. 1-26, 2018.
- [6] G. Asharov, I. Komargodski, W. Lin, K. Nayak, E. Peserico, and E. Shi, "Optorama: Optimal oblivious ram", Advances in Cryptology–EUROCRYPT 2020, Volume 12106, 2020.
- [7] S. Bajaj and R. Sion, "TrustedDB: A Trusted Hardware-Based Database with Privacy and Data Confidentiality", in IEEE Transactions on Knowledge and Data Engineering, vol. 26, no. 3, pp. 752-765, March 2014, doi: 10.1109/TKDE.2013.38.
- [8] M. T. Basu and J. K. R. Sastry, "Enhancing Data Security under Multi-Tenancy within Open Stack", International Journal of Advanced Trends in Computer Science and Engineering, vol. 9, no.1, January – February 2020.
- [9] Y. Wang, L. Liu, C. Su, J. Ma, L. Wang, Y. Yang, Y. Shen, G. Li, T. Zhang, and X. Dong, "Cryptsqlite: Protecting data confidentiality of sqlite with intel sgx, in: Networking and Network Applications (NaNA)", 2017 International Conference on Networking and Network Applications (NaNA), pp. 303–308, 2017.
- [10] S. Eskandarian and M. Zaharia, "An oblivious general-purpose SQL database for the cloud", CoRR abs/1710.00458, 2017.

- [11] A. Gribov, D. Vinayagamurthy, and S. Gorbunov, "Stealthdb: a scalable encrypted database with full sql query support", arXiv preprint arXiv:1711.02279, 2017.
- [12] C. Priebe, K. Vaswani, and M. Costa, "EnclaveDB: A Secure Database Using SGX", 2018 IEEE Symposium on Security and Privacy (SP), pp. 264-278, 2018, doi: 10.1109/SP.2018.00025.
- [13] A. Ahmad, K. Kim, M. I. Sarfaraz, and B. Lee, Obliviate: A data oblivious file system for intel sgx", 25th Annual Network and Distributed System Security Symposium, NDSS, 2018.
- [14] H. Brekalo, R. Strackx, and F. Piessens, "Mitigating password database breaches with intel sgx", SysTEX@ Middleware, p. 1, 2016.
- [15] S. Sasy, S. Gorbunov, and C.W. Fletcher, "ZeroTrace: Oblivious memory primitives from intel sgx", IACR Cryptol. ePrint Arch. 2017 (2017) 549.
- [16] P. Mishra, R. Poddar, J. Chen, A. Chiesa, and R.A. Popa, "Obliv: An efficient oblivious search index, in: 2018 IEEE Symposium on Security and Privacy (SP)", IEEE, pp. 279-296, 2018.
- [17] S. Eskandarian and M. Zaharia, "Oblidb: Oblivious query processing using hardware enclaves", arXiv preprint arXiv:1710.00458, 2017.
- [18] S. Tople, Y. Jia, and P. Saxena, "Pro-oram: Practical read-only oblivious {RAM}", 22nd International Symposium on Research in Attacks, Intrusions and Defenses ({RAID} 2019), pp. 197-211, 2019.
- [19] Y. Huang, B. Li, Z. Liu, J. Li, S. M. Yiu, T. Baker, and B. B. Gupta, "ThinORAM: Towards Practical Oblivious Data Access in Fog Computing Environment", in IEEE Transactions on Services Computing, vol. 13, no. 4, pp. 602-612, 1 July-Aug. 2020, doi: 10.1109/TSC.2019.2962110.
- [20] K. S. Al-Saleh and A. Belghith, "Radix Path: A Reduced Bucket Size ORAM for Secure Cloud Storage," in IEEE Access, vol. 7, pp. 84907-84917, 2019, doi: 10.1109/ACCESS.2019.2925789.
- [21] D. Cao, M. Zhang, H. Lu, X. Ye, D. Fan, Y. Che, R. Wang, "Streamline Ring ORAM Accesses through Spatial and Temporal Optimization," 2021 IEEE International Symposium on High-Performance Computer Architecture (HPCA), 2021, pp. 14-25, doi: 10.1109/HPCA51647.2021.00012.
- [22] Y. Che, Y. Hong and R. Wang, "Imbalance-Aware Scheduler for Fast and Secure Ring ORAM Data Retrieval," 2019 IEEE 37th International Conference on Computer Design (ICCD), 2019, pp. 604-612, doi: 10.1109/ICCD46524.2019.00087.
- [23] C. W. Fletcher, L. Ren, X. Yu, M. Van Dijk, O. Khan and S. Devadas, "Suppressing the Oblivious RAM timing channel while making information leakage and program efficiency trade-offs," 2014 IEEE 20th International Symposium on High Performance Computer Architecture (HPCA), 2014, pp. 213-224, doi: 10.1109/HPCA.2014.6835932.
- [24] M. Maas, E. Love, E. Stefanov, M. Tiwari, E. Shi, K. Asanovic, J. Kubiawicz, and D. Song, "PHANTOM: Practical Oblivious Computation in a Secure Processor", In Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security, Berlin, Germany, 4-8 November 2013, ACM: New York, NY, USA, pp. 311-324, 2013.
- [25] X. Zhang, G. Sun, C. Zhang, W. Zhang, Y. Liang, T. Wang, Y. Chen, J. Di, "Fork Path: Improving efficiency of ORAM by removing redundant memory accesses," 2015 48th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO), pp. 102-114, 2015, doi: 10.1145/2830772.2830787.
- [26] M. Sánchez-Artigas, "Enhancing Tree-Based ORAM Using Batched Request Reordering," in IEEE Transactions on Information Forensics and Security, vol. 13, no. 3, pp. 590-604, March 2018, doi: 10.1109/TIFS.2017.2762824.
- [27] C. Fletcher, L. Ren, A. Kwon, M. V. Dijk, and S. Devadas, "Freecursive ORAM: [Nearly] Free Recursion and Integrity Verification for Position-based Oblivious RAM", Proceedings of the 20th International Conference on Architectural Support for Programming Languages and Operating Systems (ASPLOS), Istanbul, Turkey, pp. 103-116, March 2015.
- [28] S. Sasy, S. Gorbunov, and C. W. Fletcher, "ZeroTrace: Oblivious memory primitives from Intel SGX", Symposium on Network and Distributed System Security (NDSS), 2018.
- [29] A. Pujol, L. Murphy and C. Thorpe, "FedORAM: A Federated Oblivious RAM Scheme," in IEEE Access, vol. 8, pp. 187687-187699, 2020, doi: 10.1109/ACCESS.2020.3027516.
- [30] T. Hoang, R. Behnia, Y. Jang, A. A. Yavuz, "MOSE: Practical Multi-User Oblivious Storage via Secure Enclaves", Proceedings of the Tenth ACM Conference on Data and Application Security and Privacy, pp. 17-28, march 2020.

Blockchain-based Secure Data Transmission for UAV Swarm using Modified Particle Swarm Optimization Path Planning Algorithm

M.Kayalvizhi¹

Research Scholar: Computing Technologies Department
SRM Institute of Science and Technology
Chennai, India

Dr.S.Ramamoorthy²

Associate Professor: Computing Technologies Department
SRM Institute of Science and Technology
Chennai, India

Abstract—With the rapid development of unmanned aerial vehicles assisted applications enabled with a communication system, they are open to various malicious attacks. As a new form of flying things, they can access the network for better communication via the aerial base station. Most of the Unmanned aerial vehicles assisted flying objects' optimal path selection schemes does not consider the path deviation. In path deviation attacks, secure data transmission are not addressed in existing works. The secure communication process between Unmanned aerial vehicles and base station are exploited through security-based attacks. Moreover, path loss issue leads to multicast packet loss and unsecured broadcast. The existing network architecture setup does not fulfill the secure data communication and privacy issues. In this paper, Blockchain is utilized to investigate the secure communication between Unmanned aerial vehicles to Wireless Unmanned aerial vehicles Base stations. Since the destination information is dynamic under an uncertain environment, it will cause a delay in data communication. Unmanned aerial vehicles are more vulnerable to security attacks. The proposed blockchain-based architecture supports secure data communication in Unmanned aerial vehicles uncertain environments. To improve network security, this paper designs a modified particle swarm optimization method for better path selection. Through these experimental results, a blockchain-based data communication scheme is outer performed concerning network security.

Keywords—Unmanned aerial vehicles; path planning; swarm optimization; denial of service attack; blockchain; security and privacy; data communication

I. INTRODUCTION

Unmanned aerial vehicles (UAV) can be enabled with high flexibility based on harsh environment data communications. The major harsh environments are landscape country border monitoring, deep-sea monitoring, Industrial Monitoring, IoT agricultural monitoring, and UAV-based thermal tracking tool. UAV is one such potential communication field. The harsh environments can be monitored through UAV in large-scale integration with network security aspects. The UAVs are moving randomly across the environments with controller specifications to collect the information about network moving objects as well static ones. A UAV-enabled communication system is considered which will be a better one in between terrestrial and air medium. However, the available routing path up-gradation of the unmanned aerial

vehicle is not enough to complete the data communication. Assuming the ideal path up-gradation is to determine the specifically targeted place of UAV or sink of the network that the UAV can carry the sensing details to reach them out. The UAV sensing data relay communication will face interrupt, distortion, and path selection issues. The analysis of relay network communication will affect the quality of data and communication time delay. The UAV data communication is defined with routing path state and data relay state. In such routing path up-gradation, the data can be broadcast via radio propagation. Once the jamming attacker enters into the UAV communication network it will remove the controller of the ground node from the attacker. The UAV network is controlled by the attacker and the UAV remote wireless sensor control ground node will be disconnected. The communication between the UAVs which are participating in the network needs to be secured since the data can be interpreted by a malicious attacker and the total mission can be compromised. The UAV device can also be compromised and it can be used against the UAV swarm. Most attacks focus on draining the resources which lead to the failure of the UAV mission. And to mitigate attacks on the modified swarm of UAVs, a secure authentication mechanism needs to be followed that identifies the participating UAVs identity and confirms that it is not malicious. The existing routing path selection process is updated through the conventional anti-jamming technique which focused only on transmit power functions with beamforming. The routing path selection should be highly controllable in the proposed algorithm. In UAV-based data communication facing optimal path selection in the wireless network and one of the recent experimental studies is conventional OSPF protocol-based path selection. The existing conventional scheme doesn't consider the successful data communication, time delay, and quality of the data. Due to the conventional path selection scheme implementing the trajectory planning didn't restrict the jammers' attack. The movements of UAVs like climbing angles and turnings are not restricted in the conventional method. However, the UAV's behaviour will affect the performance of the system.

The UAV's movements are reducing the higher risk of collision. The updated routing path will provide the ideal climbing angle to do the relay state communication. To handle these issues, UAV's multi-path selection is proposed and introducing successful data communication to improve the

performance of the UAV system. Routing path up-gradation is considered in the UAV communication process which is a novel proposal to remove the constraints. The constraints of path selection are identified as a research gap and the novel multi-path flashing meta-heuristic optimization algorithm is the proposed solution. To overcome such difficulties, a multipath flashing meta-heuristic algorithm is proposed to solve the path selection and up-gradation. The experimental numerical results show that the proposed algorithm can improve the UAV data communication process via optimized path selection design especially when there is high mobile traffic in the wireless network.

The high-speed increase of technologies in the wireless network has also simultaneously increased many challenges in data security. The data shared via networks need to be secured by strong encryption and cryptography mechanisms. The data are broken down into blocks in which each block consist of the data such as time, and the hash of the previous block. Blockchain plays a vital role to address the data security challenges and in preventing cyber-attacks. It ensures that the data available in the network cannot be tampered with or removed by any external users, who are not authenticated. The data can be added to the network only if its authenticity is verified by the peer nodes in the network. And if any malicious user tries to alter the data, the attacker needs to alter every block of the data, since the data blocks are interlinked and carries the hash of the previous block. So it will be a tedious task for the attacker to alter every consecutive block and gain access to the network.

The rest of the research paper is constructed with the following sections. In Section II, Existing works, analysis of existing objectives and results is discussed. Section III discusses the evaluation of path deciding factors for path planning. Further in Section IV, how blockchain secures UAV swarm and Section V UAV network-level Denial of Service Attack scenario further implementing blockchain settings, respectively. Section VI. The experimental level simulation settings and results are presented, further validating the blockchain performance in security and privacy in terms of data communication. Section VII discussions on simulation results and in Section VIII, the conclusion work is presented.

II. EXISTING WORK

In this section, brief review details on the network security and path selection problem for UAV are discussed. The various path selection approaches are applied to find optimal path selection for UAV data communication.

T. Zhao, X. Pan and Q. He [1], the author proposed a dynamic Ant colony algorithm for path planning in UAV where the proposed algorithm is applied in the scenario of UAV reconnaissance. The main drawback of the Ant colony algorithm is that it will be effective in only a confined space. Optimal results are not guaranteed when the distance is increased. And the authors applied the algorithm on the UAV's which are deployed in a pre-planned location. This algorithm cannot be optimal when the UAV's target location is undefined and will not be feasible in an uncertain dynamic environment where the search space can be extended.

Li, Z., & Han, R. [2], the author studied the UAV flight path planning where the ant colony algorithm is used and a digital signal map is derived. The UAV movements are tracked in both vertical and horizontal directions, which will help to stimulate the UAV flight path. The proposed algorithm is not feasible when the threat area is dynamic and can't be optimal in real-time complex scenarios.

Bai, X., Wang, P., Wang, Z., & Zhang, L. [3], the author proposed a hybrid algorithm of an artificial bee colony and A* and studied on an iterative selection of arrival time where the UAV select the arrival time which is shortest and enhances the multiple UAV sequential arrival time. The proposed algorithm will not be suitable for the complex mission where the multiple UAVs needs to operate simultaneously to complete a task and the task offloading is not possible in this case.

Muntasha, G., Karna, N., & Shin, S. Y. [4], the author designed an algorithm anti-collision algorithm using an artificial bee colony where it optimizes the velocity of the UAV to reach the target. And an alternate path is designed if obstacles are detected. The proposed algorithm will be effective when the population size is increased. And it has a high computational cost.

Priyadarsini, P. L. K. [5], the author proposed an area partitioning algorithm and the area is partitioned as rectangles and midpoints are calculated for each partitioned rectangle which is further used for optimal path planning. And a graph is constructed by joining the midpoints and the optimal path is found using firefly and particle swarm optimization algorithm, where the results show that the particle swarm optimization algorithm is better than the firefly algorithm. But the proposed algorithm is not suitable for environments with dynamic obstacles.

Wei, Y., Wang, B., Liu, W., & Zhang, L. [6] the author focused on using an improved firefly algorithm for hierarchical task assignment. The author used the Metropolis criterion to avoid local optimum. And the firefly algorithm uses a multi-neighbour search algorithm to discretize the problem. The main problem in the proposed algorithm the defined parameters do not change over time and its not optimal in an uncertain environment where the targets are obstacles are dynamic.

Aliwi, M., Aslan, S., & Demirci, S. [7], the author used the firefly algorithm to find the best coverage area for the UAV placement for better communication and to reduce the consumption of energy. But this proposed work focuses only on one UAV and doesn't concentrate on multiple UAV environments. The optimal usage of battery power of the UAV is essential for effective communication. And since the firefly algorithm has a slow convergence rate and it can easily fall into local optimum.

Wang, S., Bai, Y., & Zhou, C. [8], the author proposed a method that focuses on yaw angle and height for mapping UAV devised on particle swarm optimization. Here the algorithm calculates the fitness value of each particle and the position of each particle is updated which outputs the optimal position. The main gap in the particle swarm optimization

algorithm is that the iterations don't guarantee the optimal result and it can easily fall into local optimum.

Aggarwal, K., & Goyal, A. [9], the author used particle swarm optimization algorithm to coordinate multiple UAVs for disaster management. The work focuses on locating humans in the disaster management site. The main gap in the particle swarm optimization algorithm is that it is influenced by the inertia weight and has low flexibility.

Evsen Yanmaz, Robert Kuschig, Markus Quaritsch, Christian Bettstetter, and Bernhard Rinner., [10] discussed deterministic and probabilistic path planning algorithms, its drawback and benefits. They studied that the deterministic approach takes more time in deciding the action plan and probabilistic approaches can only give probabilistic guarantees in any task.

TarunRana, Achyut Shankar, Mohd Kamran Sultan, RizwanPatan, [11] Authors highlighting drones are controlled remotely via radio frequency and it makes the signal jamming in a susceptible manner. Radiofrequency jamming is a very frequent attempt from attackers. There are so many existing techniques that easily hack the drones and disconnect the communication channel. The UAV timestamp is a time log system that provides more security to the UAV. The timestamp follows the block which contains the hash value. The attacker changes the hash values and it creates a communication problem.

Jiyang Chen1, Zhiwei Feng2,1, Jen-Yang Wen1, Bo Liu, and LuiSha.,[12] author referring defending against UAV network internal Denial service of attack requires continuous tracking of all aspect running the system which creates huge overhead for the system. The real-time difficulties like system memory size, hardware capability, power consumption and reliability are hard to maintain the system functionality.

The above all related works in the optimal path planning in Unmanned Aerial Vehicle focuses on the coverage space which is already pre-defined and only finds an optimal solution in that defined coverage space. And the existing swarm algorithms such as Firefly, Ant colony, Artificial bee colony and Particle Swarm optimization algorithm all are capable of finding an optimal path in a search space where the target and the obstacle positions are pre-planned. It doesn't focus on dynamic targets and obstacles with the factor of uncertainty. When it comes to uncertainty, the navigation of UAVs is affected by many external factors. And the UAV system should be able to continue the mission when it is affected by external factors such as heavy gusts of wind, changing temperature, high altitude and moving obstacles. And another main security gap observed is secure communication. The data and the parameters defined should be securely communicated to the UAVs for a mission. And compromise of the data can lead to mission failure.

From the existing works, the optimal path algorithms such as Firefly algorithm, Iterative algorithm, Deterministic & Probabilistic Algorithm, GNSS and m-TSP mostly focus on the path selection in a static network environment. So, when these optimal algorithms are in an uncertain high mobility dynamic network, data loss and path deviation attacks are

expected which compromises the successful data communication among the UAVs. The most frequently used optimal path algorithms and their limitations are listed out in Table I. The main research objective is to allow authenticated UAVs to operate in a high mobility dynamic environment and despite the uncertain factors and the path selection and the data transmission should happen securely and successfully. So based on these factors, a Meta-Heuristic optimization-based path planning model is proposed for path up-gradation aided with secure data communication.

TABLE I. COMPARISON OF EXISTING ALGORITHMS

Algorithm	Comparisons of Existing Algorithms			
	Advantages	Limitations	Performance in a dynamic environment	Proposed Solution
Firefly	Low UAV Energy Consumption	Limited Coverage	Partial environment	Need high coverage
M-TSP	Multi-Target	Not in Dynamic	Trilateration Method.	Dynamic Coverage
Genetic	Easy Target Access	Small Scale coverage	Limited	Need high coverage

III. PATH DECIDING FACTOR EVALUATION IN PATH PLANNING

The heuristic optimization system installed on an unmanned aerial vehicle network can provide a lot of changes in the uncertain environment from not only static UAV network secure data communication but also in high mobility UAV network. The features can be highlighted into two different levels of improvements, heuristic optimization path planning and secure data communication.

In this section, the Meta-Heuristic optimization-based path planning model is discussed in detail. Since the proposed modified swarm optimization method is developed with dynamic UAV movement which is influenced by the nearby base station and it is also guided exact UAV position based on the entire domain. There is no restriction on range. For evaluating the optimal dynamic UAV network Metaheuristic optimization method, an evaluation method is followed which maintains the distance of intra UAV path, energy level, and throughput and packet loss. The proposed metaheuristic optimization method provides exact distance measurement of intra UAV path which reduces the UAV minimum relay link requirements between the UAV nodes. This evaluation function is proposed as the fitness sum of mentioned parameters. The parameter functions are as follows:

$$In = \alpha \times UAVm / \sum_{i=ie} + \alpha 1 \times 1 / \sum_{i=ie1} + \alpha 2 \times 1 / Tuav (\sum_{i=n} (\sum_{i=ie} + \sum_{i=ie1}) / Tuav) \quad (1)$$

In the above-mentioned equation $\sum_{i=ie}$, $\sum_{i=ie1}$ is the distance between two UAV nodes and $\sum_{i=ie}$, ie is the initial node energy level of the UAV network. After deciding the destination, the assigned UAV nodes get updated with the location of the destination, energy level and distance between the UAV nodes. These are the parameters considered in the UAV assisted UAV nodes. The Heuristic optimization

collected the UAV network data from the uncertain environment. The initial step evaluates the values of each UAV node and the instructions are proposed in the optimal path based on Meta - Heuristic optimization algorithm.

The UAV network node evaluation values are derived with the following equation (2). In this equation, the distance between two UAV nodes and UAV node data collecting capacity is utilized for UAV path deciding factors.

$$Pdf = \alpha 1 \times \sum_{i=1} \sum_{j=1} (\sum_{i=ie} \sum_{i=ie1}) + \alpha 1 \times \sum_{i=1} A dc \quad (2)$$

$\sum_{i=1} \sum_{i=ie1}$ are represented values of the two UAV nodes, $\sum_{i=1} A dc$ - Average Data Collection.

Path deciding factors (Pdf) are used to indicate the distance between UAV nodes ($\sum_{i=1} \sum_{j=1}$) Pdf. The collecting data capacity is calculated from the UAV node sensing quality which is frequently evaluated for path deciding factor.

The evolution method was initiated through UAV network node deployment and implemented Meta-Heuristic optimization, multiple UAV nodes are integrated high dynamic UAV network data communication and ensure privacy and security. Based on the UAV network, multiple numbers of UAV nodes are integrated and the evolution method calculates the path deciding values. The existing localization variable structure filtering problems and computational performance calculation occasional errors issues are overcome with evolution method path deciding values. The presented values are highlighted as deciding factors among the UAV network. In meta-heuristic optimization techniques are utilized for path planning and instant path selection. Among all the path planning and path up-gradation techniques in meta-heuristic term is mathematically optimized to select the upgraded instant path through high-level mathematical procedure specifically limited computational capacity and incomplete information structure. The path planning factors are discussed in the next section.

IV. UAV SWARM AND BLOCKCHAIN

Blockchain is a growing technology in the cyber security area and it's a promising technology in securing data and identity. It has many impacts in a wide range of areas in inventory management, the health industry and Internet of Things (IoT) in the domain of UAV.

The management of the UAV swarm is a critical task since it involves the coordination of multiple UAVs and the data communication in UAVs needs to be secured. And the security concerns are more when multiple UAVs are operating in a surveillance operation. And the main security challenge is to secure the UAVs in the network and to prevent the UAV swarm from security attacks such as denial-of-service attacks and ground control station jamming attacks. And to address these problems, Blockchain technology will be a promising solution. The UAVs in the swarm are registered with a valid key which will make them an authorized UAV in the network as depicted in Fig. 1. The UAVs which don't have valid keys will be automatically rejected by the UAV network. The blockchain maintains a distributed ledger and tracks the activity of the UAVs in the swarm network. And the collected

data in the UAV are secured and cannot be tampered with. So, once the UAVs collect and store the data, the collected information is secured and it cannot be modified. Any slight modification in the blockchain will be detected and it will be rejected by the network. So, Blockchain will be effective in securing the UAV's identity and the data collected in the UAV swarm and preventing it from malicious attacks.

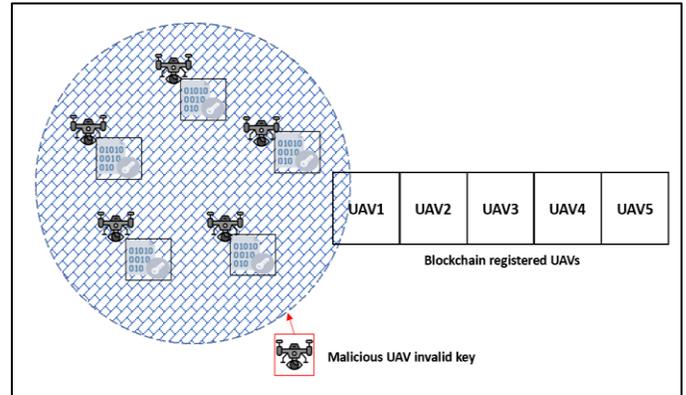


Fig. 1. A Scenario of an uncertain UAV Network.

The evolution factors are described for path planning constraint and the UAV nodes are followed updated searching state. The updated searching state is following three different segments finding the next hop duration in the assigned UAV network, UAV identity, and UAV location with the exact position. The described factors involved provide an updated routing path that ensures the security of data communication between two UAVs. UAV path planning convergence and combining matrix decomposition issues and multipath distortion errors are solved through this evolution constraints method. These three factors are updated through real-time values from the experimental part. The coordination of the factors kept maintains the updated routing table.

In such case the destination has not maintained the energy to carry over the data communication to reach the destination, the UAV communication node, exchange the data to reach the destination, the data exchange can be the safest way and the UAV network communication system should ensure the UAV node energy and threshold level. The UAV network routing table keeps the updated UAV path deciding factor parameters. To ensure the longest distance data communication between two UAV nodes, the updated parameter values are decided on the stability of the network. The local trajectory planner is applied in the decision mode which provides the current direction of motion based on parameter index. According to the current parameter values, the data communication is not suitable for direct communication then it is upgraded for indirect communication. Indirect communication is suggested if the stability of the network connection is not suited for direct communication. In this case, the routing table updates the revised path to make the indirect path.

The blockchain-based UAE server is responsible for forwarding the data. The UAV node energy details are managed through the UAV server. To improve the efficient data communication enhanced interior gateway routing protocol was implemented in the UAV mounted server

network. The high potential bandwidth creates better connectivity. This proposed blockchain-based architecture supports secure data communication in UAV uncertain environments. The enhanced interior gateway routing protocol in the UAV mounted server network is implemented which featured an advanced distance vector in x86 architecture and storage access. The secure data communication adopted asymmetric encryption and passed through meta-heuristic optimization. The enhanced interior gateway protocol updates the further position while the UAV node hovers the position in the assigned duration. So, the UAV node is prepared to move for a further position with the help of an updated routing protocol. The UAV node keeps the distributed ledger and it receives the encrypted data. The UAV node sends the encrypted data to the UAE server and the UAE server will check the encrypted data and allow meta-heuristic optimization. The meta-heuristic optimization forwards encrypted data to the UAE server and then the UAE server decrypted the data to get the actual data. The distributed ledger keeps the transaction of all the details within the UAV node and UAE server communication. The Malicious UAV node moves to the neighbour UAV nodes without following the updated routing table. The malicious UAV node exhausts the energy level due to unplanned moments in the uncertain environment.

V. DENIAL OF SERVICE ATTACK SCENARIO

The UAV network-level Denial of Service Attack scenario further implementing blockchain settings respectively are discussed. A scenario of Uncertain Environment UAV network is illustrated in Fig. 2. The heuristic optimization assists the system by protecting UAV network data Communication channel, memory and CPU utilization. The Implementation of this proposed system provides a secure UAV network.

A. System Model

The proposed heuristic optimization-assisted system is composed of a performance control system and security data system. The Optimization system controls the uncertain environment and maintains the performance. The controlling system provides optimized performance and advanced path planning with malicious activity avoidance. The proposed method running inside the uncertain environment UAV network is normally operated by industrial applications which have high secure architectures and update instant activities. The advanced optimization system will be practical to track the system and control the potential vulnerabilities.

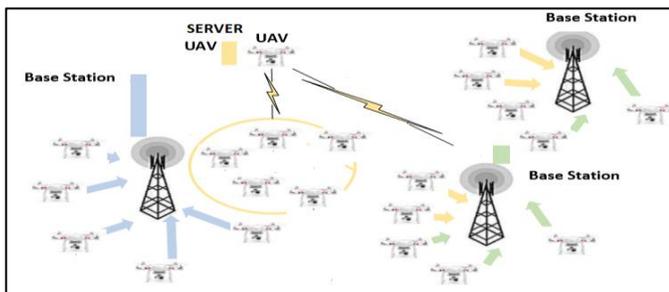


Fig. 2. A Scenario of an uncertain UAV Network.

The optimization assisted system refers to the client operating system and the security system running over on top of it. It is implemented for data security motive and maintains the simple systematic such that the system could be applied and analyzed. The client operating system process runs inside which ensures safety. The optimization controller rules the client operating system with simple modules which support the UAV network functionalities. The proposed system completely controls the uncertain environment in case of routing update failure for the path details due to a Denial-of-service attack which ensures a secure UAV network [13].

The main aim is to secure the data communication in the UAV swarm. The optimization system helps to regulate the security of the data in which it monitors the activity of the UAV nodes. So this will enable to track the position, UAV node energy capacity and distance from the base station for instant path planning.

A scenario of uncertain UAV networks is illustrated in Fig. 1. The optimization highlighted features in the uncertain environment, tracks the output from the client operating system. The identification of malicious activity, the tracking feature monitors the results from the client operating system and controls the major changes further [14].

B. Attacker Model

The real-time applications in the uncertain environment could maintain the data security in the initial stage, whereas the malicious embedded in an uncertain environment couldn't implement the optimization controller. The client operating system suffers adversary launch of Denial-of-service attack against the uncertain environment. The denial-of-service attack does not maintain the protection to overcome the optimization controller. The malicious movements do utilize the Denial-of-service attack to spoil the uncertain environment and UAV network performance [15].

C. CPU Denial of Service Attack Protection

In data security and CPU resource management, it will utilize the controlling system and maintain high performance. The CPU utilization priority improves against user requests. Every real-time application implements the first in first serve priority assignment; a high priority process could finish first and which is followed by the low priority [16]. This process helps the uncertain environment CPU utilization properly.

D. Memory Allocation and DoS Protection

The malicious movements in an uncertain environment could embed the Denial of Service (DoS) attack on the memory allocation by collecting a high amount of data from allocated memories which will affect the UAV network performance. The memory measurement feature encounters the CPU utilization in which the related system does not access the exceeding memory. The optimization controller uses the UAV network performance counter provided by the controller to monitor the memory access within the allocated period. The allocated period is maintained for accessing the memory without any restriction. It is highly suggested to resolve the memory constraint issues [17].

E. Data Communication DoS Protection

The optimization controller inside an uncertain environment maintains sensor data and utilizes client inputs to the UAV network to function properly [18]. The highlighted feature secures the system against DoS attacks. This will be required to control the uncertain environment and ensure system monitoring.

F. Simulation Mode

Times Sensible Sensors in uncertain environments are important components that should be protected from malicious activities in applications. The mandatory requirement in the simulation node is an optimization controller, where it doesn't control the memory access but will receive all necessary details from system activities. The thread activities showing in an uncertain environment will receive the data from sensor data and passes towards the optimization controller. This activity will arrest all Denial-of-service attack activities.

G. Data Security Monitoring

The scenario of an uncertain environment with a blockchain network is depicted in Fig. 3. The optimization controller maintains the network access to interface uncertain environment. To protect the uncertain environment from malicious activities, the UAV network controls have been separated in two ways.

The UAV network is deployed in an isolated application space where the UAV network does not have an internet connection to access data and through interface only it has to process the communication. An updated routing table is utilized to control the communication system which reduces the unwanted communication and damages caused by denial-of-service attacks. The modified swarm optimization method is developed with a dynamic UAV uncertain environment and identifying the positions in dynamic search space. The dynamic search space has identified the destination then the sender confirms the destination area which should not be smaller than pre-defined positions. The unrestricted area coverage is modelled with a sparse multi-link collaboration with unrestricted distance.

The optimization controller continuously monitors the results from the client operating system. The continuous monitoring system controls the uncertain environment and identifies the thread activity which diverts to the optimization controller. The consecutive sensing data receiving interval should not be set to a normal threshold and it should be set to average. The normal interval suggestions will fail the optimization controller.

VI. EXPERIMENTAL RESULTS

The experimental level simulation settings and results are presented, further validating the blockchain performance in security and privacy in terms of data communication.

In this section, the Meta-Heuristic optimization algorithm is compared in experimental models and also various UAV environments. The ContikiCooja Experimental setup is introduced. In the cooja simulation, the area of interest is a 3Km radius. The main parameters utilized in our experiment are provided in Table II. The allocated bandwidth of each UAV node is assigned as 10 MHz. The other side of the UAV network servers also carries a 20 MHz band which means the high data traffic can be scheduled on the allocated bandwidth forwarded by the UAV nodes which could avoid congestion. The airframe spectrum range is assigned as 2.6, so the 20 MHz bandwidth can produce a 32 Mbps data rate. To this segment, here the UAV nodes are uniformly distributed on a geographical position. And the UAV nodes are operating in an uncertain environment with $x = 22.45$ and $y=2.30$ at 4 GHz carrier frequency. Considering the multipath flashing technology, the entire communication UAV network resources can be planned for a 180 Mbps data rate, which is the same as 25 Mbyte/s. The p is set as 10×10^3 which equates to the packet cost as 800 bits. In each UAV node, it has the packet cost in an uncertain field of each layer of the data transaction. The identification of the UAVs height and depth-dependent parameters α (h_1) and $\delta(d_1)$ are positioned according to the uncertain environment. The highest range of the position λn_u is 24 ~36 dB while every UAV is at the height of 20m. In this experimental simulation, the value of λn_u is assigned which is equivalent to the network locations of UAV node n and UAV servers. The special attention the subordinate UAV nodes in uncertain environment series location, share and update the values in λn_u . The ideal value of the UAV network path loss is identified with the updated values and updates the location to the proposed path planning system.

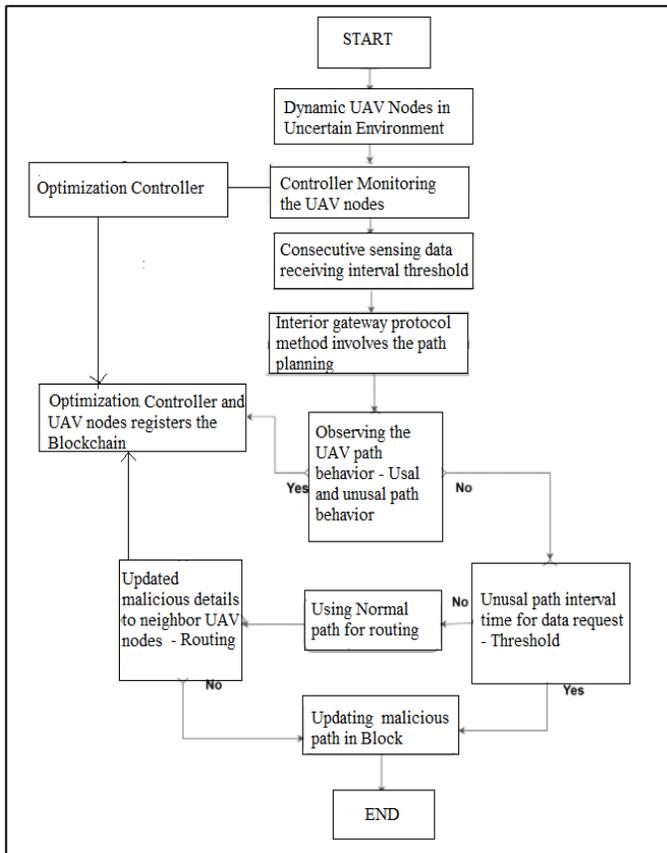


Fig. 3. A Scenario of Uncertain Environment with Blockchain Network.

TABLE II. SIMULATION PARAMETERS

Parameter	Description	Value
(X:Y)	Values in Uncertain Environment	(22.45;2.30)
ρ	Packet loss Cost (800 bit)	10×10^3
λ_{nu}	Highest Range of the position	24~36 dB
α (h1)	UAV height	20m
δ (d1)	UAV depth	20m
R_{dr}	UAV Resource data rate (25Mbyte/s)	180 Mbps
UAV_c	UAV coverage radius	100~2000m
E_{no}	Total Episodes Number	10
N	Total UAV nodes	15
S	Total UAV server	1

A. Path Selection Scheme Evaluation

In this section, the access path selection scheme performance of the proposed Meta-Heuristic optimization algorithm is evaluated under an uncertain environment. The UAV node and UAV server scenario are executed. The sequence of the scenarios is considered for performance evaluations where all UAV nodes access the UAV server, one UAV server accessing all UAV nodes, and multipath flashing method. The multi-path flashing method always processes the UAV node with multipath channel access to the UAV server until the data traffic is cleared or all the UAV nodes are getting a response from the UAV server. The Meta-Heuristic optimization algorithm is hard to obtain the multipath flashing method due to the huge area and the comparisons with other schemes verify the performance of the proposed system. The ideal transformation straight line coordination system is produced to minimize the complexity and computational cost in the UAV path planning process. The existing methods produce high computational costs due to the complex optimization method.

Fig. 4 shows that the experimental radius of the region is occupied 900m, when the UAV coverage transmission radius is moving more than the assigned value of 900m, extended the excess UAV nodes wouldn't allow the transmission range and transmission cost.

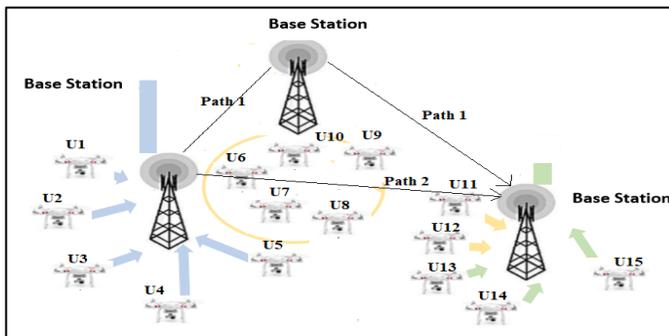


Fig. 4. Data Packet Transmission towards the UAV Network from Source to Destination.

The performance of the extended UAV nodes has a low packet transmission rate. Every uncertain environment UAV coverage is small about below 900m, the multipath flashing is done successfully in UAV node access in the UAV network. The assigned transmission range is fully occupied with resources and a scheduled pattern is achieved in the data traffic in the UAV network.

B. Multi-Path Flashing Model

This section proposes that countermeasures when multiple UAV nodes participate in the uncertain environment and investigate a scenario in which malicious activities and attacks are involved. The initial step of the environment that the attack could be using multipath signal receivers since every single attacker can spoil many numbers of receivers in its data transmission range. The attacker captures multiple signal receivers. The multiple numbers of signal receivers bounded the uncertain environment from which the attacker can be highly performed. The DoS locations depend on the UAV resource data range, called resource-based attack, constrained by the resource range between UAV nodes and UAV servers. The attacker activities purely depend on the locations, the possible position to reach the resources is suitable for them. The updated routing path keeps the updated routing details in a table. The update routing table keeps sending the details only to source and destination and the possible positions are set with two points. The fewer number of UAV nodes will entertain the attacks whereas a greater number of UAV nodes participated in uncertain environment UAV network doesn't allow to attack launch. The proposed system doesn't allow multiple UAV spoofing. The optimization method is based on defence cooperation localization. From these experimental results, the number of UAV node location is preserved and the distance maintained are safe [19]. The proposed distribution-based blockchain system spread out the defence model against spoofing attacks and the entire UAV network. The real experimental scenario offers multiple UAVs together, without any restrictions, offers opportunities for a DoS attack which encourages the malicious behaviour and captures the path. However, the defence model should also evaluate the attack behaviour and arrest the malicious activities [20].

C. Path Planning Algorithm Execution

Simulations were executed from this proposed enhanced interior gateway protocol method and tested through the following scenarios.

The testing is executed for observing the path planning of data packets from a UAV to another UAV when the attacker involves the usual routing paths. The process of sending data packets in transmission follows the usual links and avoids unusual paths where it occurs high computational costing. The experimental setup was tested using the EIGRP protocol and the computational cost and delay proves the proposed method and updates the instant path up-gradation at the time of execution. The proposed EIGRP protocol was tested through scenario 1 U1 to U11, Scenario 2 U2 to U12, Scenario 3 U3 to U13, Scenario 4 U4 to U14 and Scenario 5 U5 to U15.

TABLE III. COMPARISON VALUE OF DELAY IN PATH UP-GRADATION

Comparison value of delay in Path Up-gradation (seconds)					
Method	Scenarios				
	1	2	3	4	5
Proposed EIGRP	0.00634	0.00543	0.00435	0.00342	0.00234
Existing Routing	0.01245	0.01123	0.01103	0.01100	0.01023

The Table III results are obtained for the delay in path up-gradation resulting from the five different scenarios and the obtained delay in path up-gradation is as below:

$$1) \text{ Proposed EIGRP protocol} \\ = (0.00634+0.00543+0.00435+0.00342+0.00234)/5 \\ = 0.004376 \text{ Seconds}$$

$$2) \text{ Existing Path Up Planning Protocol} \\ = (0.01245+0.01123+0.01103+0.01100+0.01023)/5 \\ = 0.011188 \text{ Seconds.}$$

The Next scenario was tested before the path up-gradation attacker termination. The routing path considers for data packet transmission from U2 to U15 is U2 is switch UAV, Base Station 1, Base Station 2, Base Station 3 and U15 is Switch UAV. The path planning process is performed with different metric values which are utilized for sending data packets from source to destination.

$$\text{Path Planning Metric} = 256 * ((107/\text{Minimum bandwidth}) + (\text{total path up gradation delay} / 10)).$$

The path planning up-gradation for sending data packets towards U2 to U15 with a minimum bandwidth of 200 kbps, delay 40000 ms, ethernet interface 200 ms delay, Path planning metric calculation is mentioned below,

$$\text{Path Planning Metric} = 256 * (107/200 \text{ kbps} + (40000\text{ms} + 40000\text{ms} + 200 \text{ ms}) / 10) = 53253120.$$

This value indicates that the data packet will send 53253120 metric values.

Metric values are derived for total path planning for data transmission from source to destination. Based on the Metric value calculation the updated routing details are distributed through a decentralized blockchain system with the existing network routing paths. The Distributed metric values based routing details support quickly and support multiple UAV's with normal computation delay and cost to reach the destination. The Proposed path planning algorithm overcomes the existing problems like restricted area path planning and specific autonomous area path planning. The low capability and minimized routing table with limited hop counts. These are the challenges that have been solved through the proposed path planning up-gradation model.

VII. SIMULATION RESULTS

Fig. 5, Fig. 6, and Fig. 7 are illustrated that the proposed algorithm in the case of uncertain environments performs better than the existing method since the UAV data

transmission from one hop to another hop, neighbour count information, and received packets indicates the high impact created in the proposed algorithm. The proposed algorithm outperforms the novel approaches of path selection and moves directly to the uncertain UAV network environments all the time, and the improved performance gap between the proposed solution and the optimal access path selection solution is less than 3dB. The uncertain environment has the condition of attacker interception and when the average changing interval is suddenly increased, the proposed algorithm can perform the optimized path selection approach about crossing the malicious channel state path and outer performs a position with exact destination channel state, thus the overall performance is improved from the results provided by the proposed method.

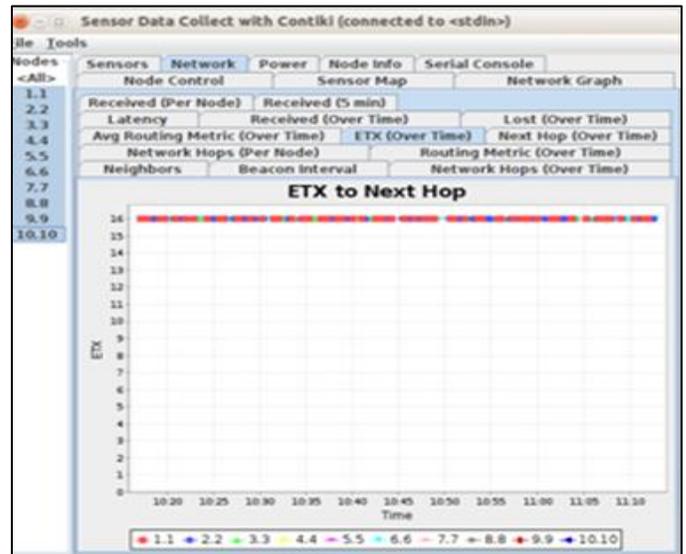


Fig. 5. Hop based Transmission Rate.



Fig. 6. Engaged Neighbour Count.

Fig. 5 shows that a high data transmission rate can reach a satisfactory result in the end, while the usage needed data transmission rate can reach a better result. Fig. 6 shows that high time engaged neighbour count can accelerate data transmission at the beginning stage; it will achieve the exact path selection methodology and does improve the data transmission in an uncertain UAV environment. Fig. 7 shows that the estimated received packets and estimated loss packets after implementing the proposed model.

The proposed algorithm is compared with GNSS based optimal access path selection approach of UAV flying object towards the same UAV network with different heights in Fig. 8. The existing Deterministic probabilistic algorithm and GNSS algorithm applied the fixed methodology to obtain the path where the fault tolerance was medium. Table IV shows the comparison of performance metrics between the existing Deterministic probabilistic algorithm and GNSS algorithm and the proposed optimization path selection and Meta-Heuristic path planning algorithm. The proposed Optimization path selection and Meta-Heuristic Path Planning algorithm apply a hybrid fuzzy possibility algorithm which creates the accurate destination path with dynamic location and overcomes the obstacle detection and radio path detection issues. Also, the Existing method does not provide proper ideology for data security against attacks whereas the proposed blockchain methodology, distributed the path location to the source point which creates smooth data delivery, no path deviation, and redirects path.

The proposed methodology reduces the time delay and improves the throughput. The uncertain UAV network environment is considered and the average channel path loss interval is set as 200s. The common value of the additional path loss λ_{nu} is very small when the UAV height is too high.

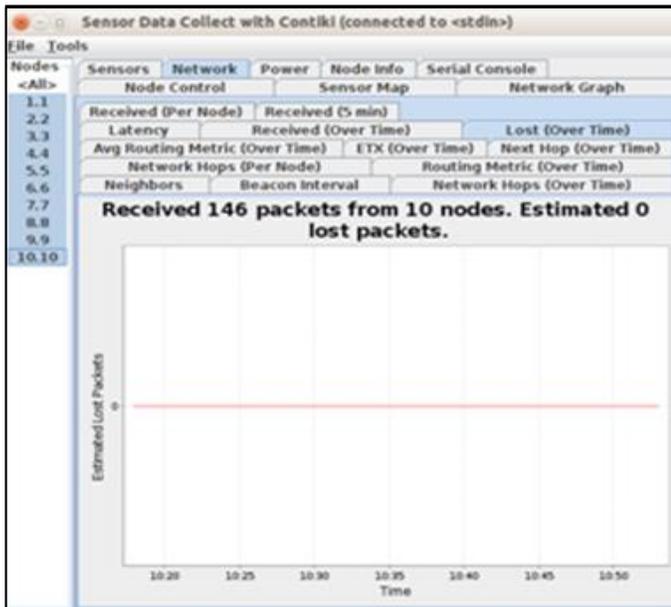


Fig. 7. Estimated Received Packets and Estimated Loss Packets.

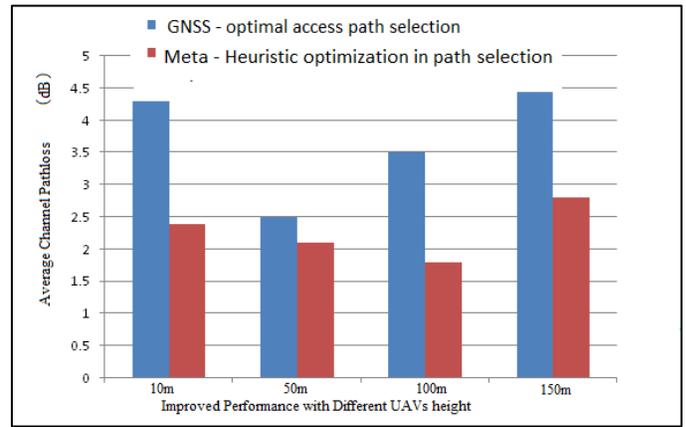


Fig. 8. Average Cost with different Values of UAV Coverage Radius.

TABLE IV. PERFORMANCE COMPARISONS OF META-HEURISTIC PATH PLANNING

Comparison Parameters	Deterministic & Probabilistic Algorithm	GNSS(Global Navigation Satellite System-based Path selection Algorithm)	Proposed - optimization path selection and Meta-Heuristic path planning
Technique Applied	Explore Obstacles	Radio Path detection	HFPCM-Hybrid Fuzzy Possibility
Throughput	Low	Low	High
Fault Tolerance	Low	Medium	High
Bandwidth	20%	25%	35%
Process Efficiency	35%	40%	50%
Node to Node Delay	30%	25%	10%
Security Improvement	Low Security	Normal Security	High Security
Overhead Latency	Low Priority & High Latency	Average Priority & Medium Latency	High Priority & Low Latency
Scalability	Low Adaptability	Medium Adaptability	High Adaptability
Packet Delivery Ratio	Low	Medium	High
Packet Loss	High	Medium	Low
Mean Time Delay	High	Medium	Low

VIII. CONCLUSION AND FUTURE WORK

In this paper, the issues in UAV assisted flying object optimal path selection schemes and the path deviation attacks against UAVs are investigated. The proposed model clearly defined the optimization path selection method and Meta-Heuristic optimization in path planning to effectively increase the secure data transmission in an uncertain environment UAV network, where extended coverage in real time scenarios of uncertain environment is successfully performed by the

proposed algorithm which is not addressed in the existing algorithms. The proposed blockchain aided UAV swarm will secure the UAV network from the security attacks. Blockchain provides promising results in the terms of preserving the security of the network. And it can be implemented in the UAV domains for rescue operations, surveillance operations and inspection of critical resources. The secure communication process is proposed using blockchain and controlled the attack activities through a blockchain based defense distribution system. The distribution-based defense blockchain system supports, updated routing table which has been scheduled and the data is transmitted perfectly. In this paper, the results have been validated and swarm optimization controls the network security. In the future, experiments with multi-agent machine learning-based path selection in UAV networks with different environments will be considered and the energy consumption of a UAV which depends on its speed and transmits power will be discussed.

REFERENCES

- [1] T. Zhao, X. Pan and Q. He, "Application of dynamic ant colony algorithm in route planning for UAV," 2017 Seventh International Conference on Information Science and Technology (ICIST), 2017, pp. 433-437, doi: 10.1109/ICIST.2017.7926799.
- [2] Li, Z., & Han, R. (2018, July). Unmanned aerial vehicle three-dimensional trajectory planning based on ant colony algorithm. In *2018 37th Chinese Control Conference (CCC)* (pp. 9992-9995). IEEE.
- [3] Bai, X., Wang, P., Wang, Z., & Zhang, L. (2019, July). 3D Multi-UAV Collaboration Based on the Hybrid Algorithm of Artificial Bee Colony and A. In *2019 Chinese Control Conference (CCC)* (pp. 3982-3987). IEEE.
- [4] Muntasha, G., Karna, N., & Shin, S. Y. (2021, April). Performance Analysis on Artificial Bee Colony Algorithm for Path Planning and Collision Avoidance in Swarm Unmanned Aerial Vehicle. In *2021 International Conference on Artificial Intelligence and Mechatronics Systems (AIMS)* (pp. 1-6). IEEE.
- [5] Priyadarsini, P. L. K. (2021, January). Area Partitioning by Intelligent UAVs for effective path planning using Evolutionary algorithms. In *2021 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-6). IEEE.
- [6] Wei, Y., Wang, B., Liu, W., & Zhang, L. (2021, July). Hierarchical Task Assignment of Multiple UAVs with Improved Firefly Algorithm Based on Simulated Annealing Mechanism. In *2021 40th Chinese Control Conference (CCC)* (pp. 1943-1948). IEEE.
- [7] Aliwi, M., Aslan, S., & Demirci, S. (2020, October). Solving UAV Localization Problem with Firefly Algorithm. In *2020 28th Signal Processing and Communications Applications Conference (SIU)* (pp. 1-4). IEEE.
- [8] Wang, S., Bai, Y., & Zhou, C. (2019, July). Coverage Path Planning Design of Mapping UAVs Based on Particle Swarm optimization Algorithm. In *2019 Chinese Control Conference (CCC)* (pp. 8236-8241). IEEE.
- [9] Aggarwal, K., & Goyal, A. (2021, March). Particle Swarm Optimization based UAV for Disaster management. In *2021 IEEE 5th Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)* (Vol. 5, pp. 1235-1238). IEEE.
- [10] E. Yanmaz, R. Kuschig, M. Quaritsch, C. Bettstetter, and B. Rinner, "On path planning strategies for networked unmanned aerial vehicles," in Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS), Apr. 2011, pp. 212–216.
- [11] Tarun Rana ., Achyut Shankar , Mohd Kamran Sultan , Rizwan Patan ., "An Intelligent approach for UAV and Drone Privacy Security Using Blockchain Methodology"Vol .4 no -13 978-1-5386-5933-5/19 -IEEE 2019.
- [12] Jiyang Chen1, Zhiwei Feng2,1, Jen-Yang Wen1, Bo Liu*3, and Lui Sha., "A Container-based DoS Attack-Resilient Control Framework for Real-Time UAV Systems"Vol .1 no -18 978-3-9819263-2-3/DATE19/ DAA 2019.
- [13] Hongzhi Guo and Jiajia Liu. Uav-enhanced intelligent offloading for internet of things at the edge. IEEE Transactions on Industrial Informatics, 2019.
- [14] Safae Lhazmir, Abdellatif Kobbane, Khalid Chougali, and Jalel BenOthman. Energy-efficient associations for iot networks with uav: A regret matching based approach. In Proceedings of the 9th International Conference on Information Communication and Management, pages 132–136. ACM, 2019.
- [15] Safae Lhazmir, Mohammed-Amine Koulali, Abdellatif Kobbane, and Halima Elbiaze. Performance analysis of uav-assisted ferrying for the internet of things. In 2019 IEEE Symposium on Computers and Communications (ISCC), pages 1–6. IEEE, 2019.
- [16] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial iot: Blockchain system with credit-based consensus mechanism," IEEE Transactions on Industrial Informatics, vol.15, no.6, pp. 3680–3689, 2019.
- [17] M. Shen, X. Tang, L. Zhu, X. Du, and M. Guizani, "Privacy-preserving support vector machine training over blockchain-based encrypted iot data in smart cities," IEEE Internet of Things Journal, vol. 6, no. 5, pp. 7702–7712, 2019.
- [18] L. Xie, Y. Ding, H. Yang, and X. Wang, "Blockchain-based secure and trustworthy internet of things in sdn-enabled 5g-vanets," IEEE Access, vol. 7, pp. 56656–56666, 2019.
- [19] F. Li, H. Yao, J. Du, C. Jiang, and Y. Qian, "Stackelberg game-based computation offloading in social and cognitive industrial internet of things," IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5444–5455, 2020.
- [20] C. Qiu, H. Yao, F. R. Yu, F. Xu, and C. Zhao, "Deep q-learning aided networking, caching, and computing resources allocation in software-defined satellite-terrestrial networks," IEEE Transactions on Vehicular Technology, vol. 68, no. 6, pp. 5871–5883, 2019.

Resource Allocation in Spectrum Deployment for Cognitive Third-party Users

Arikatla Jaya Lakshmi¹

Research Scholar, Department of
ECE, Jawaharlal Nehru
Technological University, Anantapur
Ananthapuramu, Andhra Pradesh,
India

Dr.G.N.Swamy²

Professor and HOD, Department of
EIE, V R Siddhartha Engineering
College, Vijayawada
Andhra Pradesh
India

Dr.M.N.Giri Prasad³

Professor, Department of ECE
Jawaharlal Nehru Technological
University, Anantapur
Ananthapuramu, Andhra Pradesh,
India

Abstract—Spectrum scarcity is a major challenge in wireless communication for next generation applications. The spectrum sharing and utilization of other user available spectrum is an optimal solution, which has outcome with a new mode of communication called cognitive network. Cognitive devices are capable of requesting and sharing free spectrum among each other in a communication range. The spectrums are shared among primary and secondary user (PU, SU). To extend the range of spectrum utilization, users from other clusters are requested in sharing of spectrum which is called as third party user (TSU). In detection of free spectrum a jamming based approach is proposed in recent work. Jamming approach generates a periodic jamming signal for TSU in sensing of free spectrum. The repetitive requesting of spectrum availability result in large jamming probability for engaged TSU users resulting in large delay. In minimizing the delay observed, in this paper, a new monitored jamming approach is proposed. Proposed Monitored jamming approach is develop in recent to the engagement of each TSU for communication and governing the jamming signal based on the spectrum engagement. The proposed approach minimizes the delay due to jamming signaling in existing system. The Experimental results obtained shows an enhancement to the system throughput, fairness factor and minimizes the delay metric for proposed approach.

Keywords—Slot monitoring; spectrum sensing; primary user (PU); secondary user (SU); third-party spectrum utilization (TSU)

I. INTRODUCTION

The evolution of wireless communication has resulted in the interfacing of various advanced services on portable communication devices, with many new services being integrated at a rapid pace. The incorporation of new services requires a higher data rate and high offers service quality. Wherein users are increasing rapidly, and the services integrated are also increasing, it is the need of the existing wireless communication system to improve the communication architecture to offer the best data exchange. The wireless spectrum constraint has given rise to the concept of spectrum sharing, in which users are interfaced to use the free spectrum of other users to meet the newly evolving service demand. The most suitable approach is the cognitive radio network (CRN) where each user interfaces with other users for spectrum sharing. The advantage of spectrum sharing has resulted in higher service compatibility. However, the issues of spectrum sensing, and allocation are critical in these

networks. The sensing of the available spectrum with minimal network overhead is the primary requirement for an efficient CRN operation. In the sharing of free spectrum, primary user (PU) and secondary user (SU) undergoes a communication phase for signal status sensing and based on signal energy spectrum sensing is developed. In improving the objective of spectrum sensing, new methods of recurrent learning approaches, fusion based approach and machine learning techniques were developed. In [1] the accessing data rate is increased by the sensing spectrum of side cognitive nodes which are added into the network with course of time. The sensing operation developed performs spectrum sharing minimizing the packet delivery failure in the network. A multi-scale spectrum sensor in a CRN is outlined in [2]. This method developed a spectrum sensing approach based on an interference-matched design, where more accurate information interfaces with the network for proper communication control. A Spectrum sensing approach in CRN using multi-metric monitoring in an outline in [3]. The spectrum sensing were developed based on the concurrent monitoring of traffic condition, delay and channel usage. In communication system using as frequency division multiplexing [4], spectrum sensing is developed using time-frequency signal estimation. The proposed approach was developed using a blind signal estimation approach, which enhanced the energy detection performance. In [5] for multipath and multi-channel conditions a window-based blind spectrum estimation is proposed. This approach also improved the energy detection performance and hence the spectrum sensing in cognitive radio. An adaptive threshold approach for the detection of spectrum under channel interference is outlined in [6]. This work presented a covariance approach for channel sensing where an adaptive threshold is proposed to reduce the error probability in spectrum sensing. In recent past to improve the blind sensing performance, regression models were used for a faster convergence. A Markov approach for spectrum sensing based on a distributed coordinate function (DCF) is presented in [7]. The approach derives from a Markova chain model in developing a CRN operation for spectrum sensing. In the application of a wide area network, an opportunistic spectrum sensing approach using a cognitive sensor network was presented in [8]. This approach presented a likelihood distribution of channel availability using Markov chain computing for primary users using the spatial distribution of the channel. In other techniques of spectrum sensing advanced

machine learning approaches were also introduced. In [9,10] a novel fusion model for spectrum sensing is presented. This approach used a machine learning model in which the k-nearest neighbor estimation is used in spectrum sensing. A similar approach for a trust-based spectrum sensing model based on a data fusion model was presented in [11]. The approach developed a 'mechanism design theory' for detecting false requests for spectrum sharing owing to unauthentic users in the network with cognitive nodes. A centralized data fusion model was presented to monitor the node's operation in validating user sensing requests. The author in [12] proposed a multi-channel cooperative spectrum sensing (MCSS) method for optimizing spectrum sensing in a cognitive radio network. This approach develops a novel game theory of node selection to extend energy savings in a cognitive device. In [13], a fusion center (FC) model was proposed for cooperative spectrum sensing. The proposed approach improves the throughput by minimizing the amount of reporting time in the network. The approach is a centralized monitoring scheme of spectrum sensing where the network is divided into two clusters and the spectrum sensing observations are monitored at the FC in deciding for spectrum sensing based on defined fusion rules. Under multi user environment a centralized cooperative spectrum sensing (CSS) approach is presented in [14]. This method was created using k-means shift clustering over local energy vectors. In [15] Formal paraphrase the sensing of opportunistic spectrum by a primary user in the mobility scenario is presented with authentic access to spectrum usage. A k-means approach to spectrum sensing is proposed in which the identification of suspected users in spectrum access is developed for optimal spectrum utilization. In [16] a reinforcement learning (RL) method for cooperative spectrum sensing in CRN operation is presented. This approach developed a channel scanning approach for spectrum sensing and requesting, where a confidence bound approach was proposed for secondary user (SU) spectrum sensing. An approach for a malicious free processing of spectrum allocation in a cognitive radio network was outlined in [17] where the issue of false sensing of the spectrum in the network and allocation is encountered and solved. Similar approach to energy detection for different false alarms and noise variance is outlined in [18]. The presented interface for different communication networks with cognitive devices for sensing the opportunistic spectrum is outlined. In the application of improved spectrum sensing for real time usage a cognitive Internet of Things (CIOT) was presented in [19]. Spatially correlated approach for spectrum sensing using energy-efficient processing in cognitive radio devices. However, to cope with rapid evolving service demands and user accessibility, the spectrum sharing needs a further enhancement, which is overcome by other neighboring cluster node termed as third party users [20]. These users share spectrum to nodes which are not registered into their clusters. To sense such user spectrum, nodes generate a jamming signal for reading the signaling status of the node. In this case, the random jamming signal is generated by different nodes to

detect the accessing free spectrum. However, a random jamming signal leads to delay in node operation and intern reduces the network throughput. In [21] a sparse based coding approach for detection of jamming attack is presented. This method proposed a dictionary is used in classifying the spectrum hole and a jamming state. The dictionary is used by machine learning approach in classification of the user emulation. A max-min method for the optimization of energy saving in congestive sensor network is outlined in [22]. The proposed approach schedules the request a node operational unit of the sensing spectrum based on the channel sensing of a node. A Rendezvous algorithm using channel Hopping (CH) for spectrum sensing in asynchronous and asymmetric model is presented in [23]. The jamming conditions were minimized by a Hybrid Rendezvous Algorithm which operates on jamming and non-jamming conditions. The jamming signaling was observed for minimizing the jamming conditions in cognitive network. However, the past developments observe the jamming condition based on a pre existing dictionary model or based on the channel conditions. In these approaches the requesting overhead is not addressed and a repetitive jamming signaling for spectrum sensing leads to a large delay. In this paper a new monitoring approach for user engagement based on channel occupancy is proposed. The centralized fusion monitoring of the channel engagement leads to minimization of requesting overhead for high engaged users, resulting in minimization of jamming delay. The outcomes of the presented work are:

- 1) A new method for monitoring of jamming signal based on user's engagement is proposed.
- 2) The Jamming overhead due to random scheduling is minimized.
- 3) The Delay metric is minimized and throughput is improved by the monitored approach of spectrum engagement.

The rest of this paper is outline in 6 sections. The system outline and the operation of jamming signaling in cognitive radio network for spectrum sensing is outlined in Section 2. Section 3 presents the process of spectrum allocation using jamming condition. The proposed approach of slot monitoring is outlined in Section 4. Experimental result observations for the developed approach are outlined in Section 5. Section 6 presents the conclusion of presented work.

II. SYSTEM OUTLINE

A cognitive radio network (CRN) consists of a Secondary User (SU) -Tx/Rx, a relay unit, and a Primary User (PU) -Tx/Rx unit. These communication units are equipped with a single transmitting and receiving antenna. All nodes in this connection are in full-duplex operation. In the communication of data packets, information is exchanged using a relay node. The uplink of a packet is made based on the position of the users in the network. A generic architecture of a CRN system is shown in Fig. 1.

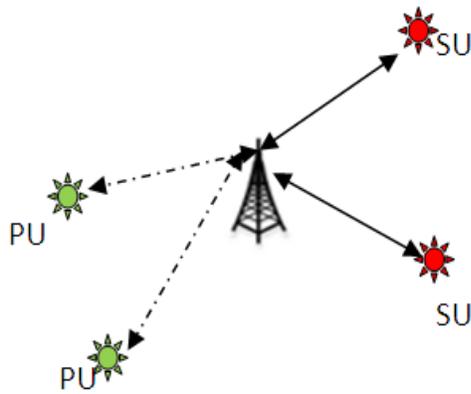


Fig. 1. Communication Architecture of the CRN System.

In the spectrum sensing operation, the Secondary User (SU) detects the freely licensed Primary User (PU) spectrum when the user does not use the spectrum to communicate. Spectrum availability is estimated using an energy detection approach of signal energy. This method uses a threshold-based estimation technique which operates under two hypotheses, h_0 and h_1 , respectively,

$$h_0 : X_i = N_i$$

$$h_1 : X_i = S_i + N_i \tag{1}$$

Hypotheses h_0 specifies the nonexistence of a signal, where h_1 denotes the occurrence of the signal and the coupling of the PU spectrum by the transmission signal S_i interfering with the additive Gaussian noise of the channel with mean zero and variance σ . Under the generalized likelihood Gaussian distribution, the probability of estimation for the two hypotheses h_0 and h_1 is defined as,

$$E' = \frac{1}{k} \sum_{i=1}^k \left(\frac{|y_i|}{\sigma} \right)^m > th \tag{2}$$

(For hypothesis h_0)

$$= \frac{1}{k} \sum_{i=1}^k \left(\frac{|y_i|}{\sigma} \right)^m < th \text{ (for hypothesis } h_1)$$

Here $m > 0$ is a random static value where the threshold is defined by the channel variance. For usage of the additional spectrum from other clusters, a third-party secondary user (TSU) was used. The spectrum sharing operation with TSU operation is illustrated in Fig. 2.

In the detracton of spectrum, a medium access control (MAC) layer approach using jamming signals termed as probing functions is used. The probing function is developed as a trial and error-based approach where a jamming signal is used in the detection of channel occupancy. This process generates a jamming signal and senses the behavior of a user in sensing the occupied channel. As a result, the holding delay for TSU is longer, resulting in a lower throughput. The delay is observed as an overhead on the network due to a jammed signal. The nodes here generate the jamming signal on a

random basis by sensing the free spectrum from TSU. The operation of the probing function in the spectrum sensing operation is outlined in Fig. 3.

The random generation of the Jamming signal results in higher overhead and introduces a large delay in the network. This overhead minimizes network throughput. To improve the sensing performance, a slot-monitored jamming system is proposed. This approach records the channel engagement, and the jamming is generated for the node with minimum channel allocated. Here, each node in the network shares the channel engagement with a monitoring central node, and all the requests are processed on the decision of this node. The illustration of the slot sensing approach is shown in Fig. 4.

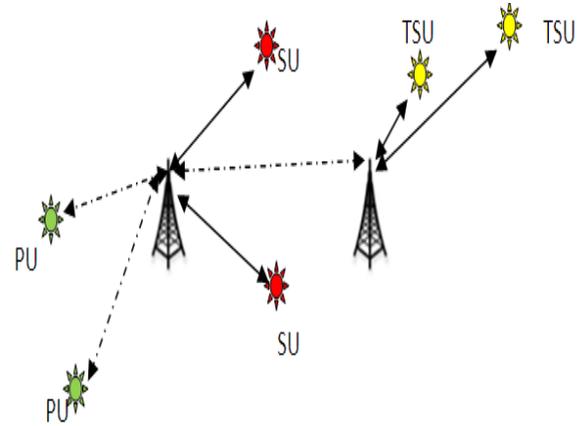


Fig. 2. CRN System with TSU Interface.

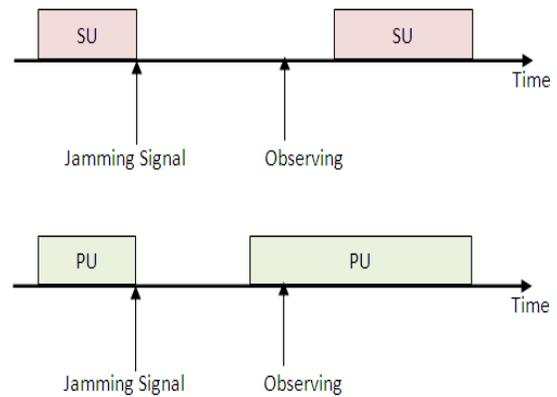


Fig. 3. Probing Function for Spectrum Sensing.

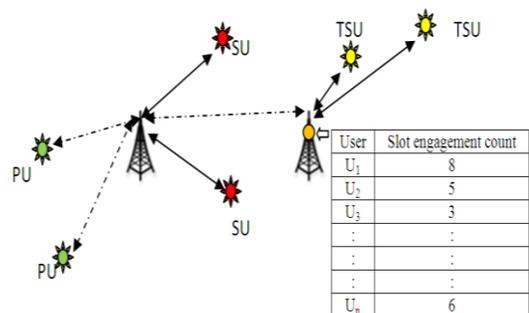


Fig. 4. The Proposed Approach of Slot Monitored Probing.

The existing approach of random jamming-based spectrum sensing, and the proposed approach of slot monitored spectrum sensing are outlined in the following section.

III. SPECTRUM UTILIZATION CODING

The signal estimators are limited by the channel diversity. The signals are estimated with prior knowledge of channel parameters and a recursive process performs the estimation error minimization in recovering the originally transmitted information. The diversity in propagating channels and the variant data rate service demand have led to a minimization of the estimation performance.

The limiting constraint to wireless communication is the convergence period where estimation is expected to be as near the actual transmitted information. In the approach of estimation, the recursion process affects the convergence period, and a larger delay is observed for a diverse channel condition. The estimator is expected to process estimation at a faster rate to minimize the convergence delay.

In the estimation of communicating signal under a channel variant condition, the communicating node is processed for spectrum sensing using an energy detection model. The estimation of the signal under the channel variation plays a critical role in the detection of free spectrum in the network.

In the allocation process, the third-party secondary user defines the spectrum sensing operation as a state of transition illustrated as Fig. 5.

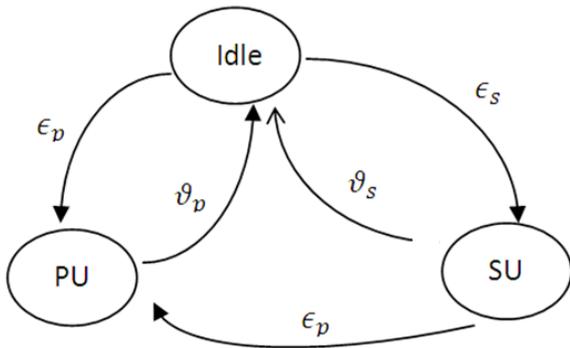


Fig. 5. Transition Diagram for Spectrum Sensing.

In the spectrum sensing process, each of the channels is processed for spectrum sensing, where the node remains in an idle state, indicating free channel availability. The PU and SU nodes represent the used and occupied channels. In spectrum sensing operations, a probing function is defined, which is integrated with a jamming operator to sense the free channel availability. In the process of the sensing operation, the jamming operator passes a value of '1' when the node has to go for sensing. The jamming probability of a node, in this case, is given by 'p' where $0 < p < 1$. The value of 'P_{min}' indicates that the winning probability of the node for a SU is obtained by jamming operation. Each time channel access is achieved, a throughput variation is observed. In this case, the throughput gain is changed from, π_p to π'_p which is given as,

Where,

$$\pi'_p = 0.99 \times \pi_p \quad (3)$$

Where,

$$\pi_p = \frac{\epsilon_p}{\epsilon_p + \nu_p} \quad (4)$$

Here, the sensing probability is based on the energy detection and rate of a jamming signal generated. The jamming condition generated in the network introduces a delay for each request generated. This gives a higher probability of delay in the spectrum sensing operation. To avoid the spectrum sensing operation, in this work a new slot allocation approach is proposed. The operation outline of the conventional approach is given, as is the arrival and departure rate of the primary user (PU).

The value of jamming probability is defined by,

$$p = 1 - (1 - p_n)^n \quad (5)$$

Here,

p_n Is the jamming rate.

n is the spectrum unit size.

In a wireless network, for spectrum sensing, the node generates a jamming signal at a probability of 'p'. The aggregated time for a k-third party user node to allocate for sensing is given by,

$$\pi_i = \sum_{i=1}^n N_i \times P_i \quad (6)$$

Where

N_i is the number of third-party secondary users increasing p_i is the probability of jamming associated with each node.

The system is developed using an assumption of known channel variation. The jamming error is taken as a reference for the prediction of signal in estimation. The maximum channel interference is defined as a non-linear time variant interference observed in the channel. The variation in channel parameters leads to an unstable condition of signal estimation and hence leads to improper sensing. To improve the estimation performance, in this study, a new approach to slot-based monitoring of channels is proposed.

IV. SLOT MONITORING PROBING FUNCTION FOR JAMMING OPERATION

For the spectrum sensing operation, each primary user requests the secondary user for a free spectrum using a jamming signal. In the process of the spectrum sensing and allocation of spectrum, the node generates multiple requests for jamming from the secondary node. This repetitive request results in overhead for the secondary node and channel congestion. To avoid the repetitive requests in this study, a

slot monitoring approach is proposed. In this approach, a monitoring parameter called slot count (s_n) is introduced. This approach monitors all the registered users' slot allocations engaged in communication. In the process of communication, each of the user nodes allocated for communication is allotted a slot to keep updated with a centralized monitoring node at a macro cell level. This node centralizes all registered users and records the allocated slots. In the occupied channel, the aggregated slot count is given by,

$$s_n = \sum_{i=1}^n s_i \quad (7)$$

indicates the channel slot that is currently occupied. Each of the allocated slots in this case is given a value of '1' when occupied and '0' when released. The aggregated slot count results from the overall occupied channels in the network. A repository for the allocated slots in the network is made at the centralized node where K TSU nodes are registered. The repository structure was built as.

$$R = [s_{n1}, s_{n2}, s_{n3}, \dots, s_{nk}] \quad (8)$$

This repository is used as a reference unit for the allocation permission for slot allocation. In the spectrum sensing operation, the primary user (PU) requests the secondary user's spectrum via a centralized monitoring node. For each of the requests generated for a SU or TSU, the centralized node searches for a slot allocation level. In this case, the monitoring unit process is used to select a node for a request that meets the minimal condition.

$$TSU_{sens} = \min(R) \quad (9)$$

This means that the minimal engaged node is selected in the process of spectrum sensing to avoid non-regular jamming of the node.

The aggregated jamming probability for a secondary node is observed as,

$$p_{agg} = \sum_{i=1}^k p_i \times t_i \quad (10)$$

Where p_i is the jamming rate for a node and t_i is the time period allocated for jamming. This delay is minimized by.

$$p_{agg} = \sum_{i=1}^k p_{isel} \times t_i \quad (11)$$

The overall spectrum sensing contention delay is minimized by the allocation of the selected node jamming rate p_{isel} for the request made. This proposed approach minimizes the overall overhead of sensing requisition and the jamming probability of a node.

The algorithm for the proposed work is outlined as follows:

Algorithm

Input: Allocated slot (S_i), Repository (R)

Output: Jamming Probability

Do,

Step 1: Create Repository (R) by registering all nodes of PU, SU and TSU to centralized monitoring node,

$$R = [s_{n1}, s_{n2}, s_{n3}, \dots, s_{nk}]$$

Step 2: Allocate '1' for a slot engaged and '0' for a free channel

Step 3: Request jamming from PU to a centralized node, for TSU

Step 4: compute slot allocation count for request TSU,

$$s_n = \sum_{i=1}^n s_i$$

Step 5: allocate jamming on satisfying allocation criterion.

Step 6: On allocation criterion not satisfied, search best possible allocation. $TSU_{sens} = \min(R)$

Step 7: allocate the probable TSU to requesting PU

Step 8: Performing a Jamming probing.

Step 9: Sense the free spectrum

Step 10: Request and allocate the TSU spectrum.

Step 11: Update the allocation status to Repository (R).

End

V. RESULT AND DISCUSSION

The proposed approach is evaluated for a cognitive network with random users deployed under channel variation conditions. The approach can update the error weight value based on the jamming operation. The basic design model of a jamming estimator is defined by a state updating process where a Jamming error response is made in the responsibility of jamming error. A set of the processing bits is shown in Fig. 6.

The request developed by the TSU node for sensing the free spectrum is received at the receiver. The jamming requests are generated for a requesting node to detect the node spectrum availability. Fig. 7 shows the jamming request received at the receiver node.

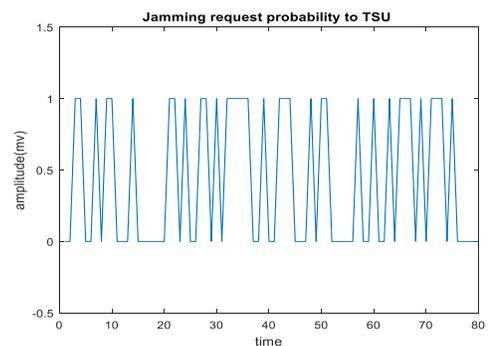


Fig. 6. Jamming Request Probability to TSU.

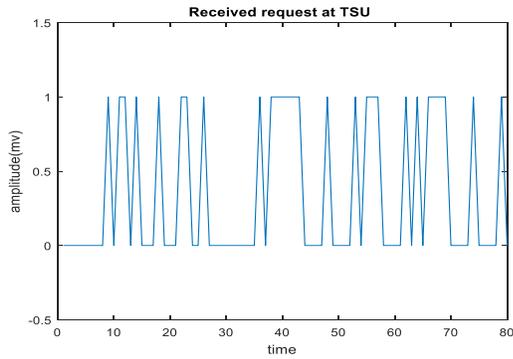


Fig. 7. Received Request at TSU.

In the detection of spectrum availability from a third-party secondary user (TSU), a copy of the received signal is measured at the receiver as illustrated in Fig. 8. The received signal is used for energy detection in the spectrum sensing approach.

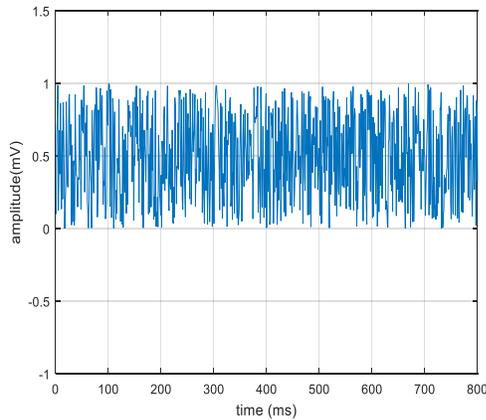


Fig. 8. Signal Received from the SU.

For this affected signal the channel estimation logic is applied. The Energy detection level for the communicating signal at the receiver is illustrated in Fig. 9.

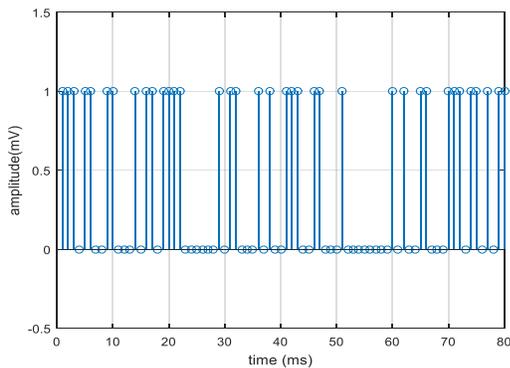


Fig. 9. Energy Detection Level at PU.

The availability of the additional spectrum by the TSU unit results in faster packet delivery. However, the spectrum sensing is made based on the offered jamming rate to the TSU unit. The overhead per node due to variation in jamming rate is presented in Fig. 10. The observation illustrates a lower

overhead by the proposed slot monitoring probing approach compared to the existing with and without probing function. A lower overhead lead to higher throughput in the network. With an increase in jamming rate, the overhead is controlled to a minimum by slot monitored probing compared to with and without probing.

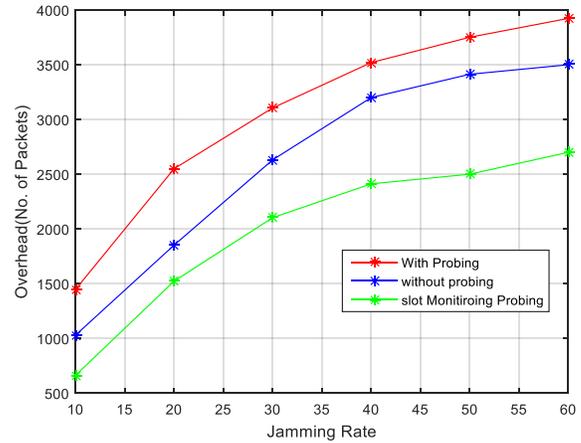


Fig. 10. Overhead for Varying Jamming Condition.

Observations of the overhead due to varying jamming rates and streaming sizes for the developed approaches are listed in Tables I and II, respectively.

In the streaming of signals, the signals are propagated over an $m \times n$ channel. The channel diversity results in dynamic distortion in communicating signals, leading to higher errors. The observed fairness to the communicating signal defined with respect to signal error is illustrated in Fig. 11.

TABLE I. OVERHEAD (%) FOR CONTROL STREAMS WITH VARYING JAMMINGRATE

Jamming Rate (p)	With probing	Without probing	Slot monitored probing
10	1448	1030	663
20	2550	1852	1523
30	3105	2631	2103
40	3520	3200	2412
50	3751	3413	2500
60	3923	3500	2700

TABLE II. OVERHEAD (%) EVALUATION WITH RESPECT TO CONTROL STREAMS WITH VARYING STREAM SIZE

Stream size	With probing	Without probing	Slot monitored probing
500	106.423	93.926	92.32
600	309.64	250.65	152.14
700	500.32	350.98	215.69
800	645.293	440.00	250.14
900	735.853	555.48	333.45
1000	887.823	748.12	447.89

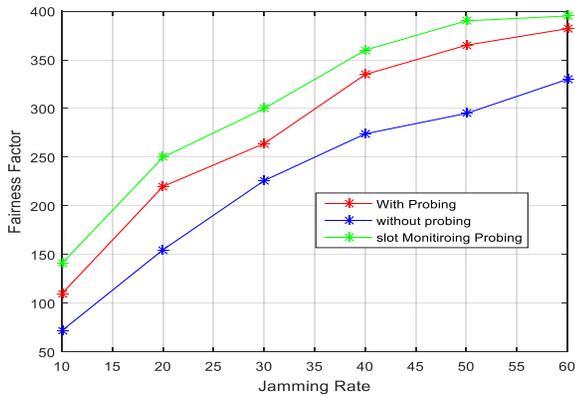


Fig. 11. Fairness Factor over Varying Jamming Rate.

TABLE III. FAIRNESS FACTOR WITH VARYING JAMMING RATE

Jamming Rate (p)	With probing	Without probing	Slot monitored probing
10	72	110	141
20	155	220	250
30	226	264	300
40	274	335	360
50	295	365	390
60	330	382	395

TABLE IV. FAIRNESS FACTOR WITH VARYING STREAM SIZE

Stream size	With probing	Without probing	Slot monitored probing
500	92	100	110
600	150	260	315
700	160	380	520
800	180	480	660
900	200	600	750
1000	220	800	890

The lower overhead in the proposed approach offers a higher communicating throughput when compared to with and without probing. The throughput increased due to slot monitoring is presented in Fig. 12. The throughput is observed to be equal at the lower jamming rate. However, with an increase in the jamming rate, the proposed approach outperforms the existing approach due to proper slot monitoring.

The diversity in the channel model results in higher interference impact which introduces distortion to the signal in a dynamic manner. The estimator units observe different convergence times for the estimation of signal in such a case. The time taken builds the overall communication delay, which is presented in Fig. 13. The delay for the proposed approach is observed to be reduced as compared to the existing approach.

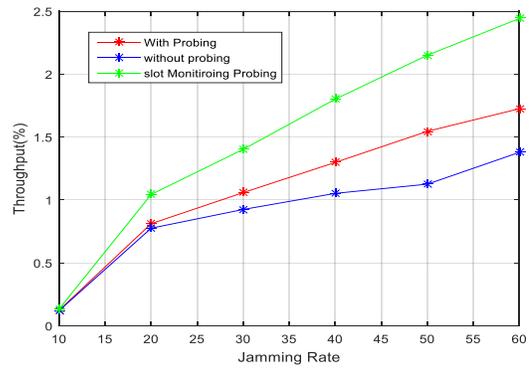


Fig. 12. Throughput over Jamming Rate for the Developed Approaches.

TABLE V. THROUGHPUT GAIN (%) WITH A VARYING JAMMING RATE

Jamming Rate (p)	With probing	Without probing	Slot monitored probing
10	0.120	0.123	0.133
20	0.775	0.811	1.043
30	0.924	1.058	1.402
40	1.052	1.298	1.801
50	1.125	1.545	2.150
60	1.378	1.725	2.442

TABLE VI. THROUGHPUT GAIN (%) WITH A VARYING STREAM SIZE

Stream size	With probing	Without probing	Slot monitored probing
500	0.500	0.520	0.536
600	0.599	0.616	0.845
700	0.725	1.025	1.425
800	1.018	1.354	2.056
900	1.858	2.256	2.547
1000	2.568	2.956	3.452

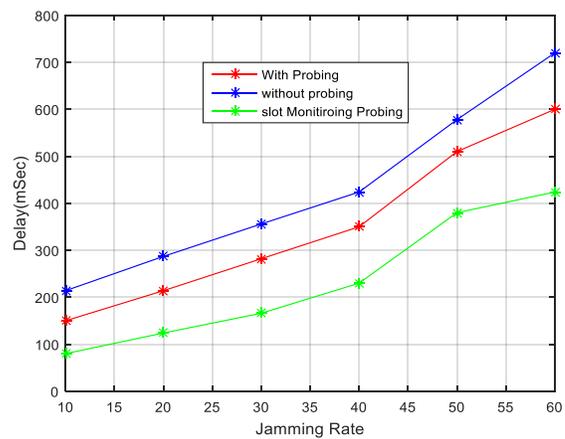


Fig. 13. Convergence Time Delay (msec) Performance for the Developed Approaches.

TABLE VII. DELAY TIMING (MSEC) WITH VARYING JAMMING RATE

Jamming Rate (p)	With probing	Without probing	Slot monitored probing
10	214	150	80
20	287	214	124
30	356	282	166
40	424	350	230
50	578	510	380
60	720	600	424

TABLE VIII. DELAY TIMING (MSEC) WITH VARYING STREAM SIZE

Stream size	With probing	Without probing	Slot monitored probing
500	261	202	35
600	350	288	55
700	434	380	74
800	517	472	103
900	705	688	170
1000	879	809	190

VI. CONCLUSION

In the process of service provisioning in a heterogeneous network, the prime issues observed are the processing overhead due to multiple network interfacing. The CRN can provide higher network connectivity; however, the CRN is limited by the device capability. Towards improving the performance of CRN operations, a third-party spectrum sensing approach has been developed. Their spectrum sensing and usage by a neighboring cell result in third-party users, which are sensed for free spectrum as an additional resource for wireless communication. The proposed approach of slot monitoring probing results in higher network throughput and reduced delay parameters. The proposed approach of slot monitoring probing results in a minimization of overhead by 1000-1500 packets with the increase in jamming rate. The fairness factor is improved to 90 packet accuracies compared to the existing approach. The throughput improved by 1.5% compared to the existing approach. The proposed approach obtains a minimization of 200msec delay. The approach developed the utilization of secondary cellular spectrum utilization for faster transmission.

REFERENCES

[1] A. Jaya Lakshmi, G. N. Swamy, M. N. Giriprasad, "Optimum channel allocation for QOS Provisioning in Cognitive Multihop radio adhoc networks," International Journal of Intelligent Engineering and Systems, Vol. 11, February 2018, pp 137-146.

[2] N. Michelusi, M. Nokleby, U. Mitra and R. Calderbank, "Multi-Scale Spectrum Sensing in Dense Multi-Cell Cognitive Networks," IEEE Transactions on Communications, Vol. 67, No. 4, pp. 2673-2688, April 2019.

[3] D.Ramesh and N. Venkatram, "Current State of Benchmarking Spectrum Sensing and Routing Strategies in Cognitive Radio Ad Hoc Networks," Journal of Theoretical & Applied Information Technology, Vol.96, 2018, pp. 3490-3510.

[4] Q. Cheng, Z. Shi, D. N. Nguyen and E. Dutkiewicz, "Deep learning network based spectrum sensing methods for OFDM systems" in arXiv:

1807.09414, 2019.

[5] J. Vartiainen, H. Karvonen, M. Matinmikko-Blue, L. Mendes, H.Saarnisaari, and A. Matos, "Energy Detection Based Spectrum Sensing for Rural Area Networks," EAI Endorsed Transactions on Wireless Spectrum, Vol. 4, April 2020.

[6] C. Charan and R. Pandey, "Intelligent selection of threshold in covariance-based spectrum sensing for cognitive radio networks," Wireless Networks, Vol. 24, November 2018, pp.: 3267-3279.

[7] J. Peng, "Throughput analysis of the IEEE 802.11 DCF in cognitive radio networks," Procedia Computer Science, Vol.151, January 2019, pp. 264-271.

[8] T. V. Saroja, L. L. Ragha, and Satyendra Kumar Sharma, "A Dynamic Spectrum Access Optimization Model for Cognitive Radio Wireless Sensor Network," ICTACT Journal on Communication Technology, Vol.8, September 2017, pp.1559-1565.

[9] H. A. Shah and I. Koo, "Reliable machine learning based spectrum sensing in cognitive radio networks", Wireless Communication Mobile Computing , vol. 2018, September 2018.

[10] H. B. Ahmad, "Ensemble classifier based spectrum sensing in cognitive radio networks," Wireless Communications and Mobile Computing, vol. January 2019, Article ID 9250562, 16 pages.

[11] J.Wang, I. Chen, Jeffrey J. Tsai, and D.Wang, "Trust-based mechanism design for cooperative spectrum sensing in cognitive radio networks," Computer Communications, Vol.116, 2018, pp.90-100.

[12] A. Bagheri, A. Ebrahimzadeh, and M.Najimi, "Game-theory-based lifetime maximization of multi-channel cooperative spectrum sensing in wireless sensor networks," Wireless Networks, Vol.26, May 2020, pp. 4705-4721.

[13] M. V. S. Sairam and M. Sivaparvathi, "Reduction of Reporting Time for Throughput Enhancement in Cooperative Spectrum Sensing Based Cognitive Radio," International Journal of Intelligent Engineering and Systems, Vol.11, February 2018, pp. 163-170.

[14] S. Zhang, Y. Wang, P. Wan, J. Zhuang, Y. Zhang and Y. Li, "Clustering Algorithm-Based Data Fusion Scheme for Robust Cooperative Spectrum Sensing," IEEE Access, Vol. 8, January 2020, pp. 5777-5786.

[15] S. Bayhan, A. Zubow, P. Gawłowicz and A. Wolisz, "Smart Contracts for Spectrum Sensing as a Service," IEEE Transactions on Cognitive Communications and Networking, Vol. 5, September 2019, pp. 648-660.

[16] W. Ning, X. Huang, K. Yang, F. Wu, and S. Leng, "Reinforcement learning enabled cooperative spectrum sensing in cognitive radio networks," Journal of Communications and Networks, Vol.22, February 2020, pp. 12-22.

[17] X. Luo, "Secure Cooperative Spectrum Sensing Strategy Based on Reputation Mechanism for Cognitive Wireless Sensor Networks." IEEE Access, Vol.8, July 2020, pp.131361-131369.

[18] M. A. Saad, S. T. Mustafa, M. Hussein Ali, M. M. Hashim, M. B. Ismail, and A. H. Ali, "Spectrum sensing and energy detection in cognitive networks," Indonesian Journal of Electrical Engineering and Computer Science, Vol.17, June 2020, No. 1, pp.465-472.

[19] R. Wan, M. Wu, L. Hu and H. Wang, "Energy-Efficient Cooperative Spectrum Sensing Scheme Based on Spatial Correlation for Cognitive Internet of Things" , IEEE Access, Vol. 8, July 2020, pp. 139501-139511.

[20] R. Ganesh Babu , Mohammad S. Obaidat, and Rajesh Manoharan, "Comparative analysis of distributive linear and nonlinear optimized spectrum sensing clustering techniques in cognitive radio network systems." IET Networks, Vol. 10, May 2020, pp.253-263.

[21] H. M. Furqan, M. A. Aygul, M. Nazzal, H.Arslan. "Primary user emulation and jamming attack detection in cognitive radio via sparse coding." EURASIP Journal on Wireless Communications and Networking, Vol-2020, No.1, 2020, pp-1-19.

[22] Zhang, Z. Jian Chen, Lu Lv, Q. Ye "Utilizing Cooperative Jamming to Secure Cognitive Radio NOMA Networks." In GLOBECOM 2020-2020 IEEE Global Communications Conference, pp. 1-6. IEEE, 2020.

[23] A. Gabriel, Y. Kim. "Hybrid Rendezvous Algorithm against Jamming Attacks for Cognitive Radio Networks." Journal of Communication, Vol.13, No.4, 2018, pp-169-174.

The Use of the Relational Concept in the Arabic Morphological Analysis

Said Iazzi¹, Abderrazak Iazzi²
LRIT Associated Unit to the
CNRST-URAC29, Faculty of
Sciences, Mohammed V University
Rabat, Morocco

Saida Laaroussi³
Laboratoire des Sciences de
l'Ingénieur, ENSA, IbnTofail
University, Kenitra, Morocco

Abdellah Yousfi⁴
Team ERADIASS
FSJES, Mohammed V University
Rabat, Morocco

Abstract—The Arabic language differs from other natural languages in its structures and compositions. In this article we have developed an Arabic morphological analyzer. For this, we have used the relational concept in the database to build our Arabic morphological analyzer. This analyzer uses a set of tables which are linked together by relationships. These relations model certain numbers of compatibility rules between different affixes. Our morphological analysis have been trained and tested on the same databases. The tests of our new approach have given good results and the numbers obtained are very close to those of existing analyzer.

Keywords—Arabic language rules; morphology; morphological analyzers; database; relational concept

I. INTRODUCTION

Morphological analysis is a central task in language processing. It consists in detecting the different morphological entities of an input word and provides a morphological representation of it. Morphological analysis has been and remains the focus of researchers in the automated processing of the Arabic language [1][6] [9][10][18].

Studies on Arabic morphology at the computer level have received great attention from computer engineers and linguists since the early eighties. A large number of morphological analyzers are designed for use in various applications. The attention is due to the richness and the complexity of Arabic morphologies, the importance also appears for the morphological analyzers in the main applications to facilitate and provide solutions in the fields of machine translation, information search and information retrieval [3] [4][8] [21].

Automatic language processing requires several efforts in the development level of all advanced computer methods and techniques [5] [7] [15] [23]. For many automatic language processing tasks, a complete and rich lexical database is essential, even a simple word list can often be an invaluable source of information. One of the most difficult problems with lexicons is that of non-vocabulary words, especially for languages that have a richer morphology like Arabic. To evaluate our morphological analysis systems, we need a body adapted to Arabic morphological analyzers that facilitate data processing tasks and have efficient results. Corpus analysis is focused on the experimental, while interpretation can be qualitative or quantitative.

We also describe the construction and the methodology of the necessary linguistic resources, a morphological dictionary and an adapted morphological corpus, and assess the effect of resource size on the accuracy of the analysis, showing what results can be obtained with limited linguistic resources [12].

II. APPROACHES USED IN MORPHOLOGICAL ANALYSIS

There are different ways to build morphological analyzers. There was research to set the rules of grammar, morphology, grammar and spelling to build morphological analyzer systems. The development requires the study of the properties of the data words by essentially raising issues concerning the morphological analysis and presentation of Arabic words [9][10][14][15].

The methods used in the construction of morphological analyzers are quite varied. Indeed, some researchers have developed methods based on finding diacritic symbols at the character level, others have exploited these methods to identify diacritics at the word level. A group of researchers has developed hybrid methods coupling approaches to improve these methods. Darwish [15] suggested classifying the approaches into the symbolic approach, the statistical approach and the hybrid approach.

Researchers in the field of morphological analyzer use several methods to analyze a word:

A. Approaches based on Linguistic Rules

For Arabic morphological analyzers several researchers use approaches based on linguistic rules. They use a knowledge base of rules written by linguists to assign solutions to different morphological attributes of Arabic words. The approach based on linguistic rules uses algorithms purely based on the morphological knowledge of the language. It requires rules to cover all morphological shapes. These rules are often classified into grammatical, structural and logical categories. This consists of using criteria and linguistic properties in the form of rules expressing the functioning of the natural language used.

The linguistic approach requires a large number of lists and tables. To develop a set of rules to find the appropriate decomposition, this approach is based on a thorough morphological analysis of the Arabic language [2][14].

The subjective linguistic approach simulates the process used by a linguistic expert. It consists of removing affixes by comparison with predefined lists and transforming what remains, the stem into the root, after a possible alteration by the addition, deletion or modification of some of its letters.

B. Dictionaries based Approach

The resources used for a morphological analyzer are a dictionary of root words that has been created manually using different resources. In addition, a morphological dictionary is used for both a morphological analyzer and a morphological generator, depending on the direction in which it is read by the system [14].

C. Approach based on Patterns of Words

The use of morphological patterns, depending on morphological affixes in all its forms, there are patterns for verbs, patterns for names, patterns for adjectives, etc. There are some common patterns between these types.

To apply this type of analysis, it was necessary to determine the morphological patterns. By counting the morphs that enter them, and the morphemes included therein and the list between them and the grammatical affixes they share with them at the beginning or at the end of the words [10], [19], [22].

D. Approach based on Graph

The graph approach has been dominant since the 1980s. The finite state approach for morphological analysis was initially studied at Xerox and the first practical application was due to Koskenniemi [20][23]; this has been used to develop wide coverage morphological analyzers for several languages.

In this type of approach, the morphotactic and spelling rules are programmed in a finite state transducer (FST), they require too much manual processing to state rules in an FST and not to analyze words that do not appear in Arabic dictionaries [11][3], [24].

Other analyzers use graphs to perform the morphological analysis of Arabic words [16][17].

E. Statistical Approaches

This approach uses the probability of succession of certain morphemes to perform the morphological analysis of a given word. Statistical data obtained by a corpus allowing to acquire knowledge on the morphology of the language, it learns prefixes, suffixes and patterns from a corpus or a list of words in the target language without any human intervention. This approach uses a list of prefixes, suffixes and patterns to transform from stem to root. The possible prefix-pattern-suffix combinations are constructed for a word in order to obtain the possible roots.

F. Hybrid Approach

Hybrid methods are algorithms that combine several approaches already mentioned. For example in the case of the Buckwalter analyzer, the latter combines linguistic rules (when it introduces the notion of compatibility between prefix, suffix and stem) and dictionaries (when it uses the dictionary

of Arabic stems) [14]. Other works use this type of approach [13][15].

III. PRESENTATION OF THE RELATIONAL DATABASE APPROACH

Our new approach is based on the relational concept between tables to perform the morphological analysis of a word.

The database used in this approach uses several tables:

- The tables of proclitics and prefixes of Arabic words.
- The tables of suffixes and enclitics of Arabic words.
- The table of surface patterns of Arabic words.
- The table of Arabic stems.

A. The Tables of Proclitics and Prefixes

The two tables are composed of the Arabic prefixes and the proclitics list. These two tables are related by links which model the prefixes and the proclitics combination rules.

The computability between proclitics and prefixes are going to be explained in Fig. 1.

For example: the prefix "ال" does not combine with the proclitic "س".

These Compatibility Tables generates a query (Query1) of prefixes attached to the proclitics which correspond to them, with other information, such as the word type, the pronoun, ... (Table I).

B. The Suffix and Enclitic Tables

The two tables are composed of the Arabic suffix and enclitic list. These two tables are related with links which model the rules of combination between suffixes and enclitics.

The computability between suffix and enclitic are going to be explained in Fig. 2.

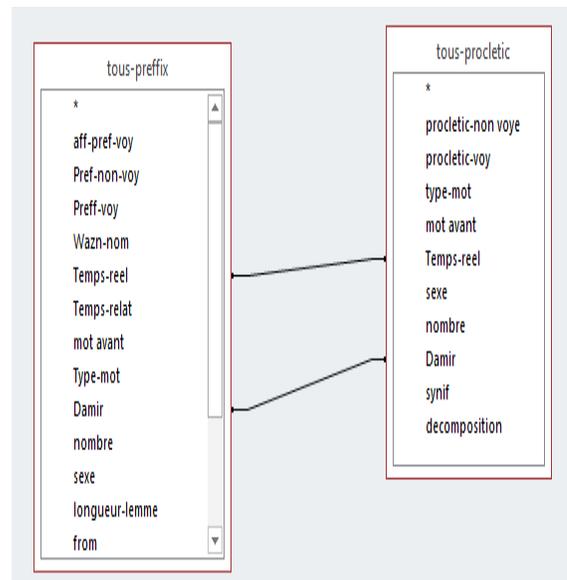


Fig. 1. Compatibility Tables between Proclitic and Prefixes.

TABLE I. EXTRACT OF THE REQUEST CREATED BETWEEN THE PREFIXES AND PROCLITICS

Prefix + proclitic	Proclitic	Prefix	Word-type	Gender of a word	Pronoun
فَلْيَ	فَلِ	يَ	المضارع المنصوب	فعل	هو
أَنْتَ	أَنْتَ	تَ	المضارع المجهول	فعل	أنت
.
فَسَنْ	فَسَنْ	نَ	المضارع المنصوب	فعل	نحن

For example: the enclitic "ف" does not combine with the suffix "ت".

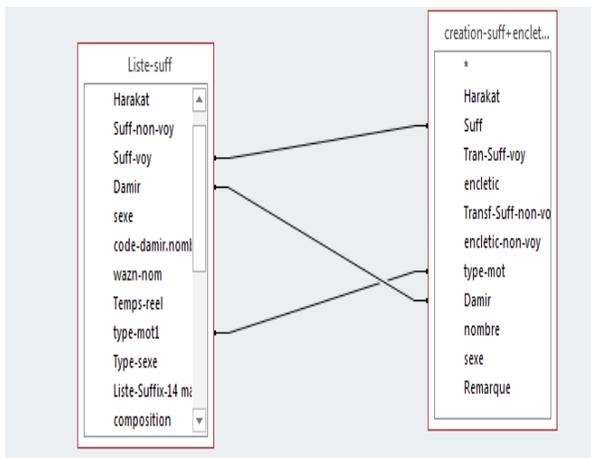


Fig. 2. Compatibility Tables between Suffixes and Enclitics.

This database generates a query (Query2) which contains several information, such as word type, gender, pronoun and numbers. To explain more, the following Table II is going to explain the request created between the suffixes and enclitics.

TABLE II. EXTRACT OF THE REQUEST CREATED BETWEEN THE SUFFIXES AND ENCLITICS

Suffix + enclitic	Enclitic	Suffix	Pronoun	number s	Genre	Type of Word
تَاهُ	هُ	تَا	هُمَا(مؤنث)	مثنى	مؤنث	فعل معلوم
تُكَنَّ	كَنَّ	ةُ	-	مفرد	مؤنث	اسم
.
يُيَهَّنْ	هَّنْ	يُنْ	-	مثنى	مذكر	اسم

C. The Tables of Surface Patterns and Stems of Non-derived Words

This table is composed of surface patterns stems and stems of non-derived Arabic names. Each record is composed of several information, such as lemma, stem of the surface patterns or word, type of word, gender, number, class of the surface patterns, etc.

D. Morphological Analysis using the Relational Model

Our approach uses the relation concept used in databases, to connect the query and the tables described previously: Query1, Query 2, and Table III. The resulting query is noted Query-main.

TABLE III. EXTRACT OF THE QUERY CREATED BETWEEN SURFACE PATTERNS AND STEMS OF NON-DERIVED WORDS

lemma	Stem-voy	Damir	number	sex	Type of Word
جَعْرَ	جُعْرَ	أنا	مفرد	مذكر	المضارع المجهول
جَاعَ	جُوغَ	أنت	مفرد	مذكر	المضارع المعلوم
الله	الله	-	-	-	اسم جلالة
نَاقَةَ	نَاقَةَ		مفرد	مؤنث	اسم حيوان
جعفر	جعفر		مفرد	مذكر	اسم علم

So the Relations between queries and tables are going to be explained in Fig. 3.

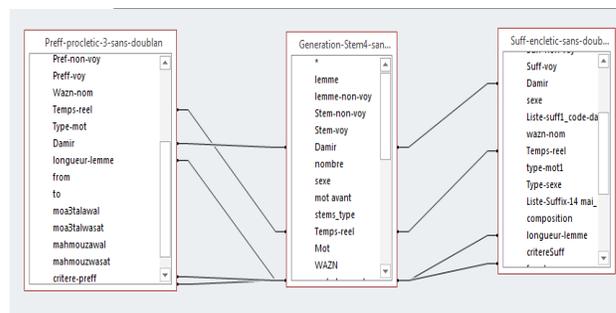


Fig. 3. Relations between Queries and Tables.

These query and table are linked by several links modeling the compatibility rules between prefix-proclitic stem and suffix-enclitic stem.

To analyze a given word, the system goes through the following steps:

- Partitioning of the word to be analyzed into a set of proclitics, prefixes, stems, suffixes and enclitics.
- Find all the surface patterns associated with each stem.
- Create a query from this information.
- For example, for the word to analyze "فدخلت", the pattern of the lemma is "جعر" associated with the proclitic "ف" and the suffix "ت", therefore, the stem calculated from the pattern of the lemma is "دخل" (Fig. 4).
- Reconstruction of solution lemmas from surface patterns of lemmas obtained in this query.
- Verification of the set of lemmas obtained, with the basis of the lemmas.

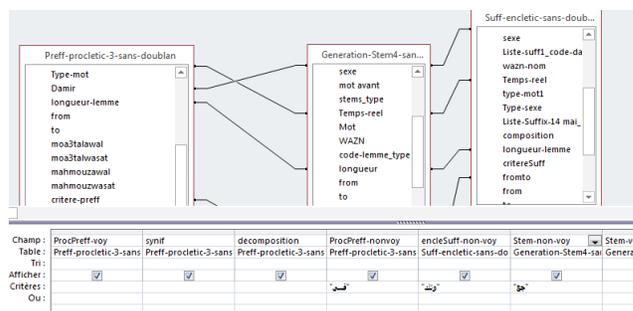


Fig. 4. Request from the Information.

Example:

For the word "أموته", we find among the solution lemmas "مات - يموت" with the prefix "أ", the enclitic "ه" and the time "فعل مضارع معلوم". But when we check in the database of the lemmas, we find that the verb "مات-يموت" does not admit a complement, which therefore implies that each verb derived from this lemma, does not admit any enclitic. This is why this solution will be excluded.

Fig. 5 illustrates the different layers and process of our analyzer.

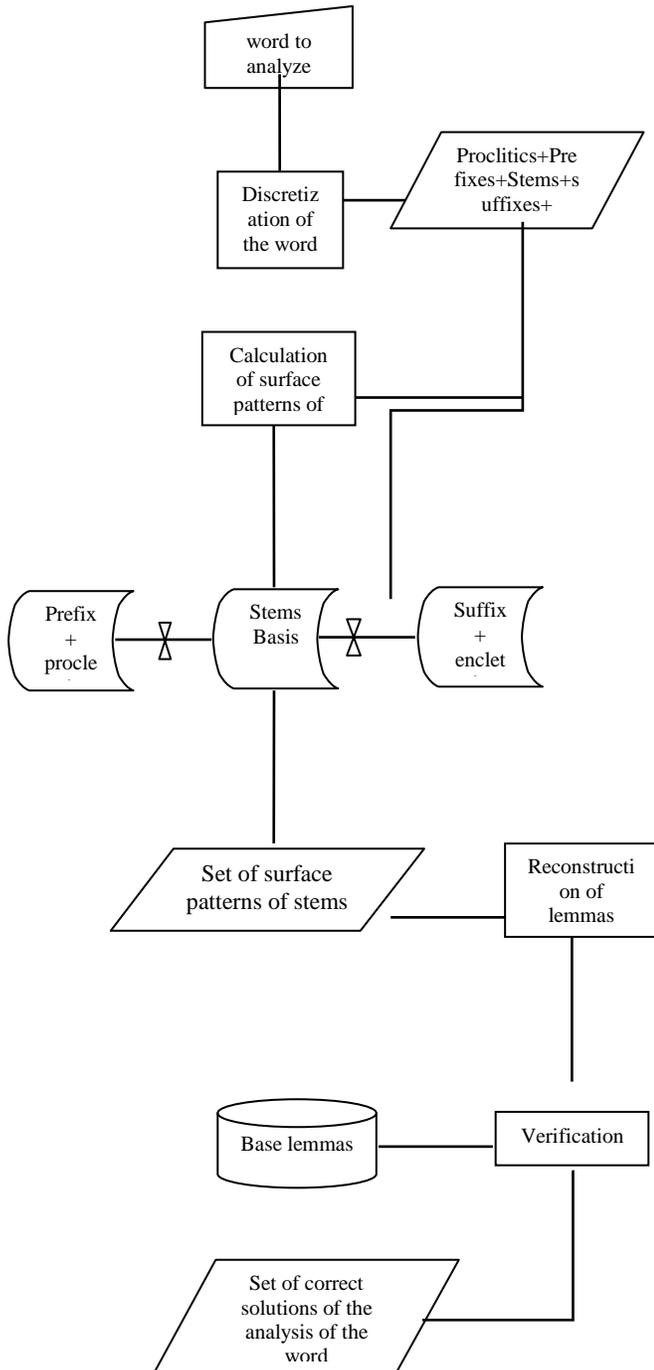


Fig. 5. Schema of the Morphological Analysis Process

IV. EXPERIMENTATION AND RESULTS

A. Implementation

We used with the Java language to build our analyzer morphological. Our application contains three layers including, the presentation layer which processes the data reading part and the result display. The second layer contains the implementation of the algorithm where the rules and filters to apply to analyze a given word as input. The third layer deals with the communication with the MySQL database. The Fig. 6 illustrates the different layers of our analyzer.

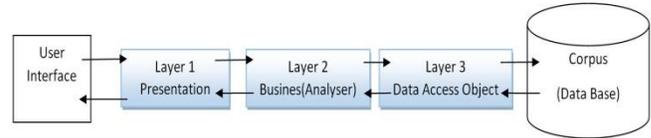


Fig. 6. Analyzer Implementation Layers.

B. Application

To see the results, we have developed a demo as a web interface that allows a user to analyze a word entered as input.

Fig. 7 shows the demo page, which contains a button to start, a text area for entering a word to analyze. The text area accepts only Arabic letters.

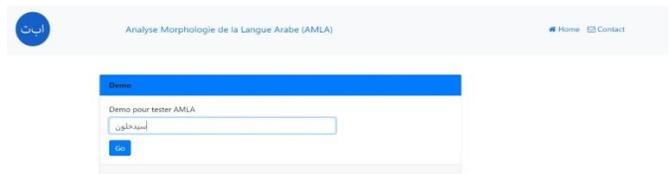


Fig. 7. User interface of our Analyzer.

Example:

For the word "أموته", our system goes through the steps:

- the possible discretizations are showed on Table IV:
- Creation of the table (noted table-sol) of the surface patterns of stems and stems, result is showed on Table V.
- The creation of a query from the table-sol as shown in Table VI.

TABLE IV. POSSIBLE DISCRETIZATION

proclitic	prefix	Stem	suffix	enclitic
		أموته		
	أ	موته		
	أ	موت		ه
		أمو	ت	ه
أ		موته		
أ		موت		ه
أ		مو	ت	ه

TABLE V. SURFACE PATTERNS OF STEMS AND STEMS

Proclitic	prefix	Stem+pattern de stem	suffix	Enclitic
		فعلل		
	أ	فعل		
	أ	فعل		ه
	أ	فول		ه
		فعل	ت	ه
		فعو	ت	ه
أ		فعلل		
أ		فعل		ه
أ		فول		ه
أ		فع	ت	ه
أ		فو	ت	ه
		أموته		
	أ	موته		
	أ	موت		ه
		أمو	ت	ه
أ		موته		
أ		موت		ه
أ		مو	ت	ه

TABLE VI. RESULT OF QUERY

Proclitic	prefix	Stem+pattern de stem	Root	suffix	enclitic
	أ	فول	موت		ه
أ		فعل	موت		ه
أ		موت	موت		ه
	أ	موت	موت		ه

C. Validation and Comparison

To validate our proposed analyzer, we performed significant experiments on the database discussed in the previous section. Our test database contains 20000 words manually constructed from the prefix, suffix and infix. These test words are validated by linguistic experts.

Several tests were performed to evaluate the recognition rate of the analyzer based on the number of words including false words and valid ones. So the Table VII is going to explain this recognition rate.

These results show a significant validation rate. Our analyzer extracts valid words with a rate of 98%. The robustness of our analyzer is demonstrated by the number of possible solutions found.

TABLE VII. THE RECOGNITION RATE

Number of test words	Invalid words	Possible solutions	Valid solutions	Validation rate
20000	1000	100000	98000	98%
15000	0	85000	84000	98.8%

The error rate of our analyzer does not exceed 2%. Most of the found errors are related to insufficient corpus used, which means that our approach is robust against possible false solutions. This robustness is validated by our corpus and the number of criteria used to filter the invalid solutions.

V. CONCLUSION

The approach presented in this article, uses the relational concept relative to databases for making the morphological analysis of Arabic words.

In this approach, the Arabic morphological rules are modeled by links between the different tables used in the main database. The main advantage of this approach is its simplicity of implementation. Moreover, all the variations and the morphological rules are included in the relations between tables. The results obtained are satisfactory and show the importance of the proposed approach.

As future work, we will focus on adding new rules to improve results. Also, we are interested to upgrade our database in order to challenge the performance of our method.

REFERENCES

- [1] Alexia Blanchard, Analyse morphologique des réponses d'apprenants en environnement d'Apprentissage Assisté par Ordinateur. Mémoire de Master, Université Stendhal-Grenoble III, UFR des Sciences du Langage, 2006.
- [2] Al-Fedaghi, S. S., and Al-Anzi, F. S. 1989. A New Algorithm to Generate Arabic Root-Pattern Forms, Proceedings of the 11th National Computer Conference and Exhibition, March, Dharan, Saudi Arabia, 391-400.
- [3] Al-Sughaiyer, I. A. and Al-Kharashi, I. A. 2004. Arabic morphological analysis techniques: A comprehensive survey. Journal of the American Society for Information Science and Technology 55(3): 189-213.
- [4] Audebert C, Jaccarini A. (1988). De la reconnaissance des mots outils et des tokens. Annales islamologiques 24, Institut francais d'archeologie orientale du Caire.
- [5] Azmi, Aqil, Reham S Almajed. 2015. A survey of automatic Arabic diacritization techniques. Natural Language Engineering, 21, pp 477–495. doi:10.1017/S1351324913000284.
- [6] Gaubert C., « Analyse morphologique d'un texte par ordinateur – Résultats et évaluation », AnIsI 29 (1996), IFAO, p. 283-311.
- [7] Jaafar, Y., Bouzoubaa, K., Yousfi, A., Tajmout, R., & Khamar, H. (2016). Improving Arabic morphological analyzers benchmark. International Journal of Speech Technology, 19(2), 259–267. doi:10.1007/s10772-016-9340-x.
- [8] Goldsmith and John.A (2001). Unsupervised learning of the morphology of a natural language. Computational Linguistics, 27(2), 153-198.
- [9] Hilal, Yahiah, 1985 : Morphological analysis of Arabic speech. In: Computer processing of the Arabic language.
- [10] Beesley.KR (1998). Arabic Morphology Using Only Finite-State Operations, Proceedings of the Workshop on Computational Approaches to Semetic languages. Montreal, Quebec, pp 50-57.
- [11] K. R. Beesley and L. Karttunen, Finite State Morphology, CLSI Studies in Computational Linguistics, vol.509, 2003.
- [12] Soudi, A., Violetta Cavalli-Sforza (2001). A Computational Lex-eme-Based Treatment of Arabic Morphology. In Proceedings of the Association for Computational Linguistics, Arabic Processing Workshop, Toulouse, July 2001, France.
- [13] Boudchiche, M., Mazrouia, A. al 2017 . AIKhalil Morpho Sys 2: A robust Arabic morpho-syntactic analyzer. Journal of King Saud University - Computer and Information Sciences Volume 29, Issue 2, April 2017, Pages 141-146.

- [14] Buckwalter.T (2002). Buckwalter Arabic Morphological Analyzer. Version 1.0. Linguistic Data Consortium, catalog. Number LDC2002L49 and ISBN 1-58563-257-0.
- [15] Darwish.K (2002). "Building a Shallow Morphological Analyzer in One Day". Proceedings of the workshop on Computational Approaches to Semitic Languages in the 40th Annual Meeting of the Association for Computational Linguistics (ACL-02). Philadelphia, PA, USA.
- [16] S.Iazzi, A.Yousfi, M.Bellafkih, D.Aboutajdine 2018 : Arabic Morphological Analysis Based On Graphs And Correspondence tables Between Affixes And Root. ISIVC 2018: 318-322.
- [17] S.Iazzi, A.Yousfi, M.Bellafkih. 2020: Comparison between the morphological analyzers based on graph and the one based on surface patterns. SITA 2020: 26:1-26:4.
- [18] Iazzi, S, Yousfi, A, Bellafkih, M, Aboutajdine, D. Graph-based morphological analysis. Journal of Computer Science and Engineering Volume 19, Issue 2 June 2013.
- [19] Iazzi, S, Yousfi, A, Bellafkih, M, Aboutajdine, D. Morphological Analyzer of Arabic Words Using the Surface Pattern. IJCSI International Journal of Computer Science Issues, Vol. 10, Issue 2, No 1, March 2013, ISSN (Print): 1694-0814 | ISSN (Online): 1694-0784.
- [20] Koskeniemi and Kimmo (1983). Two Level Morphology. A General Computational Model for Word-form Recognition and Production. Publication No. 11, Dep. of General Linguistics, University of Helsinki, Helsinki.
- [21] Yousfi.A, Iazzi.S : "نحو محلل صرفي عربي يعتمد على أوزان الكلمة". 7th International Computing Conference in Arabic (ICCA'11). Riyadh, Saudi Arabia (May 31- June 2, 2011).
- [22] Yousfi.A (2010). The morphological analysis of Arabic verbs by using the surface patterns. IJCSI International Journal of Computer Science Issues, Vol. 7, Issue 3, No 11, May 2010.
- [23] G. D. Forney, "The Viterbi Algorithm," Proceedings of IEEE, Vol. 61, No. 3, 1973, pp. 268-278.
- [24] Dichy J. & Fargaly A. (2003), Roots & Patterns vs. Stems plus Grammar-Lexis Specifications: on what basis should a multilingual lexical database centred on Arabic be built?, Proceedings of the MTSummit IX workshop on Machine Translation for Semitic Languages, New-Orleans.

Development of Wearable System to Help Preventing the Spread of Covid-19 in Public Indoor Area

Annisa Istiqomah Arrahmah¹

School of Computer Science
Bina Nusantara University Bandung Campus
Jakarta Indonesia 11480

Surya Ramadhan²

School of Electrical Engineering and Informatics
Institut Teknologi Bandung
Bandung, Indonesia

Abstract—Smart wearables as a part of the Internet of Things nowadays gaining confidence in our daily lives because of its accessibility and simplicity. Today, with the outbreak of Coronavirus around the world, a smart wearable device can become another solution to help slowing the virus spreading by ensuring public health and social measures. In this paper, a system consisting of distance detector and touchless door access is proposed to help the personal, physical and social distancing measures practice in a public indoor area. A BLE positioning method based on RSSI localization is used to ensure the physical distancing around the user. WPA2 and MAC address-based authentication for the touchless door access is used to restrict and trace the visitor of the indoor area. The system is implemented in ESP microcontroller. A proof of concept is conducted to see if the functionality of the system already satisfied the public health and social measures practice. The results show that only registered devices can give a signal to open the door and the device can guarantee the physical distance around the user with 4.51% error in indoor area.

Keywords—Wearable device; healthcare system; COVID-19; door-lock system; radio signal strength indicator (RSSI)

I. INTRODUCTION

In the past year, a massive spread of respiratory disease called COVID-19 caused by a coronavirus family has changed the human interaction with the surrounding environment [1]. Experts also suggest that the world should prepare for the inevitability of COVID-19 becoming an endemic [2]. Based on [3] issued by the World Health Organization, there are two ways that COVID-19 can spread between humans. When a sick person coughs, sneezes or breathes, a droplet that contains the virus is released. These droplets mostly fall into the nearby surface of an object such as a desk, telephone or even a door knob. A healthy person could be infected with COVID-19 by touching these contaminated surfaces and then touch their face. If the health person standing near the infected person within 1 meter, they could catch COVID-19 by inhaling these droplets. Following the information, in document [4] WHO also gives guidance strategies to help reducing the spread of COVID-19 especially in the public area in the form of public health and social measures. These measures include physical and social distancing measures to prevent transmission between infected persons to those who are not infected and personal measures to limit person to person spread and reduce contamination on frequently touched surfaces. These measures can be in the form of physical distancing, frequent hand hygiene, avoiding crowded space, contact tracing and limiting surface contact as

minimum as possible. In [5], research about the impact of physical distance measures on the transmission of COVID-19 in the UK is conducted. The research is done by comparing contact patterns during pandemic and non-pandemic situations. In the result, the researchers state that physical distance measures give a 74% reduction in average daily contact that led to a substantial impact in reducing the cases in the incoming week. Another research [6] is performed in several countries in Europe and gave similar results. As an example, the researchers state that in Germany, physical distance measures give 49% reduction, while in Italy they give 83% reduction.

In Indonesia, the personal, physical and social distance measures are established as a health protocol called 3M. Several studies shows that the health protocol awareness in Indonesia is still lower than 50% [7]–[9]. In contrast, the indoor public area such as workplace, education place and marketplace are gradually starting to allow people in. Thus, an additional system to support the health protocol enforcement is needed. A wearable system is a suitable system that can be implemented since it enables fast data and information flow, particularly relevant for the rapid infectious character of COVID-19 virus [10].

In this paper, a wearable system is proposed to help ensuring the personal, physical and social distancing measures especially in restricted public indoor areas. The system consists of two main functions; distance detector and touchless door access. The distance detector is used to ensure the physical distance in the indoor area based on the minimum distance suggested by WHO. The touchless door access has two purposes. First, limiting the surface contact area in the door handles as it is one of the most high-touch surfaces with 33% virus RNA positive rate traces [11], [12]. Second, to limit the access of the area as only people that wear the device and registered can enter the area, making it easier for contact tracing. This wearable system is implemented in embedded systems ESP microcontroller. For the distance detector module, this system adopts Bluetooth positioning method using RSSI localization. Thus, a safe social distance can be maintained around the user. The touchless door access utilizes the Wifi communication mechanism to open the gate automatically. By using WPA2 and MAC-based authentication processes, only authorized users that wear the device are allowed to enter the area.

Current system to ensure the personal, physical and social distancing is mostly done by giving regulation without any tools to strictly ensure the implementation of the measures. For example, the newest regulation in Indonesia utilizes a mobile application to track the user's indoor area visit history [13] by sharing the user's location based on GPS to the server system while the user entering the area. But this system cannot confirm the physical distancing measures among the visitors inside the area and no minimal limitations of visitors at a certain time. The proposed system encounters the shortage of the aforementioned system to ensure all measures are implemented. By using wearables system, a strict regulation without relying on user's phone can be established and future data collection for tracking and tracing can be carried out.

This paper is divided into the following sections. Section I presents the background of the research and the previous work related to this paper. Section II explains about previous research related to this research. Section III discusses basic theories used in this research. Section IV explains the proposed design. Section V shows the research implementation and testing result. Section VI concludes the research done in this paper, respectively.

II. RELATED WORK

In [10], authors suggest several approaches and principles in wearables systems and sensor recommendation used for symptom tracking and contact tracing. Mostly the suggestion is still in the initiative scale and there is no further development in specific one system to help the social and physical measures enforcement. In this research, as the wearable system consists of two main functions; touchless door access and distance detector, research and technology selection related to the mentioned functions are considered.

A. Distance Detector

There are different methods that have been used to detect, and measure the distance of objects such as Bluetooth, Wifi, or ultrasound [14]. Bluetooth and Wifi technology measure the distance using a signal strength modeling while the ultrasound using lateration. In this system, human detection should be done in 360 degrees around the user. If there are people who are too close to the user, then the system will give a warning. Based on article [15], the safe distance between humans for social distance is about 1.5 meters. By using the distance detector, the user can perform the social distancing appropriately especially in the indoor area. In [16]–[18] a distance sensing and detector system is implemented in embedded system using ultrasonic sensor. Yet, this sensor has limitations for the aforementioned condition of the system. Ultrasonic sensor has a limited angle detection range with a maximum 15° degree measuring angle. By using one sensor, the detected object is limited to only one direction. A signal strength method such as Bluetooth based or Wifi based is a decent method for the COVID-19 distance detector because they sense the object within the radius range. Another technology that can be used is BLE (Bluetooth Low Energy), a low power version of Bluetooth [19]. The comparison between Bluetooth, Wifi and BLE technologies can be seen in Table I.

TABLE I. BLUETOOTH VS WIFI MODULE TECHNOLOGIES

Comparison	SPM Method		
	Bluetooth	Wifi	BLE
Frequency	2.4 GHz	2.4,3, 5 GHz	2.4 GHz
Chip Cost	Low	High	Low
Bandwidth	1-3 Mbps	11 Mbps	1-2 Mbps
Security	Less secure	Secure	Less secure
Power Consumption (Active mode)	~600 mW	~950 mW	3 mW

In COVID-19 distance detector, the device's purpose is to detect people around the user in a fairly long period of time. Thus, the device operation time or the battery power is more considered than the positioning precision. Then, BLE is the best option method for this scenario because the system is performed in a low cost, low bandwidth and low security risk tolerance.

B. Touchless Door Access

Touchless door access adopts the mechanism of smart door lock system with the purpose to unlock the door automatically. There are several researches that have been conducted in this area. In [20]–[22], the door lock system utilizes Wifi and Bluetooth to communicate with the door lock mechanism. Authentication process is done by using a password in a mobile application. In [19], an OTP insertion is added to increase the level of security. In [23], [24], a radio signal such as Wifi and Bluetooth is used for the authentication process. In [22] they also used MAC- based authentication while in [23] they used password-based authentication. All of the aforementioned research is implemented in a mobile phone and uses a mobile application for authorization.

In this system, the touchless door access adapts the Wifi based authentication. This system is implemented in ESP embedded system. For additional level of security, MAC based authentication is added to the system. Thus, two-factor authentication is applied to ensure the genuineness of the device.

III. BASIC THEORIES

In this section, basic theories related to the proposed design are explained.

A. RSSI (Radio Signal Strength Indicator)

Received Signal Strength Indicator readings is a method to measure a distance between two Bluetooth devices. Radio Signal Strength using Bluetooth positioning has been studied in several studies[25]–[27]. This research adapts the RSSI reading method proposed in [28]. The mentioned method uses the newest Bluetooth standard mostly used in today's electronic devices. The distance between two radio devices is calculated using the RSSI and a proper radio propagation model is used. The RSSI is estimated using equation (1).

$$RSSI = -(10n \log_{10} d + A) \quad (1)$$

A and n are RF parameters for describing the network peripheral. The RF parameter A, represented by dBm, defines

the absolute energy emitted by the transmitter at 1 meter range. In other words, A is the RSSI reading at 1 meter from the transmitter. Parameter n represents the transmission constant and relevant with the signal transmission constant. Distance d is the distance between receiver and transmitter node.

The value of RF parameter A and n are calculated by using RSSI values and distance d read by the sensors. The RSSI value is the received power of the reference node while the d is the distance between two reference nodes. The transmitter constant n between two reference nodes is estimated using equation (2).

$$n_i = \left(\frac{RSSI-A}{10 \log_{10} d_i} \right) \quad (2)$$

Another way to calculate the RF parameters is using a regression stated in [29]. First, the dataset of RSSI relevant to the distance d are collected. Then equation (1) is transformed into equation (3). Parameter A and n are obtained experimentally based on the collected dataset.

$$y = -10n \log_{10} x - A \quad (3)$$

IV. PROPOSED DESIGN

A. System Architecture

In this research a wearable system to ensure the personal, physical and social distancing measures is proposed. The use case scenario of the system can be seen in Fig. 1. Based on the figure, while a person wants to enter the restricted indoor area, a prescreening and registration process should be done for data tracing. After that, they receive the registered device to be worn on their body. Thus, only a person who owns and wears the device can enter the area. Inside the area, they should maintain the distance with the other by the help of the device. If the user stands too near with another, then the device gives a warning. The wearable device uses ESP32[30] embedded platform. The schematic of the device can be seen in Fig. 2. The device consists of a switch button circuit, the microcontroller, a battery and a buzz circuit. The switch button is pressed by the user while they want to enter the building/area. The buzz circuit is used as a warning sign to the user if they violate the physical distancing rules.

B. Covid-19 Distance Detector

The distance detector utilizes the Bluetooth Low Energy (BLE) module embedded in ESP32 device. BLE is chosen for the distance detector based on Section 2. The distance detector system needs at least two devices to communicate between the BLE client and server and works as a distance detector. While the user is entering the area, the device will turn on its BLE client and server mode alternately in an infinite loop until another higher level of interrupt event occurs. The flowchart between two devices can be seen in Fig. 3.

During the client mode, the device acts as an observer and during the server mode the device acts as a broadcaster. While the BLE is set as a broadcaster, the device broadcasts its advertising data. Whereas the BLE is set as an observer, the device scans all available devices around by capturing the advertising data issued by the BLE broadcaster. During this mode, the user device captures data consisting of BLE name,

address, service UUID, TX power and RSSI. By using the captured RSSI information, the observer calculates the broadcaster origin distance using Eq. 4. If the distance of the broadcaster is less than the allowed distance, then the microcontroller gives a signal to the buzzer and the buzzer produces a warning sound.

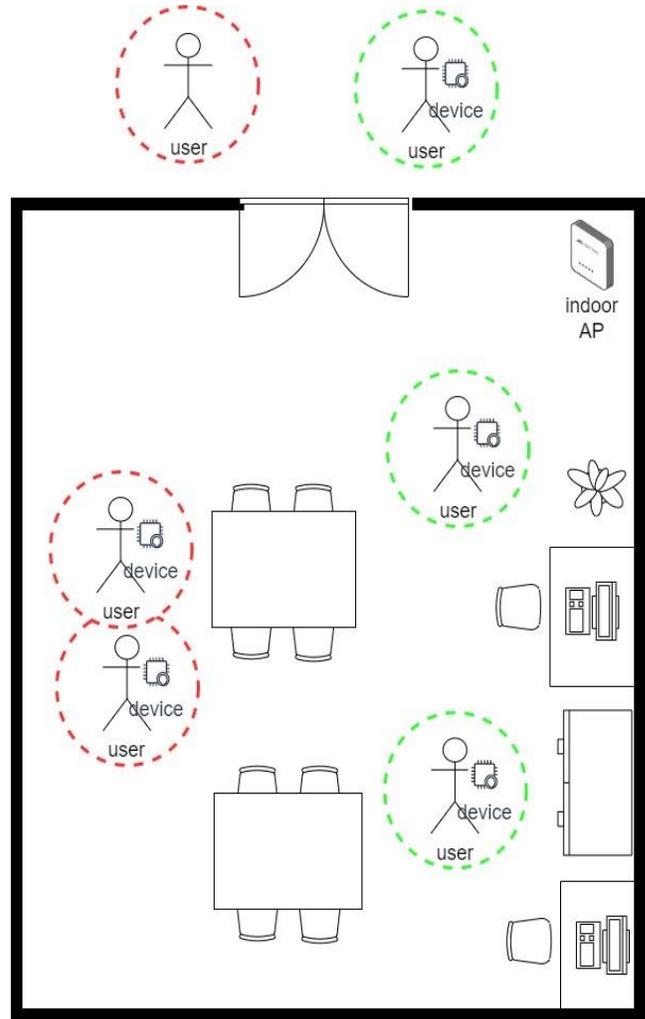


Fig. 1. Example of Physical Measures System Scenario in the Indoor Area.

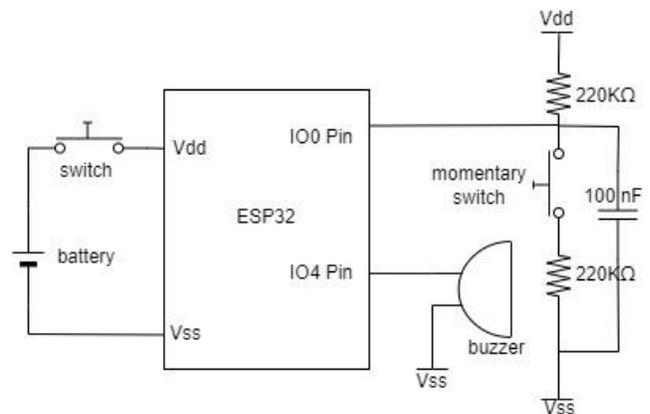


Fig. 2. Schematic of the Wearable Device.

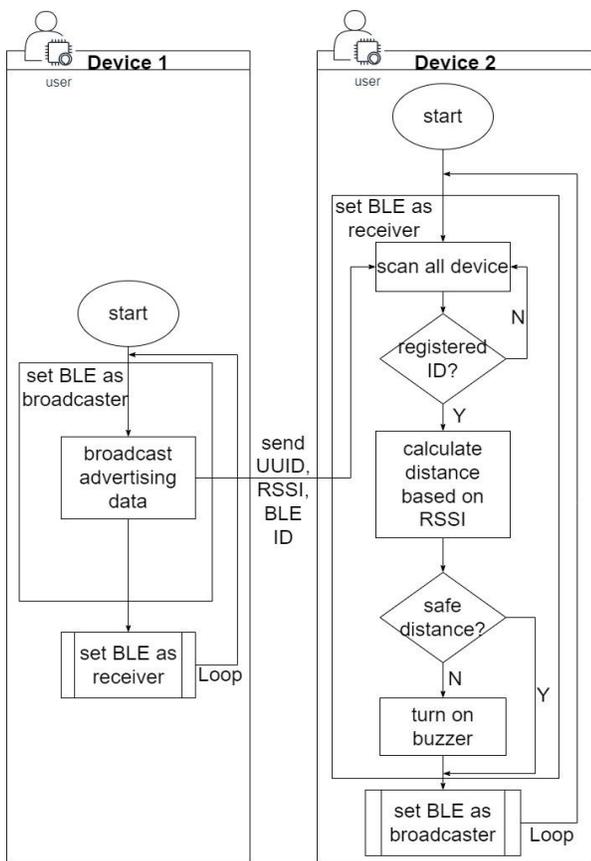


Fig. 3. Flowchart of the Distance Detector.

C. Touchless Door Access Module

The touchless door access mechanism utilizes two-way factor authentication for the authorized users' authentication. The detailed authentication processes can be seen in Fig. 4. An ESP8266[31] near the front door acts as a server (AP) while an ESP32 in the wearable device worn by the user acts as a client. The door is opened if a client device requests a connection to the Wifi AP device. A request is made by the user by pressing the switch button in the device. After the switch button is pressed, the WPA2 client mode is activated and the device requests an authentication to the AP device. If an authentication process is successful, the device requests an association to the AP by giving MAC address information. Then, the AP verifies the client's MAC address against a locally configured list of allowed addresses. If the MAC address matches, a response is sent to the device and the AP generates a signal to the door lock mechanism to open the door. The door-lock mechanism is not the scope of this paper.

The flowchart of the client device and the AP device can be seen in Fig. 5. In the client device, BLE is run as a default. The Wifi client is activated and the BLE is turned off if a GPIO interrupt occurs from a button press. Thus, a flag is raised to inform the loop function that a button has been pressed. After the flag is cleared, the Wifi client is turned on and an authentication process is performed. In the AP device, the device always turns on its AP mode, scans clients, performs authentication processes and sends a signal to the door-lock mechanism.

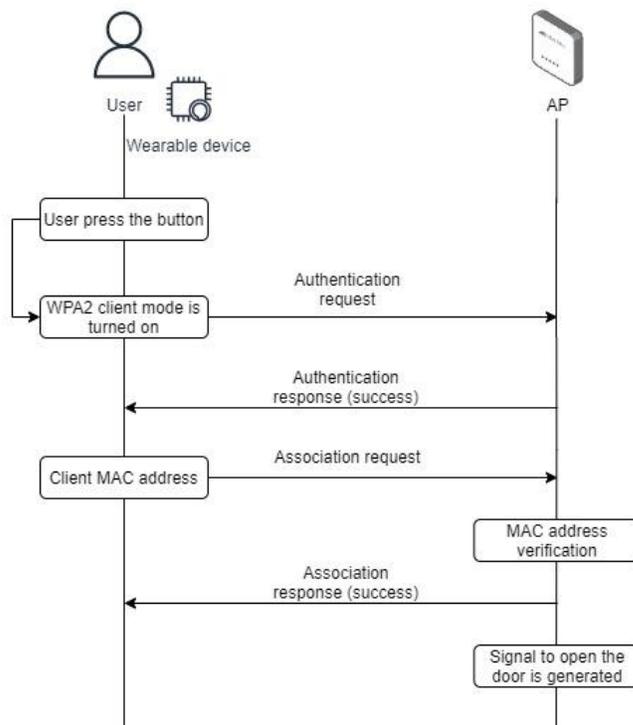


Fig. 4. Authentication Process.

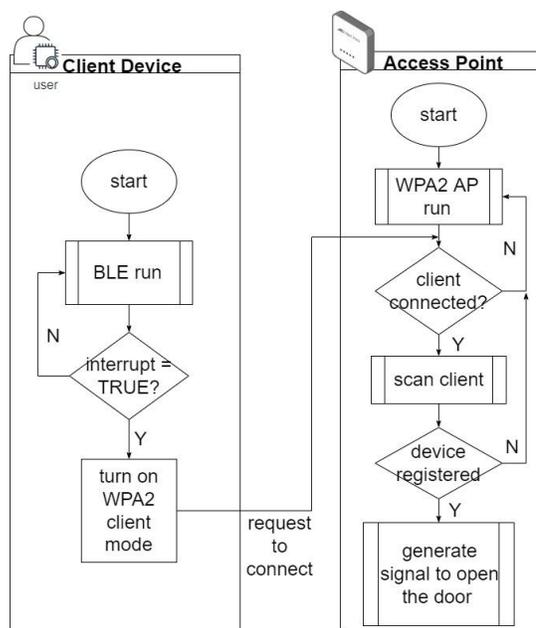


Fig. 5. AP and Client Device Flowchart.

V. RESULT AND DISCUSSION

A. System Implementation

The implementation of the device is done in a controlled experiment environment. The prototype of the wearable device is shown in Fig. 6. The components of the device are explained in Table II. For the power input, a rechargeable Lithium-ion battery is used. For the output, an active buzzer is used to give a sound alarm if another device is detected less than 1.5 meters away.

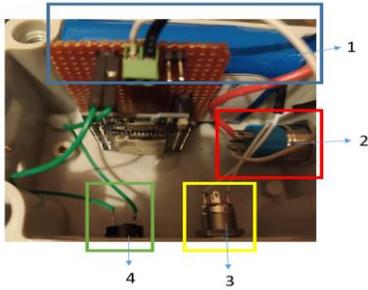


Fig. 6. Implementation of the Smart Key.

TABLE II. FIGURE 5 EXPLANATION

No.	Box Color	Component Explanation
1	Blue	Lithium-ion Battery
2	Red	Power switch
3	Yellow	Wifi switch button
4	Green	Buzzer

TABLE III. FUNCTIONALITY TEST

Function	Result	
	Trigger	Output
Distance Detector	Less than 1.5 meters	The buzzer ring
	More than 1.5 meters	The buzzer does not ring
Touchless door access	Registered Client device near the AP device	A signal to open the door is generated
	Unregistered Client device near the AP device	A signal to open the door is not generated

The functionality test result of the system can be seen in Table III. For the distance detector, another test is done by comparing the distance result using RSSI with actual distance to obtain the device accuracy. For the touchless door access, because the mechanic of the door lock system is not the scope of this system, the output is only a signal to open or to close the door that should be interpreted by the next-door lock system mechanism.

B. Distance Calculation Parameter

Based on equation (1), the RSSI values and distance *d* should be gathered to achieve the parameter *A* and *n* values. The RSSI and distance values are obtained at multiple defined points. The experiment is done inside a room with dimension 5.4m x 2.7m and the beacon is placed 0.5 meters above the ground. The RSSI are gathered 25 times at 14 specified positions. For each position, the mean value of the RSSI samples is calculated. By using this dataset of average RSSI value, a logarithmic function by using a fitting curve is made. The obtained function and the curve model can be seen in Eq. 4 and Fig. 7, respectively.

$$RSSI = -(19.38 \log_{10} d - 48.86) \tag{4}$$

C. Distance Detector Accuracy

The distance detector works by giving an alarm if another device is near the user device. Based on Section 2, the minimum distance for social distancing is 1.5 meters. The testing process is conducted by comparing the distance value computed from Eq. 4 with the actual distance. The test is taken on the fixed distance point to determine the accuracy. The accuracy of the distance detector system is determined by using measurement performance tools. For each distance point, the output distance samples for one minute are gathered. For data accuracy, the modus (mode) data of the samples are used. Based on Table IV, the error value of the output is declining while the distance is increasing. Oppositely, the data variance is increasing with the distance. The error value in the distance for social distancing (1.5m) is reasonable enough, i.e. 4.51% (average) or 0.39% (modus). The performance curve model can be seen in Fig. 8. Based on the figure, the higher the distance, the system becomes less precise.

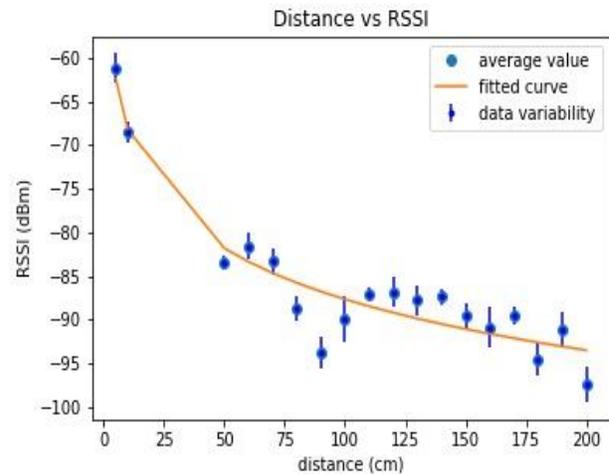


Fig. 7. Distance vs RSSI.

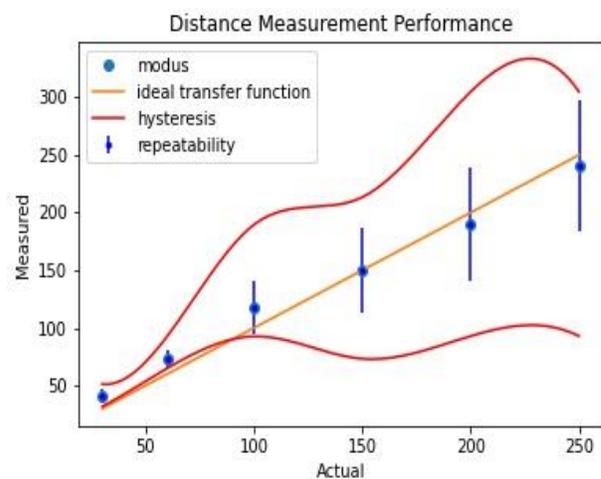


Fig. 8. Distance Measurement Performance.

TABLE IV. DISTANCE DETECTOR PERFORMANCE

Actual distance (cm)	Measured distance (cm)			
	Modus	Error (%)	Average	Error (%)
30	40.44	34.8	39.62	32.07
60	73.25	22.08	74.69	24.48
100	117.82	17.82	129.39	29.39
150	149.42	0.39	143.23	4.51
200	189.5	5.25	184.19	7.9
250	240.33	3.87	214.03	1

D. Touchless Door Access

The implementation of the two-way authentication of the touchless door access can be seen in Fig. 9. After the authentication using WPA2 successes, a MAC address verification is performed. Fig. 9(b) shows the result that the client device with E0:1F:88:66:4E:2E MAC address has not been registered to the AP device. Thus, the system generates output signal to prevent the door-lock system opening the door. Fig. 9(a) shows that the MAC address' client device is registered in the AP device and matches with the lookup table. Thus, when the client device approaches the AP device and a request is made, an output signal to open the door is generated.

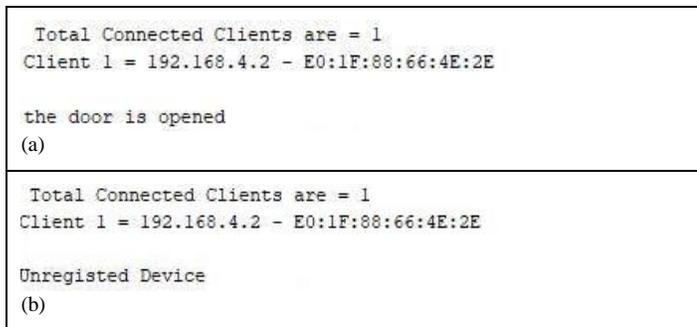


Fig. 9. (a) Registered Client (b) Unregistered Client.

VI. CONCLUSION

In this paper, a prototype of a wearable system to help public health and social measures practice in public indoor areas is proposed. The system consists of two main functions; distance detector for physical distancing measures and touchless door access for personal measures. The system is implemented in ESP32 microcontroller. The system uses MAC based and WPA2 based authentication for the touchless door access application and BLE positioning based on RSSI localization for the distance detector. The functionality test has been conducted and the system successfully generates the desired output. The touchless door access shows that only a device with a registered MAC address can access the AP and generates a signal to open the door. The BLE based distance detector module has a reasonable performance for the social distancing parameter, i.e., 1.5 m. It has an average 4.51% error around 1.5 meters with $\sigma = 6.16 - 57.2$ around the tested distance.

The performance of the system still focuses on the theoretic and technical result; thus, overall evaluation of the system as

digital contact tracing should be done in a practical scope. For the future works, the data collected from the system can be performed automatically by utilizing Internet of Things. The collected data can be processed by epidemiological for tracking, tracing and modeling purposes.

REFERENCES

- [1] H. A. Rothan and S. N. Byrareddy, "The epidemiology and pathogenesis of coronavirus disease (COVID-19) outbreak," J. Autoimmun., vol. 109, no. February, p. 102433, 2020, doi: 10.1016/j.jaut.2020.102433.
- [2] P. Hunter, "The spread of the COVID - 19 coronavirus," EMBO Rep., vol. 21, no. 4, pp. 1-3, 2020, doi: 10.15252/embr.202050334.
- [3] WHO, "Getting your workplace ready for COVID-19," World Heal. Organ., no. March, pp. 1-8, 2020, [Online]. Available: www.WHO.int.%0Awww.WHO.int%0Awww.WHO.int.
- [4] WHO, Overview of public health and social measures in the context of COVID-19, no. May. 2020, pp. 1-8.
- [5] C. I. Jarvis et al., "Quantifying the impact of physical distance measures on the transmission of COVID-19 in the UK," pp. 1-10, 2020.
- [6] E. Del Fava et al., "The differential impact of physical distancing strategies on social contacts relevant for the spread of COVID-19," medRxiv, 2020, doi: 10.1101/2020.05.15.20102657.
- [7] F. Prasetya and I. Yunawati, "Public Perception of Covid-19: Implementation Of Health Protocols in West Muna District Persepsi Masyarakat Tentang Covid-19: Penerapan Protokol Kesehatan di Kabupaten Muna," vol. 2, no. 1, pp. 32-41, 2021, doi: 10.24252/diversity.v2i1.21391.
- [8] S. Artama, Rif'atunnisa, and B. M. L., "Kepatuhan Remaja Dalam Penerapan Protokol Kesehatan Pencegahan Covid-19 Di Lingkungan Sangingloe Kecamatan Tamalatea Kabupaten Jeneponto," J. Ilm. Kesehat. Pencerah, vol. 10, no. 1, pp. 65-72, 2021, [Online]. Available: https://stikesmu-sidrap.e-journal.id/JIKP/article/view/241.
- [9] F. D. A. Pinasti, "Analisis Dampak Pandemi Corona Virus Terhadap Tingkat Kesadaran Masyarakat dalam Penerapan Protokol Kesehatan," Wellness Heal. Mag., vol. 2, no. 2, pp. 237-249, 2020, doi: 10.30604/well.022.82000107.
- [10] O. Amft, L. Lopera, P. Lukowicz, S. Bian, and P. Burggraf, "Wearables to Fight COVID-19: From Symptom Tracking to Contact Tracing," IEEE Pervasive Comput., vol. 19, no. 4, pp. 53-60, 2020, doi: 10.1109/MPRV.2020.3021321.
- [11] K. Razzini et al., "Science of the Total Environment SARS-CoV-2 RNA detection in the air and on surfaces in the COVID-19 ward of a hospital in Milan, Italy," Sci. Total Environ., vol. 742, p. 140540, 2020, doi: 10.1016/j.scitotenv.2020.140540.
- [12] J. E. Powers, M. L. Nadimpalli, T. R. Julian, and A. J. Pickering, Longitudinal monitoring of SARS-CoV-2 RNA on high touch surfaces in a community setting. pp. 1-17.
- [13] A. Fadli, "M ENGENTAL C OVID -19 DAN C EGAH P ENYEBARANNYA D ENGAN ' P EDULI L INDUNGI ' A PLIKASI B ERBASIS A NDORID," no. April, 2020.
- [14] L. Baticic and M. Tomic, "Overview of indoor positioning system technologies," 2018 41st Int. Conv. Inf. Commun. Technol. Electron. Microelectron. MIPRO 2018 - Proc., pp. 473-478, 2018, doi: 10.23919/MIPRO.2018.8400090.
- [15] N. Williams, "Social Distancing in the Covid-19 Pandemic," Occup. Med. (Chic. Ill.), vol. 70, no. 5, p. 305, 2020, doi: 10.1093/occmed/kqaa072.
- [16] N. Anju Latha, B. Rama Murthy, and K. B. Kumar, "Distance Sensing with Ultrasonic Sensor and Arduino," Int. J. Adv. Res. Ideas Innov. Technol., vol. 2, no. 5, pp. 1-5, 2016.
- [17] N. Dey, A. Paul, P. Ghosh, C. Mukherjee, R. De, and S. Dey, "Ultrasonic Sensor Based Smart Blind Stick," Proc. 2018 Int. Conf. Curr. Trends Towar. Converging Technol. ICCTCT 2018, pp. 1-4, 2018, doi: 10.1109/ICCTCT.2018.8551067.
- [18] L. Koval, J. Vaňuš, and P. Bilík, "Distance Measuring by Ultrasonic Sensor," IFAC-PapersOnLine, vol. 49, no. 25, pp. 153-158, 2016, doi: 10.1016/j.ifacol.2016.12.026.

- [19] A. Mackey, P. Spachos, L. Song, and K. N. Plataniotis, "Improving BLE Beacon Proximity Estimation Accuracy Through Bayesian Filtering," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3160–3169, 2020, doi: 10.1109/JIOT.2020.2965583.
- [20] P. Tilala, A. K. Roy, and M. L. Das, "Home access control through a smart digital locking-unlocking system," *IEEE Reg. 10 Annu. Int. Conf. Proceedings/TENCON*, vol. 2017-Decem, pp. 1409–1414, 2017, doi: 10.1109/TENCON.2017.8228079.
- [21] T. Adiono, S. Fuada, S. F. Anindya, I. G. Purwanda, and M. Y. Fathany, "IoT-enabled door lock system," *Int. J. Adv. Comput. Sci. Appl.*, vol. 10, no. 5, pp. 445–449, 2019, doi: 10.14569/ijacsa.2019.0100556.
- [22] A. Kassem, S. El Murr, G. Jamous, E. Saad, and M. Geagea, "A Smart Lock System Using Wifi Security," in *2019 4th International Conference on Advances in Computational Tools for Engineering Applications, ACTEA 2019*, 2019, pp. 222–225.
- [23] N. Hashim, N. F. A. M. Azmi, F. Idris, and N. Rahim, "Smartphone activated door lock using WiFi," *ARPN J. Eng. Appl. Sci.*, vol. 11, no. 5, pp. 3309–3312, 2016.
- [24] S. Jensen, "Proximity Door Locking," 2019.
- [25] A. K. M. M. Hossain and W. S. Soh, "A comprehensive study of bluetooth signal parameters for localization," *IEEE Int. Symp. Pers. Indoor Mob. Radio Commun. PIMRC*, 2007, doi: 10.1109/PIMRC.2007.4394215.
- [26] C. Zhou, J. Yuan, H. Liu, and J. Qiu, "Bluetooth Indoor Positioning Based on RSSI and Kalman Filter," *Wirel. Pers. Commun.*, vol. 96, no. 3, pp. 4115–4130, 2017, doi: 10.1007/s11277-017-4371-4.
- [27] H. Chen, "Bluetooth Indoor Positioning Research Based on RSSI of the Least Square Positioning Algorithm," vol. 3, no. 7, pp. 77–82, 2016.
- [28] Institute of Electrical and Electronics Engineers., "2013 IEEE 10th Consumer Communications and Networking Conference (CCNC): 11-14 January 2013, Las Vegas, USA.," pp. 837–842, 2013.
- [29] F. Vanheel, J. Verhaevert, E. Laermans, I. Moerman, and P. Demeester, "Automated linear regression tools improve RSSI WSN localization in multipath indoor environment. *EURASIP J. Wireless Comm. and Networking* 2011: 38 (2011)," *EURASIP J. Wirel. Commun. Netw.*, pp. 1–27, 2011.
- [30] Espressif, "ESP32 Series Datasheet," *Espr. Syst.*, pp. 1–61, 2019, [Online]. Available: www.espressif.com.
- [31] E. Systems, "ESP8266EX," 2020.

A Comparative Study of Segmentation Method for Computer-aided Diagnosis (CAD) Leukemia AML Subtype M0, M1, and M2

Wiharto^{1*}, Wisnu Widiarto², Esti Suryani³, Nurmajid Hidayatullah⁴
Department of Informatics, Universitas Sebelas Maret
Surakarta, Indonesia

Abstract—A computer-based diagnosis model for Acute Myelogenous Leukemia (AML) is carried out using white blood cell image processing. The stages in computer-aided diagnosis (CAD) are included pre-processing, segmentation, feature extraction, and classification. The segmentation method has many approaches, namely, clustering, region growing, and thresholding. The number of approaches that can be used requires proper selection because it will have an impact on CAD performance. This study aims to conduct a comparative study of the performance of the WBC segmentation method on the AML M0, M1, and M2 subtype leukemia CAD system. The segmentation algorithm used is k-means, fuzzy c-means, SOM, watershed, chan vese (active contour), otsu thresholding, and histogram. The feature extraction method uses GLCM, while the classification algorithms tested are SVM, Random-forest, decision tree, naive Bayesian, and k-NN. The test results show that the histogram segmentation method is able to provide the best average performance when using SVM, namely 90.3% accuracy, 85.9% sensitivity, and 92.7% specificity.

Keywords—Acute myelogenous leukemia; leukemia; segmentation; feature extraction; classification

I. INTRODUCTION

Leukemia is a blood cancer caused by the body producing too many abnormal white blood cells. Leukemia can occur in both adults and children. White blood cells are part of the immune system produced in the bone marrow. When the function of the spinal cord is disturbed, the white blood cells produced will change and no longer perform their role effectively. Leukemia has several types, including Acute myeloblastic leukemia (AML). The AML is acute myeloblastic leukemia that occurs when the bone marrow overproduces immature myeloid cells or myeloblasts. The diagnosis of leukemia AML can be made with a white blood test (WBC) for analysis. WBC analysis can be done computerized, namely by photographing the WBC, so that WBC is obtained in the form of a digital image.

One way to develop a leukemia diagnosis system model is by using a computer-based diagnostic model. This diagnostic system model is done by analyzing WBC. This analysis has a number of advantages compared to existing models, namely the process is faster. Processing is carried out in a number of stages. The stages in computer-based diagnosis include preprocessing, segmentation, feature extraction, and classification. The preprocessing stage is used to improve

image quality so that it is ready to continue with the segmentation process. At the segmentation stage, it is done to separate the object from the background. The segmentation process can use a number of approaches, namely Region growing, edge detection, thresholding, and clustering [1]–[3][4]–[6]. Each approach in segmentation also has many algorithms that have advantages and disadvantages. The next stage after segmentation is feature extraction. Feature extraction has a number of approaches, namely color, texture, statistical, and geometry [7]–[9]. The next stage is the classification process, which can be done using a number of algorithm choices, such as SVM and decision tree [10].

Many developments of AML leukemia CAD models have been carried out [11]–[14], but unfortunately many still produce low related performance. One of the factors causing the low performance is the wrong choice of the segmentation method used. To overcome this, there have been a number of studies that have also compared segmentation performance but only limited to segmentation algorithms on one approach, such as clustering [15] and thresholding [13], [16]. This makes the best algorithm only limited to that approach and has not been carried out for inter-approach. This condition causes the lack of literature that can be used to determine the best segmentation algorithm for WBC segmentation in AML leukemia, so a comparative study of a number of segmentation algorithms from several segmentation approaches is needed, such as thresholding, clustering, and region growing.

II. LITERATURE REVIEW

The segmentation approach for white blood cell (WBC) image analysis has advantages and disadvantages, so the selection of the segmentation method will affect the performance of the AML leukemia diagnosis system. The segmentation method used in the diagnosis system for leukemia AML subtypes M0, M1, and M2 mostly uses thresholding [11], [12], [14]. The weakness of using thresholding is in determining the threshold value, which is done manually so that sometimes it is not suitable for different image conditions. The weakness of thresholding with a static threshold value can be overcome by a dynamic threshold value, namely multi-Otsu thresholding. Multi-Otsu thresholding can provide good performance compared to static thresholding in the case of AML subtype M0 and M1 classification [13]. Another image segmentation method that is also widely used is active contour without edge combined

*Corresponding Author.

with watershed distance transform which is used for segmentation of AML subtypes M2, M3, and M4[17].

Another alternative approach to segmentation is to use a clustering algorithm. The concept of clustering is the same as the concept of segmentation, which separates the background and objects. Clustering will automatically form a cluster center depending on the data, and from the data center, it can be used to threshold the binary image formation process [18], [19]. A study conducted by Dhanachandra et al. [4], showed that the k-mean and subtractive clustering algorithms can be used for segmentation with good results. Good ability in segmentation is also shown in the case of segmentation in the case of AML subtype M4, M5, and M7, which uses the k-mean algorithm [20]. The k-mean algorithm is also used in image segmentation in cases of AML M2, M3, M4, and M5 leukemia diagnosis, and can give good results [21].

Referring to a number of studies that have been carried out to develop leukemia CAD models, at the segmentation stage, in choosing the segmentation method used, it is not explained in detail what the considerations are. Referring to the research conducted by Arumugadevi et al. [22] shows that the segmentation approach using clustering shows that the segmentation performance using FCM and SOM algorithms provides better performance than K-means. When referring to clustering performance using FCM and SOM, FCM is able to provide better clustering performance than SOM [23]. This shows that the selection of the segmentation method is very influential in producing the performance of the CAD system.

The low performance of the AML subtype diagnosis systems M0, M1, and M2 is not only influenced by the lack of accuracy in choosing the segmentation method, but also by the feature extraction method used for diagnosis. The diagnosis of AML M0, M1, and M2 developed in the study of Suryani et al. [24] using the features of WBC diameter, nucleus ratio, and nucleus roundness. These features are only able to provide an accuracy that is still below 80%. The analysis in this study showed that only WBC diameter could be used for features in the diagnosis of AML subtypes M0 and M1. Leukemia AML subtypes M0 and M1 are diagnosed by referring to what blast cells are dominant, each cell has different characteristics in size, shape, and color. A study conducted by Mutlag et al. [9], from feature extraction testing using leaf images, showed that the texture approach was able to provide better accuracy performance than the geometric, color, and statistical approaches. This is as shown in the research of Rawat et al. [25], where the feature extraction Gray level co-occurrence matrices (GLCM) is better than shape-based (geometry). GLCM capability is better than Local binary pattern (LBP) when combined with SVM classification algorithm, with histopathological Specimen image data [26].

Referring to previous research, this study aims to conduct a comparative study of segmentation performance with clustering, region growing, active contour, thresholding, and histogram approaches. The segmentation algorithm was used to segment WBC in cases of CAD leukemia AML subtypes M0, M1 and M2. The AML leukemia CAD model uses the GLCM feature extraction method. The performance of the

CAD system is measured using the parameters of accuracy, sensitivity, and specificity.

III. METHOD

This study uses WBC image data taken from The Hospital of Dr. Moewardi, Surakarta Indonesia. The WBC images analyzed were AML subtypes M0, M1, and M2. The total AML data used are 105 WBC images, consisting of 33 M0, 32 M1, and 40 M2. This research method uses a number of stages as shown in Fig. 1 where the main process is divided into four parts, namely pre-processing, segmentation, feature extraction, classification, and performance evaluation. At the segmentation stage, three segmentation approaches will be used as shown in Table I. The segmentation algorithm used for each approach is K-means, Fuzzy c-Means, SOM, watershed, chan vese (active contour), Otsu thresholding, and histogram.

TABLE I. SEGMENTATION APPROACH AND ALGORITHMS

No	Approach	Algorithms	References
1	Clustering-based	K-Means	[27]
		Fuzzy C-Means	[27]
		Self-Organizing Maps	[23]
2	Region-based	Chan Vese (Active Contour)	[28], [29]
		Watershed	[30]
3	Thresholding-based	Otsu Thresholding	[31], [32]
		Histogram	[33]–[35]

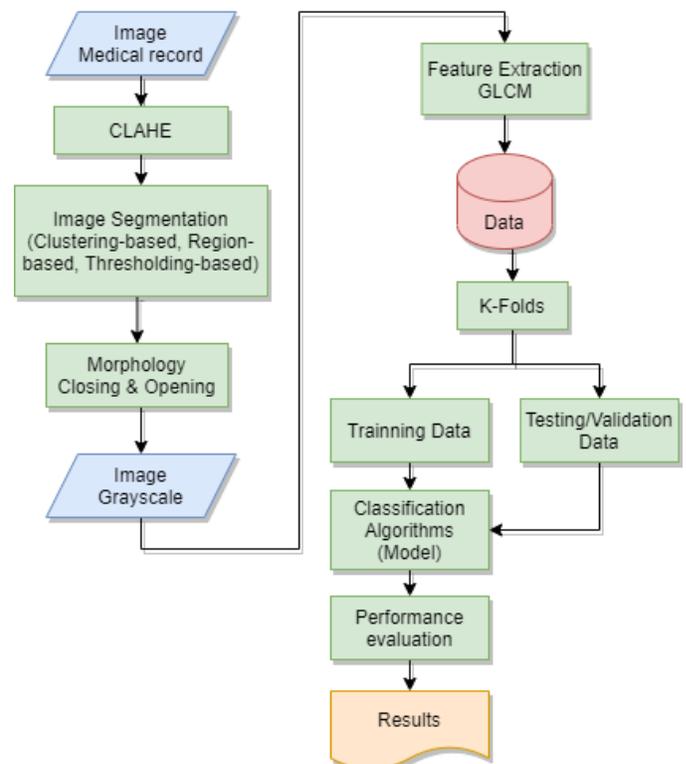


Fig. 1. Research Method.

The next step is feature extraction using Gray Level Co-occurrence Matrix (GLCM). GLCM is a texture analysis technique on the image. GLCM represents the relationship between neighboring 2-pixels that have grayscale intensity, distance, and angle. Distances (d) are expressed in pixels, while angles (θ) are in degrees. The distance between pixels is usually one pixel. The GLCM has 8 angles, including angles 0° , 45° , 90° , 135° , 180° , 225° , 270° , and 315° , in this study using angles 0° , 45° , 90° and 135° [25], [36], [37]. The resulting features for each angle are Contrast, Dissimilarity, Homogeneity, Energy, Correlation, and ASM [38]. These features can be shown in equations (1-7).

$$P(i, j) = NGLCM(i, j) \quad (1)$$

$$P(i, j) = \frac{GLCM(i, j)}{\sum_{i=0}^N \sum_{j=0}^M GLCM(i, j)}$$

$$Contrast = CT = \sum_{i=0}^N \sum_{j=0}^M (i - j)^2 P(i, j) \quad (2)$$

$$Dissimilarity = DS = \sum_{i=0}^N \sum_{j=0}^M |i - j| P(i, j) \quad (3)$$

$$Homogeneity = HG = \sum_{i=0}^N \sum_{j=0}^M \frac{P(i, j)}{1 + (i - j)^2} \quad (4)$$

$$ASM = \sum_{i=0}^N \sum_{j=0}^M [P(i, j)]^2 \quad (5)$$

$$Energy = EG = \sqrt{ASM} \quad (6)$$

$$Correlation = CR = \sum_{i=0}^N \sum_{j=0}^M \frac{(i - \mu_i)(j - \mu_j)P(i, j)}{\sigma_i \sigma_j} \quad (7)$$

The next step is to classify using a number of algorithms. The classification algorithms tested are SVM, Random Forest, decision tree, k-NN, and Naive Bayesian. The classification algorithm is applied to every angle in the feature extraction process with GLCM, the angles used are 0° , 45° , 90° , and 135° . The test is carried out using k-folds cross-validation, with the performance parameters measured are sensitivity, specificity, and accuracy. Performance calculation is done by referring to Table II, and by equation (8-10).

TABLE II. CONFUSION MATRIX

Actual Class	Predictive Class	
	Positive	Negative
Positive	TP	FN
Negative	FP	TN

$$Sensitivity = SEN = \frac{TP}{TP+FN} \quad (8)$$

$$Specificity = SPE = \frac{TN}{TN+FP} \quad (9)$$

$$Accuracy = ACC = \frac{TP+TN}{TP+FN+FP+TN} \quad (10)$$

IV. RESULTS

A. Result of Preprocessing

In the AML leukemia CAD system, before segmenting the WBC image, the steps taken are to improve the quality of the WBC image. Improvements were made using contrast limited adaptive histogram equalization (CLAHE) [39]. CLAHE is used to enhance the color and appearance of blurry objects in

an image. The results of preprocessing using CLAHE can be shown in Fig. 2.

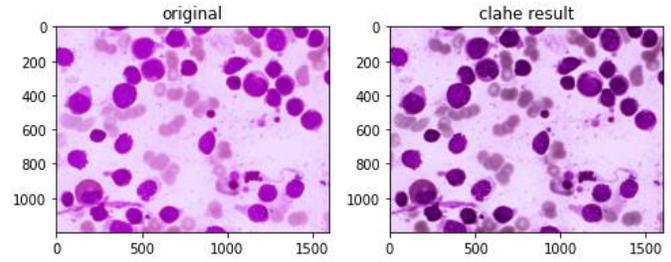


Fig. 2. Result of Preprocessing.

B. Result of Segmentation

This study uses three segmentation approaches, namely, cluster-based, region-based and thresholding-based. The segmentation algorithm for each approach is shown in Table I. In segmentation using the k-mean algorithm, the first step after the pre-processing process is to convert the image to grayscale. Segmentation is carried out with a maximum iteration value of 100 and epsilon 0.2. The clustering process carried out resulted in a total of four clusters. To separate the object with the background from the image resulting from clustering with four clusters, the separation process is carried out using the quartile value of the centroid. The quartile-1 value is used as the threshold value, if the tested pixels value is smaller than Quartile 1 than the centroid value, it is made white and vice versa. The results of the segmentation are then carried out by morphological closing and morphological opening processes [40] to smooth and eliminate noise in the image segmentation results. The complete results of the segmentation process with K-means are shown in Fig. 3. The concept for clustering using fuzzy c-means and SOM is almost the same as the k-means algorithm.

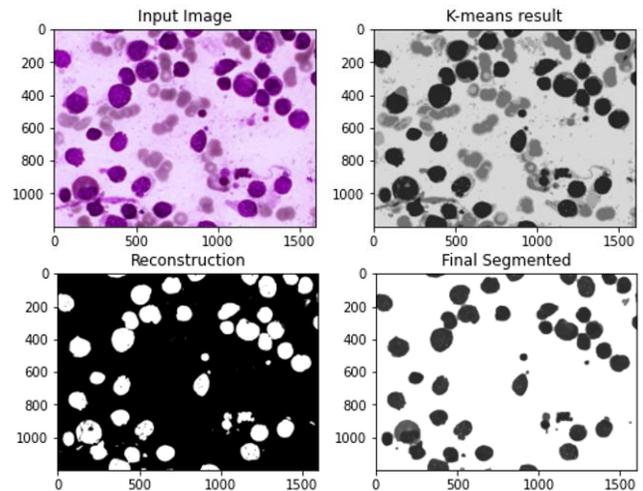


Fig. 3. The Results of the Segmentation Process with k-means.

The next segmentation model is using the thresholding approach. One of the algorithms in this approach is the histogram algorithm. In this algorithm, before the histogram process is carried out, the conversion to grayscale is done first. The grayscale image is then carried out by the histogram process so that it will produce the histogram value and bin

edges or the scale of the histogram boundary. In this study, 10 bin edges were used to form the histogram. From each edge, the middle value is searched for each edge and with this value, the quartile 1 value is sought, then used as the threshold value in separating the object from the background. The results of the segmentation are then carried out by morphological closing and morphological opening processes [40] to smooth out and eliminate noise in the image segmentation results. The results of segmentation using histograms can be shown in Fig. 4.

The next segmentation approach is a region growing. The segmentation algorithm used is Chan-Vese (active contour) [26],[27]. This algorithm is designed to group objects without clear boundaries. This algorithm is based on a set of levels developed iteratively to minimize the energy determined by a weighted value. This value corresponds to the sum of the intensity differences from the mean value outside the segmented region and a term that depends on the length of the segmented region boundary. In chan-veve active contours do not require a cropping process because of the nature of Region-based active contours that find lesions using the globalizing method [30], [41]. This is considered autonomous segmentation because the initial contour placement is the entire image and does not need to be defined [42]. The results of segmentation with the chan-veve algorithm can be shown in Fig. 5.

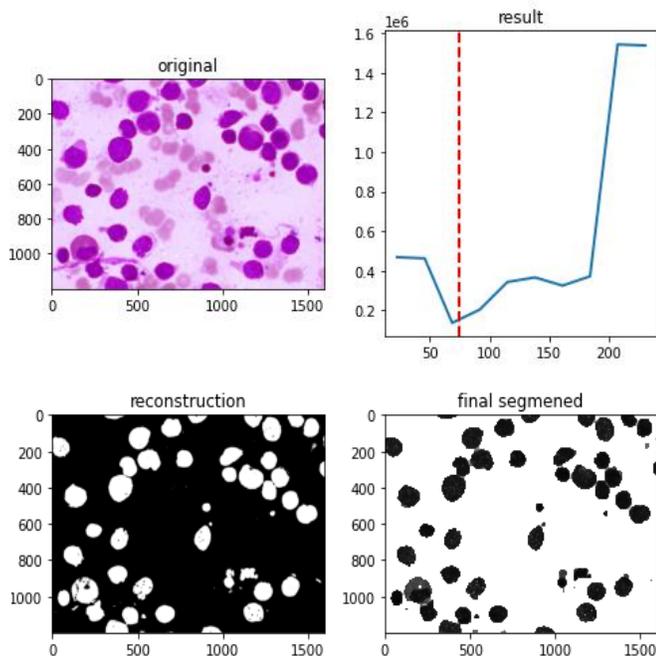


Fig. 4. Segmentation Results with Histogram.

Another region growing-based segmentation is watershed starting with conversion to grayscale, the grayscale image will then be processed using the otsu thresholding algorithm to separate objects from the background. Furthermore, morphological reconstruction is carried out to remove noise. The next stage is to find the border using the distance transform and label the peak of the object in the image, then the image will be processed by the watershed algorithm [28].

Then the results of the reconstruction are processed using morphology closing and opening morphology to smooth and remove noise in the reconstructed image. The final stage is to use the reconstructed image to take objects in the original image and convert the image to grayscale so that it is ready to be processed in the next stage. The results of this segmentation can be shown in Fig. 6.

C. Result of Feature Extraction

Feature extraction is done using the texture approach, namely by using the GLCM method. Image segmentation results will be carried out a feature extraction process with 6 features, namely Contrast, Dissimilarity, Homogeneity, Energy, Correlation, and ASM (Angular Second Moment). The GLCM method uses angles of 0° , 45° , 90° , and 135° . The results of feature extraction using GLCM at an angle of 0° , and when using the k-mean segmentation algorithm is shown in Table III. In Table III, 5 samples of each AML subtype M0, M1, and M2 are taken.

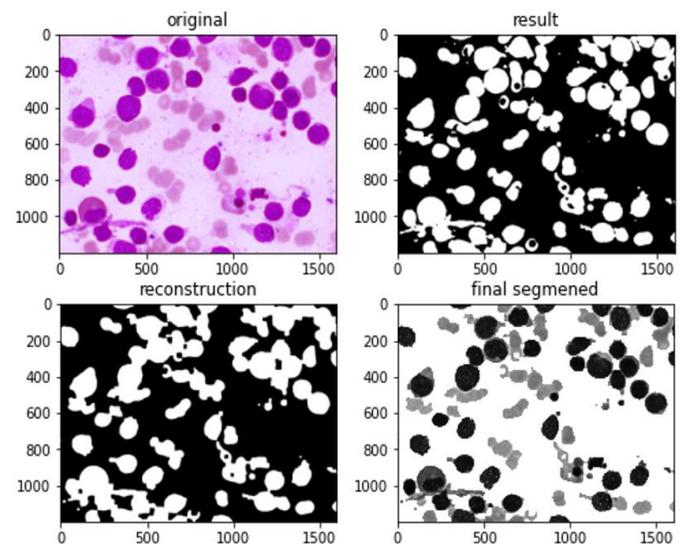


Fig. 5. Segmentation Results with Chan Verse Active Counter.

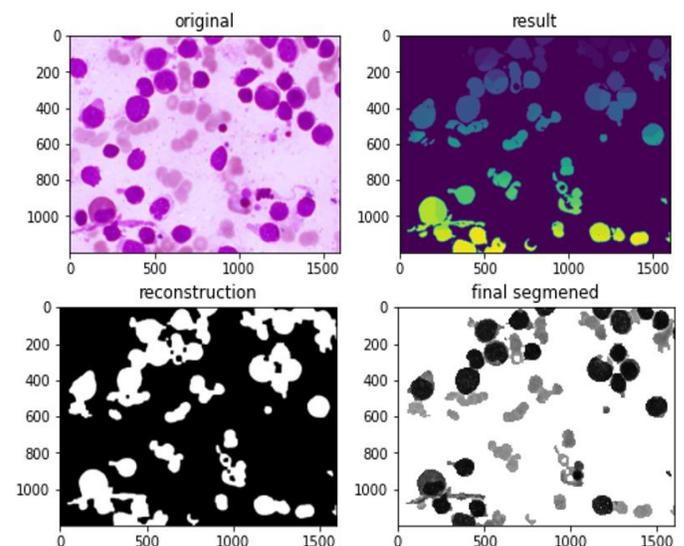


Fig. 6. Segmentation Results with Watershed.

TABLE III. EXAMPLE OF GLCM 0° FEATURE EXTRACTION RESULTS WITH K-MEANS SEGMENTATION

Type	CT	DS	HG	EG	CR	ASM
M0	1.3044	0.2308	0.9260	0.5198	0.9842	0.2702
M0	0.7966	0.1612	0.9460	0.6718	0.9882	0.4513
M0	0.5528	0.0961	0.9704	0.8087	0.9889	0.6540
M0	0.7719	0.1321	0.9603	0.7445	0.9871	0.5543
M0	0.5669	0.0987	0.9698	0.8123	0.9887	0.6599
M1	0.3386	0.0893	0.9671	0.8213	0.9911	0.6746
M1	0.4711	0.0944	0.9693	0.8097	0.9888	0.6556
M1	0.6201	0.1306	0.9564	0.7575	0.9870	0.5738
M1	0.3433	0.0727	0.9757	0.8558	0.9900	0.7324
M1	0.6437	0.1127	0.9668	0.8062	0.9839	0.6500
M2	0.5831	0.1225	0.9610	0.7209	0.9870	0.5197
M2	0.8049	0.1443	0.9568	0.6895	0.9847	0.4754
M2	0.8339	0.1592	0.9501	0.6409	0.9871	0.4107
M2	0.9491	0.1615	0.9525	0.6070	0.9865	0.3684
M2	1.0880	0.2081	0.9338	0.5733	0.9826	0.3287

D. Result of Classification

The stage after feature extraction is classification. At the classification stage, a number of classification algorithms were tested, namely support vector machine (SVM), Random Forest (RF), Decision Tree (DT), KNN, and Naïve Bayesian (NB). Performance parameters measured are accuracy, sensitivity, and specificity. Tests were carried out for each angle of the GLCM, namely angle 0°, 45°, 90°, and 135°. The test results for each angle with 5-fold cross-validation validation can be shown in Fig. 7 to Fig. 10.

Fig. 7 to Fig. 10 illustrates the performance of the CAD system when using GLCM feature extraction with the orientation angle, with values 0°, 45°, 90°, 135°. The feature extraction with GLCM will produce a co-occurrence matrix, which is a square matrix with the number of elements as much as the square of the number of pixel intensity levels in the image. Each point (p, q) in the co-occurrence matrix with orientation angle contains the probability of occurrence of a pixel worth p next door to a pixel worth q at a distance d and orientation θ and $(180^\circ-\theta)$. If the value is 0°, then the performance of the resulting CAD model is shown in Fig. 7, for the value of 45° is shown in Fig. 8, while the value of 90° and 135° are shown in Fig. 9 and Fig. 10. Fig. 7 to Fig. 10 shows that changing the orientation angle does not affect the performance of the SVM algorithm. The orientation angle of 135° can provide relatively the same performance for all types of classification algorithms, while angles of 0°, 45°, and 90° algorithms other than SVM provide poor performance. Especially for the SVM algorithm, the best performance is given at an orientation angle of 0°, when using the clustering and histogram segmentation algorithm.

Fig. 7 (GLCM with an angle of 0°) shows that the segmentation performance with histogram and k-means gives better performance than the others. Segmentation performance with clustering approach, SOM algorithm gives the lowest performance. Segmentation with thresholding approach, histogram algorithm is better than otsu thresholding, while in region growing approach, the watershed algorithm is better than chan vese. Fig. 7 to Fig. 10 shows that the performance of the classification algorithm that gives the best performance is SVM. At 135° GLCM angle, all tested classification algorithms give a good performance, while at other GLCM angles, the good performance is dominated by the SVM algorithm, while for the others it varies.

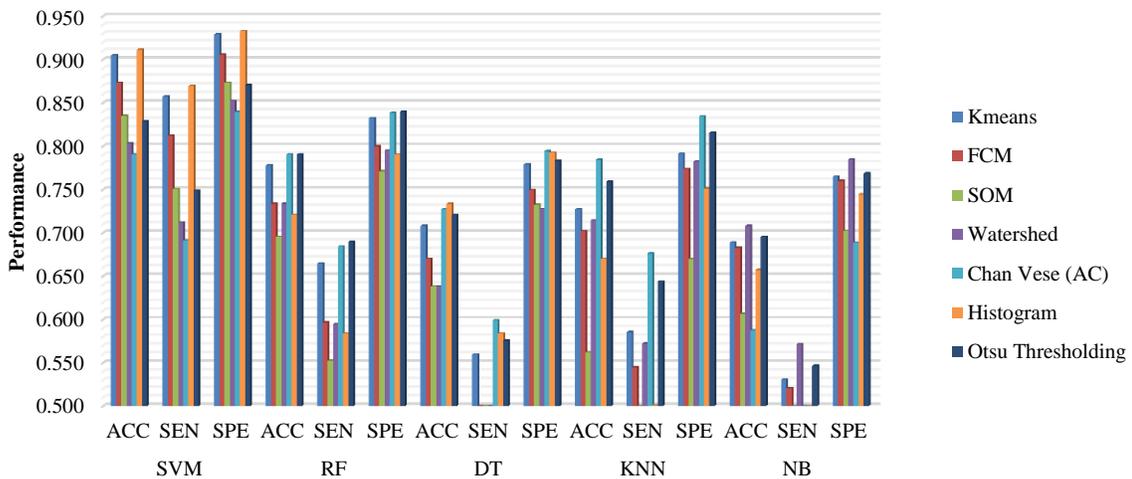


Fig. 7. Performance of Model using GLCM 0°

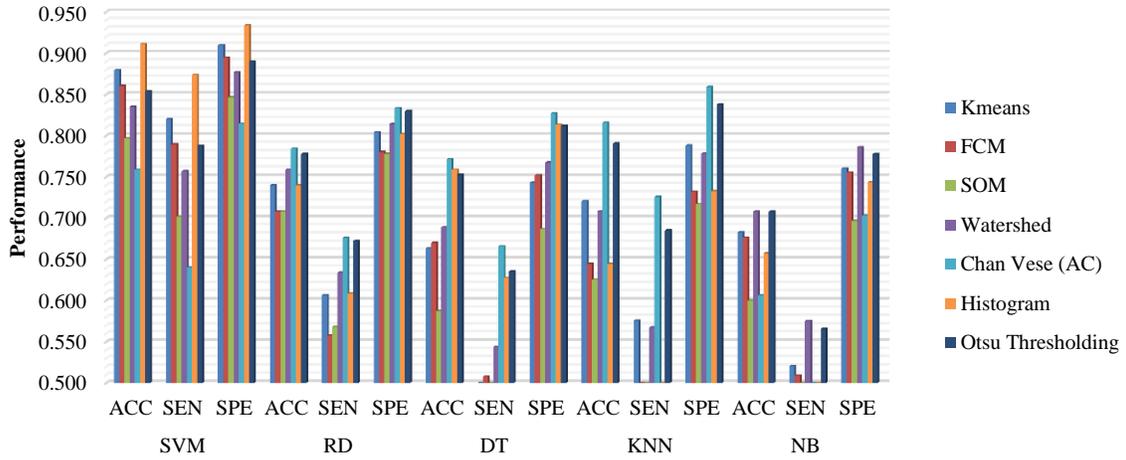


Fig. 8. Performance of Model using GLCM 45°

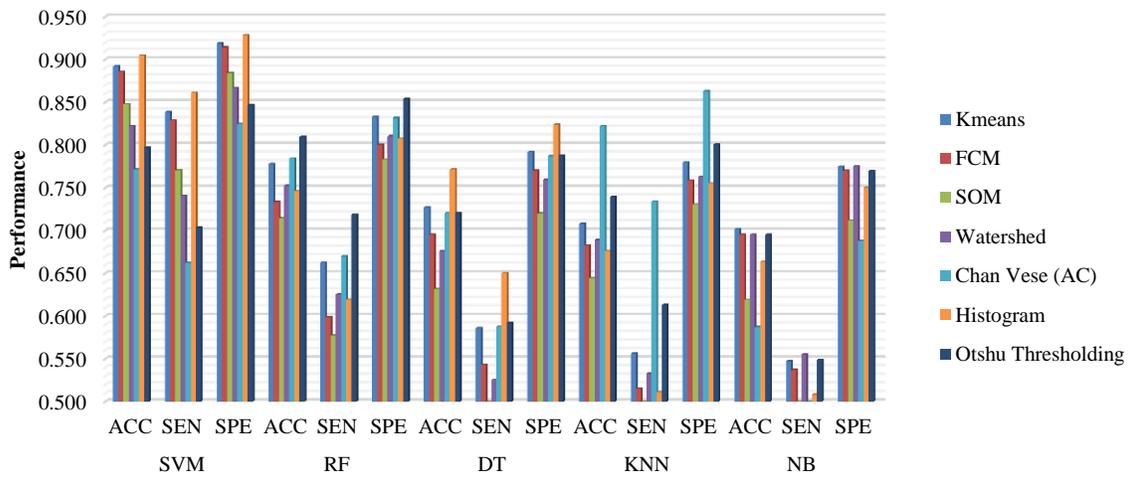


Fig. 9. Performance of Model using GLCM 90°

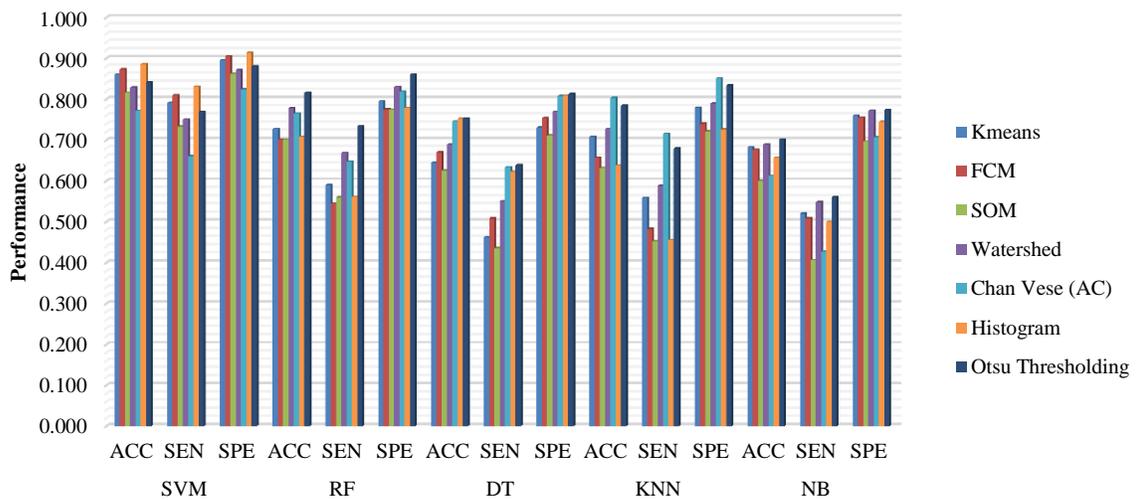


Fig. 10. Performance of Model using GLCM 135°

V. DISCUSSION

The test results of several segmentation algorithms show that the thresholding-based segmentation approach, by using the histogram method, is able to provide the best performance. The best performance is obtained, when using the SVM classification algorithm. Histogram segmentation is able to provide the best performance for all angles in GLCM when using SVM. The segmentation with the best clustering approach is given the k-means algorithm, which gives the best accuracy, for the GLCM angle of 0°, 45°, and 90°, while for the 135° angle the best performance is given by the FCM algorithm. The SOM algorithm gives the lowest performance between FCM and K-means. In the case of image segmentation of AML subtypes M0, M1, and M2, the segmentation approach that is less than optimal is shown in the region growing approach, with the Chan Vese (active contour) algorithm, where the performance for all GLCM angles is the lowest. Chan-ve's algorithm has weaknesses, namely, it is not able to divide non-uniform regions, and is sensitive to noise [43]. The Chan-Vese algorithm also has problems in terms of deviations from the class center in the Chan-Vese model. In particular, followed by inserting the energy function into the level set evolution without a re-initialization framework, the variation formulation can force the level set function to be closed to the object boundary [44].

The segmentation of the region growing approach generally shows less than optimal performance. This is not only shown by the performance of the Chan Vese algorithm, but also by the watershed algorithm. The watershed algorithm has a number of weaknesses, namely over-segmentation, manual intervention is needed, sensitivity to noise, and poor detection of significant areas with low contrast [45]. Weaknesses of the watershed algorithm confirmed the resulting performance in the diagnosis of AML leukemia subtypes M0, M1, and M2. This is different from segmentation with a thresholding approach. Histogram segmentation performance is able to provide the best classification results in the CAD system. This ability is caused by the dynamics of histogram segmentation in determining the threshold value, it's just that the weakness is when there is grayscale whose values overlap, so it becomes inaccurate [45].

The performance of computer-aided diagnosis of AML leukemia is not only influenced by the classification algorithm but also by the feature extraction algorithm used. Feature extraction GLCM is used to obtain features from the segmentation process. Comparison of values for each feature when using the GLCM angle of 0° and using the histogram segmentation method can be shown in Table IV. Table IV shows that the mean ± STD of each feature between M0, M1, and M2 has almost the same value. Referring to Table IV and supported by statistical test results, shows several features that are not significantly different between M0, M1, and M2 (p-value>0.05). The results of statistical tests with a 95% confidence level for GLCM with an angle of 0° in the complete histogram segmentation are shown in Table IV. This condition causes the results of classification, especially using algorithms other than SVM, the results are not optimal. This means that some features cannot be used to distinguish AML subtypes of leukemia M0, M1, and M2.

TABLE IV. COMPARISON OF FEATURES ON GLCM 0° (HISTOGRAM)

Feature	M0	M1	M2
	Mean±STD	Mean±STD	Mean±STD
Contrast	0.870±0.248	0.543±0.229	0.797±0.242
Dissimilarity	0.159±0.044	0.114±0.043	0.144±0.043
Homogeneity	0.950±0.015	0.962±0.014	0.956±0.014
Energy	0.681±0.097	0.773±0.093	0.687±0.103
Correlation	0.987±0.002	0.988±0.003	0.986±0.002
ASM	0.472±0.127	0.606±0.138	0.482±0.146

TABLE V. STATISTICS TEST ON GLCM 0° (HISTOGRAM)

Feature	P-value		
	M0 x M1	M0 x M2	M1 x M2
Contrast	0.000	0.169	0.000
Dissimilarity	0.000	0.100	0.007
Homogeneity	0.002	0.066	0.087
Energy	0.000	0.598	0.001
Correlation	0.110	0.035	0.000
ASM	0.000	0.574	0.001

The ability of the histogram segmentation algorithm, when viewed from the results of the significance test with a 95% confidence level, is not the best. This is indicated by the comparison between M0xM1, M0xM2, and M1xM2 features, the number of different features is significantly less compared to segmentation using k-means. Feature extraction, which was preceded by segmentation using K-means, was able to produce a feature correlation to distinguish AML M0 from AML M1, while the histogram could not differentiate. Feature correlation shows the size of the linear relationship of the neighboring pixel gray-level values.

The ability of the histogram and k-means segmentation algorithms, when viewed from statistical tests on features generated from GLCM, shows that the ability to distinguish AML M0 from AML M2 is less than optimal. Referring to Table V, only the correlation features have a significant difference, while the other features are not significantly different. In addition to feature correlation, feature homogeneity is also relatively able to distinguish, compared to other features. This condition shows that there is a close texture between M0 and M2, so it is not optimal when using the six GLCM features. Overall the performance generated when using histogram segmentation with GLCM angle 0°, the area under the curve (AUC) value [46] is above 90%, which is included in the very good category [47].

The Chan-ve's algorithm produces the lowest classification performance; this is confirmed from the results of the significance test with a confidence level of 96%, where many features generated from GLCM cannot show significant differences over M0xM1, M0xM2, and M1xM2. The test results for Chan-ve's segmentation with a GLCM angle of 0° can be shown in Table VI. In Table VI, it is shown that the features generated when using the Chan-ve's segmentation algorithm can distinguish significantly between M0, M1, and

M2, only two features, namely contrast, and dissimilarity, while for feature dissimilarity it cannot distinguish between M1xM2.

TABLE VI. STATISTICS TEST ON GLCM 0^0 (CHAN VESE)

Feature	P-value		
	M0xM1	M0xM2	M1xM2
Contrast	0.000	0.000	0.003
Dissimilarity	0.003	0.005	0.961
Homogeneity	0.132	0.054	0.544
Energy	0.397	0.928	0.354
Correlation	0.258	0.874	0.218
ASM	0.406	0.883	0.412

VI. CONCLUSION

The results of the comparison of the performance of the segmentation method based on clustering, thresholding, and region growing show that the Histogram algorithm gives the best performance. The best performance is obtained when using the SVM classification algorithm. Performance can also be seen from the features generated from GLCM, the results of the significance test show the performance of K-mean and Histogram capable of producing features that can distinguish AML M0, M1, and M2 leukemia. The conclusion that can be drawn is that histogram and k-means segmentation algorithms can be an alternative segmentation method in cases of CAD leukemia AML.

ACKNOWLEDGMENT

We would like to thank the National Research and Innovation Agency of the Republic of Indonesia (BRIN) for providing research funding under the Basic Research Grant scheme with Contract No.: 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] N. Sharma and A. Verma, "Segmentation-and-Detection-of-Optic-Disc-Using-Kmeans-Clustering.docx," *International Journal of Scientific & Engineering Research*, vol. 6, no. 8, pp. 237–240, 2015.
- [2] P. Sharma and J. Suji, "A Review on Image Segmentation with its Clustering Techniques," *International Journal of Signal Processing, Image Processing and Pattern Recognition*, vol. 9, no. 5, pp. 209–218, 2016, doi: 10.14257/ijsp.2016.9.5.18.
- [3] S. Yuheng and Y. Hao, "Image Segmentation Algorithms Overview," *ArXiv*, pp. 1–6, 2017.
- [4] N. Dhanachandra, K. Mangle, and Y. J. Chanu, "Image Segmentation Using K-means Clustering Algorithm and Subtractive Clustering Algorithm," *Procedia Computer Science*, vol. 54, pp. 764–771, 2015, doi: 10.1016/j.procs.2015.06.090.
- [5] N. Dhanachandra and Y. J. Chanu, "A Survey on Image Segmentation Methods using Clustering Techniques," *European Journal of Engineering Research and Science*, vol. 2, no. 1, p. 15, 2017, doi: 10.24018/ejers.2017.2.1.237.
- [6] N. Dhanachandra and Y. J. Chanu, "A new approach of image segmentation method using K-means and kernel based subtractive clustering methods," *International Journal of Applied Engineering Research*, vol. 12, no. 20, pp. 10458–10464, 2017.

- [7] A. Humeau-Heurtier, "Texture Feature Extraction Methods: A Survey," *IEEE Access*, vol. 7, pp. 8975–9000, 2019, doi: 10.1109/ACCESS.2018.2890743.
- [8] S. A. Medjahed, "A Comparative Study of Feature Extraction Methods in Images Classification," *IJIGSP*, vol. 7, no. 3, pp. 16–23, Feb. 2015, doi: 10.5815/ijigsp.2015.03.03.
- [9] W. K. Mutlag, S. K. Ali, Z. M. Aydam, and B. H. Taher, "Feature Extraction Methods: A Review," *J. Phys.: Conf. Ser.*, vol. 1591, p. 012028, Jul. 2020, doi: 10.1088/1742-6596/1591/1/012028.
- [10] Ahmed, Yigit, Isik, and Alpkocak, "Identification of Leukemia Subtypes from Microscopic Images Using Convolutional Neural Network," *Diagnostics*, vol. 9, no. 3, pp. 1–11, Aug. 2019, doi: 10.3390/diagnostics9030104.
- [11] 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," in *Proceedings of 2017 International Conference on Data and Software Engineering, ICoDSE 2017*, Palembang, Indonesia, 2018, vol. 2018-Janua, pp. 1–6. doi: 10.1109/ICODSE.2017.8285851.
- [12] 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.
- [13] E. Suryani, E. I. Asmari, and B. Harjito, "Image Segmentation of Acute Myeloid Leukemia Using Multi Otsu Thresholding," *J. Phys.: Conf. Ser.*, vol. 1803, no. 1, p. 012016, Feb. 2021, doi: 10.1088/1742-6596/1803/1/012016.
- [14] E. Suryani, Wiharto, A. P. Putra, and W. Widiarto, "Detection of Acute Myeloid Leukemia Based on White Blood Cell Morphological Imaging Using Naive Bayesian Algorithm," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 10, pp. 244–251, 2021.
- [15] T. Z. T. Muda and R. A. Salam, "Comparative Analysis on Blood Cell Image Segmentation," presented at the 2nd International Symposium on Computer, Communication, Control and Automation, Singapore, 2013. doi: 10.2991/3ca-13.2013.115.
- [16] S. Chand and V. P. Vishwakarma, "Comparison of Segmentation Algorithms for Leukemia Classification," presented at the Proceedings of the FIST International Conference on Advanced Scientific Innovation in Science, Engineering and Technology, ICASISSET 2020, 16-17 May 2020, Chennai, India, Chennai, India, 2021. doi: 10.4108/eai.16-5-2020.2303967.
- [17] A. Harjoko, T. Ratnaningsih, E. Suryani, Wiharto, S. Palgunadi, and N. P. T. Prakisy, "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.
- [18] W. Wiharto and E. Suryani, "The Analysis Effect of Cluster Numbers On Fuzzy C-Means Algorithm for Blood Vessel Segmentation of Retinal Fundus Image," p. 5, 2019.
- [19] W. Wiharto, E. Suryani, and M. Susilo, "The Hybrid Method of SOM Artificial Neural Network and Median Thresholding for Segmentation of Blood Vessels in the Retina Image Fundus," *IJFIS*, vol. 19, no. 4, pp. 323–331, Dec. 2019, doi: 10.5391/IJFIS.2019.19.4.323.
- [20] N. Khomairroh, R. Sigit, T. Harsono, Y. Hernaningsih, and A. Anwar, "Segmentation System of Acute Myeloid Leukemia (AML) Subtypes on Microscopic Blood Smear Image," in *2020 International Electronics Symposium (IES)*, Surabaya, Indonesia, Sep. 2020, pp. 565–570. doi: 10.1109/IES50839.2020.9231651.
- [21] F. Kazemi, T. Najafabadi, and B. Araabi, "Automatic recognition of acute myelogenous leukemia in blood microscopic images using K-means clustering and support vector machine," *J Med Signals Sens*, vol. 6, no. 3, p. 183, 2016, doi: 10.4103/2228-7477.186885.
- [22] S. Arumugadevi and V. Seenivasagam, "Comparison of Clustering Methods for Segmenting Color Images," *Indian Journal of Science and Technology*, vol. 8, no. 7, pp. 670–677, Apr. 2015, doi: 10.17485/ijst/2015/v8i7/62862.

- [23] S. A. Mingoti and J. O. Lima, "Comparing SOM neural network with Fuzzy c-means, K-means and traditional hierarchical clustering algorithms," *European Journal of Operational Research*, vol. 174, no. 3, pp. 1742–1759, 2006, doi: 10.1016/j.ejor.2005.03.039.
- [24] 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.
- [25] J. Rawat, A. Singh, H. S. Bhadauria, and J. Virmani, "Computer Aided Diagnostic System for Detection of Leukemia Using Microscopic Images," *Procedia Computer Science*, vol. 70, pp. 748–756, 2015, doi: 10.1016/j.procs.2015.10.113.
- [26] Ş. Öztürk and B. Akdemir, "Application of Feature Extraction and Classification Methods for Histopathological Image using GLCM, LBP, LBGLCM, GLRLM and SFTA," *Procedia Computer Science*, vol. 132, pp. 40–46, 2018, doi: 10.1016/j.procs.2018.05.057.
- [27] S. Ghosh and S. Kumar, "Comparative Analysis of K-Means and Fuzzy C-Means Algorithms," *International Journal of Advanced Computer Science and Applications*, vol. 4, no. 4, 2013, doi: 10.14569/ijacsa.2013.040406.
- [28] A. A. Yahya, J. Tan, and M. Hu, "A Novel Model of Image Segmentation Based on Watershed Algorithm," *Advances in Multimedia*, vol. 2013, pp. 1–8, 2013, doi: 10.1155/2013/120798.
- [29] S. Li and Q. Zhang, "Fast Image Segmentation Based on Efficient Implementation of the Chan-Vese Model with Discrete Gray Level Sets," *Mathematical Problems in Engineering*, vol. 2013, pp. 1–16, 2013, doi: 10.1155/2013/508543.
- [30] X.-F. Wang, D.-S. Huang, and H. Xu, "An efficient local Chan–Vese model for image segmentation," *Pattern Recognition*, vol. 43, no. 3, pp. 603–618, Mar. 2010, doi: 10.1016/j.patcog.2009.08.002.
- [31] M. A. Ansari and S. K. Mahraj, "A Robust Method for Identification of Paper Currency Using Otsu's Thresholding," *2018 International Conference on Smart Computing and Electronic Enterprise, ICSCEE 2018*, pp. 1–5, 2018, doi: 10.1109/ICSCEE.2018.8538424.
- [32] J. Delon, A. Desolneux, J.-L. Lisani, and A. B. Petro, "A Nonparametric Approach for Histogram Segmentation," *IEEE Trans. on Image Process.*, vol. 16, no. 1, pp. 253–261, Jan. 2007, doi: 10.1109/TIP.2006.884951.
- [33] H. T. A. Wahhab, "Classification of Acute Leukemia Using Image Processing and Machine Learning Techniques," *Disertation, University of Malaya, Malaysia*, 2015.
- [34] P. D. R. Raju and G. Neelima, "Image Segmentation by using Histogram Thresholding," *International Journal of Computer Science Engineering and Technology*, vol. 2, no. 1, pp. 776–779, 2012.
- [35] K. Qin, K. Xu, F. Liu, and D. Li, "Image segmentation based on histogram analysis utilizing the cloud model," *Computers & Mathematics with Applications*, vol. 62, no. 7, pp. 2824–2833, Oct. 2011, doi: 10.1016/j.camwa.2011.07.048.
- [36] F. Asadi, F. M. Putra, M. Indah Sakinatunnisa, F. Syafria, Okfalisa, and I. Marzuki, "Implementation of Backpropagation Neural Network and Blood Cells Imagery Extraction for Acute Leukemia Classification," in *2017 5th International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME)*, Bandung, Nov. 2017, pp. 106–110. doi: 10.1109/ICICI-BME.2017.8537755.
- [37] Y. Jusman, L. A. Dewiprabamukti, A. N. N. Chamim, Z. Mohamed, S. N. A. M. Kanafiah, and N. H. A. Halim, "Application of Watershed Algorithm and Gray Level Co-Occurrence Matrix in Leukemia Cells Images," in *2020 3rd International Conference on Mechanical, Electronics, Computer, and Industrial Technology (MECnIT)*, Medan, Indonesia, Jun. 2020, pp. 9–14. doi: 10.1109/MECnIT48290.2020.9166651.
- [38] A. R. Zubair and O. A. Alo, "Grey Level Co-occurrence Matrix (GLCM) Based Second Order Statistics for Image Texture Analysis," *International Journal of Science and Engineering Investigations*, vol. 8, no. 93, pp. 64–73, 2019.
- [39] P. Musa, F. A. Rafi, and M. Lamsani, "A Review: Contrast-Limited Adaptive Histogram Equalization (CLAHE) methods to help the application of face recognition," in *2018 Third International Conference on Informatics and Computing (ICIC)*, Palembang, Indonesia, Oct. 2018, pp. 1–6. doi: 10.1109/IAC.2018.8780492.
- [40] D. Sundararajan, "Morphological Image Processing," in *Digital Image Processing*, Singapore: Springer Singapore, 2017, pp. 217–256. doi: 10.1007/978-981-10-6113-4_8.
- [41] M. Mustafa, H. Najwa Omar Rashid, N. Rul Hasma Abdullah, R. Samad, and D. Pebrianti, "Mammography Image Segmentation: Chan-Vese Active Contour and Localised Active Contour Approach," *IJECS*, vol. 5, no. 3, p. 577, Mar. 2017, doi: 10.11591/ijeecs.v5.i3.pp577-583.
- [42] T. F. Chan, B. Y. Sandberg, and L. A. Vese, "Active Contours without Edges for Vector-Valued Images," *Journal of Visual Communication and Image Representation*, vol. 11, no. 2, pp. 130–141, Jun. 2000, doi: 10.1006/jvci.1999.0442.
- [43] L. Wang and H. Fan, "Segmentation of Ultrasonic Images Based on Modified Chan-Vese algorithm," in *Proceedings of the 6th International Conference on Electronic, Mechanical, Information and Management Society, Shenyang, China*, 2016, pp. 710–714. doi: 10.2991/emim-16.2016.147.
- [44] D. Zhou, H. Zhou, and Y. Shao, "An improved Chan–Vese model by regional fitting for infrared image segmentation," *Infrared Physics & Technology*, vol. 74, pp. 81–88, Jan. 2016, doi: 10.1016/j.infrared.2015.12.003.
- [45] R. Sarma and Y. K. Gupta, "A comparative study of new and existing segmentation techniques," *IOP Conf. Ser.: Mater. Sci. Eng.*, vol. 1022, p. 012027, Jan. 2021, doi: 10.1088/1757-899X/1022/1/012027.
- [46] E. Ramentol, Y. Caballero, R. Bello, and F. Herrera, "SMOTE-RSB *: A hybrid preprocessing approach based on oversampling and undersampling for high imbalanced data-sets using SMOTE and rough sets theory," *Knowledge and Information Systems*, vol. 33, no. 2, pp. 245–265, 2012, doi: 10.1007/s10115-011-0465-6.
- [47] F. Gorunescu, *Data Mining: Concepts, Models and Techniques*. Berlin, Heidelberg: Springer, 2011.

EC-Elastic an Explicit Congestion Control Mechanism for Named Data Networking

Asmaa EL-BAKKOUCHI¹, Mohammed EL GHAZI²
Anas BOUAYAD³, Mohammed FATTAH⁴, Moulhime EL BEKKALI⁵
Artificial Intelligence, Data Sciences and Emerging Systems Laboratory
Sidi Mohamed Ben Abdellah University, Fez, Morocco^{1, 2, 3, 5}
IMAGE Laboratory, Moulay Ismail University, Meknes, Morocco⁴

Abstract—In recent years, Named Data Networking (NDN) has attracted researchers' attention as a new internet architecture. NDN changes the internet communication paradigm from a host-to-host IP model to a name-based model. Thus, NDN permits the retrieval of requested content by name, from different sources and via multiple paths, and the use of caching in intermediate routers. These features transform the transport control model from sender to receiver and make traditional end-to-end congestion control mechanisms incompatible with NDN architecture. To deal with this problem, a reliable congestion control mechanism becomes necessary for a successful deployment of NDN. This paper presents a new hybrid congestion control mechanism for NDN, EC-Elastic (Explicit Congestion Elastic), which adopts the basic concept of Elastic-TCP to control the sending rates of the interest packets at the consumer nodes. In the intermediate nodes, a queue has been associated with the Controlled Delay-Active Queue Management CoDel-AQM to measure the packet sojourn time and notify the consumer to decrease its interest packet sending rate when it receives an explicit congestion signal. EC-Elastic was implemented in ndnSIM and evaluated with Agile-SD, CUBIC, and STCP in different scenarios. Simulation results show that EC-Elastic provides a significant improvement in bandwidth utilization while maintaining lower delay and packet loss rates.

Keywords—NDN; named data networking; congestion control; explicit congestion control; TCP-elastic

I. INTRODUCTION

The use of the internet has grown exponentially from point-to-point communications to the distribution of information everywhere. This growth has increased the number of internet users where these users are more interested in getting data in a short period of time than the location of that data. To facilitate connectivity between these users, high-speed and long-distance networks have been widely employed in many countries [1] [2]. However, this evolution poses some problems, namely, the current Transmission Control Protocol/Internet Protocol TCP/IP internet architecture and its variants have seen poor performance [3], and cannot cope with this growth, as they are designed for end-to-end communications. The use of high speed and long distance networks requires consideration of two major problems that are often encountered in this type of environment and that affect network performance negatively. The first problem concerns the use of large buffer regimes and long distances which leads to very long RTTs while the second problem concerns the need to increase the congestion window

(cwnd) as much as possible to maximize the use of available bandwidth.

The first problem concerning the current TCP/IP internet architecture has motivated the researchers to explore new architectures for the future internet [4]. Information-Centric Networking (ICN) [5] has been proposed as a new content-centric internet architecture to replace the current host-centric internet architecture. ICN has proposed several architectures that are all based on the content name rather than the IP address. Among these architectures, Named Data Networking (NDN) [6], an important research topic that has quickly encountered considerable interest from researchers. NDN uses hierarchical names to exchange two types of packets (interest packets and data packets [6]) between consumers and content producers. A consumer requests content via an interest packet, and then any node that has the requested data sends it through a data packet. These data packets follow the reverse path of interest packets. Each NDN node has three components, namely Content Store (CS), Pending Interest Table (PIT) and Forwarding Information Base (FIB) as shown in Fig. 1. Content Store (CS) : works as a content cache [7]. When CS receives data packets, it can store them temporarily in a cache and use them again in case of a request for the same data [8]. Pending Interest Table (PIT): The PIT contains interests that have been transmitted upstream but have not yet been satisfied [7]. It also contains the incoming interface list from which the interest packet for that name was received and the outgoing interface list from which the interest packet was sent [8]. Forwarding Information Base (FIB) : This is a database that contains prefix names for identifying the location of content producers, and an interfaces list for determining which interface is needed to forward the interest packet [8].

The NDN architecture has new features such as connectionless, one-interest-one-data, caching, multipath and multi-source. However, these features complicate network congestion control, because the existing TCP/IP solutions cannot be applied directly in NDN, which made congestion control an active research topic to be studied. The different characteristics between the two architectures (NDN and TCP/IP) mainly lie in:

- In NDN, communication is receiver-based and connectionless, whereas in TCP/IP it is connection-oriented between two end points.

- NDN uses a One-Interest-One-Data transport mode, the consumer is responsible for retransmitting the interest packet if the desired data is not received. There are no duplicate data acknowledgement (ACKs) as in TCP/IP.
- NDN uses caching in intermediate nodes to satisfy requests from all consumers rather than a single content source used by TCP/IP.
- The use of caching in NDN nodes allows desired data to be fetched from several sources and over several paths, which complicates the use of RTO (Retransmission Time Out) in NDN congestion control as it is intended for single-source TCP/IP communication [9].

These challenges have motivated the research community to design and develop new mechanisms for NDN networks that are able to avoid congestion, increase the use of available bandwidth while maintaining fast delivery time. However, the majority of existing mechanisms in NDN are based on the AIMD mechanism which can prevent full utilization of the available bandwidth due to the huge bandwidth-delay product (BDP: Bandwidth-Delay Product refers to the maximum quantity of data that can be sent over a link or network) in high-speed and long-distance networks, making it a waste of network resources [1] because AIMD takes a long time to reach the maximum capacity of the network links, which leads to underutilization of the bandwidth. Moreover, in case of congestion, AIMD divides the congestion window by 2, which requires more time to reach the maximum throughput again and consequently, the link performance is degraded.

To address the second problem concerning large buffer regimes and very long RTTs, this paper proposes a new hybrid congestion control mechanism for NDN named Explicit Congestion Elastic (EC-Elastic), which adapts the basic idea of Elastic-TCP [1] to control the sending rate of interest packets at the consumer nodes. EC-Elastic uses the Window-correlated Weighting Function WWF that aims to improve the bandwidth utilization of the network. In intermediate routers, EC-Elastic uses a CoDel-AQM queue for each prefix on each interface to measure packet sojourn time. This algorithm allows routers, which have a large buffer, to absorb traffic bursts and to reduce its queues through detecting congestion before the buffer is full [10] then explicitly signals congestion to inform consumers to reduce their traffic rate.

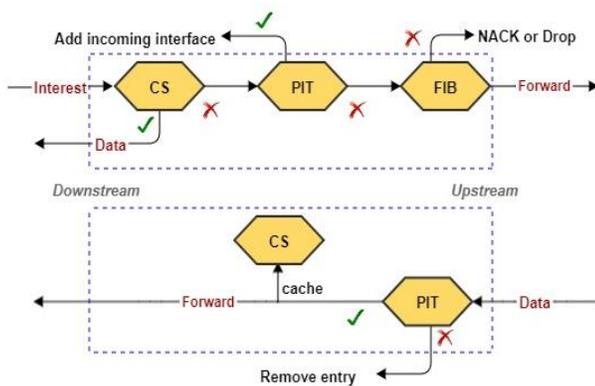


Fig. 1. Forwarding Process at NDN Node.

The rest of the paper is organized as follows: Section II presents the related work while Section III presents the principle of congestion control. Section IV details the proposed "EC-Elastic" mechanism and Section V evaluates the performance of this mechanism, it presents the topologies and measurements used as well as the results and discussion. Finally, Section VI concludes the paper.

II. RELATED WORK

In the literature, several congestion control mechanisms have been proposed for NDN networks. According to [11], these mechanisms can be classified into three categories: Receiver-based method: which is characterized by detecting congestion and controlling the sending rate of interest packets only at the consumer nodes [7]. Hop-by-hop method: which is characterized by detecting congestion and controlling the sending rate of interest packets at each intermediate node [12]. Hybrid method: which is characterized by detecting and controlling congestion at both receiver nodes and intermediate nodes [7] [12].

In NDN, the majority of congestion control mechanisms are inherited from TCP's window-based mechanisms, and most of them adjust the size of their congestion window based on the Additive Increase Multiplicative Decrease (AIMD) mechanism that increases the congestion window by Additive Increase (AI) and decreases the congestion window by Multiplicative Decrease (MD). Specifically, the authors of [13] propose ICP (Interest Control Protocol) a receiver-based congestion control mechanism that detects congestion by measuring the delay and timer expirations and adjusts the congestion window size by AIMD mechanism. The authors of [14] propose ICTP (Information Centric Transport Protocol) which also detects congestion by RTO Timeout and adjusts the congestion window size by AIMD mechanism. These two mechanisms did not consider the case of multiple source scenarios. To solve this problem, the authors of [15] propose a mechanism named ConTug that detects congestion using an RTO value for each content source and then adjusts the size of congestion window by AIMD mechanism. However, the authors of [16] propose CCTCP (Content Centric TCP) which instead of using a single RTO value for each content source, it uses a separate RTO value for each data source and then adjusts the congestion window size by AIMD mechanism. On the other hand, the authors of [17] propose predictive which maintains an RTO value for each Content Store to detect congestion and then uses the AIMD mechanism to adjust the congestion window size. In [18], the authors propose a Hop-by-hop Receiver-driven Interest Control Protocol (HR-ICP), which at the router level detects congestion using a virtual queue and then depending on the state of this queue, the consumer nodes use the AIMD mechanism to adjust the congestion window size. Other authors proposed CVUnion in [19] which detects congestion at intermediate nodes through the calculation of the average queue length of the interest packets, then once the consumer receives the feedback, it adjusts its congestion window size by the AIMD mechanism. In [20], the authors propose CHoPCoP (Chunk-switched Hop Pull Control Protocol) which detects congestion at intermediate nodes by monitoring the queue size of outgoing data packets, and then, based on the queue size, an explicit congestion notification is sent to the consumer to

adjust the congestion window size through the AIMD mechanism. The authors of [21] propose Stateful Forwarding which detects congestion by calculating the limit rate of interest packets. Stateful Forwarding generates a Negative-ACKnowledgment NACK packet that will be sent on downstream when congestion is detected. Once the downstream router receives this NACK packet, and depending on the received link state, it uses the AIMD mechanism to adjust the size of the congestion window. However, the authors of [22] [23] detected problems with the use of NACK, namely the delay in transmitting the NACK between two routers, which results in an excessive reduction in the sending rate of interest packets. Therefore, the authors propose to use three states for each interface which are, normal, congestion and check, and depending on the state of the network, the AIMD mechanism is used to adjust the congestion window size. Other authors propose to combine the multipath forwarding strategy with congestion control as in [24] where the authors deployed the forwarding strategy at the intermediate routers and the AIMD mechanism at the consumer nodes. In [25], the authors propose Standby which controls congestion in three steps: Accurate Local Congestion detection, Hop-by-hop congestion notification and Multipath strategy congestion avoidance and adjusts the congestion window size with AIMD mechanism.

In the congestion avoidance phase, AIMD increases the congestion window by $1/cwnd$. In the case of short distance, $cwnd$ is small, so the congestion window increase will be rapid and reasonable. However, in the case of long distance, $cwnd$ is large and therefore the congestion window increase will be slow. In addition, in the case of congestion, AIMD uses a Multiplicative Decrease which divides the congestion window by 2 and moves to the next phase, where the congestion window will be increased by Additive Increase to reach again the $cwnd$ maximum. In the case of short distance where the RTTs are small, this method provides acceptable throughput and reasonable bandwidth utilization. However, in the case of long distance where the RTTs are very large, this method takes too much time to reach again the maximal $cwnd$ which results in low throughput and bandwidth utilization and consequently degrades the link performance.

To address these issues, this paper proposes EC-Elastic, a Hybrid congestion control mechanism to avoid congestion, increase bandwidth utilization on long delays and high-BDP networks and achieve efficient data delivery. EC-Elastic adapts the basic idea of Elastic-TCP [8] to control the rate at which the interest packets are sent to consumer nodes. EC-Elastic controls congestion in three phases; congestion detection at intermediate routers using CoDel-AQM, then explicitly signaling congestion to inform consumers to reduce their traffic rate, and finally adjusting the congestion window based on the type of packet received by consumers.

III. PRINCIPLE OF CONGESTION CONTROL

To support high-speed applications (e.g., large-scale data transfer) and low-latency applications in NDN networks, we need a congestion control mechanism. This mechanism should contain the following steps: "Congestion detection", "Congestion signaling" and "Congestion window size adjustment". The description of each step is described above:

A. Congestion Detection

Data transfer can saturate queues, which degrades quality of service in the network. The deployment of an AQM strategy is necessary. In the literature, many AQM algorithms have been proposed such as Drop-Tail [26], RED (Random Early Detection) [27], CoDel [28] or PIE (Proportional Integral controller Enhanced) [29]. The basic idea behind these algorithms is that the current queue length is not an indication of congestion as it can be caused by bursty traffic [30].

Drop-Tail [26] was proposed as the first algorithm to solve queue management problems. This algorithm works as follows: Each queue's length is fixed at a maximum value known as the maximum packet length, and user's incoming packets will be stored in this queue. When the length of the queue hits the maximum limit, the incoming packets will be dropped. Then, when the packets are removed from the queue and its length decreases, the incoming packets will be stored in the queue again. This method can fill up the queue quickly, resulting in a high loss rate for applications; the Drop-Tail queue increases delay since it can be full for a long period of time [26].

RED [27] is an algorithm that relies on the average queue length to drop packets, i.e., as the queue length increases, the probability of packet drop increases and vice versa. RED works according to two principles: the estimation of the queue length and the packet drop decision and uses two thresholds for this purpose. When the average queue length is lower than the minimum threshold, all incoming packets will be accepted. Otherwise, when the average queue length is higher than the maximum threshold, all incoming packets will be dropped. Finally, in the case of an average queue length between the two thresholds, the incoming packets will be marked by P_i probability. This probability is directly proportional to the bandwidth of the connection to the router. One of the problems with this algorithm is that it only works well when there is enough buffer space and it is properly parameterized. Thus, it requires a variety of parameters to cope with different types of congestion.

CoDel [28] is an algorithm that has been proposed to manage the queue by calculating the sojourn time of packets in the queue. Based on this packet sojourn time, CoDel decides if the packet should be dropped or not. CoDel works as follows: It calculates the packet sojourn time (the time spent by every packet in the queue) and compares it to the threshold which is by default 5ms. If the minimum sojourn time is less than this threshold, the packet will be transmitted, otherwise if the sojourn time is greater than this threshold, the packet will be dropped. When the algorithm enters into the drop state, it starts sending congestion signals and drops packets that have a low and linearly increasing rate. CoDel starts the drop with the packet that is at the top of the queue and reduces the time interval of the next drop by a certain value. The packet drop increases if the sojourn time remains above the threshold. This algorithm can handle bursty traffic without causing packet loss. This algorithm is considered as a better predictor of congestion [30]. In EC-Elastic, we adopt the same congestion detection method as CoDel.

PIE [29] is an algorithm that controls the average latency of the queue to a target value. The PIE algorithm consists of three

components: a) Random dropping at enqueueing; calculates the dropping probability p . Based on this probability, the packets will be dropped randomly. The timestamp is not mandatory in this step. b) Latency based drop probability update; the calculation of drop probability uses the current estimate of the latency and the direction in which the latency is moving. Alternatively, the direction can be measured by subtracting the current delay from the old delay. There are two parameters used by PIE; (α) to determine the effect of the current latency on the fall probability and (β) to indicate the amount of additional adjustment based on increasing or decreasing latency. The probability of falling becomes stable at the point where the difference between the current and old latency is zero and the latency value equals the reference delay. The final balance between latency delay and latency jitter is determined by the relative weight between α and β . c) Dequeueing rate estimation; in a network, the queuing rate varies with the fluctuation of link capacity or queues that share the same link.

B. Congestion Signaling

After detecting congestion, the information of congestion should be transferred to the consumers and intermediate routers to react quickly to the congestion problem by decreasing the sending rate of interest packets. In NDN, several methods have been proposed to signal congestion to consumers and intermediate routers in order to regulate the sending rate of interest packets:

- Explicit congestion notification, which explicitly returns congestion level information in a NACK packet [22].
- Tagging data packets in the downstream direction, which allows downstream routers and consumers to reduce the sending rate of interest packets, thereby reducing congestion.
- The addition of congestion information in the Congestion Information Bits (CIB) to data packets. Adding a congestion tag to the data packet and sending it to the consumers [31].
- Random Early Marker algorithm REM [20], which explicitly marks data packets to signal the congestion state to downstream nodes.

C. Congestion Window Size Adjustment

The congestion window "cwnd" is used in all congestion control algorithms. It is used to control the quantity of sending packets between consumer and producer to avoid congestion. Despite this, congestion is not really avoidable, because the consumer always tries to maximize the available bandwidth by increasing its cwnd window, which could congest the network.

The congestion window adjustment of EC-Elastic borrows the basic idea of Elastic-TCP [1], which aims to increase the utilization of available bandwidth by using a Window Correlated Weighting Function (WWF), that handles large buffers, long delays and high-BDP networks [1].

IV. EC-ELASTIC DESIGN DETAIL

Avoiding congestion is a major concern of all network architectures. In the following section, we present in detail our

proposal EC-Elastic, which controls congestion in three steps: 1) Congestion detection based on packet sojourn time using CoDel. 2) Explicit congestion signaling. 3) Congestion window adjustment at the consumer node.

A. Motivation

As mentioned earlier, NDN is a new paradigm that is content-based rather than IP address-based. With this paradigm, data transfer evolves from host-based point-to-point transfer to more elaborate, efficient multipoint-to-multipoint transfer that is better suited for the massive and intensive use of content-based Internet. Thus, NDN adopts new features which are mainly receiver-based and connectionless transport mode, one-interest-one-data, multi-source, multi-path and caching. These new features have made TCP/IP's traditional congestion control mechanisms unable to act towards high performance in the emerging NDN paradigm. We present below, the limitations and motivations that led to our proposal:

- Congestion control in TCP/IP is based on delay and loss only at data senders, while NDN controls congestion at consumers and routers.
- The TCP/IP architecture uses end-to-end connected mode to transfer data between two endpoints and uses RTT (Round-Trip Time) and RTO (Retransmission Time Out) values as indicators of network congestion. These methods perform poorly in the NDN network, they don't provide accurate information about congestion levels because NDN is characterized by multi-path and multi-source transfer, i.e., data can be recovered from several sources and via several paths, which leads to large variations in RTT measurements.
- The use of caching in intermediate nodes allows the requested data to be retrieved directly from the intermediate nodes without needing to go through the producer. This technique minimizes data transmission time (RTT) and satisfies the interest packet when congestion losses occur on the producer route.
- In addition, NDN can aggregate interest packets having the same name into a single PIT (Pending Interest Table) entry and transmit the corresponding data packet to all the aggregated faces [10]. The recovery time of the interest packets that arrive after the first one will be shorter.
- These new features (multi-source, multipath, caching and PIT aggregation) can lead to short or long RTT measurements, which increases the detection time of packet losses (the case of long RTT) and consequently also increases the time of reaction to congestion. EC-Elastic avoids this problem by using explicit congestion signaling to react quickly to network congestion (see Section IV.3).
- If the cache is used, if it exhausts its data, the next requests will be handled by another more distant. If the route to the newer cache has a lower BDP and the number of interest packets in transit is higher, the new bottleneck queue may be overloaded before the consumer can adjust its interest packet sending rate.

Our mitigation of this problem is to use large buffers to manage temporary traffic bursts through detecting and signaling congestion using CoDel before that these buffers reach their limit (see Section IV.2).

To avoid the waste of network resources that are very expensive and important that can be caused by large buffers, we need to extend the congestion window to a large number of packets in order to fully utilize the available network bandwidth. In case of a network with high BDP (the number of interest packets in transit is higher), using RTT to increase the congestion window is not reliable because in these networks RTT is long which makes the increase of the congestion window very slow. In this case, the network spends a long period of time capturing the maximum link capacity, which underutilizes the network bandwidth. To avoid this problem, we propose to adopt the same Window-correlated Weighting Function (WWF) that was proposed by [1] to increase bandwidth utilization on TCP/IP high-BDP networks and try to prove its effectiveness on NDN networks to avoid congestion in the congestion avoidance phase and increase bandwidth utilization of NDN networks (see Section IV.4).

B. Congestion Detection based on Packet Sojourn Time using CoDel

In NDN networks, congestion detection based on packet loss or RTT (Round-Trip Time) is not reliable as in the current internet network TCP/IP because NDN is characterized by "multi-source" and "multi-path" transfer. In addition, the use of these features can increase bursty traffic that disrupts queue length and thus the production of congestion. Therefore, to absorb these bursty traffics, the buffer size must be larger than usual [30]. Active queue management (AQM) systems have been proposed to control the amount of data buffered to keep space available to absorb bursts and reduce queue delay. CoDel [28], as an AQM algorithm, is designed to control the queue by calculating the sojourn time of packets in the queue. This algorithm allows routers, which have a large buffer, to absorb traffic bursts and to reduce its queues through detecting congestion before the buffer is full [10]. In EC-Elastic, we adopt the congestion detection method proposed by CoDel.

The CoDel algorithm, presented below, calculates the sojourn time of each packet in the queue "queuing delay" and compares the minimum sojourn time over a given period of time (default: 100ms) with a threshold, by default equal to 5ms. The first time the packet sojourn time exceeds the threshold, the current time will be recorded as FirstAboveTime and the packet sojourn time will be recorded as FirstSojourn. If the minimum sojourn time over a period of time (default: 100ms) exceeds the threshold (default: 5ms), the outgoing link in the queue is considered congested. The CoDel code is presented in Algorithm 1.

Algorithm 1 CoDel algorithm

```
1: Function CheckSojournTime(Packet, Now)
2:   sojournTime  $\leftarrow$  Now - Tag.GetTime
3:   if sojournTime > Target then
4:     OverTargetForInterval  $\leftarrow$  False
5:     if FirstAboveTime == 0 then
6:       OverTargetForInterval  $\leftarrow$  False
7:       FirstAboveTime  $\leftarrow$  Now
8:     else
9:       if Now > (FirstAboveTime + Interval) then
10:        sojourn  $\leftarrow$  Now
11:        OverTargetForInterval  $\leftarrow$  True
12:      else
13:        FirstAboveTime == 0
14:        OverTargetForInterval  $\leftarrow$  False
15:      end if
16:    end if
17:  end if
18:  return OverTargetForInterval;
19: end function
20: Function DoDequeue(Packet, Now)
21:   Now  $\leftarrow$  CoDelGetTime()
22:   OkToMark  $\leftarrow$  CheckSojournTime(Packet, Now)
23:   if OkToMark then
24:     if Now > NextMarkingTime then
25:       MarkNext  $\leftarrow$  True
26:       NextMarkingTime  $\leftarrow$  Now
27:     else
28:       MarkedCount  $\leftarrow$  0
29:     end if
30:   end if
31: end function
```

C. Explicit Congestion Signaling

We use the same congestion signaling method that CoDel used, ECN marking (Explicit Congestion Notification) [32]. This signaling is done in the downstream direction by explicitly marking the concerned packets to notify the consumer of the link status, i.e., when a router detects congestion on one of its outgoing links, it marks the data packets and explicitly signals this state of congestion to the consumer nodes to reduce their sending rate of interest packets.

ECN marking is done as follows: When congestion occurs, the first packet is marked and the next packets are marked in a marking interval that corresponds to the CoDel drop spacing; This interval starts at "1.1 * the CoDel interval (100ms)" [33]. A congestion notification bit is used by ECN in the packet headers to provide feedback on network congestion. This bit is activated in the PIT entry of the packet when the packet sojourn time exceeds the threshold. Depending on the data packet received (Normal or Marked) at the consumer nodes, the authors adapt the sending rate of interest packets. An advantage of ECN marking is that consumers can be informed of congestion quickly and thus react quickly to the congestion problem.

D. Congestion Window Adjustment

This section describes in detail the algorithm used to adjust the congestion window of EC-Elastic, which is based on the Elastic-TCP mechanism. The principal purpose of this algorithm is to improve overall performance and bandwidth utilization while avoiding packet loss. Algorithm 2 describes the core functionality of EC-Elastic at the consumer node, where the congestion window *cwnd* is increased when the consumer receives a normal data packet and is decreased when the consumer receives marked packets or Timeouts.

Algorithm 2 Consumer Elastic Algorithm

```

1: On data reception do
2:   if no NACK received then
3:     if slow start then
4:        $cwnd \leftarrow cwnd + 1$ 
5:     else
6:        $RTT_{current} \leftarrow (now - sendtime)$ 
7:       if  $RTT_{current} > RTT_{max}$  then
8:          $RTT_{max} \leftarrow RTT_{current}$ 
9:       end if
10:      if  $RTT_{current} < RTT_{min}$  then
11:         $RTT_{min} \leftarrow RTT_{current}$ 
12:      end if
13:       $WWF \leftarrow \sqrt{\frac{RTT_{max}}{RTT_{current}}} * cwnd$ 
14:       $cwnd \leftarrow cwnd + \frac{WWF}{cwnd}$ 
15:    end if
16:    else
17:      if slow start then
18:         $cwnd \leftarrow cwnd \times \beta_1$ 
19:      else
20:         $cwnd \leftarrow cwnd \times \beta_2$ 
21:      end if
22:       $ssthresh \leftarrow cwnd - 1$ 
23:    end if

```

1) Design of the consumer window adjustment algorithm:

The basic idea of algorithm 2 is to use the Window-correlated Weighting Function WWF which was proposed in [1] and aims to improve the bandwidth utilization. WWF is based on the variation of RTT (Round Trip Time) according to the following formula:

$$WWF = \sqrt{\frac{RTT_{max}}{RTT_{current}}} * cwnd \quad (1)$$

Where, $RTT_{current}$ is the current RTT obtained from the last ACK, RTT_{max} is the maximum RTT and *cwnd* is the current congestion window. This function is used in the congestion avoidance phase to increase the congestion window by $cwnd + \frac{WWF}{cwnd}$. However, in the slow start phase, EC-Elastic increases its congestion window by *cwnd*+1.

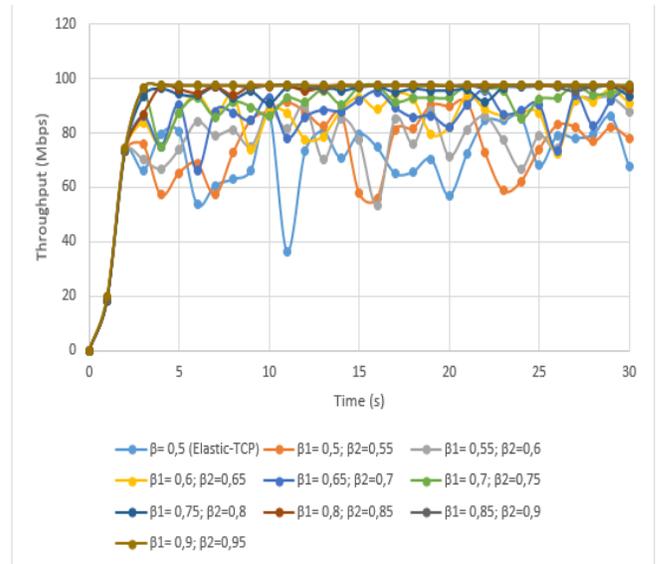


Fig. 2. Throughput of EC-Elastic by Varying the Parameter β .

In case of congestion detection or timeouts, Elastic-TCP [1] applies a multiplicative decrease that halves the *cwnd* after each loss detection regardless of the phase in which the loss is detected. In contrast, EC-Elastic uses two ways to decrease the *cwnd*, after any congestion detection. This decrease varies depending on the phase where the loss is detected. As shown in Algorithm 2, if the loss is detected in the slow start phase, EC-Elastic decreases its *cwnd* to *cwnd** β_1 of the last *cwnd*. If the loss is detected in the congestion avoidance phase, EC-Elastic decreases its *cwnd* to *cwnd** β_2 of the last *cwnd* and the *ssthresh* (the threshold) is reduced to *cwnd* -1 after any degradation to avoid switching to an undesirable slow start. Since the loss that occurs in the slow start phase is more severe than the loss that occurs in the congestion avoidance phase [34], the value of β_1 should therefore always be less than β_2 (β_1 and β_2 are two parameters used for adjusting the size of the congestion window, their values vary between 0 and 1).

Fig. 2 presents the simulation results we conducted on the first scenario (Fig. 3 and Table II) in order to find the most optimal values for choosing the coefficients β_1 and β_2 . This figure shows a comparison between using a multiplicative decrease (as in Elastic-TCP which uses $\beta=0.5$ to decrease its congestion window ", a multiplicative decrease is usually equal to 1/2") and using two parameters β_1 and β_2 in both congestion control phases. According to Fig. 2, with the increase of β_1 and β_2 , the throughput also increases and when $\beta_1 = 0,9 / \beta_2 = 0,95$, the throughput is almost the same as that of $\beta_1 = 0,85 / \beta_2 = 0,9$ which indicates that the throughput does not change when the value of β_1 is greater than 0,85 and β_2 is greater than 0,9. EC-Elastic performs better in terms of link utilization with the use of the two parameters β_1 and β_2 than the use of multiplicative decrease. Based on the experimental result (Fig. 2), we set $\beta_1 = 0,85$ and $\beta_2 = 0,9$ in our algorithm.

2) *General behavior of EC-elastic*: EC-Elastic uses a slow start phase to increase the congestion window at consumer nodes. Then, intermediate routers calculate the sojourn time of each packet in the queue (using CoDel). If this sojourn time exceeds a well-defined threshold, the router marks data packets and sends them explicitly to the consumers to react to this situation. At the consumer nodes, once the first marked packet is received; EC-Elastic reduces its congestion window $cwnd$ by the factor β_1 and enters into the congestion avoidance phase which is characterized by using the Window-Correlated Weighting Function (WWF). In this phase, EC-Elastic increases its congestion window $cwnd$ by $WWF/cwnd$ and decreases it by the factor β_2 (by receiving a marked packet). However, if a timeout is detected in any phase, EC-Elastic resets its congestion window $cwnd$ to the initial value. The main objective of EC-Elastic in NDN is the same as that of Elastic-TCP in TCP/IP network, to improve bandwidth utilization in NDN networks, where RTTs are long, buffers are very large, and packet losses are very frequent.

V. PERFORMANCE EVALUATION OF EC-ELASTIC

This work focuses on developing a new congestion control mechanism named EC-Elastic that has the capability to increase bandwidth utilization in high-speed NDN networks. Using ndnSIM [35], based on NS-3 and designed specifically for the numerical study of NDN networks, the performance of EC-Elastic is evaluated and compared to three other congestion control algorithms: Agile-SD [34], CUBIC [36] and STCP [37]. These algorithms have been implemented in NDN, in the same scenarios as EC-Elastic.

A. Simulation Scenarios

1) Scenario 1: one consumer - one producer

Fig. 3 shows the first topology which contains a consumer, a router and a producer.

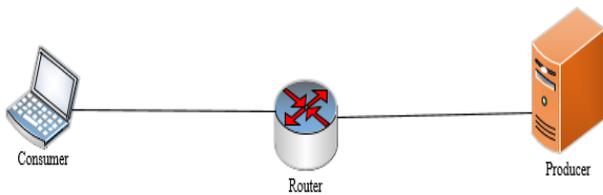


Fig. 3. Simulation Topology 1.

TABLE I. PARAMETERS OF SIMULATION TOPOLOGY 2

Parameters	Delay	Bandwidth
Consumer - Router	10ms	100Mbps
Router - Producer	10ms	1Gbps

In this scenario, the link bandwidth from the consumer to the router is fixed at 100 Mbps with a 10 ms delay while the link bandwidth from the router to the producer is fixed at 1 Gbps with a 10 ms delay, as illustrated in Table I.

2) Scenario 2: Multiple consumers - multiple producers

In this second topology (Fig. 4), six consumer nodes are connected to six producer nodes via a bottleneck link, consisting of two routers (Router 1 and Router 2).

In this scenario, each link consumer-router is set to 100Mbps with different values of link delay between different nodes in the studied topology (1ms, 10ms, 15ms, 20ms, 25ms and 30ms). The link Router1-Router2 is set to 5Mbps with a delay of 15ms. From Router 2 to producers 1/3/5, the link is set to 20Mbps with delays of 10ms, 5ms and 1ms respectively and from Router 2 to producers 2/4/6, the link is set to 10Mbps with delays of 10ms, 5ms and 1ms respectively as presented in Table II. In this scenario, the consumers request the same content. The time for both simulations is set to 30 seconds.

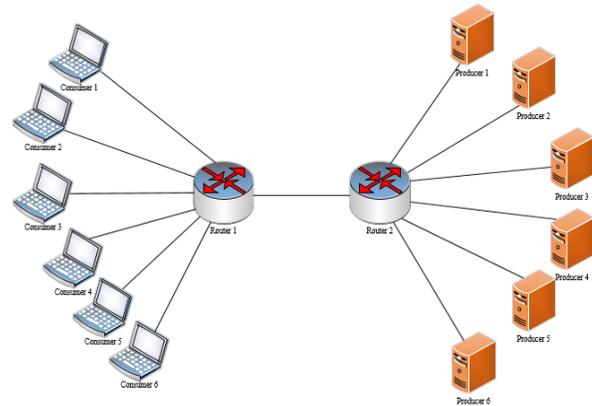


Fig. 4. Simulation Topology 2.

TABLE II. PARAMETERS OF SIMULATION TOPOLOGY 2

Parameters	Delay	Bandwidth
Consumer1 - Router1	1ms	100Mbps
Consumer2 - Router1	10ms	100Mbps
Consumer3 - Router1	15ms	100Mbps
Consumer4 - Router1	20ms	100Mbps
Consumer5 - Router1	25ms	100Mbps
Consumer6 - Router1	30ms	100Mbps
Router1 - Router 2	15ms	50Mbps
Router2 - Producer1	10ms	20Mbps
Router2 - Producer2	10ms	10Mbps
Router2 - Producer3	5ms	20Mbps
Router2 - Producer4	5ms	10Mbps
Router2 - Producer5	1ms	20Mbps
Router2 - Producer6	1ms	10Mbps

B. Simulation Results

We evaluate the performance of EC-Elastic in both study scenarios described above and are primarily interested in throughput, packet loss rate, and delay. In this study, delay is the time from sending an interest packet to receiving the corresponding data packet. Similarly, throughput, measured in bits per second, designates the number of successfully transmitted data packets from source to destination and changes with the amount of packets transmitted and the amount of packets dropped in the network [38]. Packet loss rate, designates the number of dropped packets per second and is measured as the difference between the amount of packets sent by a node and the amount of packets received by the same node, over a given period of time. In order to have reliable values, all simulations were repeated several times and the results presented in the following are an average of the obtained values.

1) *Throughput measurement:* Fig. 5 shows a comparison of throughput between EC-Elastic and the three algorithms (Agile-SD, CUBIC, and STCP) in the first study scenario, and Fig. 6 shows a comparison of throughput between EC-Elastic and the three algorithms (Agile-SD, CUBIC, and STCP) in the second study scenario while, Table III shows the throughput of both scenarios.

The objective of the first scenario (Fig. 5) is to study the ability of these mechanisms to fully utilize the available bandwidth. EC-Elastic outperforms the other mechanisms because of its fast cwnd growth resulting from the use of the Window-correlated Weighting Function WWF. It is clear that EC-Elastic can fully utilize the bandwidth and is more stable than Agile-SD, CUBIC and STCP algorithms. In the second scenario (Fig. 6), increasing consumer and producer numbers shows better performance, in terms of throughput, for EC-Elastic than those obtained by the other three algorithms Agile-SD, CUBIC and STCP. In addition, EC-Elastic has a more stable throughput than the other three algorithms in both scenarios.

EC-Elastic achieves the best and most stable throughput performance compared to the other algorithms and this is due to the use of the Window-correlated Weighting Function WWF which aims to maximize the bandwidth usage of the network. The result of this study is that EC-Elastic has the capability to perceive and predict rapidly, deal with the variation of bandwidth and adapt to NDN characteristics.

The necessity of the proposed mechanism was raised because of the incapacity of the existing mechanisms to fully utilize the available bandwidth on high speed networks where RTTs are very long and large buffers are used.

TABLE III. THROUGHPUT OF SCENARIOS 1 AND 2

Algorithms	EC-Elastic	CUBIC	Agile-SD	STCP
Scenario 1	93,778	24,282	74,116	61,366
Scenario 2	113,62	37,26	108,96	88,37

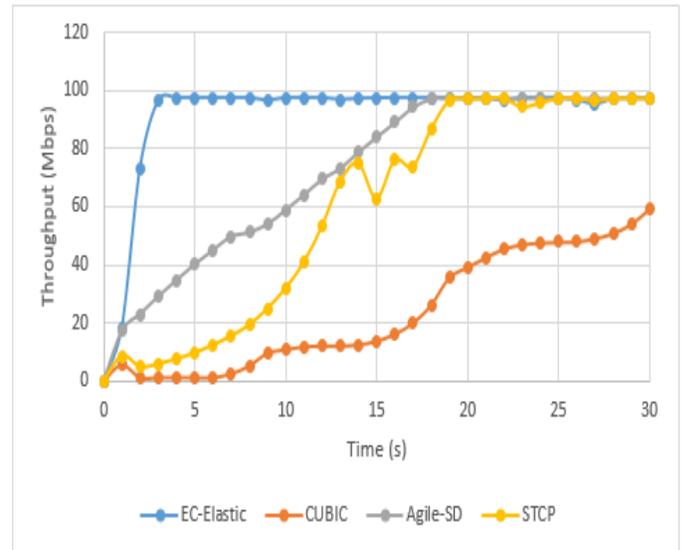


Fig. 5. Throughput of Scenario 1.

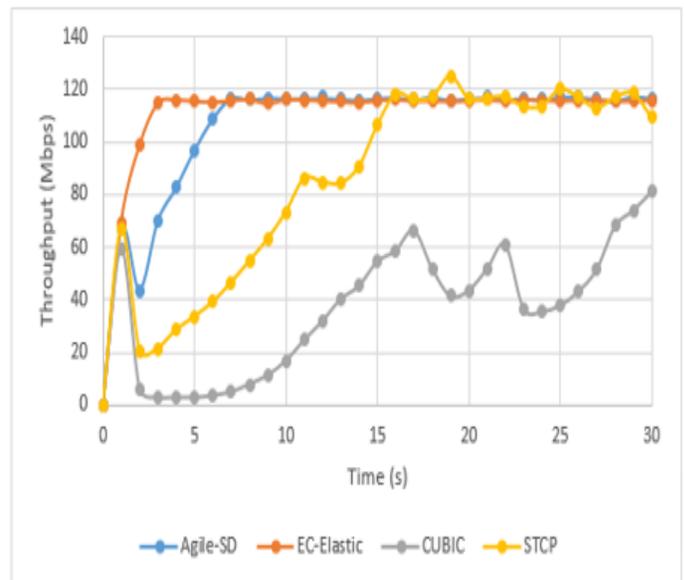


Fig. 6. Throughput of Scenario 2.

2) *Packet loss rate measurement:* The main objective of each congestion control mechanism is to maximize throughput and minimize packet loss rate. Table IV shows the packet loss rate in both scenarios. The results obtained from our numerical study, show almost identical performance for the four algorithms compared, with almost negligible packet loss rate because the use of CoDel queueing reacts before the queue reaches its limit and also reacts quickly to the congestion problem by marking packets and notifying the consumer to reduce their sending rate of interest packets. In addition, explicit congestion marking reduces retransmissions, because by notifying the consumer of the link status in case of congestion, the packet received by the consumer also contains the requested data.

TABLE IV. PACKET LOSS RATE OF SCENARIOS 1 AND 2

Algorithms	EC-Elastic	CUBIC	Agile-SD	STCP
Scenario 1	0,001	0,032	0,055	0,032
Scenario 2	0	0	0	0

3) Delay measurement: Fig. 7 and 8 show the delay measurement for Scenarios 1 and 2, respectively, and Table V shows the delay measurement for both scenarios.

For the first scenario (Fig. 7), we observe that EC-Elastic, Agile-SD, and Cubic show a lower delay measure than STCP and this measure becomes almost the same for all the mechanisms when we exceed 5s of the simulation. In the second scenario (Fig. 8), we observe that EC-Elastic and CUBIC have a lower average delay measure than that measured by STCP and Agile-SD.

The exponential increase in delay between seconds 1 and 5 is due to all algorithms rapidly increasing their congestion window at the end of the slow start phase to ensure full utilization of the available bandwidth before switching to the congestion avoidance phase, resulting in problems such as packet loss, and thus increasing the delay between sending a packet of interest and receiving its corresponding data packet. As a result, our mechanism EC-Elastic ensures a reasonable packet transmission delay.

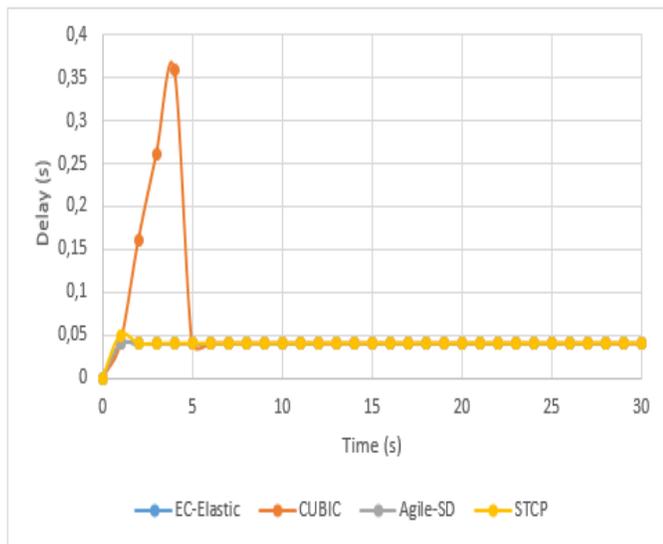


Fig. 7. Delay Analysis of Scenario 1.

TABLE V. DELAY MEASUREMENT OF SCENARIOS 1 AND 2

Algorithms	EC-Elastic	CUBIC	Agile-SD	STCP
Scenario 1	0,04	0,062	0,04	0,04
Scenario 2	0,06	0,054	0,06	0,056

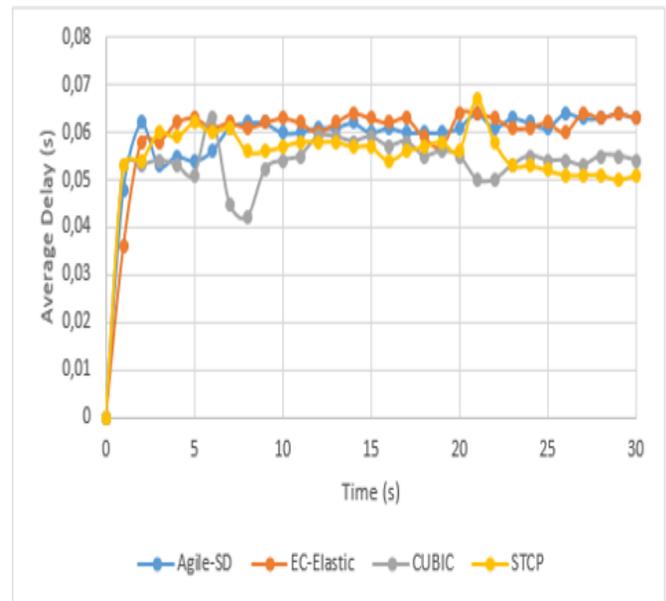


Fig. 8. Avg Delay Analysis of Scenario 2.

The numerical study performed in this work reveals that our algorithm EC-Elastic seems to give better performance, in terms of throughput, compared to those of Agile-SD, CUBIC and STCP algorithms. Thus, our algorithm can continuously fully utilize the bandwidth of the sources while keeping the delay and packet loss rate lower.

VI. CONCLUSION

This paper proposes EC-Elastic, a hybrid congestion control mechanism for NDN, to avoid congestion, increase bandwidth utilization and achieve efficient data delivery. EC-Elastic is based on the use of Window Correlated Weighting Function (WWF) which aims to improve bandwidth utilization in the network. At the intermediate routers, EC-Elastic uses AQM-CoDel queue to measure the packet sojourn time and explicitly signals congestion to inform the consumer to decrease its sending rate of interest packets, and then at the consumer nodes, EC-Elastic adopts the basic idea of Elastic-TCP to control the sending rate of interest packets. The conducted numerical study of the performance of EC-Elastic compared to Agile-SD, CUBIC and STCP in terms of throughput, packet loss rate, and delay shows that EC-Elastic can significantly improve bandwidth utilization while maintaining lower delay and packet loss rates. EC-Elastic can be a promising solution to enhance bandwidth utilization on high speed networks where RTTs are very long and large buffers are used. As a future work, we plan to implement EC-Elastic in the Internet of Health Things (IoHT) to evaluate its performance in more complex scenarios where sensitive patient data becomes a critical component of healthcare that requires ensuring its timely delivery while avoiding congestion and data loss.

REFERENCES

- [1] Alrshah MA, Al-Maqri MA, Othman M. Elastic-TCP: Flexible Congestion Control Algorithm to Adapt for High-BDP Networks. *IEEE Syst J*. 2019;:1–11.
- [2] Rhee I, Xu L, Ha S, Zimmermann A, Eggert L, Scheffengger R. CUBIC for Fast Long-Distance Networks. 2019;1:105–12.
- [3] Dong M, Li Q, Zarchy D, Godfrey PB, Schapira M. PCC: Researching congestion control for consistent high performance. *Proc 12th USENIX Symp Networked Syst Des Implementation, NSDI 2015*. 2015;:395–408.
- [4] Khelifi H, Luo S, Nour B, Mounsla H. LQCC: A Link Quality-based Congestion Control Scheme in Named Data Networks. *IEEE Wirel Commun Netw Conf WCNC*. 2019;2019-April:1–6.
- [5] Ahlgren B, Dannewitz C, Imbrenda C, Kutscher D, Ohlman B. A survey of information-centric networking. *IEEE Commun Mag*. 2012;50:26–36. doi:10.1109/MCOM.2012.6231276.
- [6] Zhang L, Estrin D, Burke J, Jacobson V, Thornton J, Diana K, et al. Named Data Networking (NDN) Project Named Data Networking (NDN) Project. 2010; May.
- [7] El-bakkouchi A, Bouayad A, ELBekkali M. A hop-by-hop Congestion Control Mechanisms in NDN Networks – A Survey. 2019 7th Mediterr Congr Telecommun. 2019;:1–4.
- [8] El-Bakkouchi A, Ghazi M El, Bouayad A, Fattah M, Bekkali M El, Mazer S. Packet Loss and Delay Measurement Analysis of TCP Variants in NDN Congestion Control. 2020 1st Int Conf Innov Res Appl Sci Eng Technol IRASET 2020. 2020;:2–6.
- [9] Ren Y, Li J, Shanshan Shi, Lingling Li, Guodong Wang. An explicit congestion control algorithm for Named Data Networking. In: 2016 IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPs). IEEE; 2016. p. 294–9. doi:10.1109/INFCOMW.2016.7562089.
- [10] Schneider K, Yi C, Zhang B, Zhang L. A Practical Congestion Control Scheme for Named Data Networking. doi:10.1145/2984356.2984369.
- [11] Ren Y, Li J, Shi S, Li L, Wang G, Zhang B. Congestion control in named data networking – A survey. *Comput Commun*. 2016;86:1–11. doi:10.1016/j.comcom.2016.04.017.
- [12] Mejri S, Touati H, Kamoun F. Hop-by-hop interest rate notification and adjustment in named data networks. *IEEE Wirel Commun Netw Conf WCNC*. 2018;2018-April:1–6.
- [13] Carofiglio G, Gallo M, Muscariello L. ICP: Design and evaluation of an Interest control protocol for content-centric networking. In: 2012 Proceedings IEEE INFOCOM Workshops. IEEE; 2012. p. 304–9. doi:10.1109/INFCOMW.2012.6193510.
- [14] Salsano S, Detti A, Cancellieri M, Pomposini M, Blefari-Melazzi N. Transport-layer issues in information centric networks. *ICN'12 - ACM Proc Information-Centric Netw Work*. 2012; August:19–24.
- [15] Arianfar S, Nikander P, Eggert L, Wong W. ConTug: A Receiver-Driven Transport Protocol for Content-Centric Networks. <http://users.piuha.net/blackhawk/contug/contug.pdf>. Accessed 12 Mar 2018.
- [16] Saino L, Cocora C, Pavlou G. CCTCP: A Scalable Receiver-driven Congestion Control Protocol for Content Centric Networking. <https://pdfs.semanticscholar.org/c539/1eb884f234a40ffcf8a7ad2a8989e13b79.pdf>. Accessed 11 Mar 2018.
- [17] Braun S, Monti M, Sifalakis M, Tschudin C. An Empirical Study of Receiver-Based AIMD Flow-Control Strategies for CCN. In: 2013 22nd International Conference on Computer Communication and Networks (ICCCN). IEEE; 2013. p. 1–8. doi:10.1109/ICCCN.2013.6614106.
- [18] Carofiglio G, Gallo M, Muscariello L. Joint Hop-by-hop and Receiver-Driven Interest Control Protocol for Content-Centric Networks. <https://conferences.sigcomm.org/sigcomm/2012/paper/icn/p37.pdf>. Accessed 11 Mar 2018.
- [19] XIA Y, WANG L, HOU F, WANG Y. Congestion Control for Content-Centric Networking Based on Protocol-Oblivious Forwarding. *DEStech Trans Comput Sci Eng*. 2017; wene.
- [20] Zhang F, Zhang Y, Reznik A, Liu H, Qian C, Xu C. A transport protocol for content-centric networking with explicit congestion control. In: 2014 23rd International Conference on Computer Communication and Networks (ICCCN). IEEE; 2014. p. 1–8. doi:10.1109/ICCCN.2014.6911765.
- [21] Yi C, Afanasyev A, Moiseenko I, Wang L, Zhang B, Zhang L. A case for stateful forwarding plane. *Comput Commun*. 2013;36:779–91. doi:10.1016/j.comcom.2013.01.005.
- [22] Kato T, Bandai M. Congestion control avoiding excessive rate reduction in named data network. 2017 14th IEEE Annu Consum Commun Netw Conf CCNC 2017. 2017;:108–13.
- [23] Kato T, Bandai M. Avoiding excessive rate reduction in rate based congestion control for named data networking. *J Inf Process*. 2018;26:29–37.
- [24] Nguyen D, Fukushima M, Sugiyama K, Tagami A. Efficient multipath forwarding and congestion control without route-labeling in CCN. 2015 IEEE Int Conf Commun Work ICCW 2015. 2015; Sepa:1533–8.
- [25] Mughtar F, Al-Adhaileh MH, Alubady R, Singh PK, Ambar R, Stiawan D. Congestion Control for Named Data Networking-Based Wireless Ad Hoc Network. Springer Singapore; 2020. doi:10.1007/978-981-15-3369-3_10.
- [26] Alwahab DA, Laki S. A simulation-based survey of active queue management algorithms. *ACM Int Conf Proceeding Ser*. 2018;:71–7.
- [27] Floyd S, Jacobson V. Random Early Detection Gateways for Congestion Avoidance. *IEEE/ACM Trans Netw*. 1993;1:397–413.
- [28] Nichols K, Jacobson V. Controlling queue delay. *Commun ACM*. 2012;55:42. doi:10.1145/2209249.2209264.
- [29] Pan R, Natarajan P, Piglione C, Prabhu MS, Subramanian V, Baker F, et al. PIE: A lightweight control scheme to address the bufferbloat problem. *IEEE Int Conf High Perform Switch Routing, HPSR*. 2013;:148–55.
- [30] Wang M, Yue M, Wu Z. WinCM: A Window based Congestion Control Mechanism for NDN. 2019; HotICN:80–6.
- [31] Liu Y, Piao X, Hou C, Lei K. A CUBIC-Based explicit congestion control mechanism in named data networking. *Proc - 2016 Int Conf Cyber-Enabled Distrib Comput Knowl Discov CyberC 2016*. 2017;:360–3.
- [32] Floyd S. TCP and explicit congestion notification. *ACM SIGCOMM Comput Commun Rev*. 1994;24:8–23.
- [33] Nichols K, Pollere I, Jacobson V, A. McGregor E, J. Iyengar E. Controlled Delay Active Queue Management draft-ietf-aqm-codel-03. *J Chem Inf Model*. 2016;53:1689–99.
- [34] Alrshah MA, Othman M, Ali B, Hanapi ZM. Agile-SD: A Linux-based TCP congestion control algorithm for supporting high-speed and short-distance networks. *J Netw Comput Appl*. 2015;55 August 2018:181–90. doi:10.1016/j.jnca.2015.05.011.
- [35] Mastorakis S, Afanasyev A, Moiseenko I, Zhang L. ndnSIM 2.0: A new version of the NDN simulator for NS-3. *NDN Proj*. 2015;:1–8.
- [36] Ha S, Rhee I, Xu L. CUBIC: A new TCP-friendly high-speed TCP variant. *Oper Syst Rev*. 2008;42:64–74.
- [37] Kelly T. Scalable TCP: Improving performance in highspeed wide area networks. *Comput Commun Rev*. 2003;33:83–91.
- [38] El-Bakkouchi A, El Ghazi M, Bouayad A, Fattah M, El Bekkali M. Performance analysis of TCP variants in named data networking. *Int J Adv Trends Comput Sci Eng*. 2020;9 1.5 Special Issue:13–20.

1D-CNN based Model for Classification and Analysis of Network Attacks

Kuljeet Singh¹

Research Scholar
Department of Computer Science &
IT, University of Jammu
Jammu, India

Amit Mahajan²

System Analyst
Department of Computer Science &
IT, University of Jammu
Jammu, India

Vibhakar Mansotra³

Professor
Department of Computer Science &
IT, University of Jammu
Jammu, India

Abstract—With the advancement in technology and upsurge in network devices, more and more devices are getting connected to the network leading to more data and information on the network which emphasizes the security of the network to be of paramount importance. Malicious traffic must be detected in networks and machine learning or more precisely deep learning (DL), which is an upcoming approach, should be used for better detection. In this paper, Detection of attacks through a classification of traffic into normal and attack data is done using 1D-CNN, a special variant of convolutional neural network (CNN). For this, the CICIDS2017 dataset consisting of 14 attack types spread across 8 different files, is considered for evaluating model performance and various indicators like recall, precision, F1-score have been utilized. Separate 1D-CNN based DL models were built on individual sub-datasets as well as on combined datasets. Also, an evaluation of the model is done by comparing it with an artificial neural network (ANN) model. Experimental results have demonstrated that the proposed model has performed better and shown great capability in detecting network attacks as the majority of the class labels had achieved excellent scores in each of the evaluation indicators used.

Keywords—1D-CNN; CICIDS2017; network attacks; deep learning

I. INTRODUCTION

The Internet has become a major aspect in today's society with people using the services of WWW for most of their day-to-day activities. People use the Internet for both personal as well as professional purposes and the majority of tasks include sharing data, information access, sending files, connecting with friends or colleagues through social media and most importantly e-commerce activities which include saving passwords, credit/debit card info. Not only individuals but organizations too depend heavily on the Internet and its services. Network attacks in the form of malicious traffic results in loss of data, privacy violation for individuals; monetary, financial and political impact on big organizations and interrupted businesses for all its shareholders [1]. Nowadays, with the effect of Covid-19 and the ongoing pandemic, work from home is becoming a new normal. This has led to personal devices being vulnerable with not so sophisticated protection mechanisms as compared to the organization's resources. The effect of the pandemic could lead to attack mechanisms getting more diverse which means cyber-security will remain verticals of critical importance in the times to come.

There are many approaches to provide cyber-security ranging from authentication, encryption to a firewall, IDS (intrusion detection system). With IDS providing monitoring and behavior analysis of network traffic and further identifying attacks from network flow, it has proven itself a better alternative to other approaches [2]. Detection of cyber-attacks is like a classification approach where it categorizes whether it belongs to benign or different types of attacks. Traditional Machine learning (ML) techniques, also known as shallow learning, have been used for intrusion detection by classifying the network traffic [3]. As the real world data gets bigger by time resulting in high dimensional space, the drop in performance of ML techniques can be observed due to its over-dependence on the features selected by the human experts. DL, with its complex architecture, overcame this limitation by automatically learning features through a massive amount of data. In this paper, we propose a 1D-CNN as a DL technique for effective feature representation and categorizing traffic into normal and different attack types. 1D-CNN's or 2D-CNN are almost identical in architecture as the core process in both of them is convolution operation.

Convolution, a mathematical operation operates on two signals by convolving them with one being input signal or data and the other known as kernel or filter. It is the process between input and kernel/filter which includes element-wise multiplication followed by summation resulting in single/scalar value. Convolution can be 1-d, 2-d or multi-dimensional depending on the problem in hand but the traditional CNNs developed [4] and the popular ones employed uses 2-d convolution which became the de facto standard for most applications in image processing and other deep learning tasks [5] [6] [7]. CNNs consist of input layer, convolution layers in the initial stages and MLP or fully connected layers in the final stages of a model preceding the output layer. The other optional but mostly used layers include sub-sampling (pooling) layer and dropout (regularization technique). General convolution operation is shown in equation 1:

$$O_t = (X * F)_t \quad (1)$$

Where X is the input vector and F is the filter or kernel used and * is the convolution operation employed. The dimensions of both X and F are 1 dimensional in 1D-CNN and subsequently vary with the CNN used.

Generally, the architecture of 1D-CNN and 2D CNN remains the same with the main difference between the two is the use of 1d array or tensor in the former and 2d matrix or tensor in the latter. This means both input data and the kernel used for convolution are in 1d array form and the kernel moves over input in 1d direction. These minor but strategic changes led to certain advantages of 1D-CNN over 2D-CNN like 1) Reduced computational complexity due to 1D tensor over 2D tensor, 2) Well suited for low-cost applications but can be used for complex problems [8]. These advantages of 1D-CNN and better compatibility with certain problem domain has led to many areas where it has been applied or can be applied such as:

- Most extensively used in Natural Language Processing (NLP), where it is quite helpful in extracting sub-sequences from sequences of words [9].
- Human activity recognition task which involves time series of sensor data [10].
- Analysis of signal data over a fixed-length period, for example, an audio recording, real-time motor fault detection [11].
- Data in tabular form.

The focus of this study is the network traffic data which is stored in tabular form where each record is represented by an individual row which is in a one-dimensional shape. Applying 2D-CNN over this type of data requires converting each 1d row into a 2d matrix shape before convolution between input and kernel can be performed. Application of 2D-CNN over images seems justifiable since images are already in 2d shape but in the case of tabular data, it takes an additional effort of converting the 1d input data (each row) into 2d matrix shape which might include padding as well. This overhead can be avoided by using 1D-CNN over 2D-CNN with the only notable difference between the two being the shape of input data and kernel vector as 1d array (or tensor) is used in the former and 2d matrix (or tensor) in the latter.

The Rest of the manuscript is organized as follows: Section 2 discusses the related work in the field of intrusion detection, Section 3 explains the methodology part which comprise sub-sections 1) dataset description 2) model architecture and 3) model evaluation. Section 4 presents the results and analysis while Section 5 concludes the paper.

II. RELATED WORK

Research on intrusion detection has been going on for many decades, still a lot of work needs to be done and lots of issues must be examined. Several Data mining/ML techniques whether supervised or unsupervised learning have been applied for the identification of malicious traffic [12] [13]. More recently DL techniques have been used for the detection of Cyber-attacks and it has achieved significant results. So our literature review revolves mostly around the DL technique used (especially CNN) or the CICIDS2017 dataset which has been utilized in the proposed work.

Detection and mitigation of the common DDoS attacks using DDoS detectors employed for network traffic

monitoring have been carried out using ANN structures, which were designed for different protocols separately [14]. In [15], authors uses NSL-KDD and Kyoto dataset for implementing their work which contains two important concepts: online sequential extreme learning machine which is the methodology used for classification and traffic profiling which makes up the preprocessing part. DL based intelligent framework have been implemented using Long short term memory (LSTM) to lessen DDoS attack in fog environment [16]. ISCX and CTU-13 were the datasets considered along with attack launching tool Hping3 for model evaluation. In [17], the applicability of restricted boltzmann machine (RBM) to differentiate between normal and abnormal Netflow traffic have been demonstrated in the ISCX dataset. A hybrid approach has been adopted in the form of a Double-Layered Hybrid Approach (DLHA) where the first layer uses naive Bayes (NB) to detect DoS and probe attacks while the second layer adopts SVM for detecting the remaining attacks in the NSL-KDD dataset [18]. In [19], authors proposed a model based on 5-layer autoencoder (AE) for detection of network anomalies. Their work also includes data preprocessing for removing outliers and error reconstruction for effective network traffic classification.

In the detection of network attacks using CNN, the majority of the academic research has been done using 2D-CNN in which input data in the linear form is transformed into a matrix form. In [20] and [21], the proposed approach revised the established LeNet-5 model for classification of attacks in the KDD99 dataset, and input data is converted into 32*32 matrix shapes for input to the model. DNN based IDS was built with 4 hidden layers and evaluated the model using the NSL-KDD dataset [22]. Dimensionality reduction using principal component analysis (PCA) and AE has been performed on the KDD99 dataset before the classification technique CNN is applied [23]. The input shape of 1*122 is transformed into 1*121 and 1*100 before being converted to 10*10 and 11*11 matrix shapes.

Both shallow and deep learning have been combined through the random forest (RF) and non-symmetric deep auto-encoders (NDAE) [24]. They exercised the NDAE technique for unsupervised learning of features, and for classification tasks, a model constructed from a combination of stacked NDAEs and the RF algorithm was implemented. Separate architectures or models were built in the form of CNN, RNN, and different variants of AE [25]. NSL-KDD dataset has been used and each record was converted into 32*32 2d form. Long short term memory (LSTM) is the variant of RNN used while Sparse, Denoising, Contractive, and Convolutional are different variants of AE used in the experiments. In [26], authors utilized the 1D-CNN based model for intrusion detection further evaluated using the NSL-KDD dataset. They compared the performance of their proposed model with different ML/DL techniques like J48, NB, RF, MLP, and RNN. In [27], authors proposed BAT as a traffic anomaly detection model for effective feature representation and network classification. The BAT model is a combination of a Bidirectional LSTM and attention mechanism.

The use of the CICIDS2017 dataset for intrusion detection has also been found in the literature. The author in his thesis

has done integration of open-source anomaly-based IDS Zeek (Bro), which uses scripts for feature extraction, and developed a model using various algorithms like RF, DT, and KNN on the CICIDS2017 dataset [28]. An ML-based hybrid model was recommended which comprises DT and RF in a stacked manner for classifying attacks in CICIDS2017 and NSL-KDD dataset [29]. The author incorporates the Fisher score as the feature selection method and performed the analysis of Supervised Learning techniques like DT, KNN, and SVM in detecting DDoS attacks from the CICIDS2017 dataset [30]. Experimental results have shown a good detection rates for DT and KNN but mediocre classification results for models built using SVM. In [31], authors applied and performed comparative analysis of 10 common ML/ DL techniques for detecting web attacks. The employed techniques include ANN, DT, KNN, SVM, CNN, NB, RF, k-means, expectation maxim and SOM. The results of the experiment conducted have shown that the NB, KNN and DT has outperformed the other models. Table I summarizes the key existing studies done in the detection of network attacks using ML or DL.

TABLE I. SUMMARY OF THE EXISTING STUDIES

Ref	Algorithm or model	Dataset used	Key points
[15]	LSTM	ISCX, CTU-13	<ul style="list-style-type: none"> Detection of DDoS attack in fog environment has been done. Attack launching tool Hping3 utilized for evaluation.
[19], [20]	CNN	KDD99	<ul style="list-style-type: none"> Established LeNet-5 model has been implemented. Each record is converted into a 32*32 matrix shape.
[22]	CNN, AE	KDD99	<ul style="list-style-type: none"> Dimensionality reduction using PCA and autoencoders. Input shape of 1*122 is transformed into 1*121 and 1*100 before converted to 10*10 and 11*11 shape.
[23]	RF, NDAE	KDD99, NSL-KDD	<ul style="list-style-type: none"> NDAE is utilized for unsupervised feature learning. For classification, stacked NDAE and RF have been combined.
[25]	CNN, RF, MLP, RNN	NSL-KDD	<ul style="list-style-type: none"> Comparative analysis of different models has been done.
[26]	RF, DT, KNN	CICIDS2017	<ul style="list-style-type: none"> Integration of Zeek IDS with ML models done. Zeek is used to extract features while models for classification.
[29]	DT, KNN, SVM	CICIDS2017 (only DDoS)	<ul style="list-style-type: none"> Fisher score is used for selecting optimal features. Different ML models evaluated for a reduced set of features for detecting DDoS attacks.
[27]	BLSTM, CNN	NSL-KDD	<ul style="list-style-type: none"> Combination of BLSTM and attention mechanism is done. CNN captures local features from traffic data.

From the literature review, it can be observed:

- Majority of the academic research is done using KDD99 and NSL-KDD dataset despite criticism from researchers about it being outdated [32].
- Applicability and deployment of DL in detecting network anomalies is still in infancy stage.
- While implementing CNN, the preferred choice is 2D-CNN although 1D-CNN has better applicability.

III. PROPOSED METHODOLOGY

The proposed 1D-CNN model for classification of attacks consists of four steps:

Step 1: Data preprocessing - This step involves methods to make data suitable for model training.

Step 2: Model Training - Includes specifying the architecture of a model and then train the model.

Step 3: Testing - Testing the model on unobserved data separated from training dataset.

Step 4: Evaluation – Evaluating the model using multiple metrics mentioned.

These steps form the basis for the overall process demonstrated in Fig. 1. First, the dataset is split into 80:20 train/test samples and then preprocessing of data is done on both. Model with basic initial architecture has been built upon which optimization is performed and training samples are then used to train the optimized model. Final model is tested using a test dataset with the help of various evaluation metrics.

These stages in the proposed 1D-CNN model along with description of the dataset used in the process are further elaborated in detail in following sub-sections.

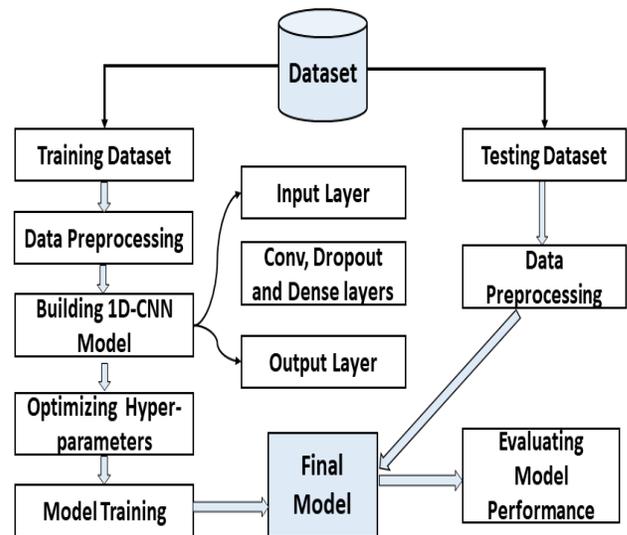


Fig. 1. Flow of the Proposed Methodology.

A. Dataset Description

As already mentioned, the CICIDS2017 dataset, created by the Canadian Institute for Cybersecurity consists of data scattered across eight files both in pcap and csv format [33]. It contains two directories containing 8 files each; GeneratedLabelledFlows has 85 features (including label) per record in each file and MachineLearningCSV, mostly used for ML/DL tasks and focus of this study, has 79 features. These features have been extracted using CICFlowMeter which is a network flow generator and most of the features extracted are time-based statistic features [34]. Csv files are the result of flow-based features extracted from pcap files using an analyzer. Data files used in our experiments contain time-related features embedded in them are further classified as:

Iat: the inter-arrival time between packets sent in backward, forward, or either direction; Psec: includes packets or bytes per second; Active/idle: specifies time a flow was active/idle before going idle/active; other: like duration, Flag count, etc.

As evident from Table II, there are 8 files out of which one file includes only benign data while the other 7 files contain benign and attack data. File1 contains two types of brute force attacks used for logging attempts and file1 includes application layer based Dos attacks launched using different tools like GoldenEye, Hulk, slowhttptest, and slowloris. Furthermore, file3 contains web related attacks like SQL injection, brute force, and XSS while file4 incorporates infiltration attack records. Lastly file5, file6, file7 include records of the bot, PortScan, and DDoS respectively.

1) *Data preprocessing*: It involves techniques for data preparation or transformation of values before data is fed to the model for training.it further consists of these steps:

a) *Handling of missing data*: There are two approaches for handling missing data; either drop the rows containing the missing value; or fill the cell with a new value. As the dataset contains a large number of missing values, the former approach looks irrational due to which the latter approach of filling these values is chosen. There are four options to select a new value ranging from a constant value like zero to the mean, mode, or median of the selective attribute. Either one could be okay but we carried out a pre-experiment with a small portion of the dataset before major experiments to find out the best replaced value.

b) *Feature scaling*: On reviewing the dataset, one can find huge disparities between values from different columns with attributes like SYN, PSH flag count have a smaller range on values while attributes like duration, total length have large magnitude values. To scale these values we use standardization which works on continuous numeric features and makes sure data in a column has 0 mean and unit variance. It is done to ensure each feature has equal weightage and let gradient descent converge quickly in the model training. The formula for standardization is given in equation 2:

$$\text{newval} = (\text{val} - \text{mean_val}) / \text{sd} \quad (2)$$

TABLE II. DATASET DESCRIPTION

S.no	Filename	Label	Records
File0	Monday-WorkingHours.pcap_ISCX.csv	Benign (Normal activities)	529918
File1	Tuesday-WorkingHours.pcap_ISCX.csv	Benign,FTP-Patator,SSH-Patator	445909
File2	Wednesday-WorkingHours.pcap_ISCX.csv	Benign, DoS GoldenEye DoSHulk, DoS slowhttptest, DoS slowloris, Heartbleed	692703
File3	Thursday-WorkingHours-Morning-WebAttacks.pcap_ISCX	Benign, Web attacks (BruteForce, Sql injection, XSS)	170366
File4	Thursday-WorkingHoursAfternoon-Infiltration.pcap_ISCX.csv	Benign, Infiltration	288602
File5	Friday-WorkingHoursMorning .pcap_ISCX.csv	Benign, Bot	191033
File6	Friday-WorkingHours-AfternoonPortScan.pcap_ISCX .csv	Benign, PortScan	286467
File7	Friday-WorkingHours-AfternoonDDos.pcap_ISCX.csv	Benign, DDoS	225745

Where val is actual value, mean_val and sd are mean and standard deviation of respective attribute.

c) *One hot encoding*: The last column/attribute representing class label in train dataset is one hot encoded to make it compatible with 1D-CNN model while training which expects target vector in said form. This results in additional columns for the output vector which is equal to the number of class labels (attacks and normal labels).

B. Model Architecture

The overall general architecture used in the experimental setup has been shown in Fig. 2. As we deal with different files the architecture of these separate models is uniform/identical albeit with minor changes. It consists of an input layer sequentially connected to 2 or 3 CNN layers intermixed by dropout and followed by flatten layer which further connects to a fully connected (FC) or dense layer and finally output layer. Input shape provided to the first Conv layer is (1* C) with 1 specifying the steps which is one row at a time and C states the number of features. With Conv layer mapping input to high dimension space, its output with dimension 1*C*f1 is the feature map containing f1 number of filters which learns network information from input data. This output is then applied to the activation function and for that purpose, the one used mostly with the Conv layer, ReLu is used. Dropout is then used to minimize the interaction of feature detectors switching off some connections randomly in the network thereby preventing model overfitting [35]. Dropout doesn't decrease the number of parameters in the model, it only prevents some of them from participating in the weight update process. The Softmax activation function is combined with an FC layer to output the classified results. The mathematical

formulae for ReLu and Softmax activation function are given in equation 3 and 4 where x and x_i are the input values while $f(x)$ and $\text{Softmax}(x)$ being the output values passed to the next layer respectively.

$$f(x) = \max(0, x) \quad (3)$$

$$\text{softmax}(x) = \frac{e^{x_i}}{\sum_j^n e^{x_j}} \quad (4)$$

1) *Parameters and Hyper-parameters*: Another important aspect of model architecture are the parameters, which are learned through training and hyper-parameters, selected or chosen manually. In the 1D-CNN model building, the type of hyper-parameters ranges from general hyper-parameters like batch size, number of iterations to the model-specific hyper-parameters like a number of layers, filters, size of the kernel, an initial rate of learning, loss function, optimizer, and activation function used. The total parameters depend on certain hyper-parameters like number of layers, filters or nodes in a certain layer and size of filter which might vary from model to model. The general architecture of the proposed model would be like: “Conv₁(f₁,k₁)-Dr₁(r₁)-Conv₂(f₂,k₂)-Dr₂(r₂)-----Conv_n(f_n,k_n)-Dr_n(r_n)-FC₁(nd₁)-FC₂(nd₂)”.

Here Conv, Dr, FC are convolutional, dropout, and fully connected layers respectively. The f_i , k_i refers to the number of filters and kernel-size in the i th convolutional layer whereas r_i signifies the rate of dropout. The nodes in the FC layers are nd_1 and nd_2 with the latter related to the nodes in the output layer and equal to the number of classes. As hyper-parameters are selected manually, the number of trainable parameters can be calculated as:

- a) No of parameters in first Conv layer= $C * f_1 * k_1 + b_1$. (b represents bias)
- b) No of parameters in other Conv layer= $f_{i-1} * f_i * k_i + b_i$.
- c) No of parameters in Dense layers = $nd_{i-1} * nd_i + b_i$.

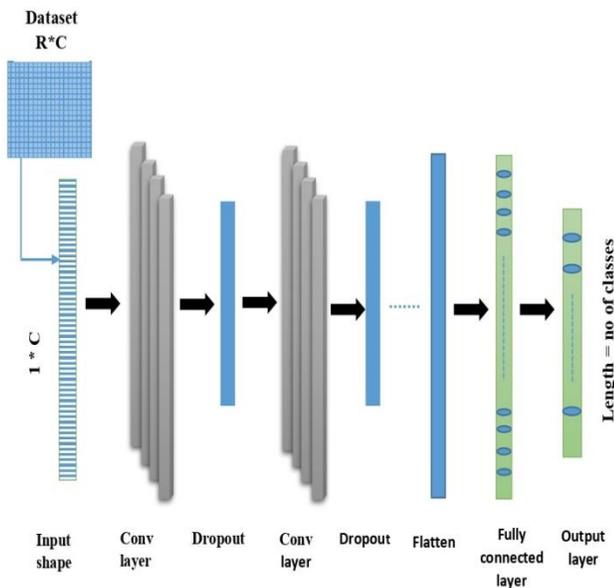


Fig. 2. Architecture of the 1D-CNN Model.

Thus, the total number of parameters in the particular model architecture is equal to the sum of parameters in all the layers. It is to be noted that the use of dropout is optional and has no effect on the number of parameters. Consider a model, for instance, with configuration “Conv(80,1)-Dr(0.2)-Conv(50,1)-Dr(0.2)-FC(50)-FC(2)”. Total number of trainable parameters could be calculated as: $(78*80*1+80) + (80*50+50) + (50*50+50) + (50*2+2) = 13022$ trainable parameters.

C. Model Evaluation

As our work is based on classification of multiple classes, multi-class confusion matrix is used to find or display correct/incorrect instances and its constituents are TP (True positive), TN (True negative), FP (False positive) and FN (False negative). Using these various evaluation indicators like Precision (Pr), Recall (Rc) and F1_score (F1_sc) can be derived to be further used for evaluation of model.

For classifying attack data, Pr or PPV (positive predicted value) specifies how many attack predictions actually belong to the attack data.

$$PPV = TP / (TP + FP) \quad (5)$$

Also Rc or TPR (true positive rate) specifies the ratio of predicted attack instances to the actual attack instances.

$$TPR = TP / (TP + FN) \quad (6)$$

Both PPV and TPR are suitable in their own way as former tells how attack predictions are relevant and latter tells the relevant records being predicted. Instead of choosing one over other there is another single metric F1_score calculating the harmonic mean of the both.

$$F1_sc = (2 * PPV * TPR) / (PPV + TPR) \quad (7)$$

IV. EXPERIMENTAL RESULTS AND ANALYSIS

A. Experimental Setup and Model Configuration

Experiments are conducted on google colab platform using python language and keras is the framework used for building 1D-CNN model with tensorflow as backend. Other important libraries used are pandas, numpy for loading/storing dataset and sklearn for preprocessing tasks and evaluating model and calculating results.

Different models built and evaluated might have distinct configurations of their architecture resulting in a different number of parameters and hyper-parameter values. The number of epochs and batch-size is not unique for each model but there are still some hyper-parameter values that are identical for all the models implemented in experiments and they are shown in Table III. Table IV shows the configuration parameters for each model, built during experimentation, with its complete model architecture.

B. Results

The overall experimental process is divided into two phases:

Phase1: Separate models built on individual files of dataset.

TABLE III. HYPER-PARAMETERS UNIFORM FOR ALL MODELS

Hyper-parameter	Value
Optimizer used	Adam
Kernel size	1
Learning rate	0.001 decay after certain epochs
Loss	Categorical Crossentropy
Activation function in all Conv layer	ReLU
Activation function in Dense layer	Softmax

TABLE IV. CONFIGURATION PARAMETERS FOR MODELS USED IN EXPERIMENTS

Model	Epochs	Batch size	Model Architecture	Trainable parameters
Model1	50	100	Conv(50,1)-Conv(40,1)-Conv(30,1)-FC(20)-FC(3)	7903
Model2	50	100	Conv(50,1)-Conv(40,1)-Conv(30,1)-FC(20)-FC(6)	7966
Model3	100	100	Conv(40,1)-Dr(0.1)-Conv(30,1)-Dr(0.1)-Conv(30,1)-Dr(0.2)-FC(20)-FC(4)	6024
Model4	20	100	Conv(80,1)-Dr(0.2)-Conv(50,1)-Dr(0.2)-FC(50)-FC(2)	13022
Model5	100	70	Conv(50,1)-Conv(50,1)-FC(25)-FC(2)	7827
Model6	60	40	Conv(40,1)-Dr(0.2)-Conv(30,1)-Dr(0.2)-FC(20)-FC(2)	5052
Model7	40	40	Conv(40,1)-Dr(0.1)-Conv(30,1)-Dr(0.1)-FC(20)-FC(2)	5052
Model(phase2)	50	100	Conv(60,1)-Conv(50,1)-Conv(40,1)-FC(20)-FC(8)	10818

Phase2: Model built on combined dataset except file0. Also some labels are combined and renamed to make it more balanced.

1) *Phase1*: During the first phase of experiments, individual files of the dataset have been used for building different models which means we have separate models for many different types of attacks. This means model1 is built on file1, model2 upon file2 and so on. This will be helpful if one wishes to detect a certain specific type of attack. For instance if you are interested in detecting DDoS attacks then model build using file7 will be useful and likewise for identifying bots model created using file5 is selected. Also processing individual files separately is good for attacks with less

instances as they have better prevalence in their respective files rather than in combined dataset. It should be emphasized that file0 is not used in the experimental process as it contains only benign traffic which means seven models were trained and evaluated. Each model built is used to classify normal and corresponding attacks in the individual files and further tested on 20% test data of their respective classes.

Table V shows the detailed evaluation of each model as their overall metrics results has not been displayed but detailed result for each class in every model as huge imbalance in the dataset would always results in better overall model performance. From the detailed analysis we can observe that attacks like XSS, Sql Injection and Bot have not performed well as compared to other attacks.

2) *Phase2*: For the second phase of experiments, combined dataset is considered for classification and all files except file0 is taken into account. As other files too containing benign records leading to large number of normal records in combined dataset, inclusion of records of file0 could led to more imbalanced data. So dataset is combined with seven files and this combined dataset contains 2,300,825 overall records. Model built on this could classify all attacks (14) in the dataset.

TABLE V. RESULTS (PHASE1)

Model	Class Label	PPV (%)	TPR (%)	F1_sc (%)
Model1	Benign	99.97	99.99	99.98
	FTP-Patator	99.87	99.62	99.75
	SSH-Patator	99.2	98.41	98.8
Model2	Benign	99.98	99.71	99.85
	DoS GoldenEye	99.8	99.06	99.43
	DoS Hulk	99.51	99.99	99.75
	DoS Slowhttptest	96.44	99.2	97.8
	DoS slowloris	99.13	99.22	99.18
	Heartbleed	100	80	88.89
Model3	Benign	99.98	99.8	99.89
	Web Attack – Brute Force	61.39	99.32	75.88
	Web Attack – XSS	100	60	75
	Web Attack – Sql Injection	22.22	1.56	2.92
Model4	Benign	100	100	100
	Infiltration	100	77.78	88.72
Model5	Benign	99.62	100	99.8
	Bot	100	64.82	79.53
Model6	Benign	99.98	99.99	99.99
	PortScan	99.99	99.98	99.99
Model7	Benign	99.96	99.98	99.97
	DDoS	99.98	99.97	99.98

As evident from the Table VI records containing benign traffic constitute 75.76% of all the instances in the concatenated dataset while attacks barring Dos/DDoS or Portscan are low prevalent. The combined dataset suffers from a class imbalance situation with some labels like Heartbleed, XSS having very few records which often results in a low detection rate for these labels [36]. We ran an experiment to build a model that would classify all 15 classes (14 attacks) in the dataset and the results are shown in Table VII where it can be easily observed that attacks with few testing records owing to their low prevalence are not classified properly. Attacks with sufficient training instances have performed satisfactory but for minority label attacks some attacks have zero correctly classified instances while others too have low detection accuracy.

TABLE VI. SHOWS PERCENTAGE OF OCCURRENCE OF EACH LABEL IN COMBINED DATASET

S no	New Attack label	Old Attack label	No. of Records	% of Total Records	No. of Records (new)	% of Total Records (new)
1	Benign	Benign	1743179	75.76	1743179	75.76
2	Brute Force	FTP-Patator	7938	0.345	13835	0.60
		SSH-Patator	5897	0.2562		
3	DoS	DoS GoldenEye	10293	0.447	252672	10.98
		DoS Hulk	231073	10.04		
		DoS slowloris	5476	0.239		
		DoS slowhttptest	5499	0.251		
		Heartbleed	11	0.0004		
4	Web Attacks	Web Attack-Brute Force	1507	0.0654	2180	0.0947
		Web Attack-XSS	652	0.028		
		Web Attack-Sql Injection	21	0.00091		
5	Bot	Bot	1966	0.085	2002	0.087
		Infiltration	36	0.0015		
6	PortScan	PortScan	158930	6.9075	158930	6.9075
7	DDoS	DDoS	128027	5.5643	128027	5.5643

To solve the class imbalance situation relabeling is done by merging minority class labels into one class label which proves to be a good measure for improving model performance. It is not done randomly but in a strategic way by merging similar categories of attacks. For example, SQL injection, XSS, and web attack-brute force are all types of web attacks so they are merged together and given new labels (web

attacks). Full details of the new attack label along with the percentage of occurrence are shown in the Table VI. After relabeling it now contains 7 classes including 6 attack labels and a model based on 1D-CNN is trained and then evaluated. The results for the same are shown in Table VIII and Table IX with the former displaying the confusion matrix based on all the labels and the latter illustrating the detailed results in metrics for all class labels. Analyzing the confusion matrix in Table VIII, the number of classifications or misclassifications with a particular class label predicted as another label can be properly seen. The same can be analyzed from Table IX as a high number of true positives were achieved for all class labels with the exception of the Bot and Web attacks label. The overall performance of the model is better as more than 99.6% output has been achieved in PPV, TPR, and F1_sc. Bot and Web attacks are the two labels with gloomy detection rate resulting in low values of TPR and F1_sc.

3) *Experiment with deep neural network:* To compare and further validate our proposed model, a DNN based on an artificial neural network has also been used. The experimental setup is identical with 1D-CNN i.e., the same preprocessing steps and evaluation metrics. DNN comprises of a) input layer with 78 nodes; b) 3 hidden layers with 60, 50, and 20 nodes, respectively; c) output layer with 8 nodes (like phase2). Also, dropout with 0.1 value is used between hidden layers to prevent overfitting. The results are depicted in Tables X and XI.

Table X displays the confusion matrix evaluated from the DNN-model and Table XI shows the comparative analysis of 1D-CNN with DNN. It can be analyzed from the latter table that 1D-CNN model has outperformed the model built using DNN in detection of network attacks.

TABLE VII. INITIAL RESULTS-15 CLASS CLASSIFICATION (PHASE2)

Label	PPV (%)	TPR (%)	F1_sc (%)
BENIGN	99.71	99.78	99.75
Bot	90.61	41.41	57.33
DDoS	99.98	99.92	99.96
DoS GoldenEye	99.57	98.47	99.12
DoS Hulk	99.09	99.20	99.15
DoS Slowhttptest	91.28	98.69	95.11
DoS slowloris	98.71	98.88	98.85
FTP-Patator	99.60	99.27	99.47
Heartbleed	100.00	66.67	80.00
Infiltration	50.00	100.00	67.00
PortScan	99.36	99.95	99.65
SSH-Patator	95.70	99.14	97.66
Web Attack Brute Force	100.0	11.89	21.58
Web Attack Sql Injection	nan	0.00	0.00
Web Attack XSS	0.00	0.00	0.00

TABLE VIII. CONFUSION MATRIX USING 1D-CNN FOR 7 CLASS CLASSIFICATION

True \ Predicted	BENIGN	Bot	Brute Force	DDoS	DoS	PortScan	Web Attacks	All
Benign	347743	3	30	11	791	205	0	348783
Bot	253	145	0	0	0	0	0	398
Brute Force	1723	0	2665	0	0	2	0	2683
DDoS	99	0	0	25534	1	0	0	25558
DoS	136	0	3	0	50043	0	0	50509
PortScan	5	0	0	0	11	31807	0	31823
Web Attacks	353	0	24	0	0	0	34	411
All	350112	148	2712	25545	50846	32014	34	460165

TABLE IX. DETAILED RESULTS- 7 CLASS CLASSIFICATION

Label	TP	FN	FP	PPV (%)	TPR (%)	F1_sc (%)
BENIGN	347743	1040	787	99.77	99.70	99.74
Bot	145	253	3	97.97	36.43	53.11
Brute Force	2665	18	56	97.94	99.33	98.63
DDoS	25534	24	11	99.96	99.91	99.93
DoS	50371	138	804	98.43	99.73	99.07
PortScan	31807	16	205	99.36	99.95	99.65
Web Attacks	34	377	0	100.00	8.27	15.28

TABLE X. CONFUSION MATRIX USING DNN FOR 7 CLASS CLASSIFICATION

True \ Predicted	BENIGN	Bot	Brute Force	DDoS	DoS	PortScan	Web Attacks	All
Benign	345697	6	69	9	2767	234	1	348783
Bot	257	141	0	0	0	0	0	398
Brute Force	31	0	2650	0	2	0	0	2683
DDoS	39	0	0	25517	2	0	0	25558
DoS	222	0	5	2	50280	0	0	50509
PortScan	51	0	0	1	11	31760	0	31823
Web Attacks	375	0	23	0	3	0	10	411
All	346672	147	2742	25529	53065	31994	11	460165

TABLE XI. COMPARISON OF 1D-CNN WITH DNN

Label	PPV (%)		TPR (%)		F1_sc (%)	
	CNN	DNN	CNN	DNN	CNN	DNN
BENIGN	99.77	99.72	99.70	99.12	99.74	99.42
Bot	97.97	95.92	36.43	35.43	53.11	51.74
Brute Force	97.94	96.47	99.33	98.77	98.63	97.61
DDoS	99.96	99.95	99.91	99.84	99.93	99.90
DoS	98.43	94.75	99.73	99.55	99.07	97.09
PortScan	99.36	99.27	99.95	99.80	99.65	99.53
Web Attacks	100.00	90.91	8.27	2.43	15.28	4.74

Analysis: While analyzing the results, it can be observed.

- In both phases, attacks with reasonable instances for training have produced exceptionally better results on testing data. Attacks like DoS, Brute force, DDoS, and Portscan have specific attack pattern and they are better detected using flow based features.
- Overall Bot and Web attacks have shown poor performance in both phases.
- Analyzing the results of Bot in phase2 (Table VIII), one can see similarities between Bot and Benign traffic as all FN and FP in case of Bot attack label belongs to benign label which indicates Bot is not classified as any other attack by the model and no other attack has been classified as Bot attack. This signifies the resemblance between the two as the distinction between bot and normal behavior is blurred.
- As for web attacks, their comparatively lower performance could be attributed to the fewer training instances in the dataset as they have less than 0.1 of total instances. Or these attacks don't have a specific pattern and they could be better detected using payload content.
- Also our proposed 1D-CNN model has outperformed the model built using DNN (Table XI).

V. CONCLUSION

In this paper, we proposed a novel way of identifying attacks in the dataset using 1D-CNN as a classification approach. The proposed 1D-CNN model has performed better with the least number of misclassifications. Experiments were conducted with a model trained and evaluated on individual files of the dataset as well on a combined dataset which was further relabeled to handle class imbalance situation. Satisfactory performance was recorded in both cases for the majority of labels as more than 99% output achieved in each of the evaluation indicators used. Some attacks with low prevalence like bot and web attacks have a comparatively lower detection rate. Experiments using DNN have also been done for comparative purposes and further validation of the proposed model.

As for future work, other DL algorithms need to be explored for training the model and a study regarding hyper-parameter optimization should be done to find the optimal model configuration. Moreover, other datasets with the latest attack types and real world traffic should be investigated for detection of cyber-attacks. Addition of records of bots and web related attacks needs to be done as more data is needed for training and to improve their detection accuracy.

REFERENCES

- [1] M. Uma, and G. Padmavathi, "A Survey on Various Cyber Attacks and their Classification," *Int. J. Netw. Secur.* 15(5), pp. 390-396, 2013.
- [2] E. Vasilomanolakis, S. Karuppayah, M. Mühlhäuser, and M. Fischer, "Taxonomy and survey of collaborative intrusion detection," *ACM Computing Surveys (CSUR)*, 47(4), pp. 1-33, 2015.
- [3] A. L. Buczak, and E. Guven, "A survey of data mining and machine learning methods for cyber security intrusion detection," *IEEE Communications surveys & tutorials*, 18(2), pp. 1153-1176, 2015.
- [4] Y. LeCun, L. Bottou, Y. Bengio, and P. Haffner, "Gradient-based learning applied to document recognition," *Proceedings of the IEEE*, 86(11), 1998, pp.2278-2324.
- [5] A. Krizhevsky, I. Sutskever, and G. E. Hinton, "Imagenet classification with deep convolutional neural networks" In *Advances in neural information processing systems*, pp. 1097-1105, 2012.
- [6] K. Simonyan, and A. Zisserman, "Very deep convolutional networks for large-scale image recognition," 2014, arXiv preprint arXiv:1409.1556.
- [7] C. Szegedy, W. Liu, Y. Jia, P. Sermanet, S. Reed, D. Anguelov, D. Erhan, V. Vanhoucke, and A. Rabinovich, "Going deeper with convolutions," In *Proceedings of the IEEE conference on computer vision and pattern recognition*, 2015 pp. 1-9.
- [8] S. Kiranyaz, O. Avci, O. Abdeljaber, T. Ince, M. Gabbouj, and D. J. Inma, "1D convolutional neural networks and applications: A survey," 2019, arXiv preprint arXiv:1905.03554.
- [9] A. Jacovi, O.S. Shalom, and Y. Goldberg, "Understanding convolutional neural networks for text classification," 2018, arXiv preprint arXiv:1809.08037.
- [10] H. Cho, and S.M. Yoon, "Divide and conquer-based 1D CNN human activity recognition using test data sharpening," *Sensors*, 18(4), p.1055, 2018.
- [11] T. Ince, S. Kiranyaz, L. Eren, M. Askar, and M. Gabbouj, "Real-time motor fault detection by 1-D convolutional neural networks," *IEEE Transactions on Industrial Electronics*, 63(11), pp.7067-7075, 2016.
- [12] S. Duque, and M.N. Omar, 2015, "Using data mining algorithms for developing a model for intrusion detection system (IDS)," *Procedia Computer Science*, 61, pp.46-51, 2015.
- [13] S. Aljawameh, M. Aldwairi, and M.B. Yassein, "Anomaly-based intrusion detection system through feature selection analysis and building hybrid efficient model," *Journal of Computational Science*, 25, pp.152-160, 2018.
- [14] A. Saied, R.E. Overill, and T. Radzik, "Detection of known and unknown DDoS attacks using Artificial Neural Networks," *Neurocomputing*, 172, pp.385-393, 2016.
- [15] R. Singh, H. Kumar, and R.K. Singla, "An intrusion detection system using network traffic profiling and online sequential extreme learning machine," *Expert Systems with Applications*, 42(22), pp.8609-8624, 2015.
- [16] R. Priyadarshini, and R. K. Barik, "A deep learning based intelligent framework to mitigate DDoS attack in fog environment," *Journal of King Saud University-Computer and Information Sciences*, 2019 <https://doi.org/10.1016/j.jksuci.2019.04.010>.
- [17] T. Aldwairi, D. Perera, and M.A. Novotny, "An evaluation of the performance of Restricted Boltzmann Machines as a model for anomaly network intrusion detection," *Computer Networks*, 144, pp.111-119, 2018.
- [18] T. Wisanwanichthan and M. Thammawichai, "A Double-Layered Hybrid Approach for Network Intrusion Detection System Using Combined Naive Bayes and SVM," *IEEE Access*, 9, pp.138432-138450, 2021.
- [19] W. Xu, J. Jang-Jaccard, A. Singh, Y. Wei, and F. Sabrina, "Improving Performance of Autoencoder-Based Network Anomaly Detection on NSL-KDD Dataset," *IEEE Access*, 9, pp.140136-140146, 2021.
- [20] Y. Liu, S. Liu, and X. Zhao, "Intrusion detection algorithm based on convolutional neural network," 2017 *DEStech Transactions on Engineering and Technology Research*, (iceta).
- [21] W.H. Lin, H.C. Lin, P. Wang, B.H. Wu, and J.Y. Tsai, "Using convolutional neural networks to network intrusion detection for cyber threats," In 2018 *IEEE International Conference on Applied System Invention (ICASI)*, IEEE, pp. 1107-1110, April 2018.
- [22] Y. Jia, M. Wang, and Y. Wang, "Network intrusion detection algorithm based on deep neural network," *IET Information Security*, 13(1), pp.48-53, 2018.
- [23] Y. Xiao, C. Xing, T. Zhang, and Z. Zhao, "An intrusion detection model based on feature reduction and convolutional neural networks," *IEEE Access*, 7, pp.42210-42219, 2019.

- [24] N. Shone, T.N. Ngoc, V.D. Phai, and Q. Shi, "A deep learning approach to network intrusion detection," *IEEE transactions on emerging topics in computational intelligence*, 2(1), pp.41-50, 2018.
- [25] S. Naseer, Y. Saleem, S. Khalid, M.K. Bashir, J. Han, M.M. Iqbal, and K. Han, "Enhanced network anomaly detection based on deep neural networks," *IEEE Access*, 6, pp.48231-48246, 2018.
- [26] A.K. Verma, P. Kaushik, and G. Shrivastava, "A Network Intrusion Detection Approach Using Variant of Convolution Neural Network," In *2019 International Conference on Communication and Electronics Systems (ICCES)*, IEEE, July 2019, pp. 409-416.
- [27] T. Su, H. Sun, J. Zhu, S. Wang, and Y. Li, "BAT: Deep learning methods on network intrusion detection using NSL-KDD dataset," *IEEE Access*, 8, pp.29575-29585, 2020.
- [28] V. Gustavsson, "Machine Learning for a Network-based Intrusion Detection System: An application using Zeek and the CICIDS2017 dataset," 2019.
- [29] B. Rababah, and S. Srivastava, "Hybrid Model For Intrusion Detection Systems," 2019, arXiv preprint arXiv:200308585.
- [30] D. Aksu, S. Üstebay, M.A. Aydin, and T. Atmaca, "Intrusion detection with comparative analysis of supervised learning techniques and fisher score feature selection algorithm," In *International Symposium on Computer and Information Sciences*, Springer, Cham, September 2018, pp. 141-149.
- [31] Z.K. Maseer, R. Yusof, N. Bahaman, S.A. Mostafa, and C.F.M. Foozy, "Benchmarking of machine learning for anomaly based intrusion detection systems in the CICIDS2017 dataset" *IEEE Access*, 9, pp.22351-22370, 2021.
- [32] J. McHugh, "Testing intrusion detection systems: a critique of the 1998 and 1999 darpa intrusion detection system evaluations as performed by lincoln laboratory," *ACM Transactions on Information and System Security (TISSEC)*, 3(4), pp.262-294, 2000.
- [33] I. Sharafaldin, A.H. Lashkari, and A.A. Ghorbani, "Toward generating a new intrusion detection dataset and intrusion traffic characterization," In *ICISSP*, January 2018, pp. 108-116.
- [34] G. Draper-Gil, A.H. Lashkari, M.S.I. Mamun, and A.A. Ghorbani, "Characterization of encrypted and vpn traffic using time-related," In *Proceedings of the 2nd international conference on information systems security and privacy (ICISSP)*, February 2016, pp. 407-414.
- [35] G.E. Hinton, N. Srivastava, A. Krizhevsky, I. Sutskever, and R.R. Salakhutdinov, "Improving neural networks by preventing co-adaptation of feature detectors," 2012, arXiv preprint arXiv:1207.0580.
- [36] S. Wang, L.L. Minku, and X. Yao, "A systematic study of online class imbalance learning with concept drift," *IEEE transactions on neural networks and learning systems*, 29(10), pp. 4802-4821, 2018.

Applying Grey Systems and Inverse Distance Weighted Method to Assess Water Quality from a River

Alexi Delgado¹, Anthonny Fernandez², Eduardo Lozano³, Dennis Miguel⁴, Félix León⁵, Jhosep Arteta⁶, Ch. Carbajal⁷
Mining Engineering Section, Pontificia Universidad Católica del Perú, Lima, Peru¹
Environmental Engineering Faculty, Universidad Nacional de Ingeniería, Lima, Peru^{2,3,4,5,6}
Administration Program, Universidad de Ciencias y Humanidades, Lima, Peru⁷

Abstract—The Cañete River basin, in Peru, has suffered an increase in pollution due to various causes, among the main ones being the lack of knowledge, culture of individuals and municipal authorities, economic activities, among others. We analyze this degree of pollution reflected in the upper part of the Cañete river basin through the Grey Clustering method, based on grey systems, which is presented as a good alternative to evaluate water quality in a comprehensive way, making use of Historical data from the monitoring program for the years 2014 and 2015 with nine monitoring points carried out by the National Water Authority (ANA), 6 parameters were defined to evaluate: Hydrogen potential (pH), Biochemical oxygen demand, Chemical demand of Oxygen, Total Suspended Solids, Total Manganese and Total Iron based on the PRATI index. For the spatial distribution, interpolation surfaces of the clustering coefficients were created, using the Spatial Analyst extension of the ArcGIS software, which provides tools to create, analyze and map data in raster format or surfaces. The interpolation method used is Inverse Distance Weighted (IDW). The results of the evaluation showed that in 2014 the monitoring points determined, through the Grey Clustering method, a level of contamination "Uncontaminated" at each point except for point P7 which gives us an "Acceptable" level according to the PRATI indices, while for the year 2015 points P1 and P2 indicate a level of contamination "Moderately contaminated", point 3 an "Acceptable" level, after points P4 to P9 they present a level of "Not contaminated". Finally, the Grey Clustering analysis method will determine the water quality in the 9 monitoring points of the upper-middle basin of the Cañete River in the years 2014 and 2015. Allowing to observe the reduction of water quality in points P1 and P2 for the period of the years 2014 and 2015 respectively, being crucial to achieve water resource management among local governments that can insert awareness and sustainable development policies.

Keywords—Grey systems; inverse distance weighted (IDW); water quality

I. INTRODUCTION

In the Cañete River basin, agriculture constitutes the main socioeconomic activity in the valley and is the activity with the highest water consumption. The intensive and unplanned use of the water resources of the Cañete River Basin puts at risk the modification of the characteristics of water availability and quality, so it is important to maintain an adequate quality of the water resource (ANA). For this, it is necessary to evaluate the

current state of water resources such as rivers that are the receivers of effluents [1].

As rivers are the main receivers of effluents generated by the population, the quality parameters of river waters have deteriorated in recent years, basically due to the misuse of wastewater management by the population and the negligence of the authorities in solving water pollution through treatment and avoidance, affecting a large part of the agricultural activity of the valley in the lower part of the Cañete River basin and consequently the health of the population [2].

In the Cañete river basin, an increase in pollution is observed due to various causes, among the main ones are environmental ignorance, the culture of the people and the municipal authorities, being crucial to achieve the management of water resources among local governments where There are awareness policies and sustainable development can be inserted in the towns of its jurisdiction avoiding the contamination of said resource with the discharge of drains into rivers and the development of industrial, mining, agricultural economic activities and among other human activities [3].

Therefore, this work has the general objective of estimating the degree of contamination reflected in the river water quality data in nine monitoring points carried out by the ANA in the Alto Cañete basin in 2014 and 2015 using the Grey Clustering method, comparing it with an international scale the PRATI Index, for the study of water quality. To achieve the purpose of the research study, the following specific objectives were established:

- 1) Define the parameters to be evaluated, based on the PRATI index, to determine the degree of contamination of the rivers.
- 2) Carry out the Grey Clustering methodology for the monitoring points.
- 3) Rank the bodies of water by level of contamination.

There have been many recent investigations on the application of the grey clustering methodology to evaluate the environmental quality of different environmental components, but the one of interest in this study is on the quality of the water bodies that can, be affected by different sources such as economic activities anthropic, natural and among others, for

this reason some investigations related to this environmental component are presented below.

Alexis Delgado et al., In 2017 evaluated the water quality of the Rímac River in its main tributaries; Río Blanco, Aruri, Río Rímac, Río Mayo and Río Santa in which the CTWF method was applied, which is based on Grey's systems theory. on the other hand, the data used were obtained from the ANA in which they were analyzed according to the water quality parameters such as O₂, BOD, COD, SS, NH₃ and NO₃. Obtaining as results using the prati la clairvoyance index that the tributaries are classified as not contaminated, however, the Santa River presents greater vulnerability to contamination of the water quality [4].

Fu and Zou, in 2018, applied the Grey Clustering methodology to evaluate the water quality of 12 monitoring points in the Yellow River basin, using as real data those obtained through the monitoring of water quality from the Ministry of Environmental Protection China in May 2016, and as standard data, the surface water environmental quality standard. The results conclude that the general quality of the water in said basin is good, thus reaffirming the real situation of the basin. It is even concluded that the Grey Clustering method applied in the evaluation of water quality is reasonable, feasible and it is convenient to calculate [5].

Alexi Delgado et al. In 2019 they carried out the study called "Water quality in areas close to mining: Las Bambas, Peru" located the study place in the district of Tambobamba, province of Cotabambas, in the Apurímac region. The contamination levels of the water bodies due to the Las Bambas mine towards the area of influence that includes the Challhuahuacho and Ferrobamba rivers were evaluated. Obtaining as results that from the six monitoring points located, carried out between February 2017 and March 2019 by ANA, the rivers would have a low or high degree of contamination [6].

The authors Alexi Delgado et al., 2020 carried out the study called "Evaluation of the quality of surface water in the upper basin of the Huallaga river, in Peru, using grey systems and Shannon entropy" where the quality of the water in the basin was evaluated Upper Huallaga river taking into account the results of the monitoring of twenty-one points carried out by the National Water Authority (ANA) analyzing nine parameters of the PRATI Index. The results showed that all the monitoring points of the Huallaga River were classified as uncontaminated, which means that the discharges, generated by economic activities, are carried out through treatment plants that meet the quality parameters [7].

II. DATA

A. Water Quality Parameters of the Cañete River Basin

According to the ANA in its report IT 148-2019-ANA-CAÑETE determines 3 studies to identify polluting sources in the years 2010, 2014, 2017 regarding the Cañete river basin that could be affecting the quality of its waters, in this report it is described that finding the location of these sources is of

utmost importance to establish measures for their recovery and preservation of the water resource, the data that it gives us is that there are 40 sources of contamination distributed throughout the basin, which is found in greater numbers In the upper part of the Cañete river basin, the ANA in the report mentions that the river is affected by the discharges of wastewater of domestic origin, as the main sources of contamination due to the lack of maintenance of the equipment of water treatment or in the absence of these. These reports can also be corroborated with the study carried out by the University of Cañete in 2018 that determines the influence of river pollution with the development of the Province of Cañete.

For the evaluation of surface water quality through Grey Clustering, use is made of monitoring reports from a reliable source. The Cañete Fortaleza Water Administrative Authority, monitors the quality of the natural bodies of surface water in the Cañete river basin, establishing itself to carry out the monitoring network of 15 monitoring points in 2014 and 20 monitoring points of monitoring in 2015 throughout the basin, as a consequence of the results of the identification of polluting sources determined in the Technical Report made by the administrative authority of the basin (N°139-2014-ANA-AAA.CF- ALA.MOC-AT/LEAP). In the same way, taking as a reference the results of the water quality monitoring for the years 2014 and 2015 (N°060-2014-ANA-DGCRH/GOCRH y N°086-2015-ANA-DGCRH/GOCRH), 9 monitoring points were determined located in the upper basin of the Cañete River, due to the presence of new activities that could generate alterations to the water quality after 2014.

The influence is established by non-experimental methodology, using the survey technique. The surveys are carried out with 100 inhabitants living on the banks of the Cañete River (the districts of Zuniga, Pacaran and Lunahuana are included in the surveys). The study concludes with a perception of moderate and high contamination of the Cañete riverbed due to the discharge of wastewater from the growing tourist activity within the districts, as well as the discharge of domestic water from the growing city, having clear what are the discharges [8].

Having clear the type of discharge that predominates, the basic parameters were chosen in a monitoring study such as pH, BOD, COD, SST and two additional parameters were also added with which are iron and manganese for study purposes as shown in Table I.

TABLE I. PARAMETERS PRIORITIZED FOR THE EVALUATION OF WATER QUALITY

Parameters	Units	Notation
pH	pH	C1
BOD	ppm	C2
DQO	ppm	C3
STS	mg/L	C4
Mn	ppm	C5
Fe	ppm	C6

III. METHODOLOGY

The development of this study is established through three approaches. At the beginning, we will proceed with the description of the study area and the different water bodies, to be considered, in said area to focus the investigation. Then, to evaluate the water bodies according to their quality, we will proceed with the Grey Clustering method. And finally, the spatial distribution of the Water quality will be analyzed using ArcGis.

The analysis of surface water quality was carried out in the upper part of the Cañete River basin (Fig. 1), which is in the central zone of Peru and has a surface area of 1,756.05 km².

A. Case Study

In 2014 and 2017, the National Water Authority has carried out identification of polluting sources in the Cañete River basin, allowing to know in detail the activities that would be affecting the quality of the water bodies in the Cañete River basin. The results indicate that there is an increase in the number of discharges of domestic wastewater discharged to the receiving body from 12 to 19. There is also a couple that are the main reference for the programming of management actions in the Cañete Basin. In order to establish measures for its recovery and conservation of surface waters [9] which is represented in Fig. 2.

For the evaluation of the surface water quality of the upper Cañete River basin, information was collected from 9 monitoring points obtained from the water quality monitoring carried out from December 15 to 19, 2014 [10] and from October 19 to 23, 2015 (ANA, 2015) by the Cañete Fortaleza Water Administrative Authority and the Mala Omas Cañete Local Water Authorities which is represented in Fig. 3.

B. Data Processing: Grey Clustering

This section describes the method established in Grey Clustering, based on grey systems. Being originally developed by Deng [11] in his Grey System Theory. Where the central point triangular standardization weight function (CTWF) will be used to test if the observation objects belong to predetermined classes, so that they can be treated accordingly to their characteristics [12].

1) Explanation of the Grey Clustering method:

a) *Step 1: Data Sizing:* The dimensioning of the water quality monitoring data of each environmental indicator and of the selected Water Quality Index parameters is carried out.

b) *Step 2: Grey Clustering Classification:* The Grey classification is established from the Environmental Quality Index chosen by the CTWF method, as can be seen in Fig. 4.



Fig. 1. Cañete River Basin, Peru.

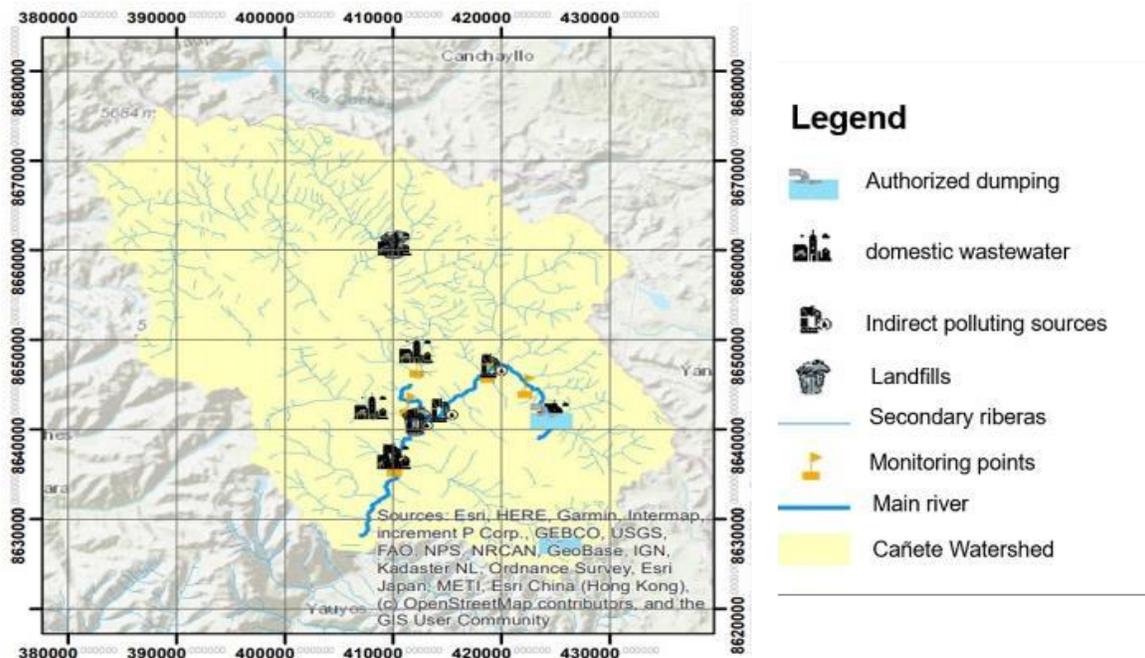


Fig. 2. Pollutant Sources of the upper Cañete River Basin.

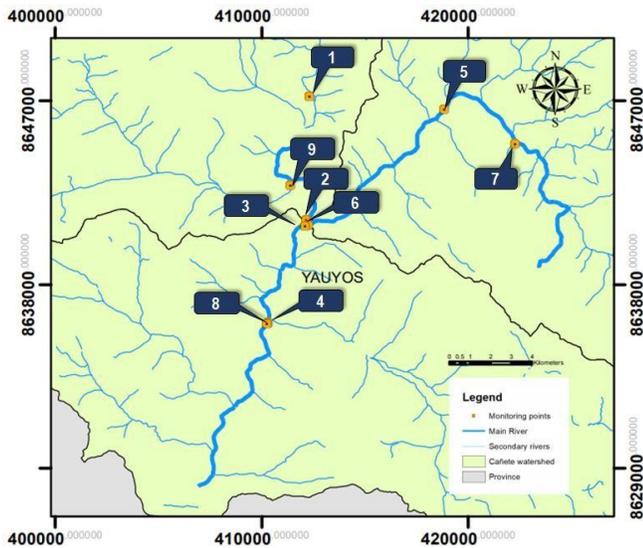


Fig. 3. Control Points for the Quality of Surface Waters in the Upper Cañete River Basin.

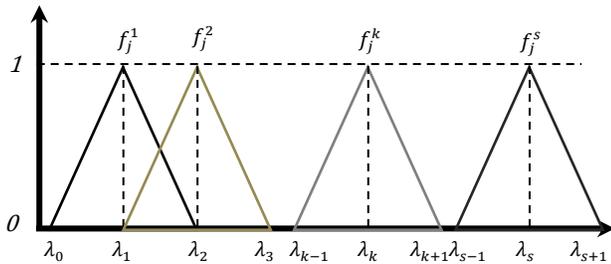


Fig. 4. Central Point Triangular Standardization Weight Function in Relation to the Selected Environmental Quality Index.

If there is a greater range of environmental quality, more functions will be increased, following the same procedure. Once the Grey classification has been established using the CTWF method, these are calculated from the k-nth class grey, $k = 1, 2, 3, 4, 5 \dots n$ of the j-nth parameter, $j = 1, 2 \dots n$, for a value of water quality monitoring X_{ij} according to the following functions [13]:

$$f_j^1(x_{ij}) = \begin{cases} 0; & x \notin [0, \lambda_j^2] \\ 1; & x \in [0, \lambda_j^2] \\ \frac{\lambda_j^2 - x}{\lambda_j^2 - \lambda_j^1}; & x \in [\lambda_j^1, \lambda_j^2] \end{cases} \quad (1)$$

$$f_j^m(x_{ij}) = \begin{cases} 0; & x \notin [\lambda_j^{m-1}, \lambda_j^{m+1}] \\ \frac{x - \lambda_j^{m-1}}{\lambda_j^m - \lambda_j^{m-1}}; & x \in [\lambda_j^{m-1}, \lambda_j^m] \\ \frac{\lambda_j^{m+1} - x}{\lambda_j^{m+1} - \lambda_j^m}; & x \in [\lambda_j^m, \lambda_j^{m+1}] \end{cases} \quad (2)$$

$$f_j^k(x_{ij}) = \begin{cases} 0; & x \notin [\lambda_j^k, \alpha] \\ \frac{x - \lambda_j^k}{\lambda_j^{k+1} - \lambda_j^k}; & x \in [\lambda_j^k, \lambda_j^{k+1}] \\ 1; & x \in [\lambda_j^{k+1}, \alpha] \end{cases} \quad (3)$$

c) Step 3: Weight of each parameter of the selected Environmental Quality Index: We proceed with the calculation of the weight of each parameter of the environmental quality index in an objective way, known as arithmetic weight, which is calculated according to Equation 4.

$$n_j^k = \frac{1/\lambda_j^k}{\sum_{j=1}^m 1/\lambda_j^k} \quad (4)$$

d) Step 4: Determination of the environmental quality classification of the evaluated point: Once the values evaluated in the Whitenization functions and the weights of each parameter have been determined, the Clustering coefficient is calculated for each value obtained in the different grey classifications by means of Equation 5 with the one with the highest value being σ_i^k the value that defines the environmental quality classification of the evaluated point according to Equation 6.

$$\sigma_i^k = \sum_{j=1}^n f_j^k(x_{ij}) \cdot n_j \quad (5)$$

$$\max_{1 \leq k \leq s} \{\sigma_i^k\} = \sigma_i^{k^*} \quad (6)$$

2) Application of the Grey Clustering method:

a) Step 1: PRATI water quality standard and its determination of central points: Table II shows the classification of the water quality level according to the PRATI Index. Being assigned as follows:

λ_1 : Not Contaminated.

λ_2 : Acceptable.

λ_3 : Moderately Acceptable.

λ_4 : Contaminated.

λ_5 : Highly Contaminated.

Then we proceed to determine the midpoints of each level of water quality established by the PATRI index. These points corresponding to each level (Table III) will be the central points to consider for the aforementioned symbology: $\lambda_1, \lambda_2, \lambda_3, \dots, \lambda_5$.

TABLE II. PRATI INDEX STANDARD DATA FOR WATER QUALITY ASSESSMENT

Parameters	Quality Status Index				
	λ_1	λ_2	λ_3	λ_4	λ_5
pH	6.5-8.0	8.0-8.4	8.4-9.0	9.0-10.1	>10.1
BOD (ppm)	0.0-1.5	1.5-3.0	3.0-6.0	6.0-12.0	>12.0
COQ (ppm)	0-10	10-20	20-40	40-80	>80
SST (mg/L)	0-20	20-40	40-100	100-278	>278
NH3 (ppm)	0-0.1	0.1-0.3	0.3-0.9	0.9-2.7	>2.7
NO3 (ppm)	0-4	4-12	12-36	36-108	>108
Cl (ppm)	0-50	50-150	150-300	300-620	>620
Mn (ppm)	0-0.05	0.05-0.17	0.17-0.50	0.50-1.00	>1.00
Fe (ppm)	0-0.1	0.1-0.3	0.3-0.9	0.9-2.7	>2.7

TABLE III. CORE VALUES OF THE PRATI INDEX

Parameters	Nomenclature	λ_1	λ_2	λ_3	λ_4	λ_5
pH	C1	7.25	8.20	8.70	9.55	10.40
BOD	C2	0.75	2.25	4.50	9.00	13.50
COD	C3	5.00	15.00	30.00	60.00	90.00
TSS	C4	10.00	30.00	70.00	189.00	308.00
Mn	C8	0.03	0.11	0.34	0.75	1.16
Fe	C9	0.05	0.20	0.60	1.80	3.00

Table IV and Table V present the results of the monitors in 9 points of the Cañete River in the upper middle basin of the same name, carried out by the ANA in the years 2014 (N°060-2014-ANA- DGCRH/GOCRH) and 2015 (N°086-2015-ANA-DGCRH/GOCRH).

b) *Step 2: Sizing the PRATI Index and the water quality monitoring data:* Table VI shows the oversized values of the PRATI Index, as well as the oversized values (Table VII) of the monitoring carried out by ANA in 2014 and 2015.

c) *Step 3: Clustering weights of the parameters:* Based on the values in Table IV, the values of the Clustering weights of each parameter of the Water Quality Index - PRATI were determined according to Equation 4. The values are shown in Table VIII.

d) *Step 4: Obtaining the Whitening functions and their evaluation:* To obtain the Whitening functions, with the five Grey classifications, the values of Table III were substituted in Equation 1, Equation 2 y Equation 3. Next, the data in Table VI was evaluated in the Whitening functions formed, yielding the following values shown in Table IX and so on for the remaining points except for P3 and P6.

e) *Step 5: Results using the max. Clusterization Coefficients:* To conclude, we proceed to calculate the highest value of $\{\sigma k\}$, based on Equation 6. With this, it was possible to determine to which Grey Class each monitoring point belongs and what water quality each of the nine monitoring points, the results are observed in Table X and Table XI, for the years 2014 and 2015 respectively.

TABLE IV. VALUES OF THE MONITORING PARAMETERS OF THE NINE POINTS OF THE UPPER MIDDLE BASIN OF THE CAÑETE RIVER CARRIED OUT IN 2014

Results of water quality monitoring for the year 2014						
Points	C1	C2	C3	C4	C5	C6
P. 1	0.959	0.167	0.125	0.012	0.006	0.021
P. 2	0.964	0.167	0.125	0.012	0.003	0.013
P. 3	0.959	0.167	0.125	0.012	0.015	0.035
P. 4	0.963	0.167	0.125	0.012	0.003	0.016
P. 5	0.882	0.167	0.125	0.063	0.148	0.168
P. 6	0.884	0.167	0.125	0.012	0.028	0.036
P. 7	0.947	0.333	0.25	0.064	0.232	0.286
P. 8	0.85	0.167	0.125	0.063	0.005	0.022
P. 9	0.827	0.333	0.25	0.071	0.02	0.203

TABLE V. VALUES OF THE MONITORING PARAMETERS OF THE NINE POINTS OF THE UPPER MIDDLE BASIN OF THE CAÑETE RIVER CARRIED OUT IN 2015

Results of water quality monitoring for the year 2015						
Points	C1	C2	C3	C4	C5	C6
P. 1	0.956	0.633	0.303	0.018	15.142	0.42
P. 2	0.965	0.5	0.403	0.008	16.998	0.004
P. 3	0.946	0.617	0.403	0.008	26.004	0.006
P. 4	0.961	0.583	0.505	0.008	16.674	0.004
P. 5	0.974	0.5	0.505	0.008	16.255	0.086
P. 6	0.956	0.5	0.403	0.008	37.322	0.005
P. 7	0.968	0.6	0.303	0.008	14.314	0.196
P. 8	0.959	0.667	0.303	0.008	7.755	0.039
P. 9	0.823	0.667	0.303	0.008	5.619	0.019

TABLE VI. OVERSIZED VALUES OF THE PRATI INDEX

Parameters	Nomenclature	λ_1	λ_2	λ_3	λ_4	λ_5
pH	C1	0.822	0.930	0.986	1.083	1.179
BOD	C2	0.125	0.375	0.750	1.500	2.250
COD	C3	0.125	0.375	0.750	1.500	2.250
TSS	C4	0.082	0.247	0.577	1.557	2.537
Mn	C8	0.053	0.231	0.704	1.576	2.437
Fe	C9	0.044	0.177	0.531	1.593	2.655

TABLE VII. DIMENSIONING OF THE WATER QUALITY PARAMETERS OF THE MONITORING CARRIED OUT BY THE ANA FOR THE YEARS 2014 AND 2015

Sizing of the water quality parameters for the year 2014						
Points	C1	C2	C3	C4	C5	C6
P. 1	0.959	0.167	0.125	0.012	0.006	0.021
P. 2	0.964	0.167	0.125	0.012	0.003	0.013
P. 3	0.959	0.167	0.125	0.012	0.015	0.035
P. 4	0.963	0.167	0.125	0.012	0.003	0.016
P. 5	0.882	0.167	0.125	0.063	0.148	0.168
P. 6	0.884	0.167	0.125	0.012	0.028	0.036
P. 7	0.947	0.333	0.250	0.064	0.232	0.286
P. 8	0.850	0.167	0.125	0.063	0.005	0.022
P. 9	0.827	0.333	0.250	0.071	0.020	0.203
Sizing of the water quality parameters for the year 2015						
Points	C1	C2	C3	C4	C5	C6
P. 1	0.956	0.633	0.303	0.018	15.142	0.42
P. 2	0.965	0.500	0.403	0.008	16.998	0.004
P. 3	0.946	0.617	0.403	0.008	26.004	0.006
P. 4	0.961	0.583	0.505	0.008	16.674	0.004
P. 5	0.974	0.500	0.505	0.008	16.255	0.086
P. 6	0.956	0.500	0.403	0.008	37.322	0.005
P. 7	0.968	0.600	0.303	0.008	14.314	0.196
P. 8	0.959	0.667	0.303	0.008	7.755	0.039
P. 9	0.823	0.667	0.303	0.008	5.619	0.019

TABLE VIII. CLUSTERING WEIGHTS FOR EACH PARAMETER

Clustering weights of each parameter						
Points	C1	C2	C3	C4	5	C6
λ_1	0.018	0.118	0.118	0.179	235	0.333
λ_2	0.053	0.130	0.130	0.198	212	0.276
λ_3	0.116	0.153	0.153	0.199	162	0.216
λ_4	0.222	0.160	0.160	0.154	153	0.151
λ_5	0.290	0.152	0.152	0.135	141	0.129

TABLE IX. FUNCTIONS VALUES FOR EACH PARAMETER

Whitening function evaluated at P3 (2014)							
	C1	C2	C3	C4	C5	C6	σ_i^k
f_1	0.000	0.832	1.000	1.000	1.000	1.000	0.962
f_2	0.482	0.168	0.000	0.000	0.000	0.000	0.047
f_3	0.518	0.000	0.000	0.000	0.000	0.000	0.060
f_4	0.000	0.000	0.000	0.000	0.000	0.000	0.000
f_5	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Whitening function evaluated at P6 (2014)							
f_1	0.424	0.832	1.000	1.000	1.000	1.000	0.970
f_2	0.576	0.168	0.000	0.000	0.000	0.000	0.052
f_3	0.000	0.000	0.000	0.000	0.000	0.000	0.000
f_4	0.000	0.000	0.000	0.000	0.000	0.000	0.000
f_5	0.000	0.000	0.000	0.000	0.000	0.000	0.000
Whitening function evaluated at P3 (2015)							
f_1	0.000	0.000	0.000	1.000	0.000	1.000	0.512
f_2	0.720	0.356	0.927	0.000	0.000	0.000	0.205
f_3	0.280	0.644	0.073	0.000	0.000	0.000	0.143
f_4	0.000	0.000	0.000	0.000	0.000	0.000	0.000
f_5	0.000	0.000	0.000	0.000	1.000	0.000	0.141
Whitening function evaluated at P6 (2015)							
f_1	0.000	0.000	0.000	1.000	0.000	1.000	0.512
f_2	0.540	0.667	0.927	0.000	0.000	0.000	0.236
f_3	0.460	0.333	0.073	0.000	0.000	0.000	0.116
f_4	0.000	0.000	0.000	0.000	0.000	0.000	0.000
f_5	0.000	0.000	0.000	0.000	1.000	0.000	0.141

3) *Spatial distribution of the condition of water quality:* To perform the spatial distribution, it was established to create interpolation surfaces of the clustering coefficients, where the Spatial Analyst extension of the Arcgis software is used, which provides tools to create, analyze and map data in raster format or surfaces. Water quality interpolations will be carried out to estimate the pollution values in the selected section of the Cañete River Basin. The interpolation method used is the Inverse Distance Weighted or "IDW" (Inverse Distance Weighted). Where the IDW assumes that each water quality monitoring point has a local influence that decreases with distance. This is observed in more detail in Fig. 5 of the years 2014 and 2015, therefore, these images were the result of the spatial distribution analysis thrown by ArcGIS.

For the interpolation of the water quality data, the 8 monitoring points were located to generate the area of influence of the 50-meter section around the Cañete River channel so that it can be visible on an adequate scale. The area of influence established by the monitoring from the ANA, starts from downstream from the town of Llapay and the Laraos river (RCañe4) to downstream from the Viti district (RCañe1) and upstream from the Huancachi town center (Ralis3).

The value determined by the Grey Clustering for the Z value field was used and the size of the grid or cell was defined as 1 meter. The area of influence is used to delimit the interpolated values. Finally, the IDW water quality surfaces were generated for each of the areas of influence. Where the maximum clustering coefficients were classified to classify the stretch of river in 5 classes established in the PRATI Index:

- Not contaminated.
- Acceptable.
- Moderately polluted.
- Contaminated.
- Highly polluted.

TABLE X. EVALUATION OF WHITENING FUNCTIONS IN THE NINE POINTS FOR THE YEAR 2014

Parameter	Maximum Clusterization Coefficient	Water Quality Level
P1	0.9623	Not contaminated
P2	0.9623	Not contaminated
P3	0.9623	Not contaminated
P4	0.9623	Not contaminated
P5	0.5404	Not contaminated
P6	0.9700	Not contaminated
P7	0.5927	Acceptable
P8	0.9756	Not contaminated
P9	0.5092	Not contaminated

TABLE XI. EVALUATION OF WHITENING FUNCTIONS IN THE NINE POINTS FOR THE YEAR 2015

Parameter	Maximum Clusterization Coefficient	Water Quality Level
P1	0.308	Moderately polluted
P2	0.799	Moderately polluted
P3	0.512	Not contaminated
P4	0.512	Not contaminated
P5	0.407	Not contaminated
P6	0.512	Not contaminated
P7	0.423	Acceptable
P8	0.546	Not contaminated
P9	0.564	Not contaminated

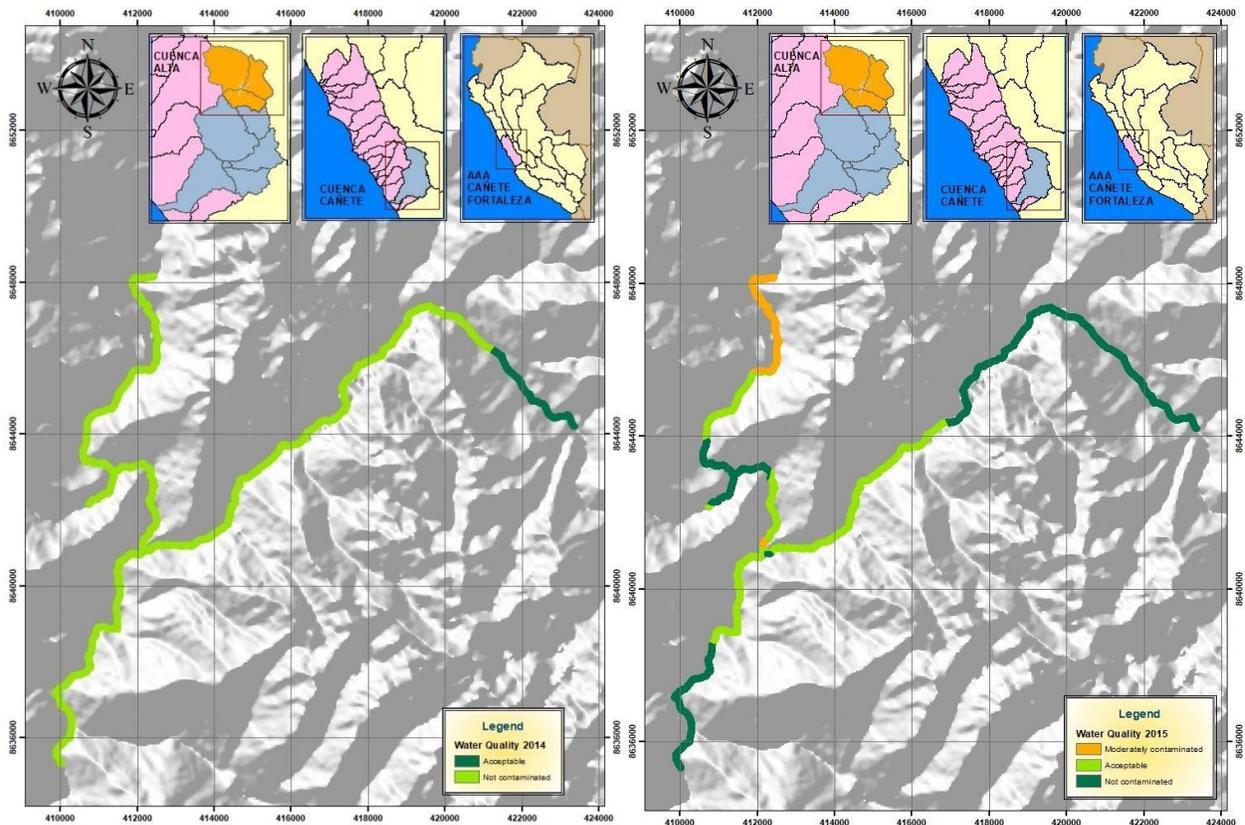


Fig. 5. Distribution of Water Quality in 2014 (Left) and 2015 (Right).

IV. RESULT AND DISCUSSION

A. About the Case Study

It is shown that for the year 2014, in Table X, that 8 monitoring points resulted in an uncontaminated water quality except for monitoring point 7, which has an Acceptable water quality, however, a comparison can be made of the quality level according to the maximum Clusterization coefficient.

Likewise, for the year 2015, in Table XI, 6 monitoring points resulted in an "uncontaminated" water quality, while monitoring points 1 and 2 have a "Moderately contaminated" water quality except for the point of monitoring 3 that has an "Acceptable" water quality and a comparison of the quality level was made according to the maximum Clusterization coefficient.

According to Fig. 6, for the years 2014 and 2015, the maximum clustering coefficients decrease progressively and the majority is of "Unpolluted" quality, this because the study area is located in the upper basin of the Cañete River, where the affection of the water resource is not high compared to the middle or lower part of a basin.

B. Application of the ArcGIS Tool for Digitizing the Results of the Grey Clustering Method

The applied methodology uses a mixture of two tools the ArcGIS and the Grey method that are combined to show us the quality of the water on a geographical plane, indicating a thematic graph and of clear order, with respect to the Grey method, it offers an alternative to evaluate the quality of the

water, comprehensively considering the uncertainty within the analysis, as Delgado et al. tell us, 2020, due to taking as a section the upper part of the Chillón River Basin, a study of physicochemical parameters would not be sufficient because the river flow is not stationary and the concentrations over time are not therefore that this method takes that uncertainty in its methodology, therefore the method is well adapted for the evaluation of quality in the upper part or the stretch of the Cañete river, continuing with the use of the GIS tool (ArcGIS) defines us that it is system that allows to collect, organize, manage, analyze, share and distribute geographic information, that is why this tool projects the results to us throughout the section that was studied on a map where it could be analyzed in a more interactive way since it reflects the data in something visible [14].



Fig. 6. Variation in Water Quality in 2014 and 2015.

C. Analysis of the Results in the Year 2014-2015

It is observed that in 2014 the monitoring points determined, through the Grey Clustering method, a null contamination at each point except for point P7 which gives us an acceptable level according to the PRATI indices, this is explained because according to the Report IT 060-2014-ANA-CAÑETE the values of the points taken do not present high concentrations with respect to the ECA-water [7]. Another point to consider is that there is no contamination by mining companies because the 2014 report does not show that the metals present concentrations that exceed the ECA, it is corroborated that a correct characterization of the parameters was taken because they were not took the parameter of thermo-tolerant coliforms because in the report of the aforementioned year it indicates in its results and discussion the coliforms parameter does not represent a risk because these concentrations of each point did not exceed the ECA and also for a point not taken from This report exceeds the ECA but studies indicate that it will not generate health hazards because they are not conservative to their activity since it is influenced by their temperature, biological activity and the physicochemical composition of water bodies.

For the year 2015, it presents a variation to the previous year because points P1 and P2 indicate a moderately contaminated contamination, point P3 shows us an acceptable level, after point P4 to P9 it presents us with an uncontaminated level. According to IT 086-2015-ANA CAÑETE, the Mn parameter presents higher concentrations compared to the previous year that even exceeds the ECA. This report indicates that the variation is due to the geochemical nature of the basin, however, the number of discharges has not changed and the concentrations in 2014 were below the ECA. This variation may be influenced by the presence of 3 authorized discharges to the Cañete River basin that appear on IT 086-2015-ANA CAÑETE, these are from the companies.

LNG SRL, whose discharges are from a mixed chamber, sewage from the manhole and industrial wastewater, respectively, this variation from point P1 to P4 can be contrasted with IT 148-2019- ANA CAÑETE since it indicates that point one o P1 is located below a district called "Vitis" which is at the height of a fish farm, while from point P2 to P4 there is a decrease in pollution due to factors such as a mixture of sections between the Cañete and Alis rivers.

D. Joint Analysis

The graph presented in the results gives us an indication of a variation in points P1 to P4 and at the other extreme points P6 to P8, having a variation in the year 2014-2015, according to report IT 148- 2019-ANA CAÑETE these points are found in the vast majority below districts such as Vitis, Laraos and a rise and fall is generated because the other points are present or in the mixing zone of rivers or the mixing zone of the sections [15].

V. CONCLUSION

The Grey Clustering analysis method allowed determining the water quality in the 9 monitoring points of the upper-middle basin of the Cañete River in the years 2014 and 2015. Allowing to observe the reduction of the water quality in the

points P1 and P2 for the period of the years 2014 and 2015 respectively. The first point is in the upper area of the Basin and the second point is at the confluence of the Alis and Cañete rivers. Thus, the loss of quality of the water resource is observed. The deterioration of the water quality in these points may cause, in the future, if the necessary mechanisms for the conservation of the water resource are not used, effects on the health of the surrounding populations and damage to their agriculture and livestock.

In the Grey Clustering methodology, in the stage of the evaluation of the Whitening Functions and use of the maximum Clusterization coefficients, it is observed that the points close to the point P2 have a water quality level cataloged as No Contaminated, however in the evaluations mentioned at the beginning of the paragraph it was observed that these points, P3 and P6, have a high probability of qualifying as Moderately Contaminated as they have Classification Coefficients close to these values. With this, it can be concluded that the points that are at the confluence of the Ríos Alis and Cañete are or are likely to vary their water quality, this due to the influence of the actions of the population found close to this area of the Cañete River.

The implementation of the IDW methodology complements what was developed in the Grey Clustering methodology, because it positions the quality level in a section by distributing it on a geographical map, generating a greater perception of the places that It has been altered and establishing a relationship between the present activities or geographical characteristics of the place, in which a greater analysis would be sought in the section in which it has been altered to verify the degree of impact and see a greater relationship against to the present activities.

REFERENCES

- [1] W. Zhuang, X. Zhao, F. Zhu, J. Liu, and H. Y. Xu, "Application of water quality evaluation model based on gray correlation analysis and artificial neural network algorithm," in Proceedings of 2017 9th International Conference On Modelling, Identification and Control, ICMIC 2017, Mar. 2018, vol. 2018-March, pp. 993-997, doi: 10.1109/ICMIC.2017.8321601.
- [2] S. A. Kumar, H. Kumar, V. Dutt, and H. Soni, "Self-Health Analysis with Two Step Histogram based Procedure using Machine Learning," in 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV), Feb. 2021, pp. 794-799, doi: 10.1109/ICICV50876.2021.9388427.
- [3] V. E. Cabrera, P. E. Hildebrand, and J. W. Jones, "Modelling the effect of household composition on the welfare of limited-resource farmers in Coastal Cañete, Peru," *Agric. Syst.*, vol. 86, no. 2, pp. 207-222, Nov. 2005, doi: 10.1016/J.AGSY.2004.08.009.
- [4] A. Delgado and I. Romero, "Social impact assessment on a hydrocarbon project using triangular whitenization weight functions," CACIDI 2016 - Congreso Argentino de Ciencias de la Informatica y Desarrollos de Investigacion. 7785998, doi: 10.1109/CACIDI.2016.7785998.
- [5] X. Q. Fu and Z. H. Zou, "Water Quality Evaluation of the Yellow River Basin Based on Gray Clustering Method," *IOP Conf. Ser. Earth Environ. Sci.*, vol. 128, no. 1, 2018, doi: 10.1088/1755-1315/128/1/012139.
- [6] 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.
- [7] V. Bax, W. Francesconi, and A. Delgado, "Land-use conflicts between biodiversity conservation and extractive industries in the Peruvian

- Andes,” *J. Environ. Manage.*, vol. 232, 2019, doi: 10.1016/j.jenvman.2018.12.016.
- [8] V. Duong, A. Ahmed, and O. Farook, “A model template green environment initiative for recycling plastic bottles with progressive entrepreneurship partnership,” *PICMET 2018 - Portl. Int. Conf. Manag. Eng. Technol. Manag. Technol. Entrep. Engine Econ. Growth, Proc.*, pp. 1–5, 2018, doi: 10.23919/PICMET.2018.8481786.
- [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] A. N. del A. D. de G. de C. de los R. Hídricos, “Resultado del monitoreo de la calidad de agua de la cuenca del río Cañete (realizado del 15 al 19 de Diciembre de 2014): Informe técnico,” *Aut. Nac. del Agua*, 2014, Accessed: Oct. 27, 2021. [Online]. Available: <https://repositorio.ana.gob.pe/handle/20.500.12543/2574>.
- [11] Sifeng Liu and Jeffrey Yi Lin Forrest, *Grey Systems: Theory and Applications*. 2014.
- [12] S. Liu and Y. Lin, *Grey Systems Theory and Applications*, vol. 68. Springer Berlin Heidelberg, 2011.
- [13] A. Delgado, A. Aguirre, E. Palomino, and G. Salazar, “Applying triangular whitenization weight functions to assess water quality of main affluents of Rimac river,” *Proceedings of the 2017 Electronic Congress, E-CON UNI 2017, 2018-January*, pp. 1-4, doi: 10.1109/ECON.2017.8247308.
- [14] C. M. Viana, P. Abrantes, and J. Rocha, “Introductory Chapter: Geographic Information Systems and Science,” *Geogr. Inf. Syst. Sci.*, no. November, 2019, doi: 10.5772/intechopen.86121.
- [15] S. C. Wu, K. Y. Ke, H. T. Lin, and Y. C. Tan, “Optimization of Groundwater Quality Monitoring Network Using Risk Assessment and Geostatistic Approach,” *Water Resour. Manag.*, vol. 31, no. 1, pp. 515–530, 2017, doi: 10.1007/s11269-016-1545-x.

Unsupervised Machine Learning Approach for Identifying Biomechanical Influences on Protein-Ligand Binding Affinity

Arjun Singh

Student, Watchung Hills Regional High School
Warren, New Jersey, United States

Abstract—Drug discovery is incredibly time-consuming and expensive, averaging over 10 years and \$985 million per drug. Calculating the binding affinity between a target protein and a ligand through Virtual Screening is critical for discovering viable drugs. Although supervised machine learning (ML) can predict binding affinity accurately, models experience severe overfitting due to an inability to identify informative properties of protein-ligand complexes. This study used unsupervised ML to reveal underlying protein-ligand characteristics that strongly influence binding affinity. Protein-ligand 3D models were collected from the PDBBind database and vectorized into 2422 features per complex. Principal Component Analysis (PCA), t-Distributed Stochastic Neighbor Embedding (t-SNE), K-Means Clustering, and heatmaps were used to identify groups of complexes and the features responsible for the separation. ML benchmarking was used to determine the features' effect on ML performance. The PCA heatmap revealed groups of complexes with binding affinity of $pK_d < 6$ and $pK_d > 8$ and identified the number of CCCH and CCCCCH fragments in the ligand as the most responsible features. A high correlation of 0.8337, their ability to explain 18% of the binding affinity's variance, and an error increase of 0.09 in Decision Trees when trained without the two features suggests that the fragments exist within a larger ligand substructure that significantly influences binding affinity. This discovery is a baseline for informative ligand representations to be generated so that ML models overfit less and can more reliably identify novel drug candidates. Future work will focus on validating the ligand substructure's presence and discovering more informative intra-ligand relationships.

Keywords—Drug discovery; unsupervised machine learning; feature engineering; protein-ligand binding affinity; virtual screening

I. INTRODUCTION

Drug discovery is the basis of the modern pharmaceutical market and encompasses most of the industry's research and development funding [1]. On average, it takes 12-15 years and \$985 million to deliver a drug to market, demonstrating the exhaustive time and effort required to complete the drug discovery process [2, 3]. Drug-Target Interaction (DTI) analysis is one of the most critical parts of drug discovery, and it involves calculating the binding affinity between a target protein and a ligand molecule so that appropriate ligand candidates for drugs can be chosen. These ligand candidates go on to be included in in vitro experimentation in order to identify lead compounds for the final drug. The affinity of a

ligand to bind with a protein depends on the atomic interactions between the ligand and the binding region (referred to as the "binding pocket") on the protein, as shown in Fig. 1 [4]. Calculating the binding affinity between a protein and ligand can be completed through Virtual Screening (VS), shown in Fig. 2, where compounds are screened and binding affinity calculated using molecular simulation software [5].

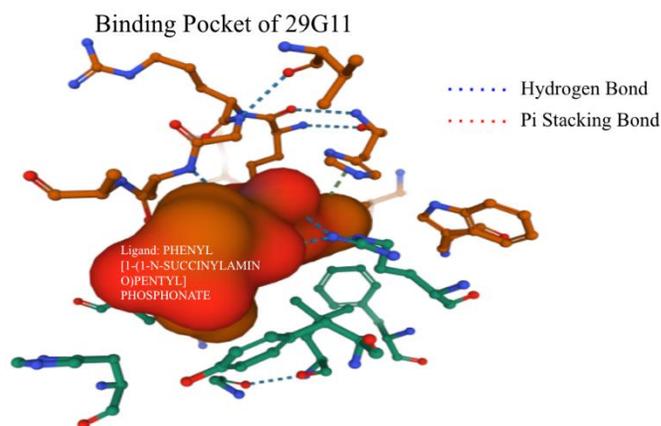


Fig. 1. Molecular view of Complex between 29G11 Protein and PHENYL [1-(1-N-SUCCINYLAMINO) PENTYL] PHOSPHONATE, Generated using Mol*.

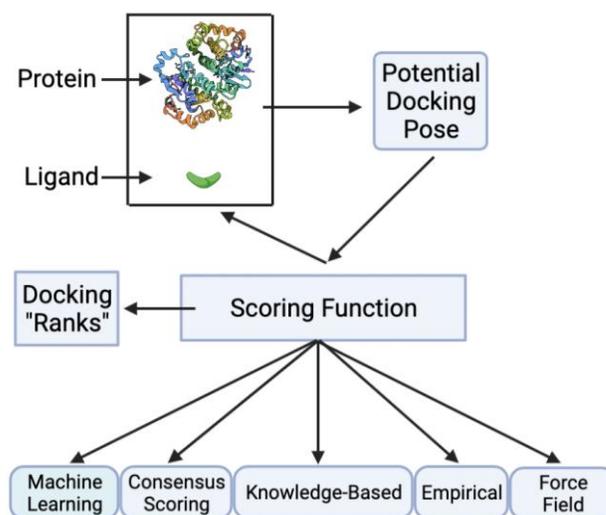


Fig. 2. Virtual Screening Workflow.

The “Scoring Function”, which is the function used to calculate binding affinity, is critical for VS. Machine Learning (ML) algorithms have demonstrated considerable promise as a scoring function compared to other standard function types [6]. Given a set of training data, ML algorithms are able to learn pharmaco-like features from protein-ligand models through supervised learning functions. This allows them to accurately predict the binding affinity based on learned features that have statistically high influence [7-9, 11]. However, ML algorithms “overfit”, or learn patterns that do not correlate to a physical phenomenon but still decrease error by chance [7-9, 11, 12]. This reduces their ability to generalize to out-of-distribution (OOD) data, making them unreliable for analyzing novel ligand candidates [7]. It is necessary to uncover underlying relationships between the features of protein-ligand data in order to inform the development of ML models that experience less overfitting [8].

Supervised learning techniques used to predict binding affinity can also analyze features, yet the results suffer from inconsistency and unreliability due to the overfitting of their parent algorithms [10, 13, 14, 18]. In comparison, unsupervised learning techniques such as Principal Component Analysis (PCA) are effective at identifying important features from protein-ligand models without overfitting because they are not designed to only minimize prediction error [15, 17]. t-Distributed Stochastic Neighbor Embedding (t-SNE) is also useful at visualizing the features of proteins due to its ability to retain high-dimensional information [16]. However, unsupervised learning has not been applied to analyze the differences between protein-ligand complexes in regard to binding affinity. This research can be filled help develop ML models that overfit considerably less.

The paper is structured as follows: Section II discusses the methodology, Section III presents and discusses the results, and Section IV concludes the study and proposes future work.

A. Objectives

There is a pressing need to reliably identify specific biomechanical features that influence binding affinity and quantify their effect on ML performance. Current literature either suffer from drawbacks in reliability and consistency caused by supervised learning or do not specifically analyze the variance in binding affinity caused by protein/ligand features. The objectives of this study are three-fold: 1) Discover the presence of underlying biomechanical interactions that influence binding affinity, 2) Identify specific pharmaco-like features responsible for high variance in binding affinities, and 3) Determine the effect of these features on the performance of ML models in predicting binding affinity.

Gathering a greater understanding of which features influence binding affinity is necessary for designing ML models that do not overfit to training data and interpret noisy features as important patterns. Models will thereby be more generalizable to OOD data, and more successful at identifying lead compounds for inclusion in innovative drugs.

II. METHODOLOGY

A. Dataset Preprocessing

In this study, protein-ligand models were collected from the PDBBind database [19, 41]. The 2015 “Refined” set and the 2015 “Core” set were downloaded. In order to extract relevant quantitative features of each model, a workflow described in [40] was utilized, as shown in Fig. 3.

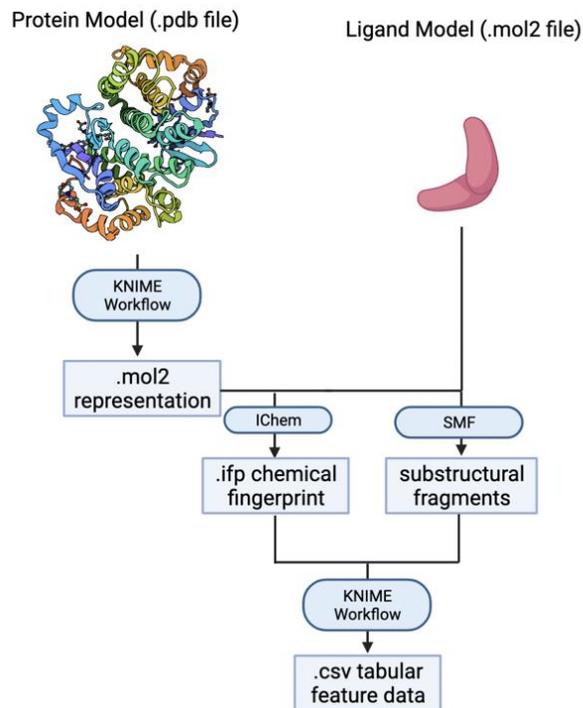


Fig. 3. Computational Workflow used to Translate 3D Molecular Models into 1D Tabular Data.

For each complex, 2422 quantitative features were collected. The frequency of 2282 unique substructural molecular fragments was collected. The remaining 140 features were frequencies of amino-acid interactions, with seven types of interactions per amino acid: 1) Hydrophobic, 2) Face-to-face aromatic, 3) Edge-to-edge aromatic, 4) H-bond accepted by ligand, 5) H-bond donated by ligand, 6) Ionic bond (ligand partially negative), and 7) Ionic bond (ligand partially positive). Files with a resolution of $<2.5 \text{ \AA}$ were retained to ensure the accuracy of all feature counts, resulting in 3481 complexes from the “Refined” set and 180 from the “Core” set.

B. Feature Analysis

To reveal underlying feature correlations in the dataset, a combination of PCA, t-SNE, K-Means Clustering, and heatmap projections shown in Fig. 4 were performed using Python and the Scikit-Learn, Pandas, and NumPy packages.

C. PCA/K-Means

PCA ($n=2$) was performed to transform the 2422-feature data into two dimensions for visualization and to capture the features with the highest variance. K-Means Clustering ($k=10$) was performed on this transformation to determine if there were categories of complexes. The similarity of the clusters was calculated using the Davies-Bouldin Score (DBS). The

presence of sparse categories and a low DBS would indicate an underlying biomechanical phenomenon between features. Another PCA (n=3) with K-Means Clustering (k=10) was performed to verify the outcome of the 2D PCA.

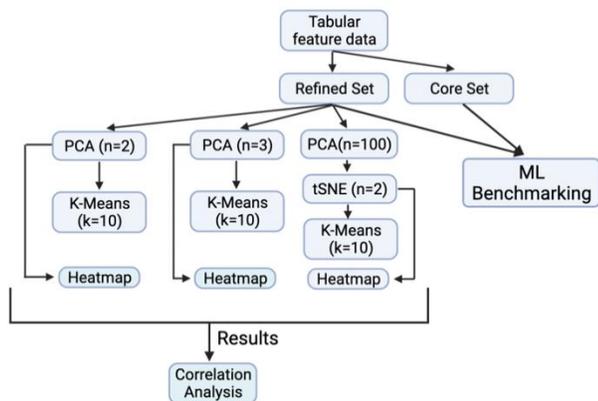


Fig. 4. Feature Analysis Workflow.

D. PCA/t-SNE/K-Means

Due to the ability of t-SNE to interpret non-linearity, a PCA (n=100) and then t-SNE (n=2) was performed to retain high-dimensional characteristics of the data. K-Means Clustering (k=10) was then performed to determine if the high-dimensional characteristics could describe separable categories of complexes. DBS was again used to score the similarity of the clusters.

E. t-SNE Heatmap

In order to determine if a biomechanical relationship could be demonstrated without clustering, a heatmap was generated of the t-SNE results where the “heat” was determined by the binding affinity. The quality of grouping was calculated using an adjusted R^2 correlation value. It is significant to note that there are 2422 features per complex; therefore what may seem to be low R^2 correlation values may actually be statistically significant due to the large number of features.

F. PCA Heatmap

In order to verify or refute the results of the t-SNE heatmap, a heatmap was generated with the PCA components in the same manner as the t-SNE heatmap. Similarly, the quality of grouping was evaluated using an adjusted R^2 correlation value.

G. Correlation Analysis

Although each clustering plot and heatmap could determine the presence of a biomechanical relationship, only the PCA plots could indicate which specific features are statistically responsible for it because each Principal Component is organized along the variance of each feature. Whichever 2D PCA plot (clustered plot or heatmap) indicated separable groups had the variance of each feature in its Principal Components returned to find the two most informative features. A covariance matrix was generated to identify the direction of the relationship between the features. The Spearman Correlation Coefficient was calculated to determine

the strength of the covariance between the two features and the strength of each feature’s covariance to the binding affinity. A heatmap of the features’ correlation to binding affinity was generated to confirm the Spearman Correlation calculations. The results of this analysis suggested what specific biomechanical relationship may exist between the features.

H. Machine Learning Benchmarking

To determine the effect of the features on ML performance, five state-of-the-art ML models were trained/tested on two datasets: one with and one without the features. The five models were as follows: 1) Random Forests, 2) Support Vector Machine, 3) K-Nearest Neighbors, 4) Decision Tree, and 5) LightGBM Regressor. The “Refined” set was used for training and validation, and the “Core” for testing. The “Refined” set was split such that a random 80% of complexes went into the training subset and the other 20% into the validation subset. The Root Mean Squared Error (RMSE) and Pearson Correlation Coefficient (PCC) of each model’s testing predictions were calculated to evaluate the model.

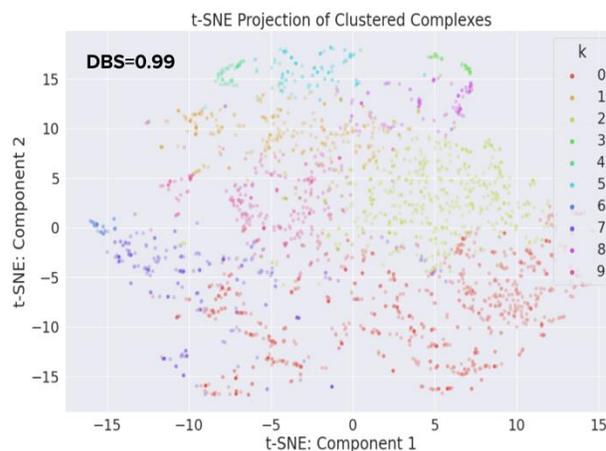


Fig. 5. Projection of t-SNE (n=2) Transformed Data after being Reduced using PCA (n=100) and Clustered using K-Means (k=10).

III. RESULT AND DISCUSSION

A. PCA/K-Means

A PCA (n=2) was performed and the transformed data was clustered using K-Means (k=10). Another PCA (n=3) was used to verify the 2D PCA. The 2D PCA exhibited a high DBS (>0.5) of 0.83 and dense clusters shown in Fig. 6A. The 3D PCA exhibited a similar outcome as the 2D PCA, with a higher DBS of 0.93, as shown in Fig. 6B. The clusters indicate that separable categories of complexes do not exist, suggesting that the PCA and clustering was unable to capture a biomechanical relationship between features.

B. PCA/t-SNE/K-Means

A PCA (n=100) followed a t-SNE (n=2) transformation was performed. The transformed data was clustered using K-Means (k=10). The t-SNE plot in Fig. 5 shows dense clusters and a high DBS of 0.99, suggesting that the t-SNE/clustering was also unable to identify a biomechanical relationship.

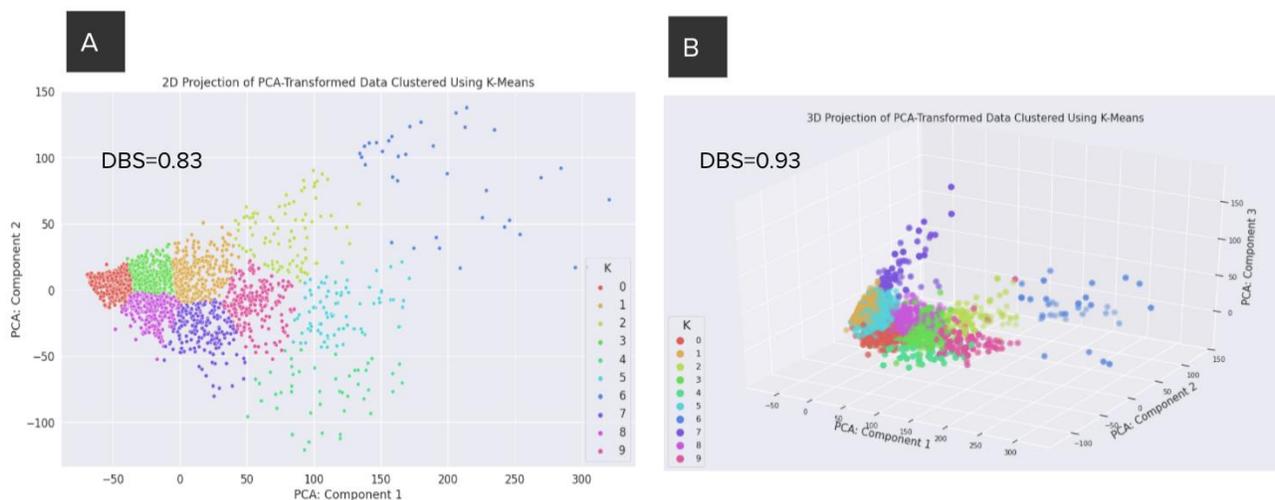


Fig. 6. Projection of PCA (n=2, A) and PCA (n=3, B) Transformed Data after being Clustered using K-Means Clustering (k=10).

C. t-SNE Heatmap

The t-SNE (n=2) transformed data was projected to a heatmap, where the “heat” was determined by the binding affinity. The plot exhibited no significant groups and an R^2 value of 0.0007, as shown in Fig. 7. The low R^2 and lack of groups reinforce the indication that the t-SNE components were unable to identify distinguished groups of complexes and therefore unable to identify a significant relationship between features.



Fig. 7. Heatmap of t-SNE (n=2) Transformed Data with “Heat” Determined by binding Affinity.

D. PCA Heatmap: 2D

The PCA (n=2) results were projected to a heatmap in the same manner as the t-SNE heatmap. The PCA heatmap showed a notable difference between complexes with binding affinity of $pKd < 6$ (blue-purple group) and those with $pKd > 8$ (orange-yellow group) at a higher adjusted R^2 value of 0.17, as shown in Fig. 8. The R^2 supports that there does exist a biomechanical relationship between features which is significantly responsible for binding affinity. A select number of features from the Principal Components are likely to have significant chemical importance in determining binding affinity [20-25].

E. PCA Heatmap: 3D

Another PCA (n=3) was performed and projected to a 3D heatmap to verify the results of the 2D PCA. If a similar grouping was evident in the 3D PCA as the 2D, the grouping

would be more statistically likely to be significant rather than by chance. The 3D heatmap did show a similar phenomenon as the 2D heatmap, with a noticeable grouping of complexes with $pKd < 6$ (blue-purple group) and $pKd > 8$ (orange-yellow group) at a similar R^2 correlation value of 0.18, as shown in Fig. 9.

The grouping supports the indication that the Principal Components were able to identify a biomechanical relationship that significantly affects binding affinity. High-variance features from the Principal Components are likely to be responsible for this relationship [20-25].



Fig. 8. Heatmap of PCA (n=2) Transformed Data with “Heat” Determined by binding Affinity.

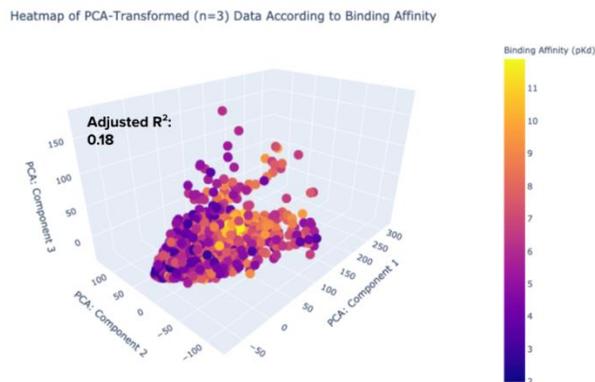


Fig. 9. Heatmap of PCA (n=2) Transformed Data with “Heat” Determined by binding Affinity.

F. Correlation Analysis

In order to determine which specific features were most likely involved in the biomechanical relationship, the feature with the highest variance in each Principal Component was returned. It was found that the CCCH and CCCCCH substructural ligand fragments features had the highest variance in the first Principal Component and the second Principal Component, respectively. In order to verify the presence of a relationship between CCCH and CCCCCH fragments, a covariance matrix was calculated between the two fragment counts. A direct (positive) relationship is evident with a covariance value of 358.34, as shown in Fig. 10. The covariance suggests that the specific relationship between the fragments is that they are both part of a larger molecular substructure within the ligand that is critical in determining binding affinity [26-28].

In order to verify the implication of the covariance matrix, the Spearman Correlation Coefficient was calculated between each combination of fragments and the binding affinity. The CCCH and CCCCCH fragments showed a high correlation of 0.8337. Each fragment and the binding affinity had a moderate correlation of 0.4286 and 0.3457, respectively, as shown in Table I. The high correlation between the fragments supports that they have a biomechanical relationship and that both fragments are part of a larger molecular substructure [26-28]. The moderate correlation between each fragment and binding affinity suggests that both fragments are involved in chemically determining binding affinity [29, 30].

The correlation calculations did not measure correlation between both fragments together and the binding affinity. Therefore, a heatmap of the fragment counts with the binding affinity was generated to verify that the fragment relationship influences binding affinity.

The same grouping that was evident in the PCA heatmaps occurred, with one group of complexes with pKd<6 and another with pKd>8 at a significant R² correlation of 0.18 as shown in Fig. 11. The grouping suggests that the CCCH-CCCCCH relationship is significantly responsible for determining the binding affinity with a protein. The CCCH-CCCCCH relationship is likely a critical influence on the optimal docking pose between the ligand and protein [31].

Covariance Matrix Heatmap between CCCH and CCCCCH Molecular Fragments

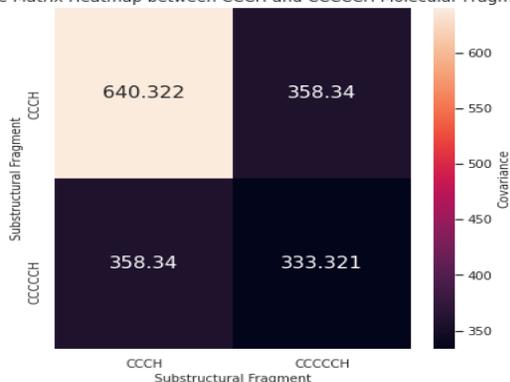


Fig. 10. Heatmap of Covariance Matrix between CCCH and CCCCCH Substructural Molecular Fragments.

TABLE I. SPEARMAN CORRELATION COEFFICIENTS BETWEEN HIGH-VARIANCE FEATURES AND BINDING AFFINITY

Rank Variable #1	Rank Variable #2	Spearman Correlation Coefficient	P-Value
CCCH Count	CCCCCH Count	0.8337	0.0
CCCH Count	Binding Affinity	0.4286	8.25e-125
CCCCCH Count	Binding Affinity	0.3457	5.82e-79

Heatmap of CCCH-CCCCCH Substructural Fragment Count Correlation to Binding Affinity

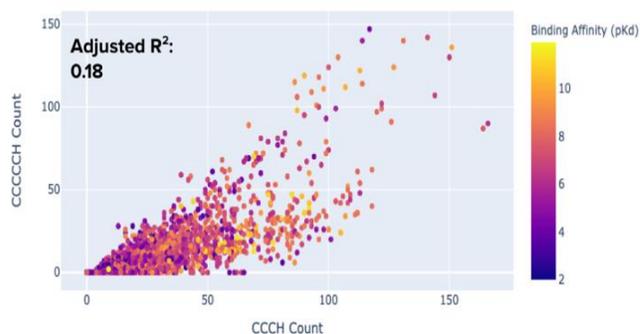


Fig. 11. Heatmap of Correlation between CCCH-CCCCCH Fragment Count and binding Affinity.

G. Machine Learning Benchmarking

In order to determine the effect of the CCCH-CCCCCH relationship on the performance of ML models in predicting binding affinity, five models were trained/tested on datasets with and without the fragment counts. The absence of the counts had an insignificant effect on most models except for the Decision Tree, which experienced an increase in RMSE of 0.09 and a decrease in PCC of 0.05, as shown in Table II. The insignificant effect on most models suggests that there are other factors with notable influence on binding affinity. The decreased performance of the Decision Tree suggests that the CCCH/CCCCCH count is an important decision rule for tree-based learning algorithms [32].

TABLE II. EFFECT OF CCCH AND CCCCCH ON MACHINE LEARNING PERFORMANCE

Model	With CCCH and CCCCCH fragment counts		Without CCCH and CCCCCH fragment counts	
	RMSE	PCC	RMSE	PCC
Random Forests	1.49	0.77	1.50	0.77
Support Vector Machine	1.70	0.68	1.69	0.69
K-Nearest Neighbors	1.71	0.64	1.69	0.66
Decision Tree	1.95	0.57	2.04	0.52
LightGBM Regression	1.46	0.77	1.44	0.77

IV. CONCLUSION AND FUTURE WORK

The biomechanical relationship discovered in this study serves as a baseline for further ligand interactions to be found. Including the relationship elucidated through this work, more interactions can be gathered to develop a corpus of ligand fragment relationships that influence binding affinity. This will produce a more accurate representation of ligand chemistry in regard to protein binding, improving the performance of predictive ML models [33, 34, 36]. Understanding the effect of ligand relationships on ML, as was done in this study, will also help researchers improve model performance [35].

Most importantly, uncovering specific ligand relationships will result in ML models that overfit less, making them more generalizable to new datasets and thus reliable for analyzing novel drug candidates [37-39].

The effect of generalizable ML models on effective VS is profound. It has already been demonstrated that for certain proteins such as Interleukin-1 receptor associated kinase-1 (IRAK1), ML models can increase novel ligand hit rates by over 1000% compared to standard scoring functions [40]. Developing ML models that are more generalizable can result in similar increases across wide ranges of proteins because models will be able to screen novel ligands without significant decreases in reliability. Using the relationship uncovered in this study as well as others to develop generalizable ML models is therefore critical for identifying promising drug candidates for innovative medicines.

It is significant to note that the relationship discovered in this study is useful in other scientific contexts, such as synthetic drug design. Using known information on fragments such as the two discussed in this study (CCCH and CCCCH), synthetic ligands can be chemically designed to bind optimally to a target protein [42, 43]. Computational tools (including, but not limited to, ML models) can also be developed to design novel synthetic drugs using known relationships between ligand fragments [44-46]. Gathering a clear, data-driven understanding of ligand fragment activity is a significant method by which synthetic drug design for new medications can be improved [48].

There are several limitations in this work that present promising directions for future research. Only several unsupervised learning techniques were used in this study, yet multiple other unsupervised/self-supervised techniques such as Uniform Manifold Approximation and Projection (UMAP) and Autoencoder Networks can be used to verify the results of this study [50]. Further, multicollinearity between features was not analyzed in this study, but can significantly affect feature selection methods. Therefore, multicollinearity analysis will validate the presence of the larger substructure (containing CCCH and CCCCH fragments) suggested in this study's results [47]. Should it exist, in-vitro experimentation can be performed to determine how the substructure affects ML performance in predicting binding affinity, revealing important information on the usefulness of such substructures in VS [49]. In addition, the protein-ligand models used in this study came from a single dataset, which introduces dataset bias and may affect the results of feature analysis. Therefore, incorporating data from other reliable datasets will verify/refute the results of

this study and decrease potential bias. Future work based on this study will aid in significantly progressing protein-ligand binding affinity research.

REFERENCES

- [1] D. Taylor, "The Pharmaceutical Industry and the Future of Drug Development," PiE, pp. 1-33, 2015.
- [2] A. Pandey, "Drug Discovery and Development Process," Learning Center, 2020. Available at: <https://www.nebiolab.com>.
- [3] M. Terry, "The Median Cost of Bringing a Drug to Market is \$985 Million, According to New Study," Biospace, 2020. Available at: <https://www.biospace.com/>.
- [4] S. Anusya, M. Keshewani, K. Priya, A. Vimala, G. Shanmugam, D. Velmurugan, and M. Gromiha, "Drug-Target Interactions: Prediction Methods and Applications," Current Protein and Peptide Science, vol. 19, no. 6, pp. 537-561, 2018.
- [5] E. Lionta, G. Spyrou, D. Vassilatis, and Z. Cournia, "Structure-Based Virtual Screening for Drug Discovery: Principles, Applications, and Recent Advances," Current Topics in Medicinal Chemistry, vol. 14, no. 16, pp. 1923-1938, 2014.
- [6] K.A. Carpenter and X. Huang, "Machine Learning-based Virtual Screening and Its Applications to Alzheimer's Drug Discovery: A Review," Current Pharmaceutical Design, vol. 24, no. 28, pp. 3347-3358, 2018.
- [7] D. Jones, H. Kim, X. Zhang, A. Zemla, G. Stevenson, W. F. D. Bennett, D. Kirshner, S. E. Wong, F. C. Lightstone, and J. E. Allen, "Improved Protein-Ligand Binding Affinity Prediction with Structure-Based Deep Fusion Inference," Journal of Chemical Information and Modeling, vol. 61, no. 4, pp. 1583-1592, 2021.
- [8] H. Ozturk, A. Ozgur, and E. Ozkirimli, "DeepDTA: deep-target binding affinity prediction," Bioinformatics, vol. 34, no. 17, pp. i821-i829, 2019.
- [9] M. M. Stepniewska-Dziubinska, P. Zielenkiewicz, and P. Siedlicki, "Development and evaluation of a deep learning model for protein-ligand binding affinity prediction," Bioinformatics, vol. 34, no. 21, pp. 3666-3674, 2018.
- [10] K. Wang, R. Zhou, Y. Li, M. Li, "DeepDTAF: a deep learning method to predict protein-ligand binding affinity," Briefings in Bioinformatics, 2021.
- [11] M. A. Rezaei, Y. Li, D. Wu, X. Li and C. Li, "Deep Learning in Drug Design: Protein-Ligand Binding Affinity Prediction," IEEE/ACM Transactions on Computational Biology and Bioinformatics, December 2020.
- [12] L. Rice, E. Wong, and J. Z. Kolter, "Overfitting in adversarially robust deep learning," in Proceedings of the 2020 International Conference on Machine Learning (ICML), 2020.
- [13] Y. Kwon, W. Shin, J. Ko, and J. Lee, "AK-Score: Accurate Protein-Ligand Binding Affinity Prediction Using an Ensemble of 3D-Convolutional Neural Networks," International Journal of Molecular Sciences, vol. 21, no. 22, 2020.
- [14] J. Hochuli, A. Helbling, T. Skaist, M. Ragoza, and D. R. Koes, "Visualizing Convolutional Neural Network Protein-Ligand Scoring," Journal of Molecular Graphics and Modeling, vol. 84, pp. 96-108, 2018.
- [15] V. Subramanian, H. Xhaard, P. Prusis, and G. Wolfhart, "Predictive protochemometric models for kinases derived from 3D protein field-based descriptors," Medicinal Chemistry Communications, vol. 7, no. 5, 2016.
- [16] D. S. Karlov, S. Sosnin, M. V. Fedorov, and P. Popov, "graphDelta: MPPN Scoring Function for the Affinity Prediction of Protein-Ligand Complexes," American Chemical Society Omega, vol. 5, no. 10, pp. 5150-5159, 2020.
- [17] S. Khan, U. Farooq, and M. Kurnikova, "Protein stability and dynamics influenced by ligands in extremophilic complexes – a molecular dynamics investigation," Molecular BioSystems, vol. 13, pp. 1874-1887, 2017.
- [18] W. Torng and R. B. Altman, "Graph Convolutional Neural Networks for Predicting Drug-Target Interactions," Journal of Chemical Information and Modeling, vol. 59, no. 10, pp. 4131-4149, 2019.

- [19] R. Wang, X. Fang, Y. Lu, C. Yang, and S. Wang, "The PDBbind database: methodologies and updates," *Journal of Medicinal Chemistry*, vol. 48, no. 12, pp. 4111-4119, 2005.
- [20] G. Tang and R. Altman, "Knowledge-based Fragment Binding Prediction," *PLOS Computational Biology*, 2014.
- [21] E. Grant, D. Fallon, M. Hann, K. Fantom, C. Quinn, F. Zappacosta, R. Annan, C. Chung, P. Bamborough, D. Dixon, P. Stacey, D. House, V. K. Patel, N. C. O. Tomkinson, and J. T. Bush, "A Photoaffinity-Based Fragment-Screening Platform for Efficient Identification of Protein Ligands," *Angewandte Chemie International Edition*, vol. 59, 2020.
- [22] D. A. Erlanson, B. J. Davis, and W. Jahnke, "Fragment-Based Drug Discovery: Advancing Fragments in the Absence of Crystal Structures," *Cell Chemical Biology*, vol. 26, no. 1, pp. 9-15, 2018.
- [23] M. Peters, "THE APPLICATION OF SEMIEMPIRICAL METHODS IN DRUG DESIGN," Ph.D. dissertation, DC, UF, Florida, 2007, Available at: http://etd.fcla.edu/UF/UFE0021354/peters_m.pdf.
- [24] P. Kenny, "The nature of ligand efficiency," *Journal of Cheminformatics*, vol. 11, no. 8, 2019.
- [25] T. Patsar and A. Poso, "Binding Affinity via Docking: Fact and Fiction," *Molecules*, vol. 23, no. 8, pp. 1899, 2018.
- [26] F. Chevillard, H. Rimmer, C. Betti, E. Pardon, S. Ballet, N. Hilten, J. Steyaert, W. E. Diederick, and P. Kolb, "Binding-Site Compatible Fragment Growing Applied to the Design of α 2-Adrenergic Receptor Ligands," *Journal of Medicinal Chemistry*, vol. 61, no. 3, pp. 1118-1129, 2018.
- [27] P. Matricon, A. Ranganathan, E. Warnick, Z. Gao, A. Rudling, C. Lambertucci, G. Marucci, A. Ezzati, M. Jaiteh, D. D. Ben, K. A. Jacobson, and J. Carlsson, "Fragment optimization for GPCRs by molecular dynamics free energy calculations: Probing druggable subpockets of the A2A adenosine receptor binding site," *Scientific Reports*, vol. 7, no. 6398, July 2017.
- [28] J. Robston-Tull, "Biophysical screening in fragment-based drug design: a brief overview," *Bioscience Horizons*, vol. 11, 2019.
- [29] P. Kirsch, A. M. Hartman, A. K. H. Hirsch, and M. Empting, "Concepts and Core Principles of Fragment-Based Drug Design," *Molecules*, vol. 24, no. 23, pp. 4309, 2019.
- [30] F. Giordanetto, C. Jin, L. Willmore, M. Feher, and D. E. Shaw, "Fragment Hits: What do They Look Like and How do They Bind?" *Journal of Medicinal Chemistry*, vol. 62, no. 7, pp. 3381-3394, 2019.
- [31] C. Jacquemard, M. N. Drwal, J. Desaphy, and E. Kellenberger, "Binding mode information improves fragment docking," *Journal of Cheminformatics*, vol. 11, no. 24, 2019.
- [32] H. Deng and G. Runger, "Feature selection via regularized trees," in *Proceedings of the 2012 International Joint Conference on Neural Networks (IJCNN)*, pp. 1-8, 2012.
- [33] H. Deng and G. Runger, "Feature selection via regularized trees," in *Proceedings of the 2012 International Joint Conference on Neural Networks (IJCNN)*, pp. 1-8, 2012.
- [34] X. Xu, C. Yan, and X. Zou, "Improving Binding mode and Binding Affinity Predictions of Docking by Ligand-based Search of Protein Confirmation: Evaluation in D3R Grand Challenge 2015," *Journal of Computer-Aided Molecular Design*, vol. 31, no. 8, pp. 689-699, 2017.
- [35] S. Holderbach, L. Adam, B. Jayaram, R. C. Wade, and G. Mukherjee, "RASPD+: Fast Protein-Ligand Binding Free Energy Prediction Using Simplified Physicochemical Features," *Frontiers in Molecular Biosciences*, vol. 7, pp. 393, 2020.
- [36] D. D. Wang, H. Xie, and H. Yan, "Proteo-chemometrics interaction fingerprints of protein-ligand complexes predict binding affinity," *Bioinformatics*, 2021.
- [37] G. G. Ferenczy and G. M. Keseru, "Thermodynamic profiling for fragment-based lead discovery and optimization," *Expert Opinion on Drug Discovery*, vol. 15, no. 1, pp. 117-129, 2019.
- [38] Z. Meng and K. Xia, "Persistent spectral-based machine learning (PerSpect ML) for protein-ligand binding affinity prediction," *Science Advances*, vol. 7, no. 19, 2021.
- [39] H. Goel, A. Hazel, V. D. Ustach, S. Jo, W. Yu, and A. D. MacKerell, "Rapid and accurate estimation of protein-ligand relative binding affinities using site-identification by ligand competitive saturation," *Chemical Science*, vol. 12, pp. 8844-8858, 2021.
- [40] S. Wan, A. P. Bhati, S. J. Zasada, and P. V. Coveney, "Rapid, accurate, precise and reproducible ligand-protein binding free energy prediction," *Interface Focus*, vol. 10, no. 6, 2020.
- [41] S. Kumar and M. Kim, "SMPLIP-Score: predicting ligand binding affinity from simple and interpretable on-the-fly interaction fingerprint pattern descriptors," *Journal of Cheminformatics*, vol. 13, no. 28, 2021.
- [42] Z. Liu, Y. Li, L. Han, J. Li, J. Liu, Z. Zhao, W. Nie, Y. Liu, and R. Wang, "PDB-wide collection of binding data: current status of the PDBbind database," *Bioinformatics*, vol. 31, no. 3, pp. 405-412, 2015.
- [43] A. Kashyap, P. K. Singh, O. Silakari, "Counting on Fragment Based Drug Design Approach for Drug Discovery," *Current Topics in Medicinal Chemistry*, vol. 18, no. 27, pp. 2284-2293, 2018.
- [44] M. Bissaro, M. Sturlese, and S. Moro, "The rise of molecular simulations in fragment-based drug design (FBDD): an overview," *Drug Discovery Today*, vol. 25, no. 9, pp. 1693, 2020.
- [45] Y. Bian and X. Xie, "Computational Fragment-Based Drug Design: Current Trends, Strategies, and Applications," *American Association of Pharmaceutical Scientists Journal*, vol. 20, no. 59, 2018.
- [46] V. D. Mouchlis, A. Afantitis, A. Serra, M. Fratello, A. G. Papadiamantis, V. Aidinis, I. Lynch, D. Greco, and G. Melagraki, "Advances in de Novo Drug Design: From Conventional to Machine Learning Methods," *International Journal of Molecular Sciences*, vol. 22, no. 4, pp. 1676, 2021.
- [47] Q. Bai, S. Tan, T. Xu, H. Liu, J. Huang, and X. Yao, "MolAICal: a soft tool for 3D drug design of protein targets by artificial intelligence and classical algorithm," *Briefings in Bioinformatics*, vol. 22, no. 3, 2021.
- [48] L. R. S. Neto, J. T. Moreira-Filho, B. J. Neves, R. L. B. R. Maidana, A. C. R. Guimaraes, N. Furnham, C. H. Andrade, and F. P. Silva, "In silico Strategies to Support Fragment-to-Lead Optimization in Drug Discovery," *Frontiers in Chemistry*, vol. 8, pp. 93, 2020.
- [49] M. J. Caplin and D. J. Foley, "Emergency synthetic methods for the modular advancement of sp³-rich fragments," *Chemical Sciences*, vol. 12, pp. 4646-4660, 2021.
- [50] M. Aldeghi, V. Gapsys, and B. L. de Groot, "Accurate Estimation of Ligand Binding Affinity Changes upon Protein Mutation," *American Chemical Society Central Science*, vol. 4, no. 12, pp. 1708-1718, 2018.
- [51] J. O. Spiegel and J. D. Durrant, "AutoGrow4: an open-source genetic algorithm for de novo drug design and lead optimization," *Journal of Cheminformatics*, vol. 12, no. 25, 2020.

Statistical Analysis of Cybersecurity Awareness Issues in Higher Education Institutes

Latifa Alzahrani

Department of Management Information Systems
College of Business Administration, Taif University, Saudi Arabia

Abstract—Now-a-days, computers and the Internet are becoming increasingly indispensable tools in several aspects of our lives, including academic study, professional work, entertainment, and communication. Despite the significant advantages of information technology, particularly in information accessibility and internet applications, cyber security has risen to become a national concern in Saudi Arabia, and cyber security threats now need to be taken more seriously. Therefore, computer and network security are a concern not only for traditional security awareness organisations, for example, military, bank, or financial institutions, but also for every individual and government official who use computers. Besides, nowadays, more and more organisations' valuable assets are stored in the computerised information system; security has become an essential and urgent issue. However, it is remarkable that most systems today are designed with little attention to security concerns. This study aims to examine and analyse cyber security issues, including cyber risk, cyber security, cyber security awareness, and cyber trust, among higher education students in Saudi Arabia. Based on an analysis of the collected data using SPSS, the findings of this study highlight a lack of awareness of basic information related to cyber security among Saudi students. In addition, the number of students attending training programs was very low. Considering other security issues, this study reveals that while Saudi students are aware of cyber risk, they are not aware of cyber security. In addition, Saudi students are not aware of and do not have cyber trust.

Keywords—Cyber security; cyber security awareness; educational institutes; cyber risk; higher education; cyber trust

I. INTRODUCTION

The persistent threats from cyber attackers are a real danger, so much so that they rise to the level of a national security concern. Cybersecurity breaches are an all too common occurrence; seemingly every day, a new attack, data theft or other intrusion makes the news [1]. The U.S. Cyber Command protects Department of Defense networks and works to guard other federal agencies against malicious activity; the FBI, Secret Service, and Department of Homeland Security are among the agencies that investigate cybercrimes. But it is still up to the private industry to secure its networks. According to Internet World Stats 2017, the Internet users in Asia accounted for approximately half of Internet users worldwide. However, they are still immature with cybersecurity, exercises or cooperation to counter cyber incidents or cyber-attacks [2]. In fact, in 2016, hackers attacked some Asian countries by withdrawing US\$81 million from the Bangladesh Central bank, accessing and leaking details of 3.2 million customer cards from several Indian banks, stealing

US\$65 million of bitcoins from Hong Kong-based digital currency exchange Bifinex, using malware to steal US\$2.17 million from eight banks in Taiwan. In 2017, a remarkable attack in Korea was recorded, indicating that seven main banks were threatened by distributed denial of service attacks claiming ransom payment [3].

The security and privacy of cyber and cyber-physical systems are increasingly considered a major issue in many industries [4, 5]. Cyber security has become a national concern in Saudi Arabia because of worrying threats to be taken more seriously [6-9]. However, many users are still not knowledgeable about the online threats; therefore, they do not have an effective awareness of secure behaviour online. A recent study by McPhee and Weiss [10] highlights that lack of knowledge is an important factor that contributes to insecure online behaviour by Internet users. Awareness and education can provide Internet users with the ability to recognise and avoid any apparent risks [11-13]. Currently, there is a growing concern about cyber threats, the most dangerous ones worldwide. They can cause huge damage to finance, the economy, politics, and other aspects of life [10]. As a result, identifying types of cyber threats is a critical and urgent need not only for individuals and businesses but also for governments and organisations to increase awareness of cybersecurity and national security and find solutions to mitigate or reduce the damage from them [3]. Moreover, it was expected to figure out the differences in security cooperation among Asian nations to identify which model is suitable for small nations, including Saudi Arabia and its neighbours in the Asian region [2].

In the past, cyber-crime was considered with two major categories: computer as a target of the attack and computer as a means of attack. Firstly, the computer as a target of the attack - the attackers use some special tools to get unauthorised access and illegally manipulate the confidentiality, integrity, and availability of data—secondly, traditional offences with the assistance of computers, computer networks, and communication technology. For example, the blackmailers use the computer to spread a thousand blackmails or spam messages to the victim computers [7]. Moreover, cybercrime offences have also ranged from economic offences like fraud, theft, terrorism, extortion, etc. On the other hand, cybercrime includes some non-money offence activities such as programming viruses, spam, and spyware on the computer network or posting confidential business information on the Internet [10]. The current cybercrimes are no different from traditional criminals because they want to make money as fast

as possible. However, the current computer crimes are more sophisticated than the old ones with many forms on the Internet like child pornography, copyright or trademark infringement, money laundering, cyberbullying, online gambling, etc. As a result, cybercrime is currently separated into two main categories: machine-made attacks and man-made attacks [4, 9]. Machine-made attack defines some cyber-attacks by using computer network environment as a tool to exploit illegal sensitive data and sabotage them, especially in financial damage.

In contrast, a man-made attack is considered a cyber-terrorist attack by an individual or group of people with the purpose of politics and military [14]. In Europe, each country has different strategies to ensure its national security, especially cybersecurity. As each country has its contexts, strengths, technology development, and policies, it may be not easy to cooperate and operate the same strategy [8]. The results of this research are very important for Saudi Arabia because the study was conducted there on a certain sample of students in higher education. In Saudi Arabia, cyber-attacks are increasing due to the rise in digital devices (computers, tablets, and smartphones), lack of security awareness among Internet users, terrorism, politics, and an increase in cybercrime groups [15]. While Saudi organisations continue to protect computer systems and their information against cybercrimes, a recent report from Kaspersky Lab highlights that Saudi Arabia has one of the highest numbers of Web threat incidents [7, 16]. Consequently, this study first presents the level of awareness of cyber security in Saudi Arabia. It then proposes strategies to increase awareness and training on cyber security in line with Saudi Vision 2030 [17, 18]. Preliminary research has shown that studies on cyber security in Saudi Arabia are very few, and further research is needed in this area. These results will also be of great importance to all managers and decision-makers in the fields of information security and cyber security because it provides a clear and comprehensive picture of the concept of CSA from the field of higher education. This paper aims to investigate and analyse CSA levels among higher education students in a business college in Saudi Arabia. It also aims to examine students' knowledge and attitude towards the following major security issues related to cyber security: cyber risk, cyber security, cyber awareness and cyber trust.

Section II reviews the literature on cyber security, cyber threats, cybercrimes, cyber-attacks, and the like. Moreover, it clarified the differences between cybercrime and cyberwar to consider the new trends of cyber security and cyber threats. Furthermore, it primarily expressed an urgent need for Saudi Arabia cybersecurity strategies toward the new cybersecurity trends in the world. Section III explains the methodology of our study in which the dataset, tool, and workflow has been explained. Section IV presents the results through five analysis tools: the frequency distribution of variables, multiple response analysis, factor analysis for grouping different types of security, a reliability test, and descriptive analysis. Section V presents the discussion that provides a deeper understanding of students' awareness and their basic understanding of cyber security issues. Section VI provides some significant implications for research, and Section VII explains the

summary of research findings, proposed method, and contributions to the research problem.

II. RELATED WORK

Cyber security has been defined as “the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance, and technologies that could be used for protecting the cyber environment and organisation and user’s assets” [19]. Individuals and families and organisations, governments, educational institutions, and businesses are now concerned about cyber security. Kritzing and Von Solms [14] studied that cyber security is critical for families and parents to safeguard children and family members from online fraud. In terms of financial security, it's critical to safeguard financial information that might impact one's financial situation. As a result, understanding how to protect oneself against online fraud and identity theft is critical for Internet users. Kim [4] concluded that even though technology has done a lot to safeguard end-users information systems, security experts claim that technology alone cannot protect these systems adequately. Appropriate learning about online behaviour and system security decreases vulnerabilities and makes the Internet a safer place to be. Because of limited resources and a lack of sufficient cyber security expertise, small and medium-sized businesses face a variety of security difficulties [8, 14, 20]. Because the continual advancement of technology makes cyber security increasingly difficult, we do not offer lasting answers to this troubling situation. Nonetheless, we're attempting to provide a variety of frameworks or solutions to safeguard our networks and data. All of these measures, however, only give protection in the near run. Better security knowledge and methods may aid in the protection of intellectual property and trade secrets, as well as the reduction of financial and reputational harm [14, 21]. Large volumes of data and private documents are held digitally by the federal, state, and municipal governments, making them prime targets for a cyber-assault [8, 22]. Governments are frequently exposed to dangers due to low financing, inadequate infrastructure, and a lack of knowledge. Government agencies must offer dependable services to society, maintain good citizen-to-government contacts, and safeguard sensitive information [20, 21, 23].

With around 26 million inhabitants, Saudi Arabia is one of the largest countries in the Middle East. About 0.002% of Internet users are from Saudi Arabia [7, 24]. However, the number of cyberattacks experienced by Saudi Arabian users are far larger than the population of Internet users, i.e., 1.81% in 2009 and 1.77% in 2010 [25, 26]. Although Saudi Arabia is as highly censored as Iran, and the number of Internet users in Iran is also higher than in Saudi Arabia, the number of cyber-attacks is greater in Saudi Arabia than in Iran. Saudi Arabia is reported to be the ninth largest country in 2008 in terms of cyber-attacks and the incidence of information security attacks. It became the seventh-largest in 2009. The reasons behind such a larger number of attacks are a lack of CSA among the general public of Saudi Arabia. Alzahrani and Alomar [7] has revealed that information security awareness is very low, and there is a higher level of risk related to cyberspace in Saudi Arabia.

TABLE I. DIFFERENT CATEGORIES OF CYBER-CRIME [22]

Category	Definition
Hacking	The destruction and concealment of information from the victim's operating system by attacking the weaknesses and loopholes are known as hacking. It is usually done by installing some sort of backdoor programs by hackers on the computer of victims to obtain access to the information.
Cyber theft	When the victim's computer information is stolen through electronic attacks, this is known as cyber theft. The most common example of cyber theft is credit card fraud and illegal money transfers.
Viruses and worms	Viruses and worms are designed to damage the computers attached to other programs and documents in the computer. They appear to perform some other function, but the primary function of the virus is to corrupt the operating system of the computer.
Spamming	Spamming is done by sending massive numbers of emails to users that usually contain links designed to harm the programs of the victim's computer.
Financial fraud	This cybercrime is also known as a phishing scam, formed through social engineering and designed to obtain the victim's bank details.
Identity theft and credit card theft	In this cybercrime, emails are sent to users to induce them to provide their identity card and credit card information. The attacker represents him or herself as a representative of some well-known company, and hence unaware users provide their sensitive details by responding to these emails.
Cyber harassment	Cyber harassment is harassing and bullying individuals using electronic means; one such example is cyberstalking.
Cyber laundering	The transfer of illegally obtained money between two parties is known as cyber laundering.
Website cloning	Copying the websites of renowned companies and attacking the users who are unaware of this is a new category of cybercrime. Unaware consumers provide their details to the fraudster's personal database.

According to a report in 2016, the number of Internet users in Saudi Arabia has reached 22.4 million. These users belong to different sectors such as health, education, government, and other service sectors. However, with the growth of digital devices, the rate of cyber-attacks in Saudi Arabia also increases more quickly. To tackle this increasing problem, the CSA of the general public should be improved, and the government of Saudi Arabia is now taking practical steps to counter these problems. The report suggests that around 40% of companies in Saudi Arabia were the victim of cyber-attacks in 2015, leading to the leakage of the confidential data of Saudi employees. The primary step that the Saudi government could take to reduce the number of cyber-attacks is to increase CSA and educate children and young people about anti-cybercrime laws [14] [7] [27]. Very recent reports about the CSA level in Saudi Arabia have suggested that the government has yet taken no practical measures to respond to the issues of cyber-attacks. As a result, a large number of attacks have been experienced. Table I presents the different categories of cyber-crime.

III. METHODOLOGY

This study used a quantitative research technique to emphasise the relation between students' cyber security awareness and their cyber security practices. Quantitative research designs are either descriptive (in which subjects are generally measured just once) or experimental (subjects are measured many times). A relationship between variables is established in a descriptive investigation; causation is established in an experimental study. According to Quantitative Methods, objective measurements and statistical, mathematical, or numerical analysis of data collected through polls, questionnaires, and surveys, or by manipulating pre-existing statistical data using computational techniques, are the most important aspects of quantitative methods [28, 29]. Quantitative research collects statistical information and the generalisation or description of phenomena across groups of individuals. A pilot study was carried out for the questionnaire.

The pilot study aimed to test the understandability of the questionnaire before it was presented to the sampling frame of this study [30] [28] [31]. To analyse the collected data, SPSS was utilised to measure students' awareness about cyber security. With a wide range of graphs, methods and charts, SPSS provides many types of statistical analysis for quantitative research. The techniques of screening and cleaning data within SPSS are useful for future analysis. Because the issue of cyber security is an important topic in Saudi Vision 2030, this study was conducted in Saudi Arabia. Cyber security in Saudi Arabia still faces many challenges that need to be addressed. The sample selected for this study comprises Saudi students in a business college in a Saudi university. Questionnaires were distributed by both an online link and in hard copy to Saudi students. The online link was sent to students' emails, while hard copies of the questionnaire were distributed in classrooms. Table II lists the questionnaire items used in this study.

TABLE II. QUESTIONNAIRE ITEMS

I usually change my password.
I use different passwords for different systems.
I usually change the default password of the administrator account.
I use wireless encryption.
I keep the wireless device firmware up to date.
I share my personal information on social networks.
I trust the applications in social networks.
I check links before clicking on them on social networks.
I share my files, documents, and photo online.
I set a password to access shared files.
I read about the security and privacy policies of services providers.
I understand the risk of emailing passwords.
I understand the risk of email attachments.
I understand the risk of clicking on email links.
I understand the risk of smartphone viruses.
I have an anti-virus program for my smartphone.

IV. RESULTS

To achieve the objectives of this research given the nature of the data collected, five analysis tools were utilised: the frequency distribution of variables, multiple response analysis, factor analysis for grouping different types of security, a reliability test, and descriptive analysis. The following paragraphs provide more details for each tool. Table III shows the demographics of the survey participants, revealing that the majority of respondents were 18–30 years old (94.5 percent) or 31–40 years old (4.7 percent). Overall, most respondents were between the ages of 18 and 30, indicating that a younger generation was more engaged in this study. Table III shows that the female population (52.0%) was somewhat greater than the male population (48.0 percent). In terms of educational attainment, the biggest cohort (96.2 percent) had a bachelor's degree, followed by a master's degree (3.8 percent). Finally, 46.5 percent of participants had 6–10 years of experience using the Internet, followed by 26.3 percent with 1–5 years of experience, and 15.3 percent with 11–20 years of experience.

The results in Table IV show that 82.5% of students do not know what cyber security means. The results in Table V also show that 97.4% of students are not attending any training or educational programs in cyber security.

TABLE III. RESPONDENT DETAILS

Variable	Group	Frequency	Percentage (%)
Age	18–30 years old	518	94.5
	31–40 years old	26	4.7
	41–50 years old	4	0.7
	51–60 years old	0	0
	Total	548	100.0
Gender	Male	263	48.0
	Female	285	52.0
	Total	548	100.0
Education level	Bachelor's degree	527	96.2
	Master's degree	21	3.8
	Total	548	100.0
Internet experience	1–5 years	144	26.3
	6–10 years	255	46.5
	11–20 years	84	15.3
	21–30 years	9	1.6
	None	56	10.2
	Total	548	100.0

TABLE IV. RESULTS FOR "DO YOU KNOW WHAT CYBER SECURITY MEANS?"

	Frequency	Percent (%)	Valid (%)	Cumulative (%)
Yes	96	17.5	17.5	17.5
No	452	82.5	82.5	100.0
Total	548	100.0	100.0	

Considering the behaviour of maintaining up-to-date protection software, the results (Table VI) show a variation in the participants' responses. Here, 38.1% of the participants automatically update their protection software. However, 40%

fail to update their software. In addition, just over 10% annually update their software.

A multiple response analysis was utilised to answer the question, "What types of protection software do you use?" As shown in Table VII, 43.6% of respondents do not know what protection software they are using for protection. In addition, 36.6% of respondents use an anti-virus program for software protection, and 11.5% of respondents use a firewall for software protection. Only 6.4% use anti-spyware software, and 1.9% use anti-spam software.

Table VIII presents the results of Kaiser–Meyer–Olkin (KMO) and Bartlett's tests. The KMO measure of sampling adequacy and Bartlett's test of sphericity were used in this research. KMO must be greater than 0.7 to be considered good. In Table VIII, the value of KMO is 0.795, which indicates that factor analysis is appropriate for these data. In addition, Table IX presents the total variance explained results, where all the variables are grouped into four components with eigenvalues greater than 1.

TABLE V. RESULTS FOR "ARE YOU ATTENDING ANY SECURITY TRAINING OR EDUCATION PROGRAMS?"

	Frequency	Percent (%)	Valid (%)	Cumulative (%)
Yes	14	2.6	2.6	2.6
No	534	97.4	97.4	100.0
Total	548	100.0	100.0	

TABLE VI. RESULTS FOR "HOW OFTEN DO YOU UPDATE PROTECTION SOFTWARE?"

	Frequency	Percent	Valid Percent	Cumulative Percent
Automatically	209	38.1	38.1	38.1
Weekly	33	6.0	6.0	44.2
Monthly	84	15.3	15.3	59.5
Annually	41	7.5	7.5	67.0
Never	181	33.0	33.0	100.0
Total	548	100.0	100.0	

TABLE VII. RESULTS FOR "WHAT TYPES OF PROTECTION SOFTWARE DO YOU USE?"

	Responses		Percent of Cases (%)
	N	Percent (%)	
Anti-virus	229	36.6	42.1
Firewall	72	11.5	13.2
Anti-spam	12	1.9	2.2
Anti-spyware	40	6.4	7.4
I don't know	273	43.6	50.2
Total	626	100.0	115.1

a. Dichotomy group tabulated at value 1.

TABLE VIII. RESULTS FOR KMO AND BARTLETT'S TEST

KMO measure of sampling adequacy		.795
Bartlett's test of sphericity	Approx. chi-square	1766.468
	Df	136
	Sig.	.000

TABLE IX. TOTAL VARIANCE EXPLAINED RESULTS

Component	Initial Eigenvalues			Extraction Sums of Squared Loadings			Rotation Sums of Squared Loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	3.851	22.653	22.653	3.851	22.653	22.653	3.124	18.376	18.376
2	1.859	10.933	33.586	1.859	10.933	33.586	1.819	10.701	29.077
3	1.442	8.483	42.069	1.442	8.483	42.069	1.648	9.693	38.770
4	1.057	6.219	48.288	1.057	6.219	48.288	1.618	9.518	48.288
5	.946	5.563	53.851						
6	.910	5.356	59.206						
7	.848	4.989	64.195						
8	.810	4.764	68.959						
9	.774	4.554	73.513						
10	.731	4.300	77.813						
11	.674	3.966	81.779						
12	.652	3.834	85.613						
13	.615	3.615	89.228						
14	.573	3.368	92.596						
15	.512	3.012	95.608						
16	.461	2.712	98.320						
17	.286	1.680	100.000						

Extraction Method: Principal Component Analysis.

TABLE X. ROTATED COMPONENT MATRIX

	Component			
	Cyber Risk	Cyber security	Cyber trust	Cyber Awareness
I understand the risk of emailing passwords.	.722			
I understand the risk of email attachments.	.775			
I understand the risk of clicking on email links.	.776			
I understand the risk of smartphone viruses.	.642			
I keep the wireless device firmware up-to-date.	.521			
I check links before clicking on them on social networks	.546			
I usually change my passwords.		.695		
I use different passwords for different systems.		.612		
I usually change the default password of the administrator account.		.643		
I use wireless encryption.		.537		
I share my personal information on social networks.			.743	
I trust the applications in social networks.			.782	
I share my files, documents, and photos online.			.637	
I set passwords to shared access files.				.518
I read about security policies and privacy.				.712
I have an anti-virus program for my smartphone.				.720

Extraction Method: Principal Component Analysis.
Rotation Method: Varimax with Kaiser Normalization.

a. Rotation converged in five iterations.

Table X presents the rotated component matrix, which presents the four groups (components) along with their items. As shown in Table X, cyber risk has six items, and cyber security has four items. The reliability of a group of variables is tested with Cronbach’s alpha method. If Cronbach’s alpha is greater than 0.7, then the data are reliable as shown in Table XI. Both cyber trust and cyber awareness have three

items. The results of descriptive statistics (Table XII) show a high cyber risk score with a mean of 3.19 and a lower score for cyber security (mean = 2.01). In addition, both cyber awareness (mean = 2.37), cyber trust (mean = 2.41) have low scores. Overall, the findings of this study highlight a lack of awareness of basic information related to cyber security among Saudi students.

TABLE XI. RELIABILITY STATISTICS

Variables	Cronbach's Alpha	No. of Items
Cyber Risk	.786	6
Cyber Security	.753	4
Cyber Trust	.757	3
Cyber Awareness	.4712	3

TABLE XII. DESCRIPTIVE STATISTICS

	N	Minimum	Maximum	Mean	Std. Deviation
Cyber Risk	548	1.00	5.00	3.1934	1.05231
Cyber Security	548	1.00	5.00	2.0132	.79557
Cyber Trust	548	1.00	5.00	2.4148	.87477
Cyber Awareness	548	1.00	5.00	2.3710	1.01231
Valid N (listwise)	548				

In addition, the number of students attending training programs was very low: 92% have never taken any type of security training. Considering other security issues, this study reveals that while Saudi students are aware of cyber risk, they are not aware of cyber security and the important steps and processes needed to protect their personal information. Thus, Saudi students need to increase their awareness about cyber security to become educated about protecting their online data.

V. DISCUSSION

This study provides a deeper understanding of students' awareness and their basic understanding of cyber security issues. Additionally, this study contributes significantly by investigating students' behaviour about the major topics related to cyber security: the security issues related to passwords, emails, wireless, social networks, and smartphones. SPSS was employed to analyse students' awareness and reveal their behaviour. The following subsections first discuss the results of general information about cyber security and then discuss major topics related to cyber security. Finally, some strategies are recommended to increase student awareness about cyber security. The results of this survey indicate that the participants' level of awareness about cyber security was generally unsatisfactory. A total of 82% of the participants were not aware of cyber security. The results also show that 97% of the participants have not had any related training, which suggests a lack of training programs available to the students.

The knowledge about cyber risks of the participants was very good. Most of the participants from all demographic distributions had a good understanding of the importance of password security rules, had an accurate knowledge of password security, and recognised that passwords should not contain only real words or significant dates or names. There were, however, some aspects of wireless technology about which many students lacked knowledge. An excellent level of participant awareness about social security was recorded. Most of them are aware that they should not share their personal information on social applications. Even though a minority of

the participants use cloud storage to save their files, most do not use passwords to secure their data while sharing them. In addition, most of the participants are aware of the risk of using smartphones. However, few of them use anti-virus programs to protect them.

To summarise, this section discussed in-depth Saudi students' awareness of and their behaviour towards cyber security. The study results show that students in higher education need to increase their awareness about cybercrime and cyber security by involving them in training programs, workshops, and lessons. Universities in Saudi Arabia must take on more responsibility in encouraging CSA and practice. Several strategies were recommended for individuals, network users, and organisations to enhance CSA and practice.

Currently, the cyber-threats are very complicated for all countries in general and Saudi Arabia in specific. As a result, the Saudi Arabian government established several decrees and programs to promote cybersecurity awareness and human resources. They gave Decree No. 99/QĐ-TTG and 153/QĐ-TTG to develop human cybersecurity resources, attract experts or students, individuals in government offices, and increase the number of students studying abroad in ICT from 2014 to 2020. Moreover, the Saudi Arabian Information Security Association also organised annual national contests and conferences for students of all universities and colleges to introduce artificial intelligence to safeguard cybersecurity and information security in ICT, IoT and protect critical databases or infrastructure.

In summary, Saudi Arabia is a developing country that quickly approaches ICTs and innovative technologies, but it is a newbie in cybersecurity protection. A series of cyber-attacks on government, companies, agencies, and airport websites greatly damaged data loss, data leakage, and finance. Hence, the Vietnamese government paid attention to making cyber laws, legal documents, and legal infrastructure to ensure the safety of critical infrastructure protection. Regarding the connection between government organisations and private sectors, it helps strengthen the safety of critical infrastructure systems and cyber resilience capacity, develop research and training, and promote cybersecurity solutions, products or services. Besides, the Vietnamese government also considered the important role of international cooperation as a key factor to boost cybersecurity development to a new level in the same region.

The cyber risks and challenges in the industry are diverse, spanning technological and organisational competencies, stemming from purpose-built components that operate in an ecosystem where cybersecurity is an afterthought. Practical and xi reasonable recommendations to address these problems are discussed to close the gap, some specific and unique to the manufacturing industry. In contrast, other fundamental applications discussed with a manufacturing industry lens are commonly ignored due to perceived complexity, cost, or lack of awareness. Lastly, several of these recommendations were selected for further evaluation and implementation; challenges, approaches, benefits, and outcomes are shared, showing measurable improvements to the organisation's cybersecurity posture.

VI. STUDY IMPLICATIONS

This study provides some significant implications for research. First, it extends the literature on cyber security by providing a critical and comprehensive literature review as the primary theoretical contribution of this study. The findings of this review reveal an insufficient number of research studies in the field of CSA. Most researchers focus only on the technical aspects of information technology, with limited consideration of users' security awareness and their security behaviour. Gefen et al. [32] agree that it is important to study the issue of cyber security from the aspect of users' security awareness to have a clear understanding of the concept of CSA and to address the issue of security behaviour as a whole successfully. Thus, more research should address the issue of cyber security from the perspective of users' awareness as the existing research on this topic has somewhat ignored this issue.

Second, a quantitative survey was developed to consider basic information about CSA and investigate other security issues related to cyber security, such as passwords, emails, cloud storage, social networks, wireless networks, and smartphones. Analysing the collected data using SPSS revealed a lack of awareness of basic information related to cyber security among Saudi students. In addition, the number of students attending training programs was very low.

This study also has some fundamental implications for Saudi universities. Universities in Saudi Arabia need to empower their students by increasing their awareness of cyber security. Thus, Saudi universities must adopt mass media for educational purposes and introduce cyber security concepts. In addition, universities could offer seminars, lectures, and workshops on the negative impacts of cybercrimes and the importance of cyber security. This approach would encourage students to practice effective security behaviours and then increase the cyber security culture among students. In addition, Saudi Universities could publish such information in newsletters, and magazines, which would help to increase student's awareness about cyber security and encourage them to adopt secure behaviour.

Training Compromises via social engineering techniques are an ever-evolving threat landscape. The attackers devise sophisticated schemes to gain personal information and/or entry into an environment. A specific counter-action cannot mitigate these attack schemes; however, preventing and protecting against breaches can be accomplished by applying a defence-in-depth approach and an effective security awareness training program. Specific to the educational institutes, as part of creating a comprehensive security awareness program, organisations need to deliberately and consciously educate individuals. As part of this comprehensive approach, organisations need to educate personnel on the threat vectors and downstream effects of using social media and how compromising can lead to other lateral advances.

1) *Security awareness training*: Relative to a security awareness program, studies by Gartner showed that there are four key objectives when deploying an effective security awareness program that drives real meaningful actions [16].

2) *Build a knowledge base*: Creation of a referenceable and easy to understand security and risk knowledge base across the workforce results in a shared understanding of what is important to the organisation (e.g. password management, encryption of removable media). Make it available to end-users and market its' usefulness.

3) *Ability to comply with regulatory requirements*: Where required, a regulated enterprise must maintain a cybersecurity training program to ensure that the culture is aligned with the regulatory body requirements. This involves the identification of specific provisions for compliance, capturing specific criteria to satisfy the regulation(s) and applying the necessary controls/provisions to demonstrate adherence.

4) *Define a behavioural baseline*: To hold an individual accountable for adhering to the organisation's security policies, the organisation's expectations must be clearly defined. Additionally, proper education must be provided with objective evidence (signing an acknowledgement form, etc.) indicating the employee has been educated on the required policy and related practices.

5) *Motivate secure behavior*: Encouraging positive actions while disapproving of undesired behaviours is necessary to achieve the desired representative behaviours. Using classical conditioning techniques via reward and penalty systems, the desired and undesired behaviours must be identified and described in enough detail to enable targeted monitoring and reinforcement. Educational institutes need to begin applying the same importance and rigour to cybersecurity with overall human safety. It can be expected that in some organisations, cybersecurity training is either not addressed or only executed to "check the box" for insurance or regulatory purposes.

6) *Communication/Social media exposure to the network*: Organisations should ensure that there is a clear separation between the functions (email, internet access, etc.) that can be performed on P.C.s with access to the factory operations network(s) and those that should be conducted outside of the network entirely.

In addition, Saudi universities need to adopt effective training programs for students, with the major consideration being students' security behaviours. In addition, it is important to involve students in the training programs by researching cyber security. If students were involved in the development process, they would be regularly asked how to develop a secure system and the important steps to encourage students to adopt secure behaviours. Having the students participate in the process and consulting them for their views will create a cyber security culture among students. According to Chun et al. [33], citizens are not just recipients of e-government. They are also the key chain that guides policy formulation through their opinion and views. Carter and Bélanger [34] state that 74.2% of government agencies in the U.K. have a website. However, 90.5% of these agencies have not surveyed to see what online services their citizens and businesses want. Thus, the students' levels of CSA would increase when they are informed of the importance and strategies of cyber security.

VII. CONCLUSION

The purpose of this research was to look into and analyse cyber security concerns in Saudi Arabia. According to the conclusions of this survey, Saudi students are unaware of the importance of cyber security. This research indicated a poor score for training and awareness, with 92 percent of respondents have never received any form of cyber security training. According to the findings of this study, Saudi institutions should teach their students about anti-cybercrime legislation and the key information security awareness issues discovered in this study. Much more research is needed to establish how students' knowledge levels might be increased by implementing appropriate awareness-raising initiatives. Further research may be needed to identify how best practices might improve the issue areas identified in this study.

REFERENCES

- [1] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, and M. Xu, "A Survey on Machine Learning Techniques for Cyber Security in the Last Decade," *IEEE Access*, vol. 8, pp. 222310-222354, 2020.
- [2] A. H. Cordesman, J. G. Cordesman, and J. G. Cordesman, *Cyber-threats, information warfare, and critical infrastructure protection: defending the US homeland*: Greenwood Publishing Group, 2002.
- [3] K. Shaukat, S. Luo, S. Chen, and D. Liu, "Cyber Threat Detection Using Machine Learning Techniques: A Performance Evaluation Perspective," in *2020 International Conference on Cyber Warfare and Security (ICWS)*, 2020, pp. 1-6.
- [4] L. Kim, "Cybersecurity matters," *Nursing management*, vol. 49, pp. 16-22, 2018.
- [5] S. Musman and A. Turner, "A game theoretic approach to cyber security risk management," *The Journal of Defense Modeling and Simulation*, vol. 15, pp. 127-146, 2018.
- [6] K. E. Eichensehr, "Public-private cybersecurity," *Tex. L. Rev.*, vol. 95, p. 467, 2016.
- [7] A. Alzahrani and K. Alomar, "Information security issues and threats in Saudi Arabia: a research survey," *International Journal of Computer Science Issues (IJCSI)*, vol. 13, p. 129, 2016.
- [8] H. Kruger, L. Drevin, and T. Steyn, "A vocabulary test to assess information security awareness," *Information Management & Computer Security*, 2010.
- [9] H. A. Kruger and W. D. Kearney, "A prototype for assessing information security awareness," *Computers & security*, vol. 25, pp. 289-296, 2006.
- [10] C. McPhee and T. Bailetti, "Editorial: Cybersecurity," *Technology Innovation Management Review*, vol. 4, pp. 3-4, 2014.
- [11] I. Gupta and P. Mishra, "Special Issue on Cyber Security," *Defence Science Journal*, vol. 66, p. 557, 2016.
- [12] K. Parsons, A. McCormac, M. Pattinson, M. Butavicius, and C. Jerram, "A study of information security awareness in Australian government organisations," *Information Management & Computer Security*, 2014.
- [13] J. Liu, Y. Xiao, S. Li, W. Liang, and C. P. Chen, "Cyber security and privacy issues in smart grids," *IEEE Communications Surveys & Tutorials*, vol. 14, pp. 981-997, 2012.
- [14] E. Kritzing and S. H. von Solms, "Cyber security for home users: A new way of protection through awareness enforcement," *Computers & Security*, vol. 29, pp. 840-847, 2010.
- [15] K. Shaukat, S. Luo, V. Varadharajan, I. A. Hameed, S. Chen, D. Liu, et al., "Performance comparison and current challenges of using machine learning techniques in cybersecurity," *Energies*, vol. 13, p. 2509, 2020.
- [16] T. I. Baig, T. M. Alam, T. Anjum, S. Naseer, A. Wahab, M. Imtiaz, et al., "Classification of human face: Asian and Non-Asian people," in *2019 International Conference on Innovative Computing (ICIC)*, 2019, pp. 1-6.
- [17] S. A. Alashi and H. A. Aldahawi, "Cybersecurity Management for Virtual Private Network (VPN) Applications: A Proposed Framework for the Governance of their Use in the Kingdom of Saudi Arabia," *Journal of Information Security and Cybercrimes Research*, vol. 3, pp. 31-57, 2020.
- [18] T. M. Alam and M. J. Awan, "Domain analysis of information extraction techniques."
- [19] R. Von Solms and J. Van Niekerk, "From information security to cyber security," *computers & security*, vol. 38, pp. 97-102, 2013.
- [20] Y. Rezgui and A. Marks, "Information security awareness in higher education: An exploratory study," *Computers & security*, vol. 27, pp. 241-253, 2008.
- [21] S. Atkinson, S. Furnell, and A. Phippen, "Securing the next generation: enhancing e-safety awareness among young people," *Computer fraud & security*, vol. 2009, pp. 13-19, 2009.
- [22] I. Frank and E. Odunayo, "Approach to cyber security issues in Nigeria: challenges and solution," *International Journal of Cognitive Research in science, engineering and education*, vol. 1, 2013.
- [23] E. B. Kim, "Recommendations for information security awareness training for college students," *Information Management & Computer Security*, 2014.
- [24] T. M. Alam, M. Mushtaq, K. Shaukat, I. A. Hameed, M. U. 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.
- [25] A. E. M. Aloufi, *A Cognitive Theory-based Approach for the Evaluation and Enhancement of Internet Security Awareness among Children Aged 3-12 Years*: Rochester Institute of Technology, 2015.
- [26] 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," in *2021 The 4th International Conference on Software Engineering and Information Management*, 2021, pp. 193-198.
- [27] 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.
- [28] M. N. Saunders and F. Bezzina, "Reflections on conceptions of research methodology among management academics," *European management journal*, vol. 33, pp. 297-304, 2015.
- [29] 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.
- [30] A. Bryman and E. Bell, *Business research methods (Vol. 4th)*, "Glasgow: Bell & Bain Ltd, 2015.
- [31] K. Shaukat, T. M. Alam, I. A. Hameed, W. A. Khan, N. Abbas, and S. Luo, "A Review on Security Challenges in Internet of Things (IoT)," in *2021 26th International Conference on Automation and Computing (ICAC)*, 2021, pp. 1-6.
- [32] D. Gefen, G. M. Rose, M. Warkentin, and P. A. Pavlou, "Cultural diversity and trust in IT adoption: A comparison of potential e-voters in the USA and South Africa," *Journal of Global Information Management (JGIM)*, vol. 13, pp. 54-78, 2005.
- [33] S. Chun, S. Shulman, R. Sandoval, and E. Hovy, "Government 2.0: Making connections between citizens, data and government," *Information Polity*, vol. 15, pp. 1-9, 2010.
- [34] L. Carter and F. Bélanger, "The utilization of e - government services: citizen trust, innovation and acceptance factors," *Information systems journal*, vol. 15, pp. 5-25, 2005.

Ontology-based Daily Menu Recommendation System for Complementary Food According to Nutritional Needs using Naïve Bayes and TOPSIS

Mujahidah Showafah, Sari Widya Sihwi*, Winarno

Informatics Department, FMIPA, Universitas Sebelas Maret, Surakarta, Indonesia

Abstract—Babies begin to be given complementary feeding at the age of 6 to 24 months. Complementary foods given to babies need to meet nutritional needs according to their ages. Since, at these ages, babies are just learning to eat, it is necessary to plan a complementary food menu referring to the nutritional needs and the baby and mother's preferences. It is certainly not an easy thing for a mother. Therefore, a recommendation system is needed to determine the baby's daily menu according to those all. This research proposes a complementary food menu recommendation system that considers the balanced composition of three significant nutrients (carbohydrates, protein, and fat) in the diet. It also takes into account the baby and mother's preferences. The ontology contains Knowledge-based about food and its nutritional content and the nutritional needs of babies according to their ages. Naive Bayes is used to prepare menu options according to user preferences. TOPSIS method is used in this study to provide optimal recommendations regarding nutritional balance and user preferences. Several mothers who have had babies aged 6-24 months and mothers of babies aged 6-24 months were asked to test the recommendation system. The results of the usability testing of the system using SUS showed a good level of user satisfaction.

Keywords—Calorie; complementary food; babies; Naïve Bayes; nutrition needs; ontology; recommendation system; SUS; TOPSIS

I. INTRODUCTION

Even though food is a basic necessity of human life, deciding what kind of food to be eaten is sometimes not easy. Many criteria should be taken, such as preferences, health issues, cultural and religious issues, and others that are individually different—having more criteria and alternatives to be considered means having more complexity. Nevertheless, using computer applications has turned to be a solution.

A recommendation system is a computer application that can be used to recommend anything favorable for users, including foods. Some researchers formulated applications to suggest food for different typical users and different intentions. Some examples are [1] recommends menu by considering the user's preferences and restrictions, [2] predicts the days required for a person to gain a healthy BMI status with the recommended food, and [3] suggests food should be given to which patient base on the disease and other features, and many more.

Like adult foods, determining children's foods is not a simple matter. It can even be more serious since they need appropriate nutrition for optimal growth and development.

Having improper intake can cause malnutrition problems and even death. However, based on some facts, for many different reasons, it is ignored. In the article [4], it was written that 67 babies were reported to have died due to suffering from malnutrition. Based on basic health research [5], in 2013, malnutrition in infants and children in Indonesia reached 19.6%, an increase of 1.7% compared to 2010 (17.9%). This is why some studies were focused on giving food recommendations to children, such as [6][7][8] [9][10][11]. Furthermore, few researchers concentrate on a specific period of children's age called the golden period.

The golden period often refers to the range of age from 0-24 months. It is highly recommended to breastfeed the baby in the first six months of a baby's life without giving other intakes. After that, it recommends providing complementary foods for infants aged 6-24 months [12]. Complementary food is any food or drinks containing nutrients given to infants aged 6-24 months to meet nutritional needs other than breast milk [12]. To meet the nutritional needs of infants, complementary food needs to be adjusted to the nutritional needs according to the baby's age. This adjustment certainly requires accuracy and effort that is not easy, especially if a set of routines needs to be done every day. Therefore, a recommendation system is needed. An example of works that focus on this domain is [10]. It presents a daily menu set resulting from implementing Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) by considering carbohydrates, protein, and fat as criteria.

Some researches in this domain utilize ontology as the knowledge base of complementary food, such as [8],[11],[10]. Ontology is the theory of content about an object, the properties of objects, and the relationships between objects that are incorporated in a knowledge domain [13]. Ontology-based approaches derive the new extended terms by semantically mapping knowledge represented in terms of classes (concepts) properties and relationships as depicted in domain ontologies [14]. Hence, it can show the knowledge and concepts of relations in a clear manner [15]. It can also improve the access and the integration of heterogeneous information from various sources [16]. Thus, it is often considered as one of the essential components to build any intelligent system [17].

This research extends the work in [11]. Research [11] proposes a complementary food recommendation system by using ontology as its knowledge base. It improved research [8] by adding consideration of users' past preferences. Each food

*Corresponding Author

ingredient in a recipe recommended to the user is given a score reflecting the user's feedback on the recommended meal recipe. Naïve Bayes computes the ingredients' preferences scores to produce a personal recommendation that is needed and liked by the infant individually. Research [8] and [11] also consider the condition of the children, such as allergies suffered or malnutrition suffered, in giving the recommendation. However, neither studies consider the balance of carbohydrates, proteins, and fats needed by infants as practiced by research [10].

Therefore, in the present work, we propose a recommendation system at the top of the complementary food ontology, as its knowledge-based, by considering the balance of carbohydrates, proteins, and fats, and based on the user's past preference for food with the implementation of the Naïve Bayes method and TOPSIS. As its consequences, this work has two main tasks (which are also the contributions). First, we improve the complementary food ontology in [11] so that filtering by nutrient adequacy can be done. For that reason, some additions and modifications in the ontology should be made. Second, we combine Naïve Bayes and TOPSIS to bring a recommendation result in the form of a daily menu set by considering babies' preferences individually as well as their nutrient adequacy. In a daily meal plan, we consider a breakfast menu, an evening meal menu, a dinner menu, and snacks (two times), though not all of them will be suggested to a baby (depending on the baby's age).

The following sections of this paper give a detailed picture of our work. The following section presents a review of the domains that will be discussed. Section three describes the methodology used in this work. In section four, we bring the result of our experiment and also the analysis on them. Finally, we conclude with the conclusion and future work in the last section.

II. LITERATURE REVIEW

A. Naïve Bayes

Naïve Bayes is a classification with probability and statistical methods that predict future opportunities based on experience [18]. The Naïve Bayes formula is as follows:

$$P(C|F_1, \dots, F_n) = \frac{P(C)P(F_1, \dots, F_n|C)}{P(F_1, \dots, F_n)} \quad (1)$$

Where variable C represents class and variable F_1, \dots, F_n represents characteristic instructions that are needed for classification. $P(C|F_1, \dots, F_n)$ or posterior is a probability for the entry of specific characteristic samples into the class. $P(C)$ or prior is a probability class before entering the sample. $P(F_1, \dots, F_n|C)$ or likelihood of evidence is the probability for the emergence of sample characteristics in class. $P(F_1, \dots, F_n)$ or evidence is the probability characteristics globally [11].

B. Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)

The Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS) was proposed by Hwang and Yoon (1981) to determine the best alternative based on the concept of

choosing a solution with the shortest Euclidean distance from the ideal solution and the Euclidean distance farthest from the negative ideal solution [19]. The steps in calculating TOPSIS are [20]:

- Build a decision matrix and determine the weight of the criteria.
- Calculate the normalized decision matrix. The formula for calculating a normalized decision matrix:

$$n_{kj} = \frac{x_{kj}}{\sqrt{\sum_{k=1}^n x_{kj}^2}} \quad (2)$$

- Calculate the weight of the normalized decision matrix. The normalized weight v_{kj} is calculated by the formula:

$$v_{kj} = w_j n_{kj} \text{ for } k = 1, \dots, n; j = 1, \dots, m \quad (3)$$

Where w_j is the weight of criteria- j , $\sum_{j=1}^m w_j = 1$.

- Determine the positive and negative ideal solutions. The formula of positive ideal alternative A^+ is:

$$A^+ = (v_1^+, v_2^+, \dots, v_m^+) = \left[[\max v_{kj} | j \in I], [\min v_{kj} | j \in J] \right] \quad (4)$$

The formula of negative ideal alternative A^- is:

$$A^- = (v_1^-, v_2^-, \dots, v_m^-) = \left[[\min v_{kj} | j \in I], [\max v_{kj} | j \in J] \right] \quad (5)$$

Where I associated with the profit and J associated with the cost, $k = 1, \dots, n; j = 1, \dots, m$.

- Calculate the distance from a positive ideal solution and a negative ideal solution. The formula for a positive ideal solution and a negative ideal solution are:

$$D_k^+ = \sqrt{\sum_{j=1}^m (v_{kj} - v_j^+)^2}, k = 1, \dots, n \quad (6)$$

$$D_k^- = \sqrt{\sum_{j=1}^m (v_{kj} - v_j^-)^2}, k = 1, \dots, n \quad (7)$$

- Calculate the relative proximity to a positive ideal solution by using (8).

$$R_k = \frac{D_k^-}{D_k^- + D_k^+} \quad (8)$$

Where $0 < R_k < 1, k = 1, 2, \dots, n$.

- Sort alternatives that have values close to 1.

C. Energy Needs

Energy requirements of complementary food are obtained from reducing the daily energy requirements of infants by breast milk energy intake [21]. The daily energy requirements of infants referring to [22] n can be seen in Table I, while the energy intake from breast milk can be seen in Table II. In Table III, the amount of mealtime the infants have is shown. Infants have different amounts of mealtime according to their age.

TABLE I. THE DAILY ENERGY NEEDS OF INFANTS [22]

Age (months)	Energy (Kkal)	Carbohydrate (g)	Protein (g)	Fat (g)
6	550	58	12	34
7 – 8	725	82	18	36
9 – 11	725	82	18	36
12 – 24	1125	155	26	44

TABLE II. THE ENERGY INTAKE FROM BREAST MILK [21]

Age (months)	Energy (Kcal/day)
6 - 8	413
9 – 11	379
12 – 24	346

TABLE III. THE AMOUNT OF FEEDING TIME [10]

Age (months)	Amount of Main Mealtime	Amount of Snack Time
6	2	0
7 – 8	3	0
9 – 1	3	1
12 – 24	3	2

III. METHODOLOGY

A. Data and Knowledge Collection

The data used in this study are food material data and food recipes. The knowledge applied is nutritional adequacy rates for infants and energy intake from breast milk.

B. Ontology Modeling

The ontology used in this study is ontology [11], with several changes in the structure and instances. In addition, some knowledge was added to the ontology. The changes on the ontology were made using Protégé.

C. Analysis of Method Implementation

1) *Combination of recipes*: In this study, the recommended menu will be adjusted to the amount of mealtime and the infant's energy needs. The flow in making a recipe combination is shown in Fig. 1.

2) *Application of the methods*: The method used in this research is TOPSIS and Naïve Bayes. The first method applied to the system is the TOPSIS method. The criteria for TOPSIS are the nutritional content of carbohydrates, proteins, and fats with weights using nutritional adequacy values. The next step is to calculate the Naïve Bayes value from the existing recipe combination. Naïve Bayes calculations are influenced by user feedback on recipes that have been tried. The steps to calculate Naïve Bayes in this study are,

a) *Calculate the probability of a preferred material*: The probability is counted by using (9). Laplace (add-one) smoothing is used in the equation to avoid getting zero outcomes for the probability when a new application is used or when a menu has never been selected.

$$(C = c) = \frac{\text{amountOfLiked}(v_i, \text{recipe}(c)) + 1}{\text{Ingredients}(\text{recipe}(c)) + \text{All_ingredients}}, i = 1, 2, \dots, n \quad (9)$$

where:

- v_i : one type of food ingredients,
- $\text{amount of liked}(v_i, \text{recipe}(c))$: The number of occurrences of a food item that has a "like" feedback value by the user,
- $\text{Ingredients}(\text{recipe}(c))$: The amount of food ingredients in the recipe that is rated "like" by the user,
- All_ingredient : Total ingredients in the database.

b) *Calculate the probability of a preferred recipe*: The probability is counted by using (10).

$$P(\text{recipeLiked}|C) = P(\text{recipeLiked}) * P(v_1) * P(v_2) * \dots * P(v_n) \quad (10)$$

where:

- $P(\text{recipeLiked}|C)$: The probability of a recipe to be liked,
- $P(\text{recipeLiked})$: The probability of a preferred recipe,
- $P(v_n)$: The probability of food ingredients in the recipe.

D. System Testing

System testing is done by measuring system usability and user satisfaction. Measurement of system usability is done by distributing SUS questionnaires to users. Questionnaire questions that are used are based on the SUS questionnaire [19]. A list of SUS questions can be seen in Table IV taken from [23]. Each question will be given five choices with criteria according to Table V. The results of the questionnaire will be calculated individual SUS values with equation (11). Then, the results will be averaged to get the overall SUS value. The SUS value will be used to classify the system eligibility by mapping it to Table VI [24]. The purpose of this test is to measure the level of system usability for users.

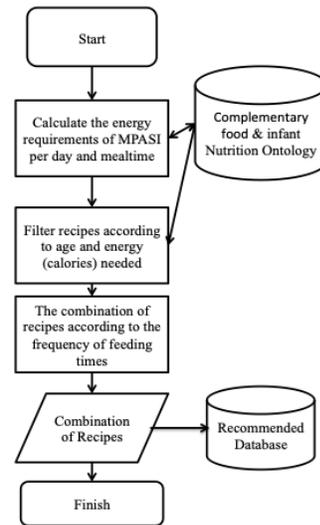


Fig. 1. Flow in Making a Recipe Combination.

The next test is testing the level of user satisfaction by distributing questionnaires to system users with a list of statements. The statements are "Information provided by the system is as expected" and "Sustainability to use the system next time." The purpose of this test is to measure the level of user satisfaction with the system.

$$SUSscore = ((P1 - 1) + (5 - P2) + (P3 - 1) + (5 - P4) + (P5 - 1) + (5 - P6) + (P7 - 1) + (5 - P8) + (P9 - 1) + (5 - P10)) \times 2.5 \quad (11)$$

TABLE IV. THE LIST OF SUS QUESTIONS [23]

No.	Code	Statement
1.	P1	I think that I would like to use this system frequently
2.	P2	I found the system unnecessarily complex
3.	P3	I thought the system was easy to use
4.	P4	I think that I would need the support of a technical person to be able to use this system
5.	P5	I found the various functions in this system were well-integrated
6.	P6	I thought there was too much inconsistency in this system
7.	P7	I would imagine that most people would learn to use this system very quickly
8.	P8	I found the system very cumbersome to use
9.	P9	I felt very confident using the system
10.	P10	I needed to learn a lot of things before I could get going with this system

TABLE V. MEASUREMENT CRITERIA LIKERT SCALE

Score	Criteria
1	Strongly Disagree
2	Disagree
3	Neutral
4	Agree
5	Strongly Agree

TABLE VI. THE SAURO-LEWIS CURVE GRADING SCALE [24]

SUS Score Range	Grade	Percentile Range
84.1 – 100.0	A+	96 – 100
80.8 – 84.0	A	90 – 95
78.9 – 80.7	A-	85 – 89
77.2 – 78.8	B+	80 – 84
74.1 – 77.1	B	70 – 79
72.6 – 74.0	B-	65 – 69
71.1 – 72.5	C+	60 – 64
65.0 – 71.0	C	41 – 59
62.7 – 64.9	C-	35 – 40
51.7 – 62.6	D	15 – 34
0.0 – 51.6	F	0 – 14

IV. RESULTS AND DISCUSSION

A. Data and Knowledge Collection

The data used in this study are food material data obtained from the Food Composition List issued by the Ministry of Health (2005) and food recipes that already exist in ontology [11]. The knowledge used in this study is nutritional adequacy figures data for infants [22] and energy intake data from breast milk [21]. The data collected were 366 food items and 160 recipes. All data and knowledge were entered into ontology.

B. Ontology Modeling

In ontology [11], there are some additions regarding food material data on food sources class and nutritional adequacy figures data and energy intake data from breast milk in instances in the 'babyAge' class. Some changes that were made to the ontology, there are:

- Making 'foodsources', 'makingProcess', 'taste', and 'texture classes' become a subclass of the 'food' class since the four classes are still a part of the 'food' class.
- Adding 'foodquantity' subclass to 'food' class as additional knowledge about kitchen units in grams.
- Adding another subclass to the 'food' class, namely: 'combined_food', which contains complementary foods recipes.
- Changing the subclass in the 'foodSource' class to 'animal_based', 'fat_oil', 'plant_based', and 'other'. This was done to fit the distribution of materials in the Food Composition List.
- Adding the 'dairy_product', 'egg', 'fish', and 'meat' subclasses to the 'animal_based' class to adjust the distribution of ingredients to the Food Composition List.
- Adding subclasses of 'fruits', 'nuts', 'tubers', and 'vegetables' to the 'plant_based' class to adjust the distribution of ingredients to the Food Composition List.
- Adding 'macronutrient' and 'micronutrient' subclasses to 'nutrients' class. in order to increase the knowledge, then nutrition is divided into two types, namely macro nutrition and micronutrition. All these changes can be seen in Fig. 2.
- Changing the instances of 'babyAge' to '6_months', '7-8_months', '9-11_months', and '12-24_months' to adjust the nutritional adequacy figures data distribution. These changes are presented in Fig. 3.

C. Analysis and Results of Application of Methods to The System

1) *Combination of recipes*: Calculating Complementary Food Energy Needs per Day and per Mealtime: Complementary food energy requirements, as seen in Table VII, are obtained from reducing daily energy requirements by breast milk energy intake. Therefore, the energy requirement is the energy should be fulfilled by a set of

menu recommended. The number of menus provided is compatible with the amount of mealtime, except for six months. For ages six months, the menu provided is one for two mealtimes. Each mealtime has a different percentage in meeting the daily energy adequacy. Table VIII [25] shows the percentage distribution of energy sufficiency from the total complementary food energy needs in a day. The application of the percentage of energy sufficiency per mealtime at each age is shown in Table IX.

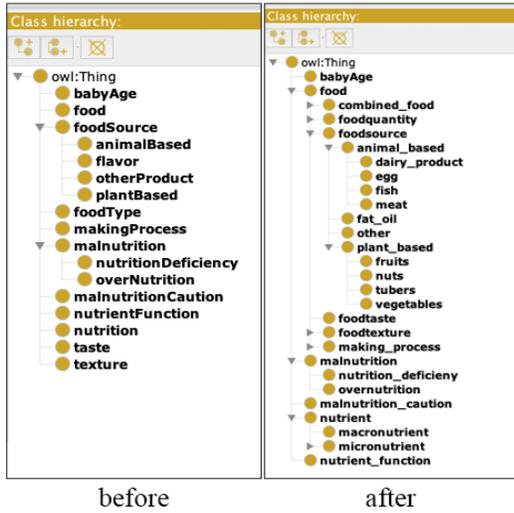


Fig. 2. Changes in the Ontology.

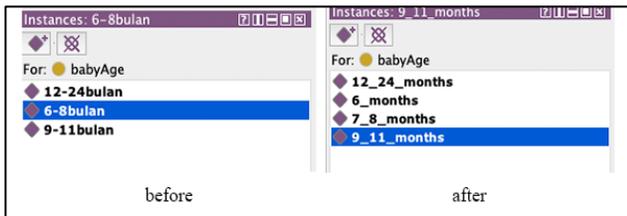


Fig. 3. Changes on the BabyAge Class.

TABLE VII. THE COMPLEMENTARY FOOD ENERGY NEEDS PER DAY

Age (months)	Daily Energy Needs (kcal)[22]	Breast Milk Energy Intake (kcal) [21]	Complementary Food Energy Needs (kcal)
6	550	413	137
7 – 8	725	413	312
9 – 11	725	379	346
12 – 24	1125	346	779

TABLE VIII. THE PERCENTAGE OF ENERGY ADEQUACY PER MEALTIME [25]

Mealtime	Percentage
Breakfast	25 – 30%
Lunch	30 – 40%
Dinner	25 – 30%
Snack	8 – 10%

TABLE IX. THE APPLICATION OF ENERGY ADEQUACY PERCENTAGE PER MEAL TIME AT EACH AGE

Mealtime	6 Months	7 - 8 Months	9 - 11 Months	12 - 24 Months
Breakfast	50%	30%	25%	25%
Lunch	50%	40%	40%	30%
Dinner	-	30%	25%	25%
Snack	-	-	10%	10%

TABLE X. THE ENERGY RESULTS AT EACH MEAL TIME WITH MINIMUM AND MAXIMUM LIMITS AT AGE 12 - 24 MONTHS

Breakfast (Kkal) 25%	Min (Kkal)	175.27
	Needed (Kkal)	194.75
	Max (Kkal)	214.22
Snack 1 (Kkal) 10%	Min (Kkal)	70.11
	Needed (Kkal)	77.90
	Max (Kkal)	85.69
Lunch (Kkal) 30%	Min (Kkal)	210.33
	Needed (Kkal)	233.7
	Max (Kkal)	257.07
Snack 2 (Kkal) 10%	Min (Kkal)	70.11
	Needed (Kkal)	77.90
	Max (Kkal)	85.69
Dinner (Kkal) 25%	Min (Kkal)	175.27
	Needed (Kkal)	194.75
	Max (Kkal)	214.22

a) *Filtering recipes according to age and energy needed:* In this stage, the minimum energy value (− 10%) and the maximum energy value (+ 10%) are calculated at each meals time. Energy results for each meal with a minimum and maximum limit for ages 12-24 months can be seen in Table X. After that filtering prescriptions are done. Table XI shows an example of recipes for breakfast results at 12-24 months.

b) *Recipe combination according to the number of meals:* After getting a recipe for every meal, a combination of recipes is done to get the complementary food menu per day. In the previous stage, a minimum energy limit (− 10%) and a maximum energy limit (+ 10%) were determined at each mealtime. This results in a combination of menus with total energy exceeding energy requirements, around 30 - 50% according to the amount of time the baby eats. Therefore, at this stage, filtering the total energy possessed by a combination of recipes according to the energy requirements of complementary food per day with a minimum energy limit (− 10%) and a maximum energy limit (+ 10%). Table XII shows an example of a recipe combination for infants aged 12-24 months.

2) *Application of the method to the system:* Fig. 4 shows the system development flowchart. The first step is to add the infant's data like age and allergies. Next, the system will filter

the combination of recipes based on the infants' age and allergies. Then, the system will calculate the preference value with TOPSIS and Naive Bayes.

a) *Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS)*: The application of the TOPSIS method is carried out to obtain recommendations that consider the adequacy of carbohydrates, proteins, and fats. The nutritional content of carbohydrates, proteins, and fats is used as a criterion in calculating TOPSIS in this study. The weight of each criterion is obtained from the nutritional adequacy rate of each criterion divided by the sum number of nutritional adequacy figures of carbohydrates, protein, and fat. Table XIII shows the weight of each criterion for a 12-24-month baby. In this step, 50 combinations will be taken with a value of R_k close to one. Table XIV shows five combinations that have values close to one.

b) *Naïve Bayes*: This method is used to get menu recommendations on the system according to the user preferences. User preferences are obtained from user feedback on recipes that have been tried. Feedback is given in the form of opinions; the categories are 'like', 'dislike', or 'allergic' to recipes. Each category has its own value 'like' is one, 'dislike', and 'allergy' is zero. Table XV shows the feedback given by users with infants of 12 months. The results of the final recommendation can be seen in Table XVI.

TABLE XI. THE EXAMPLE OF FILTERING RECIPES FOR BREAKFAST AT AGE 12-24 MONTHS

Recipe	Energy (Kkal)
Tomato Banana Porridge	209.84
Tempe porridge	177.58
Apricot Tahu	247.35
Oatmeal Dates	209.43
Cork Fish Noodle Soup	179

TABLE XII. AN EXAMPLE OF COMBINATION RECIPES AT AGE 12-24 MONTHS

Menu	Breakfast	Lunch	Dinner	Snack 1	Snack 2
1	Tomato Banana Porridge	Apricot Tofu	Tomato Banana Porridge	Papaya Orange Pudding	Papaya Orange Pudding
2	Tomato Banana Porridge	Apricot Tofu	Tempe porridge	Papaya Orange Pudding	Papaya Orange Pudding
3	Tomato Banana Porridge	Apricot Tofu	Oatmeal Dates	Papaya Orange Pudding	Papaya Orange Pudding
4	Tomato Banana Porridge	Apricot Tofu	Cork Fish Noodle Soup	Papaya Orange Pudding	Papaya Orange Pudding
5	Tomato Banana Porridge	Red Rice Porridge	Tomato Banana Porridge	Papaya Orange Pudding	Papaya Orange Pudding

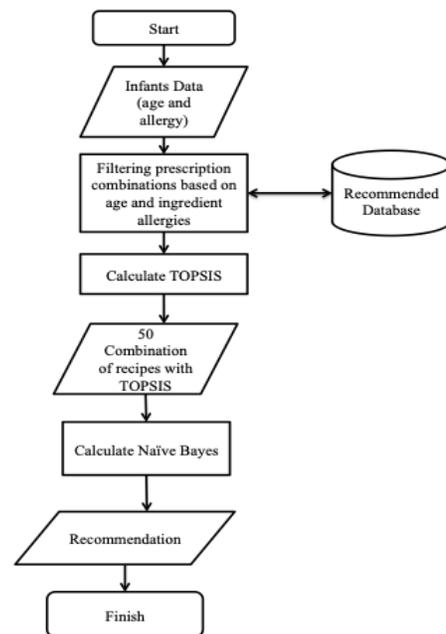


Fig. 4. The System Development Flowchart.

TABLE XIII. WEIGHT OF EACH CRITERION FOR AGES 12 - 24 MONTHS

Nutrient	Nutritional Adequacy Rate Score	Total	Weight
Carbohydrate	155	225	0.6889
Protein	26	225	0.1156
Fat	44	225	0.1956

TABLE XIV. TOPSIS VALUE FOR EACH COMBINATION

ID Menu	R_k
20338	0.9671
20266	0.9659
20336	0.9659
20339	0.9643
20374	0.9643

TABLE XV. THE FEEDBACK LIST OF RECIPES

Recipe	Ingredients	Feedback
Banana Smoothies	Banana, Honey, Vanilla Yoghurt	Like
Apricot Porridge	Oatmeal, Pear, Apricot, Banana	Like
Banana Smoothies	Banana, Honey, Vanilla Yoghurt	Like
Banana Smoothies	Banana, Honey, Vanilla Yoghurt	Like
Orange Papaya Pudding	Papaya, Jelly, Maizena, Orange	Like
Steamed Apple Potatoes	Potato, Apple	Dislike
Banana Smoothies	Banana, Honey, Vanilla Yoghurt	Like
Orange Papaya Juice	Papaya, Orange	Like

TABLE XVI. RECOMMENDATION RESULTS

Menu	Breakfast	Lunch	Dinner	Snack1	Snack2
1	Tempe porridge	Banana Smoothies	Tempe porridge	Papaya Orange Pudding	Papaya Orange Pudding
2	Tomato Banana Porridge	Milk Corn Porridge	Tomato Banana Porridge	Papaya Orange Pudding	Papaya Orange Pudding
3	Tomato Banana Porridge	Yellow Pumpkin Soup	Tomato Banana Porridge	Papaya Orange Pudding	Papaya Orange Pudding
4	Tempe porridge	Banana Smoothies	Tomato Banana Porridge	Papaya Orange Pudding	Papaya Orange Pudding
5	Tomato Banana Porridge	Milk Corn Porridge	Oatmeal Dates	Papaya Orange Pudding	Papaya Orange Pudding

D. Display of The Application: Fig. 5 shows the menu Display on the Application. There are three main menus, which are:

1) 'Rekomendasi' menu: This menu will display the results of recommendations using the TOPSIS and Naïve Bayes methods regardless of whether the ingredients have been tried or not. Display on this menu can be seen in Fig. 6. The system will display five recommended menus. Each menu consists of a recipe for breakfast, lunch, dinner, snack 1, and snack 2 according to the amount of mealtime each age.

2) 'Bahan Sudah Dicoba': This menu will display a list of food ingredients that users have tried. After the user chooses one food ingredient that has been tried, the application will display five recommended menus using the TOPSIS method and Naïve Bayes containing the selected food ingredients. This menu display can be seen in Fig. 7.

3) 'Bahan Belum Dicoba': This menu will display a list of food ingredients that the user has not tried. After the user chooses one food ingredient that has not yet been tried, the application will display five recommended menus using the TOPSIS and Naïve Bayes methods containing the selected food ingredients. This menu display can be seen in Fig. 7.

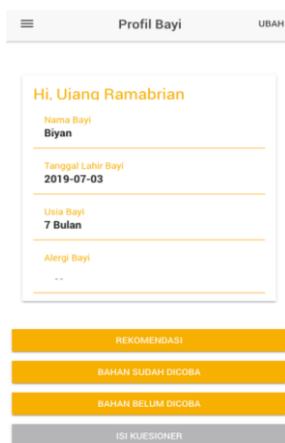


Fig. 5. The Display Menu in Applications.

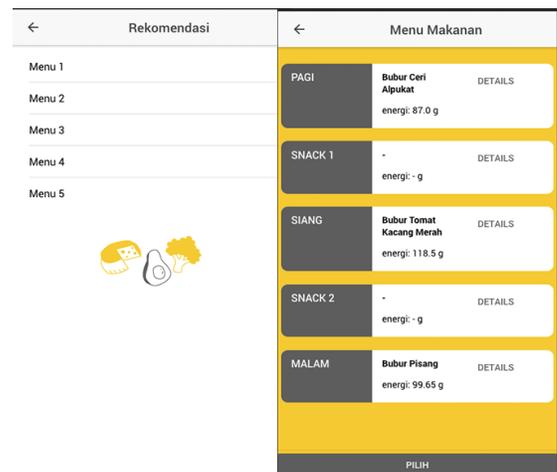


Fig. 6. The Display 'Rekomendasi' Menu.



Fig. 7. Displaying all Ingredients having been Tried by the Infant (Right) and all New Ingredients for the Infant (Left).

E. System Testing

We did the system testing by measuring system usability and also user satisfaction. Usability measurement of this system was done by distributing SUS questionnaires to 30 application users consisting of mothers who have experience with babies aged 6-24 months and mothers of babies aged 6-24 months.

From the result, we get the overall SUS value by calculating the average individual SUS value. The overall SUS values obtained are as follows:

$$SUS\ Score = \frac{\sum individual\ SUS\ score}{\sum number\ of\ respondents} = \frac{2307.5}{30} = 76.92$$

By referring to Table VI, the SUS score shows that the system gains grade B. It means that the usability of the system is good.

The next test is testing the level of user satisfaction. This test aims to measure the level of user satisfaction with the system. Testing was done by distributing the questionnaire to 10 potential users. The results of the questionnaire can be seen in Table XVII. From it can be concluded that the information provided by the system is as expected. In addition, it also indicates that they will continue to use the system.

TABLE XVII. USER SATISFACTION QUESTIONNAIRE RESULTS

No.	Statement	Score										Mean
		1	2	3	4	5	6	7	8	9	10	
1.	Information provided by the system is as expected.	4	4	4	4	3	4	4	4	4	4	3.9
2.	Sustainability to use the system next time.	4	4	4	5	3	4	4	4	5	4	4.1

V. CONCLUSION

This study succeeded in making a recommendation system that uses ontology as data, as well as Naïve Bayes and TOPSIS methods for recommendations for daily complementary feeding menus according to nutritional adequacy (carbohydrates, protein, and fat) and user preferences of foodstuffs. Based on the system testing results, the system has a usability value of 76.92, which is in category B. The information provided by the system is considered as expected, and users will continue to use the system. Another further development that can be done is to provide recommendations by considering the preferences of other users, especially to recommend menus that have new recipes from food ingredients that they do not like before or new recipes that have never been tried before.

REFERENCES

- [1] N. Thongsri, P. Warintarawej, S. Chotkaew, and W. Saetang, "Implementation of a personalized food recommendation system based on collaborative filtering and knapsack method," *Int. J. Electr. Comput. Eng.*, vol. 12, no. 1, pp. 630–638, 2022, doi: 10.11591/ijece.v12i1.pp630-638.
- [2] A. K. Gopalakrishnan, "A Food Recommendation System Based on BMI, BMR, k-NN Algorithm, and a BPNN," in *Machine Learning for Predictive Analysis*, 2021, pp. 107–118.
- [3] C. Iwendi, S. Khan, J. H. Anajemba, A. K. Bashir, and F. Noor, "Realizing an Efficient IoT-Assisted Patient Diet Recommendation System Through Machine Learning Model," *IEEE Access*, vol. 8, no. January, pp. 28462–28474, 2020, doi: 10.1109/ACCESS.2020.2968537.
- [4] V. Rossa, "72 Tahun Merdeka, 906 Ribu Balita Indonesia Alami Gizi Buruk," 25 Januari 2018. [Online]. Available: <https://www.suara.com/news/2018/01/25/140117/72-tahun-merdeka-906-ribu-balita-indonesia-alami-gizi-buruk>. [Accessed 11 April 2019].
- [5] Kementerian Kesehatan RI, "Kementerian Kesehatan Republik Indonesia," 1 Desember 2013. [Online]. Available: <http://www.depkes.go.id/resources/download/general/Hasil%20Risksesda%202013.pdf>. [Accessed 11 April 2019].
- [6] K. Namgung, T. H. Kim, Y. S. Hong, and S. Nazir, "Menu Recommendation System Using Smart Plates for Well-balanced Diet Habits of Young Children," *Wirel. Commun. Mob. Comput.*, vol. 2019, 2019, doi: 10.1155/2019/7971381.
- [7] A. A. Shari et al., "Mobile Application of Food Recommendation For Allergy Baby Using Rule-Based Technique," in *2019 IEEE International Conference on Automatic Control and Intelligent Systems (I2CACIS)*, 2019, pp. 273–278.
- [8] A. Paradhita, S. widya sihwi, and R. Anggrainingsih, "Decision Support System of Complementary Breastfeeding Based on Ontology Modeling," 2018, pp. 338–342, doi: 10.1109/ISRITI.2018.8864303.
- [9] Namgung, K., Kim, T. -, Hong, Y. -, & Nazir, S. (2019). Menu recommendation system using smart plates for well-balanced diet habits of young children. *Wireless Communications and Mobile Computing*, 2019.
- [10] S. W. M. H. S. R. W. B. Sihwi, "Sistem Rekomendasi Menu Harian Makanan Pendamping Air Susu Ibu (MPASI) Berdasarkan Kebutuhan Kalori Bayi dengan Metode TOPSIS," *Jurnal Ilmu Komputer dan Agri-Informatika*, vol. 3, no. 2, p. 122, 2017.
- [11] A. N. Fadhilah, "Sistem Rekomendasi MPASI dengan Pemodelan Ontologi dan Metode Naïve Bayes," 2018.
- [12] Departemen Kesehatan RI, 2006. [Online]. Available: <https://agus34drajat.files.wordpress.com/2010/10/pedoman-pemberian-makanan-pendamping-asi-lokal.pdf>. [Accessed 11 April 2019].
- [13] B. J. J. R. Chandrasekaran, "What Are Ontologies , and Why Do We Need Them ?," no. May 2016, 1999.
- [14] B. Abu-Salih, H. Alsawalqah, B. Elshqeir, T. Issa, P. Wongthongtham, and K. K. Premi, "Toward a knowledge-based personalised recommender system for mobile app development," *J. Univers. Comput. Sci.*, vol. 27, no. 2, pp. 208–229, 2021, doi: 10.3897/jucs.65096.
- [15] M. Klabunde, D. Collado, and C. Bohon, "A Systematic Review of Nutrition Recommendation Systems: With Focus on Technical Aspects," *J. Psychiatr. Res.*, vol. 94, no. 3, pp. 36–46, 2017.
- [16] V. Subramaniaswamy et al., "An ontology-driven personalized food recommendation in IoT-based healthcare system," *J. Supercomput.*, vol. 75, no. 6, pp. 3184–3216, 2019, doi: 10.1007/s11227-018-2331-8.
- [17] R. Manna, D. Das, and A. Gelbukh, "Question-answering and recommendation system on cooking recipes," *Comput. y Sist.*, vol. 25, no. 1, pp. 223–235, 2021, doi: 10.13053/CYS-25-1-3899.
- [18] A. Saleh, "Penerapan Data Mining Dengan Metode Klasifikasi Naïve Bayes Untuk Memprediksi Kelulusan Mahasiswa Dalam Mengikuti English Proficiency Test (Studi Kasus : Universitas Potensi Utama)," Medan, 2015.
- [19] G.-H. T. J.-J. Huang, *Multiple Attribute Decision Making Methods and applications*, Boca Raton: Taylor & Francis Group, 2011.
- [20] E. Roszkowska, "Multi-Criteria Decision Making Models By Applying The TOPSIS Method To Crisp And Interval Data," 2009.
- [21] World Health Organization, *Guiding Principles for Complementary Feeding of The Breastfed Child*, Washington, D.C, 2003.
- [22] H. S. A. S. M. R. H. Hardinsyah, "Ringkasan - Angka Kecukupan Gizi (AKG) yang dianjurkan bagi Orang Indonesia 2012," November 2012.
- [23] A. Garcia, "UX Research Standardized Usability Questionnaire," 23 November 2013. [Online]. Available: <https://chaione.com/blog/ux-research-standardizing-usability-questionnaires>. [Accessed 28 October 2019].
- [24] J. R. Lewis, "Measuring Perceived Usability: SUS, UMUX, and CSUQ Ratings for Four Everyday Products," *International Journal of Human-Computer Interaction*, pp. 1044-7318, October 2018.
- [25] H. Mulyasari, *Sistem Rekomendasi Resep Makanan Pendamping Air Susu (MPASI) dengan Metode TOPSIS*, Surakarta: Universitas Sebelas Maret, 2015.

Emerging Requirement Engineering Models: Identifying Challenges is Important and Providing Solutions is Even Better

Hina Noor¹, Maheen Tariq², Anam Yousaf³, Hafiz Wajid Ali⁴, Engr. Arqam Abdul Moqet⁵
Abu Bakar Hamid⁶, Mahek Hanif⁷, Huma Naz⁸, Nabeel Tariq⁹, Prof. Dr. Ijaz Amin¹⁰, Osama Naseer¹¹
Department of CS & IT, Sialkot College of Physical Therapy, Sialkot, Pakistan^{1, 2, 3, 4, 5, 10, 11}
Department of CS & IT, University of Lahore, Gujrat Campus, Gujrat, Pakistan^{6, 7, 8, 9}

Abstract—Requirement Engineering is one of the most crucial tasks because it serves as the foundation for any software. Four pillars of requirement engineering procedures underpin the entire software. The bricks that make up the software edifice are functional and non-functional needs. Finally, design, implementation, and testing add stories to the foundation, allowing a full software tower to be built on top of it. As a result, the foundation must be strong enough to support the remainder of the software tower. Requirement engineers have various hurdles to design successful software for this purpose. Requirement Engineering (RE) is emerging as an increasingly important discipline to promote the development of web applications, as these are designed to meet various stakeholder requirements, additional functional, information, multimedia, and usability requirements compared to traditional software applications. The requirements of software systems are a very important area in software engineering. The success of software systems depends on how it effectively meets the requirements of users. In this paper, the review of current state of requirements engineering in which requirements from users are checked analyzed with their consistency and correctness is presented, and then identifies the emerging models of requirement engineering. Firstly, the paper highlight the current activities that enable the understanding of goals and objectives for developing proposed software systems, then the focus is on the techniques for improving the precision, accuracy, and variety of requirements. Next, identification of the challenges of emerging requirement engineering models is explained. The challenges like security and global trend that posed by emerging models of the future. Finally, we are trying to suggest some solutions for the mentioned challenges.

Keywords—Requirement engineering; current requirement engineering methods; emerging models for requirement engineering; challenges; pros and cons

I. INTRODUCTION

Requirement engineering is a mechanism in which the development team collects requirements from users and develops a system that satisfies the user's needs. The requirement is a very important activity in product development it's like a blueprint for the product. It is the process that involved identifying the real user of the system their requirement and expectation about a system so it is necessary to understand the requirements and negotiate with users and validate the requirements for successful

development of the system [1][2]. Requirements collection is not simple as it sounds. It is a difficult task but it is important to understand what the user wants. Inappropriate requirements may lead to failure in terms of cost, customer dissatisfaction, and quality [3]. Different ways used to collect requirements even some organization develop their development method [4]. "Requirements invariably contain a mixture of problem information, statements of system behavior and properties, and design and implementation constraints (Sommerville and Sawyer 1997)."

Requirements are of two types namely: user requirements and system requirements. User requirements referred to user needs that what user wants or what type of system is expected by the user. And what type of activities the user wants to perform on a system. System requirements are divided into functional and non-functional requirements. Functional requirements are those that user needs to perform their work on the system. On-functional requirements are all remaining requirements that are not covered by functional requirements like accessibility, availability, accuracy, error handling, failure management, and maintainability, etc.

Effective requirements are those which completely consistently records user needs. Good qualities of requirements are that they must be traceable, feasible, modifiable, independent, and unambiguous [6]. It must be necessary to develop a plan for requirements collection during the early phase of the proposal. And it helps us to determine how the requirements will evolve because a user may not describe the actual requirements at the beginning. We also face some barriers while collecting requirements like lack of requirement engineering knowledge, management may not understand what is going to be building. For these problems we should develop abilities to think out of the box that how to requirements will be evolved in the future [7], [26]. Requirement validation is also the process of requirement engineering in which we ensure that we going in the right direction for finding solutions to problems. It certifies that it is according to customer intents. Different techniques are used for requirements validation like preparing experiments and analyze the results of experiments [24].

The study's goal is to identify the critical factors that influence RE process model selection from the perspective of business practitioners. Several future options for the RE

process in software engineering are discussed, including application-specific elicitation approaches, requirements pre-processing, and requirements prioritisation, among other things.

The paper is structured as follows: Section 2 summarizes the related work. Section 3 will discuss current requirement engineering models and also elaborated their pros and cons. Then the Section 4 will propose emerging RE models and their challenges. In the next section, we will try to suggest some solutions for the challenges. The last section concludes the whole discussion and suggests some future work as well.

II. RELATED WORK

Geshwaree Huzoore & Vimla Devi Ramdoo (February 2015) proposed that many problems occur when the requirements are not correctly defined. Problems may include: customer's dissatisfaction, quality of software may suffer, cost overreach, and increase the cost of maintenance. Requirement Engineering includes four steps: Requirement extraction, requirement arrangements, and analysis, requirement specification, and validation. In requirement extraction, lots of challenges will be occurring. The challenges may include stack holder may not correctly be defined what he wants or he may not be the actual end-user, May the method use for requirement extraction is not effective, minimum involvement of stack holder. Requirements analysis is also a very difficult phase because the development teams may deal with multiple stack holders. So, it creates conflict between requirements, because every stack holder defines requirements in his specific way. Other challenges may also face during requirements analysis like lack of communication skills, lack of time, etc. Requirements specification also includes different key challenges like knowledge sharing, physical distance, incorrect requirements, etc.

Requirements validation also includes different challenges: requirements may not complete and consistent, requirement uncertainty, etc. [5]. Requirement engineering plays a very important role in successful software development, because it's directly related to the quality of product and customer satisfaction. So this paper describes currently challenges that different organization face in requirement engineering but now in the emerging technology era, there are other advanced challenges that different organization face that needs to be addressed like excessive requirements, adopting the technique for elicitation, requirement missing, requirements security. The major challenge in requirement engineering also needs to be addressing that how the requirement is to manage when the development is offshore. Because the development team needs to face the challenge of physical distance, language problems, difficulty to maintain long-distance meetings and it will lead to a lack of communication and cost of rework also difficult to maintain [12].

Mahrukh Umar and Asghar, Sohail, proposed other RE challenges: time constraint, the process of requirement engineering, economic crises, a conflict between users, technical crises. There is no best requirement engineering tool to collect the requirements. Lots of challenges are generating with the advancement of technology. Unsolved challenges increase the cost of the product. External events are another

crucial challenge of requirement engineering in which the development team has to consider security, loss of valuable data, viruses, etc. [13].

Requirement engineering is a critical phase in different products development that is demanded from customers. Finding the best technique for the development of a system is very difficult because it may affect the quality of the system. It might be acceptable for a system but not suitable for another system. It may affect the process of requirement engineering. It is mandatory to develop a model that provides guidelines to practitioners regarding the quality of the product and develop a product in a specific time, avoid problems that lead to system failure. SDLC consists of different stages of testing, deployment, maintenance that helps to improve the product quality and meets the needs of user requirements [8]. Developers, the analyst also play a very important role in the process of requirements engineering. They are familiar with problems that may occur while doing the software development process. Even they are familiar with the future direction system related to requirements like modeling, enhancements, and requirements changing. Organizational issues are also important in the process of the requirement engineering process. Issues are like requirements may be collected from malevolence users that may lead to failure of system development [9]. We should also consider the strength and weaknesses of the RE process. The main focus of RE is to find the stack holder's needs, finding the conflict between requirements, specifying the risks that might occur during development, defining requirements in a more concise way that leads to the successful development of a product. The weakness in the requirements engineering process is the guidelines that may not understand by the practitioners. The weaknesses may occur due to fewer reasons. Many IT personnel involved in software developments like programmers, analyst, and designers that have insufficient knowledge of RE that may lead to the problems. So it is necessary to understand the scope of the problem because it is considered to be less technical than other software development processes [10]. Developing a system, the first time without any error is not possible because an error is human. So it is not possible to develop a system without any error. An error may occur because of misunderstanding and ambiguity in documents. And Errors may occur at that stage where is difficult to handle. It is necessary to use a different technique that helps to prevent errors. In this regard, validation ensures the correct functionality of the system. The main focus of requirements validation is to ensure that the specifications of user requirements must be consistent, complete, and have no conflict between requirements [11].

Saleh, Mohammed, et al proposed different challenges that occur in agile Requirements engineering. Currently, there are lots of challenges in advanced product development. The organization wants agile software developments where the development team needs to face many challenges because of rapid changes, many any of projects because of vague requirements. Requirements collected using traditional activities include elicitation, specification, validation are important but agile developments need to adopt some advanced activities include prioritizing requirements,

modeling, the collaboration of the developments team and stack holders. Challenges that arise during advanced product development include minimum involvement of customers, inappropriate architecture, a budget of a project, and contractual issues about the evaluation of the product [14].

Limitation of this paper is that it's only discussed problems during product development like customer involvement, poor requirement traceability but did not provide any alternatives or solution.

Schön, Eva-Maria, et al listed different key challenges that development teams may face in agile requirement engineering. The challenges are:

- 1) In requirement engineering, different teams involved in development need to coordinate with each other for technical dependencies.
- 2) Stakeholders have to understand and give a right to the development team that they can take decisions independently.
- 3) A development team must not lose focus on the final picture or vision of the product.
- 4) It is a challenge for a development team to be always ready for changes. Change management is important because the product is not final at the beginning.
- 5) The team must work with end-users who directly going to interact with the system.
- 6) Continuous involvement of end-users throughout the development of the product will lead to success.

They also proposed some solutions for all listed challenges:

Solution 1: coordination problem can be solved by enhancing communication, organizing meetings, provide training to teams.

Solution 2: Show the complete picture to stack holders, present problems and solutions, present the consequences of products.

Solution 3: Continuously focus on the product vision; define goals and sub-goals that may help to understand what type of changes can occur.

Solution 4: Challenge of change can be handled by continuously communicating with end-users and the team reviews the results regularly.

Solution 5: In friendly environment conduct interviews with end-users, observe user behavior.

Solution 6: Involve the minimum number of end-users in the software development procedure. It helps to understand the requirements. Present goals to these users. Involve these users in regular planning to get their feedback [15]. They proposed different challenges and their solution in their paper the major problems that they didn't define are that it is difficult to involve end-user throughout the development. Even end-users may not have the technical knowledge that is required for requirements gathering. He may not be clear about the requirements. It is required technical training is required for end-users who are directly involved in product development.

In different recent papers strength and weakness of RE process model are described, but in our paper we also discuss different key challenges in requirements engineering and proposed possible solution of all these challenges.

Research Questions:

- 1) What are the emerging requirement engineering models?
- 2) What are the challenges in emerging requirement engineering models that we are facing?
- 3) What are the solutions to these challenges?

III. CURRENT REQUIREMENT ENGINEERING METHODS

A. GORE's Method (Goal-oriented Requirement Engineering)

A method which is called (A new Requirements Engineering Approach for Manufacturing based on Petri Nets) presented here is based on the combination of GORE's Method (goal-oriented requirement engineering) and Petri Nets as a substitute to the requirements for manufacturing a system that is capable to deal with digital twins. Using these two a new approach of RE is developed which is more sophisticated and service-oriented because it is based on a systematic approach – it means though each and every one will be goal-oriented but also will be in a systematic way. As an example, a car sequencing system presented in Fig. 1 is used here to solve the real problem [16]. Petri Nets of car sequencing problem is presented in Fig. 1.

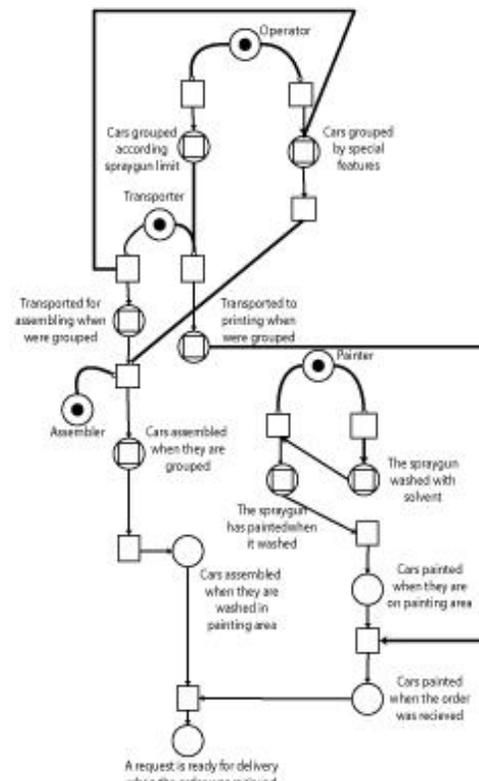


Fig. 1. Petri Nets of Car Sequencing Problem.

Pros:

- 1) Realistic manufacturing products or projects will be done using this model
- 2) Rather than small projects this model can be applied to large scale.

Cons:

- 1) In case of any deviation from steps an alarm system is activated which will activate the detailed verification process?

B. MBSE (Model-based System Engineering)

The 2nd method is used for the product development, here a conventional system is converted into a modular system, which as a result will produce increases the complexity and will have so many modules to handle. So, the MBSE (model-based system engineering) approach is being used for the development of modular kits to reduce the complexity [17]. Four key challenges were observed during the development of the modular kit. Structure of the system of objectives for modular kits is shown in Fig. 2.

- 1) The scheme of the objectives is scrappy (due to large requirements, it is likely to have the situation that some of the requirements were not fulfilled).
- 2) Not every stakeholder is familiar with the latest version of the system of objective (which can be the reason for the complexity i-e it will be challenging to keep all stakeholders up to date).
- 3) Paucity of analysis about the consequences of the systems of objectives (stakeholders must inquire and fully understand all the objectives, requirements, and constraints).
- 4) Varying degree of maturity and inflexibility (investment of more and more time which will result in lacking more and more information).

To resolve these challenges a hybrid module was structured, diagram of that model can be shown in Fig. 2, [17] according to the hybrid module one requirement s can have multiple values or aspects, also reusability of the requirements can be acquired. Another feature of the structure is to identify the highest or technically most provocation value of each requirement.

Pros

- 1) This model can represent the large scale, interdependency, and variety of the module's system of objectives.
- 2) Reusability of the requirements can be acquired and due to this a lot of time can be saved for the next challenge/innovation.

Cons

- 1) If the modular kits remain stick to the same questionnaire for a long period, it will be difficult for the innovation.
- 2) Securely extending the modular kits with new ones will change the whole beauty of the original ones.

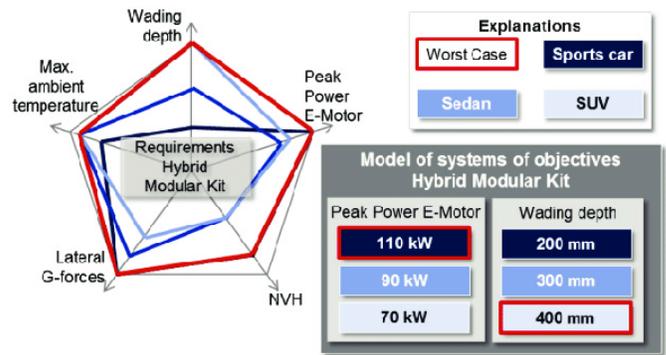


Fig. 2. Structure of the System of Objectives for Modular Kits.

C. CREWS Method

The main concern is to be looked upon as a reusable component. Their concern was described in 2 ways i-e scenario-based approach is represented at first in a modular way, identification of the design context at second in which these approaches can become reusable to facilitate. To achieve this, scenario-based approach is represented as method components called scenario method chunks. These chunks are divided into 2 levels; [18] a) Method knowledge level— it deals with the knowledge that is necessary for the chunk selection and retrieval, here knowledge is captured and presented in SGML (Standard Generalized Markup Language) b) Method meta knowledge level— it means dealing with the representation of the reclaimable knowledge to the method base users and is described in HTML format which can be graphical or in informal explanation of guidelines. Fig. 3 represents the SGML part of the CREWS method base on the tree. The structure of SGML part of the method base is elaborated in Fig. 3.

Pros

- 1) By dividing into 2 parts it will be easy for the developers to retrieve the exact information (representation and description of the products).
- 2) Reusability of the chunks can be time-saving and helpful for the new developers.

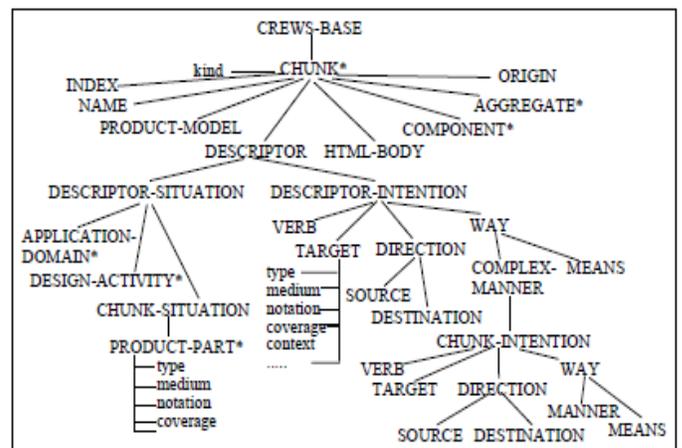


Fig. 3. The Structure of SGML Part of the Method base.

Cons

1) It will be much expedient if this model has some kind of instruction set or guidelines because its effectiveness can also bothersome of the new developers as well as customers.

D. Multidisciplinary Modeling

A multidisciplinary modeling technique is used in (A multi-disciplinary modeling technique for requirements management in mechatronic system engineering) [19] which allows modeling and evaluation of the requirements throughout the engineering process, how to model the requirements and test them using simulations. The main objective to present these techniques is to keep the number of concepts as minimum as it can be possible to understand at the early stages. Tasks that have been performed for modeling and testing were:

Conception—the creation and elaboration of components with the defined concepts.

Simulation—system behavior testing with an integrated physics simulation.

Refinement—a refinement of the modeling aspects using discipline-specific tools (constraints are checked during the process execution) [19].The workflow of the multidisciplinary model is visualized in Fig. 4.

Pros

1) Researchers have tried their best to minimize the techniques for modeling.

2) For the proper system functionality continuous integration system was introduced.

Cons

1) For the academic case study, this technique is useful, but as compared to the industrial system the complexity will be limited.

2) Quality measurement for the modeling an ore fine-grained assessment of the system behavior is not included

E. Agile RE

Agile Requirement Engineering aims to capture the current state of the art of the literature related to Agile RE while keeping because of stakeholders and users' collaboration. As agile software development has gone with online delivery and customer satisfaction thus its main aim is to deliver business values in short iterations. As the old Agile methodologies (Scrum, Kanban, and Extreme Programming) lacks in defining the right kind of products, to overcome this situation for good user experience a hybrid development approach including Human-Centred Design (UCD) are applied. Three important approaches have been raised in this process:

1) What approach exists, which involves stakeholders in the process of RE and is compatible with Agile Software Development (ASD). For this, some of the sub-categories were made to check which approach will be compatible:

- Stakeholders must collaborate.
- The user must be involved directly.
- Using a process to involve the stakeholders
- Possibility of the existence of the iterations during the development process
- A specific method is used to retrieve data [20].

If these categories exist in the project, then for the stakeholders and users' involvement weekly meetings, conceptual model representation, and surveys, etc. will be the best approach.

2) What are those agile methodologies, which are capable of presenting the user's viewpoint to stakeholders?

Some sub-categories were also made to check the agile methodology. It is concluded here that the ad-hoc nature of the user collaboration and design feedback methodology will be suitable and capable for the representation of users' perspectives to stakeholders.

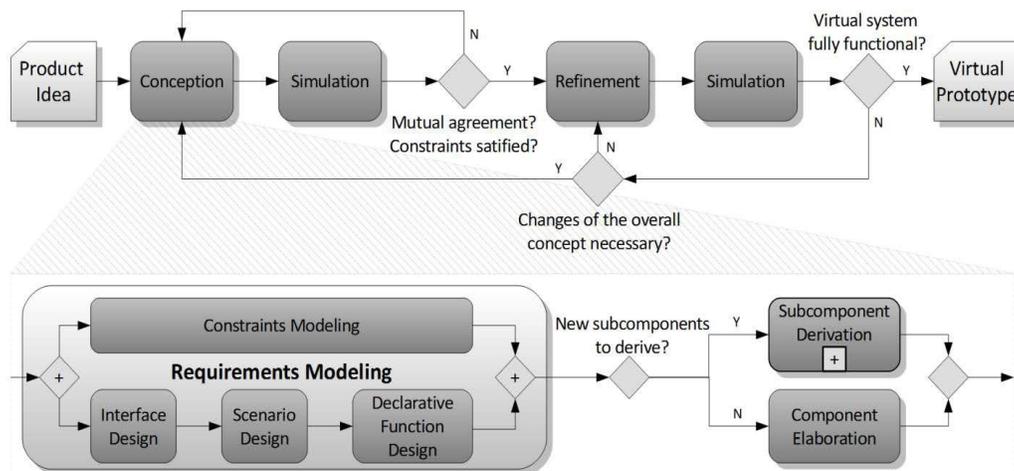


Fig. 4. The Workflow of the Multidisciplinary Model.

3) What is the common way for requirement management in ASD? [20].

Some of the artifacts were selected for the requirement management, i.e.

- User story
- Task
- Prototype
- UI pattern
- Use case scenario
- Pictures
- Story card
- Essential use case
- Persona
- Videos
- Vision
- Mind map
- UML diagram
- UI specification
- Storyboard
- Kanban board

These artifacts are changeable according to the project requirement. Using artifacts, a lot of hidden possibilities of error in projects can be resolved to some extent. It will be more accurate if a guideline/instruction set is added here Fig. 5 shows the requirement engineering phases.

Pros

1) To avoid the problems that can be aroused by users' inappropriate involvement some of the methods are identified that aims to increase the knowledge regarding user's needs.

Cons

1) A shared understanding of the user's perspective is not well established.

2) Inappropriate user involvement can arise a lot of miscommunication.



Fig. 5. Requirement Engineering Phases.

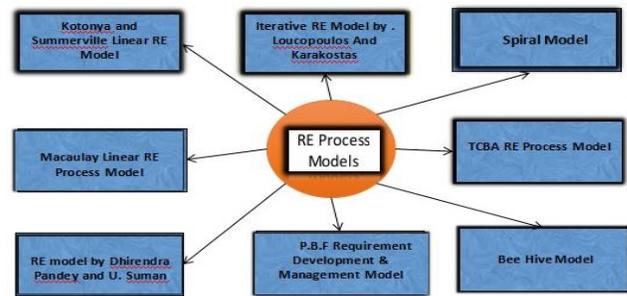


Fig. 6. Requirement Engineering Process Models.

IV. EMERGING MODELS OF REQUIREMENT ENGINEERING

We are living in a digital environment where software evaluation is important to meet the stack holder's requirements. So it is required to evaluate the requirement engineering methods and models for handling the challenges that occur in the requirement engineering process. Marcelino-Jesus, Elsa, present in their paper that requirement engineering consists of four phases that are used to access the requirements. And the common four phases that include in the requirement engineering process are requirement elicitation, analysis, specification, and validation [21], [25].

The elicitation phase is used to find the appropriate requirements that provide the solution for the development. In the analysis phase, requirements are analyzed in such a way that continuous negotiation with stack holders to identify which requirements is to need to be considered for development. In the specification phase, the requirements arrange in a documented form that is understandable, readable by anyone. The validation phase is used to validate that requirements are complete and consistent and clearly express the stack holder's needs. In Requirement engineering methodology there is the additional phase that is included in RE processing that is a preparation of information [22], [28]. The 8 requirement engineering process models are presented in Fig. 6.

Requirement engineering methodology is drafted in Fig. 7. Mehmood M and Ijaz BB [23] define different requirement engineering process models that were presented by different researchers. Requirement engineering process models are shown:

A. Linear RE Process Model

Sommerville and Kotonya presented that model. This model includes different activities that are repeatable perform. The activities are requirements elicitation, analysis of requirements, negotiation, documentation, and validation of requirements. This model is very useful where requirements are accurate. The model includes the repetition of the activities until all the stack holders satisfy as presented in Fig. 8.

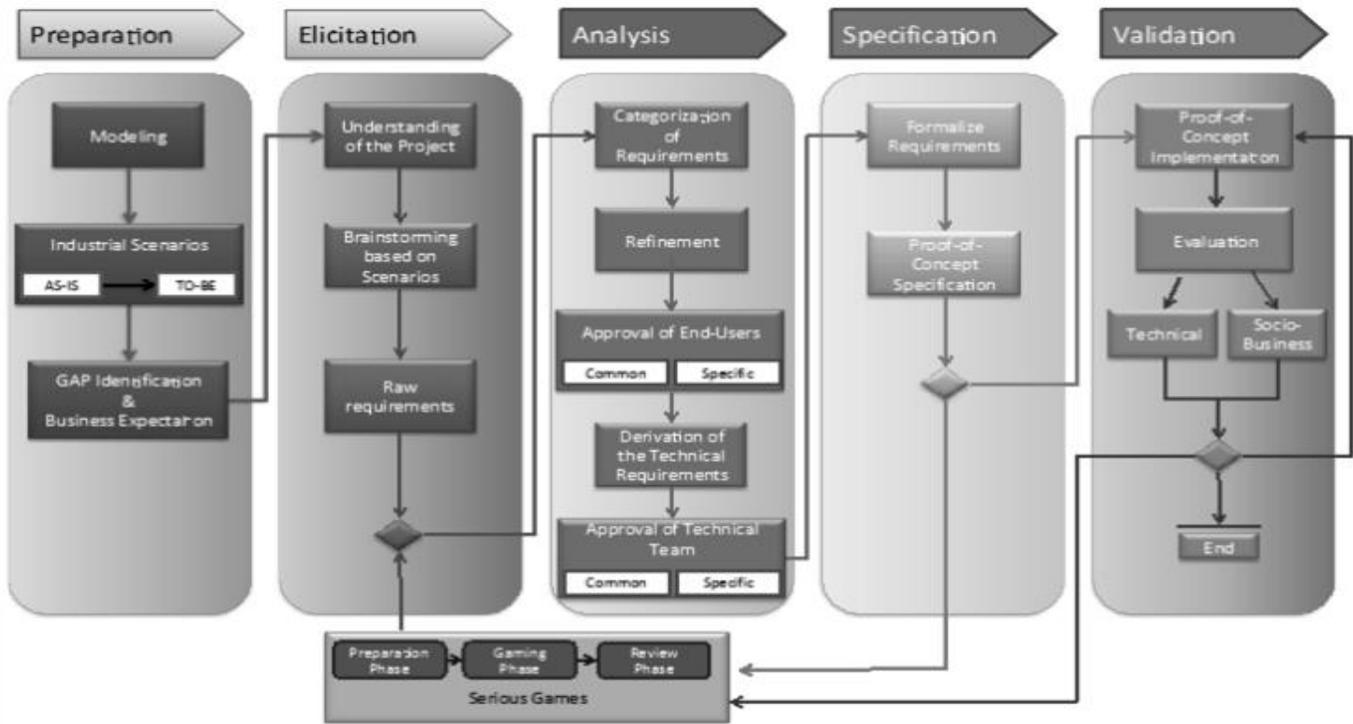


Fig. 7. Requirement Engineering Methodology.

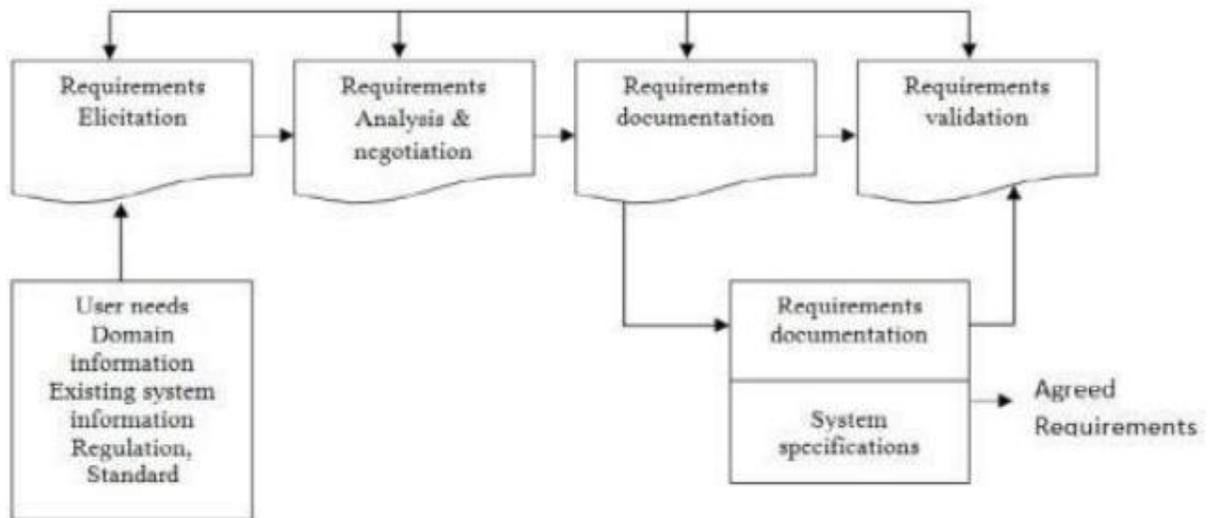


Fig. 8. Linear RE Process Model.

Challenges:

- 1) Difficult to handle the risk.
- 2) No concept supports the user feedback.
- 3) It does not provide a facility for requirements validation.
- 4) It does not support when requirements continuously change.
- 5) It does provide preprocessing activities for requirements.
- 6) It cannot estimate the effort based on requirements.

B. Macaulay Linear Requirements Engineering Process Model

The overall challenges of requirements engineering process models are summarized in Table I.

This model is presented by Macaulay. This model work in a linear fashion in which all activities are performed sequentially [27]. It includes five activities that are: problems analysis, concepts, analysis of feasibility study, and modeling and documentation of requirements as shown in the Fig. 9.

Challenges:

- 1) It does not provide the facility of reversing the engineering process.
- 2) This model also does not support user feedback.
- 3) There are no preprocessing activities for requirements.
- 4) It does not support dynamic requirements.
- 5) There is no concept of effort estimation.
- 6) It does not provide any method for risk management.

C. Iterative Requirements Engineering Process Model

This model was proposed by “Karakostas and Loucopoulos”. The model includes the different phases are: Elicitation, specification, and problem domain. This model follows the iterative development shown in Fig. 10.

TABLE I. CHALLENGES OF REQUIREMENT ENGINEERING PROCESS MODEL

Sr.no	Model	Challenges
1	linear Requirement Engineering model by Summerville and Kotonya	No concept supports the user feedback.
2	Macaulay Linear RE Model	It does not provide the facility of reversing the engineering process.
3	Loucopoulos And Karakostas Iterative RE Process Model	It does not support the concept of effort estimation.
4	Spiral Model Of Requirements Engineering Process	It does not provide any method that is used to find requirements priorities.
5	(TCBA) RE Process Model	In the beginning, product cost may not be accurate.
6	An Effective Requirements Engineering Process Model by Dhirendra Pandey and U. Suman	It does not provide any effective method for managing the risk.
7	Model In Highly Turbulent Environments Model G. P.B.F. Arts Requirements Development & Management	It uses only the brainstorming method for elicitation of requirements.

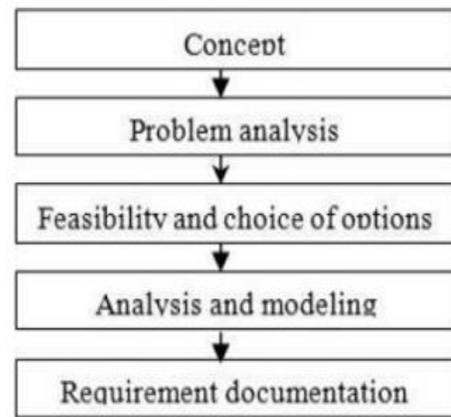


Fig. 9. From the Work of Macaulay.

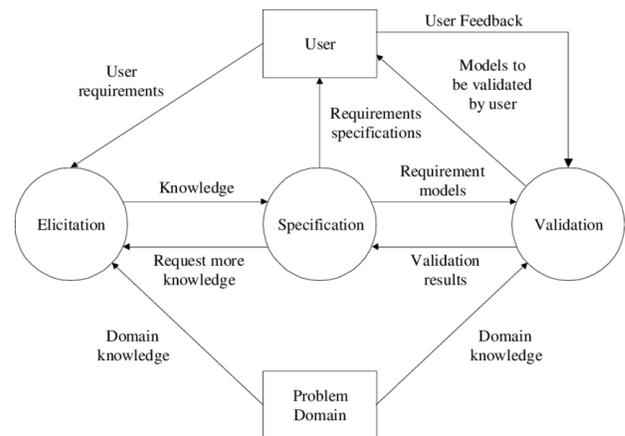


Fig. 10. From the Work by Loucopoulos and Karakostas.

Challenges:

- 1) It does not support the concept of effort estimation.
- 2) It does not support when requirements frequently change.
- 3) It does not support preprocessing activities for requirements.
- 4) It does not provide the criteria for finding application-specific requirements.
- 5) No method can handle the risk.

D. Spiral Model of RE Process

This model is recommended by Summerville and Kontoya. This model works on spirals. It includes four activities are: elicitation, analysis, and negotiation, documentation, validations of Requirements as shown in Fig. 11.

Challenges:

- 1) It does not provide any method that is used to find requirements priorities.
- 2) It does not provide any mechanism that supports finding the application-specific requirements.
- 3) It does not provide preprocessing activities for requirements.
- 4) There is no concept of cost estimation.

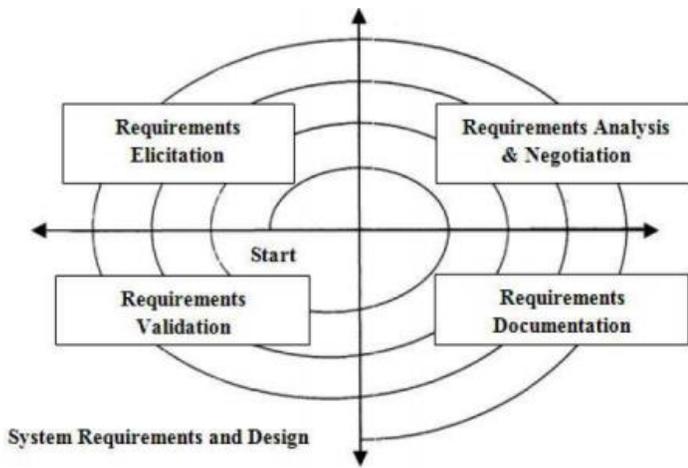


Fig. 11. From the Work of Kontonya and Summerville.

E. Tool Cost-Benefit Analysis (TCBA) Requirement Engineering Process Model

This model is presented by “Mr. Qadeem Khan, Mr. Shams-Ul-Arif, S. A. K. GahyurTools. This model includes two processes:

- 1) If you can arrange meetings with the stack holders that use the survey method for requirement elicitation.
- 2) If there is a minimum number of stockholders use the interview method. Fig. 12 and 13 has shown this model.

Challenges:

- 1) In the beginning, product cost may not be accurate.
- 2) Difficult to find requirements priorities.
- 3) This model also not supports the preprocessing activities.

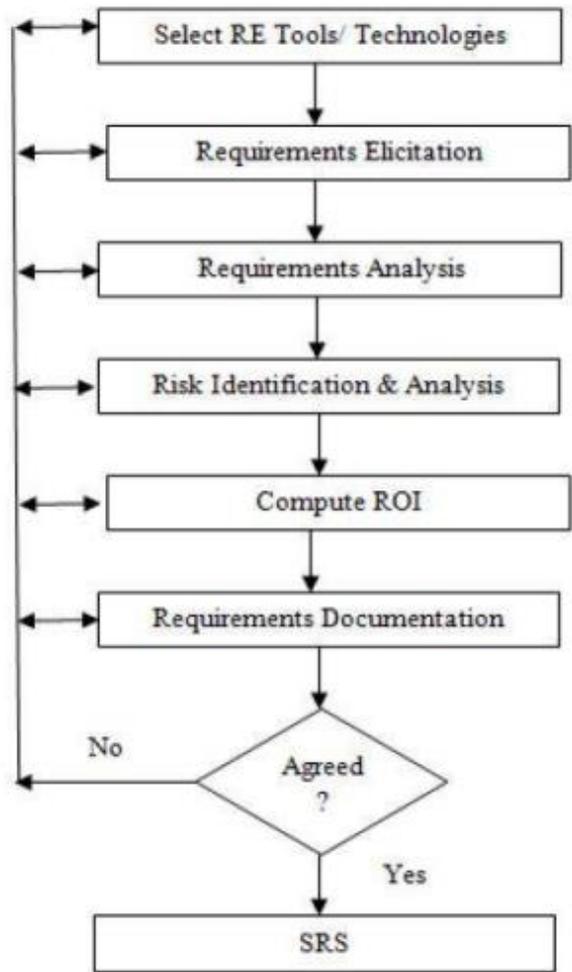


Fig. 13. TCBA RE Process Model.

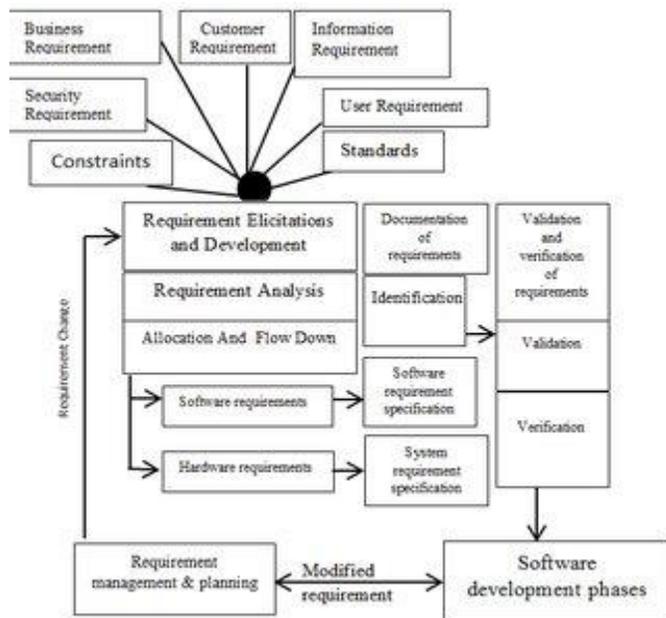


Fig. 12. TCBA RE Process Model.

F. Dharendra Pandey and U. Suman an Effective Requirements Engineering Process Model

This requirement engineering process includes: Business, Customer requirements, User requirements, Constraints of Security requirements, requirements of Information, Standards as Fig. 12 is presenting this model.

Challenges:

- 1) This model also not provides any method that how to estimates the efforts.
- 2) It does not provide any effective method for managing the risk.
- 3) It does not provide any method to find application-specific requirements.

G. P.B.F. Arts Requirements Development & Management Model in Highly Turbulent Environments

This model has three aspects are intake, startup, initiation. In the startup phase, it provides a technical method for elicitation of requirements. In initiation phase is used to prioritize the requirements and get feedback from stack holders and also validate the requirements as shown in Fig. 14.

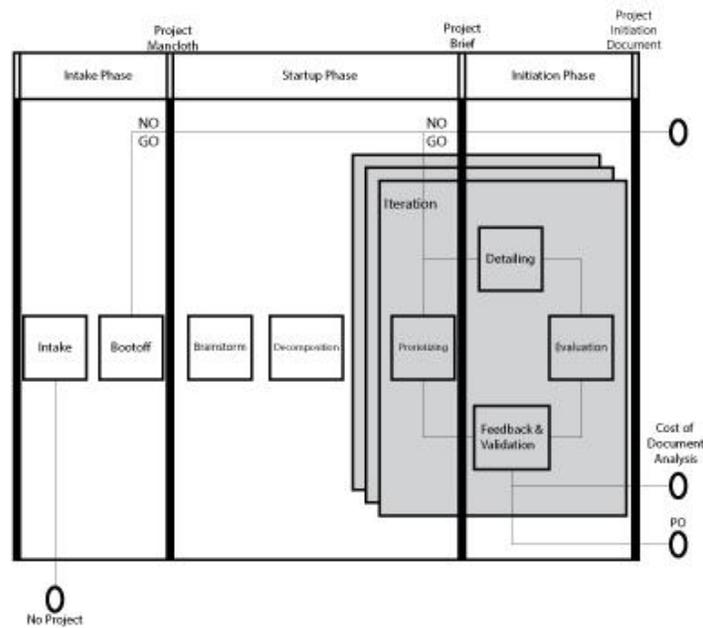


Fig. 14. Requirement Development and Management Model in Highly Turbulent Environments.

Challenges:

- 1) Difficult to manage the requirements.
- 2) It uses only the brainstorming method for elicitation of requirements.
- 3) It does not provide any method for documentation of requirements.
- 4) It does not provide any effective mechanism to handle the risk.
- 5) Difficult to measure the efforts that are required for requirements.

H. Bee Hive Model

This model is presented by “K S Swarnalatha, G.N Srinivasan, and Pooja S Bhandary”. This model includes the following phases: Background Research Elicitation, Analysis of requirements, Prototyping, Verification of requirements, Validation of Requirement Specification. Bee Hive model help to find the actual time required for gathering requirements from stack holders for designing the prototype of a product.

Challenges:

- 1) Required a large amount of time for the feasibility study.
- 2) There is no preprocessing activity for requirements.
- 3) Risk management is difficult
- 4) It does not support application-specific requirements.

V. SOLUTIONS TO OVERCOME THESE CHALLENGES

- In Kotonya and Sommerville Linear RE Process Model, further examination needs be done to consolidate prerequisites approval action alongside help with a client to guarantee the precision, breadth, and consistency of specification.

- Reverse Engineering risk management strategy must need to be undertaken in Macaulay Linear Requirements Engineering Process Model.
- Preprocessing RE strategy needs to be developed in Loucopoulos and Karakostas Iterative Requirements Engineering Process Model.
- Specific requirements elicitation technique needs to be incorporate in Spiral Model.
- Further, the examination might be finished by consolidating the idea of requirement preprocessing and requirement prioritization in the TCBA model.
- Future research needs to be done include effort estimation in Dharendra Pandey and U. Suman Effective Requirements Engineering Process Model.
- In P.B.F. Arts Requirements Development & Management Model in Highly Turbulent Environments and Be Hive Model is important to develop the preprocessing RE and management strategy.

VI. CONCLUSION

The paper shows several issues in the domain of requirement engineering. These issues have been researched using a variety of sources. Requirements are the first step for a project and this may increase the possibility that project estimates may be inaccurate if they are not explicitly and unambiguously specified, since the nature of the project/activity has not been established. Even if there are several existing models and structures for handling requirements, each model represents only one possible insight on the inner truth that will be captured and reused: The slogan "one size does not fit all" may be rephrased as "one style does not fit all". Thus, in the areas of issues needed, at least 2 (or more) models/frameworks should be considered for improving

your processes (whatever they are). In these paper firstly current requirements engineering models has explained and then their pros and cons are presented. After that, emerging RE models is presented and discusses their challenges, at the end we try to give some solutions to overcome the challenges that are facing in emerging RE models. In the future, we further plan to work more on emerging models and techniques our future research will discuss the key characteristics of many Requirement Engineering Process models, which aid in the selection of the most appropriate model for Requirement Engineers and practitioners in the industry, We will offer an effective requirements engineering process model for producing high-quality software requirements, with a focus on providing a full overview of Elicitation methodologies, including their characteristics, strengths, and weaknesses. Some of the strengths and weaknesses discovered during the extensive analysis are also ordered and scheduled, which aids in the proper selection of the RE Process model and explain solutions in a better way. On the basis of current literature, this study covers a wide range of research topics, allowing other scholars to expand on the work. In terms of cost and time, the appropriate choice of Process Model combined with the right technique is beneficial to any professional.

REFERENCES

- [1] Javier Martinez Silva, Raul Javales, Jos'eReinaldo Silva— A new Requirements Engineering approach for Manufacturing based on Petri Nets 2019, IFAC (International Federation of Automatic Control).
- [2] Helmut Scherer, Albert Albers, Nikola Bursac— Model-Based Requirements Engineering for the Development of Modular Kits, 27th CIRP Design 2017.
- [3] JolitaRalyté—Reusing Scenario-Based Approaches in Requirement Engineering Methods: CREWS Method Base, CRI, Université Paris1-Sorbonne 90, rue de Tolbiac, 75013 Paris (1999).
- [4] Georg Hackenberg, ChristophRichterb, Michael F. Zäh—A multi-disciplinary modeling technique for requirements management in mechatronic systems engineering, 2nd International Conference on System-Integrated Intelligence: Challenges for Product and Production Engineering, Procedia Technology 15 (2014).
- [5] Eva-Maria Schön., JörgThomaschewski, María José Escalona, Agile Requirements Engineering: A systematic literature review, (2017).
- [6] D. Pandey, U. Suman, and A. Ramani, An Effective Requirement Engineering Process Model for Software 2010 International conference.
- [7] Development and Requirements Management, in Advances in Recent Technologies in Communication and Computing (ARTCom), 2010 International Conference on, 2010, pp. 287–291.
- [8] J. Siddiqi, M.C. Shekaran, Requirements engineering: the emerging wisdom, IEEE Software 13 (2) (1996) 15– 19.
- [9] G. Kotonya, I.Sommerville, Requirements engineering with viewpoints, BCS/IEEE Software Engineering J., vol. 11, no. 1, 1996, pp. 5–18.
- [10] H. Kaindl et al., Requirements Engineering and Technology Transfer: Obstacles and Incentives, Requirements Eng., vol. 7, no. 3, 2002, pp. 113–223.
- [11] A Systematic Study on Requirement Engineering Processes and Practices in Mauritius GeshwareeHuzooree ,Vimla Devi Ramdoe February 2015.
- [12] Requirement Engineering version 1.0 by Sparx Systems & Stephen Maguire.
- [13] The Requirement Engineering Handbook by Ralph R.Young.
- [14] Requirements Engineering Techniques in Software Development Life Cycle Methods: A Systematic Literature Review AdetobaBolaji. T, Ogundele Israel. O.
- [15] Requirement Engineering Research Dharendra Pandey.
- [16] The Strength and Weakness of Requirement Engineering (RE) Process AzlenaHaronShamsulSahibuddin.
- [17] Challenge of validation in requirements engineering SourourMaalem,NacereddineZarour
- [18] Challenges in understanding software requirements in agile-based offshore development Muhammad Omair August 2008.
- [19] Asghar, Sohail, and Mahrukh Umar. "Requirement engineering challenges in the development of software applications and selection of customer-off-the-shelf (COTS) components." International Journal of Software Engineering 1.1 (2010): 32-50.
- [20] Saleh, Mohammed, et al. "A Systematic Literature Review of Challenges and Critical Success Factors in Agile Requirement Engineering." (2018): 242-247.
- [21] Schön, Eva-Maria, et al. "Key challenges in agile requirements engineering." International Conference on Agile Software Development. Springer, Cham, 2017.
- [22] Marcelino-Jesus, Elsa, et al. "A Requirements Engineering Methodology for Technological Innovations Assessment." ISPE CE. 2014.
- [23] Mehmood and Ijaz, J ArchitEng Tech ,A Review of Requirement Engineering 2018, 7:1 DOI: 10.4172/2168-9717.1000215.
- [24] Düchting, Markus, Dirk Zimmermann, and KarstenNebe. "Incorporating user-centered requirement engineering into agile software development."
- [25] International Conference on Human-Computer Interaction. Springer, Berlin, Heidelberg, 2007.
- [26] Shah, Tejas, and V. S. Patel. "A review of requirement engineering issues and challenges in various software development methods." International Journal of Computer Applications 99.15 (2014): 36-45.
- [27] Chazette, Larissa, and Kurt Schneider. "Explainability as a non-functional requirement: challenges and recommendations." Requirements Engineering 25.4 (2020): 493-514.
- [28] Inkermann, D., et al. "Model-based requirement engineering to support development of complex systems." Procedia CIRP 84 (2019): 239-244.
- [29] Ghozali, Reginald Putra, et al. "Systematic literature review on decision-making of requirement engineering from agile software development." Procedia Computer Science 157 (2019): 274-281.

An Advanced Ontology based Deep Learning for Computer-aided Interpretation of Mammography Images

Hamida Samiha Rahli¹, Nacéra Benamrane²

Laboratoire SIMPA, Département d'Informatique, Faculté des Mathématiques et d'Informatique
Université des Sciences et de la Technologie d'Oran Mohamed Boudiaf, USTO-MB, BP 1505, EL Mnaouer, 31000, Oran, Algérie

Abstract—Computer assisted detection (CAD) are able to detect and characterize suspicious mammographic images, micro calcifications, masses or more difficult, architectural distortion. With the exploitation of these different characteristics, the system can specify and predict the severity of the tumor to assess the risk in terms of Malignity/Benignness. Our work involves the development of a new method for screening breast cancer, this is achieved by developing a whole strategy of knowledge extraction through deep learning and medical ontology appropriate for the classification of regions selected from digital mammograms, for each radiological sign considered, namely, masses and micro calcifications. First, we extracted the parameters characterizing the images used as input to a deep convolutional neuron network CNN. The learning is supervised because the images used are images from the MARATHON database of the University of Florida; they are already diagnosed by experts. The second phase aims to add a semantic level to our classification through a specialized ontology developed for this purpose based on the BIRADS characterization system. Based on the evaluation performed, the proposed approach provides better classification results than the usual methods for assisting in the computer aided detection of breast cancer.

Keywords—Computer assisted detection (CAD); breast cancer; the digital database for screening mammography (DDSM); ontology; deep learning; breast imaging-reporting and data system (BIRADS)

I. INTRODUCTION

Breast cancer is the leading cause of cancer death among women; in addition to the second most common cancer in the population after prostate cancer [1]. Several actions can be put in place to promote early detection of breast cancer. The interest is to be able to cure this cancer more easily and to limit the sequel related to certain treatments.

The generalization of organized screening for breast cancer requires the implementation of double reading, which reduces the false negative rate of screening, but can be difficult to organize.

Computer assisted detection system (CAD) are constantly improving and are able to detect and characterize suspicious mammographic images, micro calcifications, masses or more difficult, architectural distortion. The digital and computer analysis of mammography images can then serve as a second computer reading for the radiologist, the goal of these expert

systems being to increase the sensitivity of mammography while reducing the number of false positives.

In computer vision [2], it is generally accepted that the image analysis is performed by a series of procedures that form the image processing chain. This chain is certainly not universal and each stage is conditioned by a priori specific knowledge of the domain that is being treated. Studies have shown that each step can be approached through an expert system, especially the segmentation stage that is crucial for interpretation. Interpretation is the last step in this chain of treatment. It is at the same time influenced by the treatments which were carried out previously (possibly complex or partially solved and by the final goal (research of pathologies, evocation of syndromes, aid with the diagnosis).

A classification is an organized and hierarchical classification system of "objects". Depending on the objects considered (living species, diseases, products or services, stars, documents in a library ...), various classification systems developed. Interpretation is among the different areas that use classification,

Two approaches to image classification can be distinguished:

- The supervised approach: The supervised classification is based on a prior knowledge of the data to classify, the nature and the numbers of classes contained in the image are known in advance.
- Unsupervised approach: For these methods, the data are classified according to their characteristics, without any prior information on the nature of the objects to be classified, that is to say that they do not require any knowledge a priori of the user. Either there is a universal collection of classes already defined, or the number of classes or their characteristics are automatically determined within the classification itself.

Regarding image classification, the analyst who attempts to classify the characteristics of an image, uses elements of visual interpretation to identify homogenous groups of pixels, in order to extract knowledge from these images. Moreover, to do this, we must choose from several algorithms and methods such as for example neural networks [3], genetic algorithms [4], fuzzy logic [5], taboo search [6].

The purpose of this article is to present a decision aid to the doctor responsible for breast cancer screening by developing a strategy for extracting knowledge from biomedical data (mammographic images) for the detection of possible pathologies. This is achieved by developing a whole new strategy for extracting knowledge through deep learning and appropriate medical ontology for classifying regions in terms of malignancy / benignity.

First, we developed a system for detecting tumors by deep learning, the images used are images from the University of Florida's MARATHON database, they have already been diagnosed by experts. Then to give information a semantic aspect in the decision-making process, we propose to model knowledge in the form of ontology.

The rest of the article is organized as follows: in the second section, we describe the techniques that exist in the literature to accomplish the detection of different suspicious radiological signs in mammography. Then we will talk about the approach studied, the deep learning models used and the ontologies while exposing the results obtained.

II. RELATED WORK

Our main goal is to develop a mammography-based, quasi-automatic mammography diagnostic aid system for radiologists as a second reading for early detection of breast cancer by one of the first pathological signs. : The mammary masses. So, this system should not be seen as an attempt to replace the doctor but to offer him powerful tools that help him in the heavy task of analyzing mammograms during screening campaigns. In this point, ontology and deep learning can be a solution for the distinction between malignant and benign tumors.

In paper [7], the authors suggest first a construction of domain ontology about the disease of breast cancer. Then the annotation of images on breast cancer by the ontology concepts "OntoSein" allow, thus their semantic Interpretation. They have chosen to establish the annotation in a semi-automatic way using the "PhotoStuff" which is a tool based on a library of Java classes called Jena, The hierarchy and relationships between classes make it possible to interpret the metadata attached to each image.

An ontology built in the framework of the European project MICO (Cognitive Microscope) in which a team from the IPAL laboratory participated, in order to provide the pathologist with a relevant tool to help diagnosis and prognosis by allowing the detection, according to the Scale, regions of interest in microscopic biopsy images, annotation and analysis of these images and provide scoring and assessment capabilities for breast cancer [8].

In Meriem et al. [9], the authors propose a methodology for extracting objects of biological interest in histopathological images. For this, they first used low-level specific procedures such as nucleus, mitosis and tubule segmentation, and then they designed OWL-DL ontology and SWRL rules for the annotation of histopathological images.

The authors [10] created an enriched ontology of breast cancer that consists of formalizing a set of mammographic

knowledge. Using this tool which is based on semantic technologies, it provides the pathologist with a relevant tool for diagnosis and prognosis by enabling the detection, the proposal of the possible treatment, the integration of the information used for characterization of breast cancer.

The proposed approach [11] is to create a diagnostic support system for breast cancer using ontology to provide physicians with a second opinion of their patients. This semantic annotation is done by tools such as ePAD, and saved in AIM format. This system can help radiologists to obtain a higher interpretation rate because the accuracy of the experts is obtained through training and experience.

In this paper, [12] deep convection neural networks (CNNs) and media carrier machines (SVMs) were used to design a breast cancer diagnostic support system. The approach begins with preprocessing to resize the image and improve the image quality [13]. Deep convulsion neural networks were applied for feature extraction and classification with media vector machines (SVM). The mammograms studied come from the DDSM and MIAS databases, to test the performance of this approach. Evaluation measurements were calculated such like Accuracy, Sensitivity, Specificity and area under the curve (AUC) and compared to other methods. Results show that proposed framework has attained accuracy 93.35% and 93% sensitivity.

In this work [14], the authors propose an end-to-end learning model in order to directly classify pre-segmented mammary masses into two classes as benign and malignant. They used the digital database for screening mammography (DDSM) in their experiments [15]. In the first place, they analyzed the effect of network initialization with prior learning on the ImageNet dataset, and then developed on mammography images. The results of this approach exceed the human performances and show the interpretability of this model.

III. PROPOSED MODEL

A. Breast Mass Classification from Mammograms using Deep Convolutional Neural Networks

Deep learning is a new branch of machine learning research that has been introduced to make machine learning more intelligent. It is about learning several levels of representation and abstraction which allows a better understanding of the hidden structure of data such as images, speech and text.

In this article, we propose a system based on Deep Convolutional Neural networks CNN able to detect the presence or not of anomaly on a mammogram for computer-aided Diagnosis (CAD) system, we used 321 images we divide them into two sets the first set of images is used for the training of the system (321image) the second set is used for system testing (18 frames).

We will give an overview on the architectures of the models used in this work.

1) *AlexNet*: In 2012, Alex Krizhevsky gave birth to a project named AlexNet [16]. This project succeeded in

winning the first prize in ILSVRC 2012 (ImageNet Large Scale Visual Recognition Challenge). This project has benefited from years of progress bringing more computing power and more data to learn.

AlexNet also included a stack of convolutional layers instead of the previous approach, where a pooling layer [17] followed each convolutional layer. The calculations make it possible to use a large database with a large amount of images at a high learning speed. Fig. 1 shows the overall architecture of AlexNet, which consists of 5 convolutional layers, and 3 FCs. These 8 layers combined with 2 new concepts for activation that are MaxPooling and ReLU.

2) *VGG Net*: During the ILSVRC 2014 challenge, an interesting new architecture appears, the VGG Net [18]. This architecture was proposed by a group of students from Oxford University. It should be mentioned here that this architecture did not win the top prize but it just won the error rate to 7.3%. The authors experimented with different architectures with a number of layers between 11 and 19 (see Fig. 2) and choose a homogenous 16-layer architecture using 3 x 3 filters with a stride of 1 to preserve the spatial resolution after the convolutional layers are combined with those of MaxPooling with a stride of 2. The authors noticed that when we use convolutional layers with very small kernels in a row, this has the same impact on larger kernels while keeping the same advantages. That said, 3layer with a 3x3 kernel has the same

effect as a 7x7 single-layer kernel, it decreases the number of parameters and allows the user to implement 3ReLU layers instead of 1. It is important to say that the number of parameters remains enormous at 140 million which implies a longer time. VGG Net expands the number of filters after each MaxPooling layer as shown in Fig. 2. The idea of decreasing the spatial dimensions but increasing the third dimension (depth) is seen as important as is the depth (number of layers) of the network.

3) *ResNet*: The Microsoft research group has suggested going deeper into architectures [19]. It offers a deeper architecture called ResNet.

Fig. 3 contains 152 layers and was the first prize architecture of the 2015 ILSVR challenge with an error rate of 3.6%.

The residual neural network - or Residual Network - better known by the name ResNet [19] arises due to the problem of back propagation of the gradient and the increase in learning error. Indeed, when the neural network is too deep, the gradient is reduced to zero and becomes very weak to update the weights of the different layers.

The idea is therefore to bypass the learning operation by adding the input to the output of the block (generally followed by an activation function). The authors have shown that they are able to train neural networks with up to 1,202 hidden layers using this method.

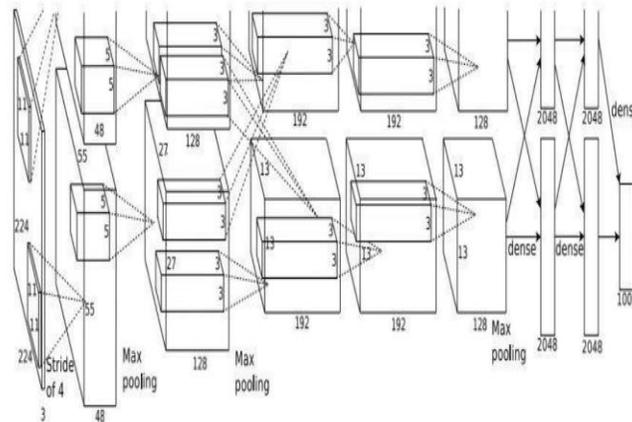


Fig. 1. AlexNet Architecture [17].

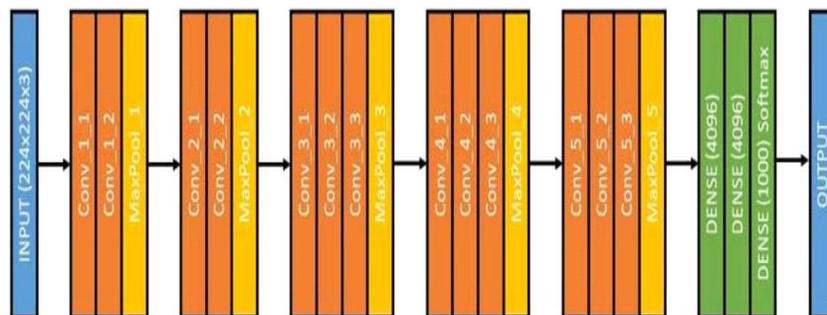


Fig. 2. VGG Net Architecture [18].

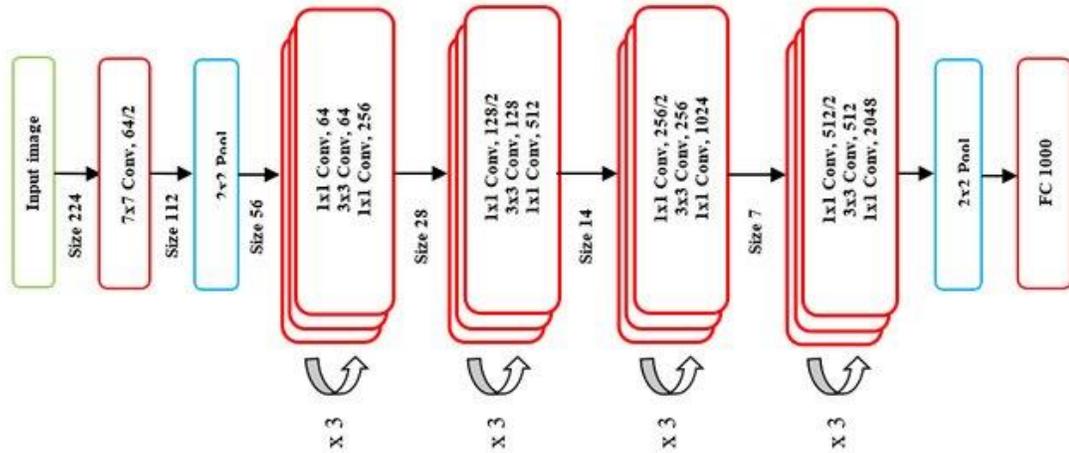


Fig. 3. The Global Architecture of ResNet [19].

B. Mammography Ontology

Generally, neural networks produce patterns that are often incomprehensible and require a high learning time. To remedy this insufficiency, we have used ontology for the automatic manipulation of information at the semantic level with the use of the SWRL language, which enriches the semantics of an ontology defined in OWL based on the BIRADS characterization system [20]. Breast Imaging Reporting and Data System. It is a classification, in five categories, of mammographic images according to the degree of suspicion of their pathological characters.

We build our ontology that we called Mammogram Cancer, according to the classification criteria. With the help of the expert, we extracted concepts (classes and their properties) and the relationships between these concepts (class hierarchy) necessary for the conceptualization of ontology.

In ontology development, we tried to similar reasoning the radiologist in breast cancer diagnosis. The description part of the lesion is based on the BI-RADS language. This has allowed describing the anomalies encountered by specifying their characteristics [21]. Mammogram Cancer ontology is composed of the Lesion concept which locates the different types of abnormalities (Mass, Calcification) of mammography of which each type represents itself a concept (subclass Lesion), each concept is constituted of a number of attributes for example: attributes: shape, density, outline for the concept Mass. Fig. 4 shows a part of Mammography ontology and relations.

1) *Mammography annotation tool*: In this article, we propose a new approach that takes advantage of both ontology and deep learning concepts in a system for annotating mammography images using JAVA programming language. We used a subset of the manually selected DDSM database. The learning set and the tests must contain each type of lesion (Benign, Cancer, and Benign without callback). We also used various mammographic images: images containing micro-calcifications and images containing masses.

This approach consists mainly of three steps as illustrated in Fig. 5:

- Processing module: used to prepare data for different treatments. In this module, the data is formatted according to the median filter.
- Module detection the presence or absence of abnormalities on mammograms by deep learning. For this purpose, 321 images are used, divided into two sets, the first one used for learning (288 images) and the second set used for testing the system (18).
- Loading the Mammocancer ontology to allow the test image to affect a new object to one of the classes (benign or malignant), using a SWRL decision rule integrating the results of the phase learning.

C. SWRL Rules

SWRL is an expressive OWL-based rule language. SWRL makes it possible to write inference rules and this provides more powerful reasoning capabilities than OWL alone [22]. Semantically, SWRL is built on the same description logic foundation like OWL and it provides similar formal guarantees when performing inference [17].

The body part (swrl: body) specifies the conditions that must be checked and the header (swrl: head) specifies the actions to be taken if the conditions of the rule are satisfied. Here is an example of a SWRL rule that uses the built-in predefined `greaterThan` : `Patient(?p) ^ hasAge(?p, ?age) ^ swrlb:greaterThan(?age, 40) ^ Mammogram(?x) ^ containM(?x, ?y) ^ TypeForme(?y, "IRREGULAR") ^ TypeContour(?y, "ILLDEFINED") ^ hasCategory(?x,?z) ^ ACR4(?z)`.

This rule states that if the age of a patient is greater than 40 years and her mammogram contains irregularly shaped masses and a poorly defined contour, then this patient has a mammogram classified as ACR4. Question marks in a SWRL rule used to declare variables.

In order to make reasoning and to deduce new knowledge from the executing ones, the rules of inference are written in SWRL. Fig. 6 illustrates the SWRL rules used.

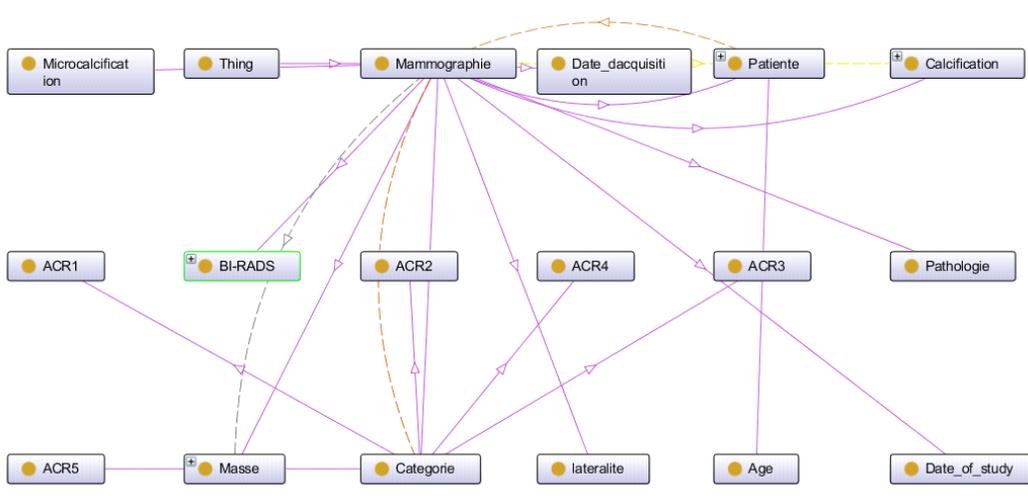


Fig. 4. Part of Mammography Ontology and Relations.

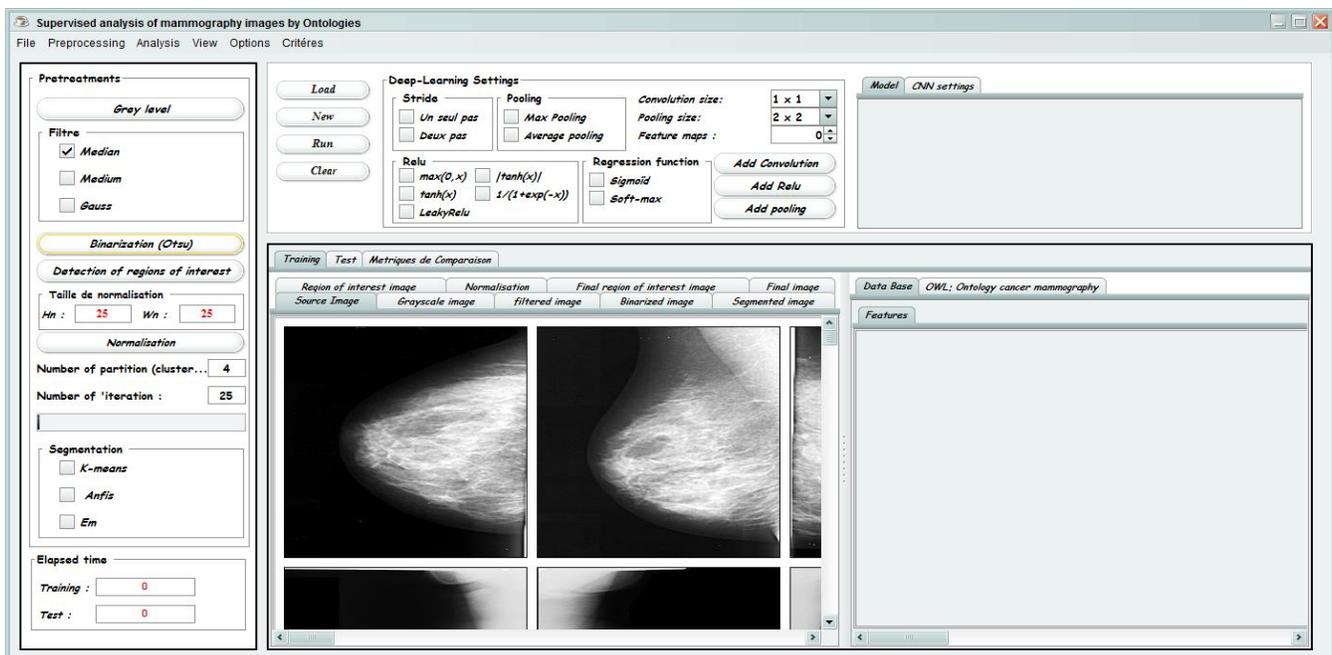


Fig. 5. Main Graphical Interface of our Prototype.

Enabled	Name	Expression
<input type="checkbox"/>	Rule-1	$\rightarrow \text{Patiente}(\text{?P}) \wedge \text{hasAge}(\text{?p}, \text{?age}) \wedge \text{swrlb:greaterThan}(\text{?age}, 39) \wedge \text{hasMammogram}(\text{?P}, \text{?x}) \wedge \text{containM}(\text{?x}, \text{?y}) \wedge \text{hasTypeFor}...$
<input type="checkbox"/>	Rule-10	$\rightarrow \text{Patiente}(\text{?P}) \wedge \text{hasMammogram}(\text{?P}, \text{?x}) \wedge \text{containM}(\text{?x}, \text{?y}) \wedge \text{hasTypeForme}(\text{?y}, \text{"LOBULATED"}) \wedge \text{hasTypeContour}(\text{?y}, \text{"ILL_C}...$
<input type="checkbox"/>	Rule-11	$\rightarrow \text{Patiente}(\text{?P}) \wedge \text{hasMammogram}(\text{?P}, \text{?x}) \wedge \text{containC}(\text{?x}, \text{?y}) \wedge \text{hasTypeMorphologie}(\text{?y}, \text{"PLEOMORPHIC"}) \wedge \text{hasTypeDistribution}...$
<input type="checkbox"/>	Rule-12	$\rightarrow \text{Patiente}(\text{?P}) \wedge \text{hasMammogram}(\text{?P}, \text{?x}) \wedge \text{containC}(\text{?x}, \text{?y}) \wedge \text{hasTypeMorphologie}(\text{?y}, \text{"PLEOMORPHIC"}) \wedge \text{hasTypeDistribution}...$
<input type="checkbox"/>	Rule-13	$\rightarrow \text{Patiente}(\text{?P}) \wedge \text{hasMammogram}(\text{?P}, \text{?x}) \wedge \text{containC}(\text{?x}, \text{?y}) \wedge \text{hasTypeMorphologie}(\text{?y}, \text{"PLEOMORPHIC"}) \wedge \text{hasTypeDistribution}...$
<input type="checkbox"/>	Rule-14	$\rightarrow \text{Patiente}(\text{?P}) \wedge \text{hasMammogram}(\text{?P}, \text{?x}) \wedge \text{containC}(\text{?x}, \text{?y}) \wedge \text{hasTypeMorphologie}(\text{?y}, \text{"PLEOMORPHIC"}) \wedge \text{hasTypeDistribution}...$
<input type="checkbox"/>	Rule-15	$\rightarrow \text{Patiente}(\text{?P}) \wedge \text{hasMammogram}(\text{?P}, \text{?x}) \wedge \text{containM}(\text{?x}, \text{?y}) \wedge \text{hasTypeForme}(\text{?y}, \text{"OVAL"}) \wedge \text{hasTypeContour}(\text{?y}, \text{"CIRCUMSCF}...$
<input type="checkbox"/>	Rule-16	$\rightarrow \text{Patiente}(\text{?P}) \wedge \text{hasMammogram}(\text{?P}, \text{?x}) \wedge \text{containM}(\text{?x}, \text{?y}) \wedge \text{hasTypeForme}(\text{?y}, \text{"LOBULATED"}) \wedge \text{hasTypeContour}(\text{?y}, \text{"CIRCL}...$
<input checked="" type="checkbox"/>	Rule-17	$\rightarrow \text{Patiente}(\text{?P}) \wedge \text{hasMammogram}(\text{?P}, \text{?x}) \wedge \text{containC}(\text{?x}, \text{?y}) \wedge \text{hasTypeDistribution}(\text{?y}, \text{"CLUSTERED"}) \wedge \text{hasCategory}(\text{?x}, \text{?z}) \rightarrow...$

Fig. 6. Part of the Rules Written in SWRL Language for Reasoning Inferential.

IV. RESULTS AND DISCUSSION

The experimental tests were conducted on a Core i5 laptop and 8GB of main memory. Our system has been implemented in the Eclipse development environment on Java.

To examine the practical effectiveness of our system, we conducted a series of experiments on a DDSM database.

In the test phase in the step of detecting tumors by the deep learning method, the selected network was injected with parameters associated with the images of the test set which consists of 18 images not used in the learning phase, for see the ability of the network to detect the presence or absence of abnormality on the mammograms of the test set.

For the test set, 18 mammograms were used which represent the following characteristics:

- 9 normal mammograms.
- 7 mammograms have abnormalities with an approximate radius of the circle surrounding the anomaly from 20 to 54 pixels.

After loading the database, we choose the parameters of our CNN and which are summarized under: stride, pooling, convolution size, pooling size and feature maps (characteristic map) as shown in Fig. 7. We launch the CNN part which will make it possible to extract the characteristics of each image.

Once the learning is complete, we tackle the test phase by first loading the dedicated database, and we restart the CNN part on this basis with the same parameters as those configured previously.

To estimate and validate the performance of our proposed approach, we compared the AUC of our ROC curve with other AUC values of recently proposed methods. The sensitivity (SN) or true positive rate (TPR), specificity (SP), false positive rate (FPR) and accuracy (AC) metrics are calculated by using the following statistical formulas [18]:

The sensibility:

It represents the classification rate where the class is a zero (detected correctly by the classifier) compared to the total number of zero classes.

$$\text{Sensitivity (SN)} = \text{True Positive Rate (TPR)} = \text{TP} / (\text{TP} + \text{FN}) \quad (1)$$

The specificity:

It represents the classification rate of examples where the class is not zero is predicted to be non-zero (Detected correctly by the classifier) relative to the total number of non-zero classes.

$$\text{Specificity (SP)} = 1 - (\text{FP} / (\text{FP} + \text{TN})) \quad (2)$$

TP, TN, FP and FN denote respectively:

- A-True positive: an example where the class is a zero is correctly predicted.
- b- True negative: an example where the class is not zero is predicted not zero.
- C-False positive: an example where the class is not a zero is predicted to be zero.

D-False negative: an example where the class is zero is predicted not to be zero.

False Positive Rate (FPR):

It is the probability that a false alarm will be raised: that a positive result will be given when the true value is negative.

$$\text{False Positive Rate (FPR)} = \text{FP} / (\text{FP} + \text{TN}) \quad (3)$$

Accuracy:

It is the number of correctly predicted data points out of all the data points. More formally, it is defined as the number of true positives and true negatives divided by the number of true positives, true negatives, false positives, and false negatives.

$$\text{Accuracy (AC)} = (\text{TP} + \text{TN}) / (\text{TP} + \text{FP} + \text{FN} + \text{TN}) \quad (4)$$

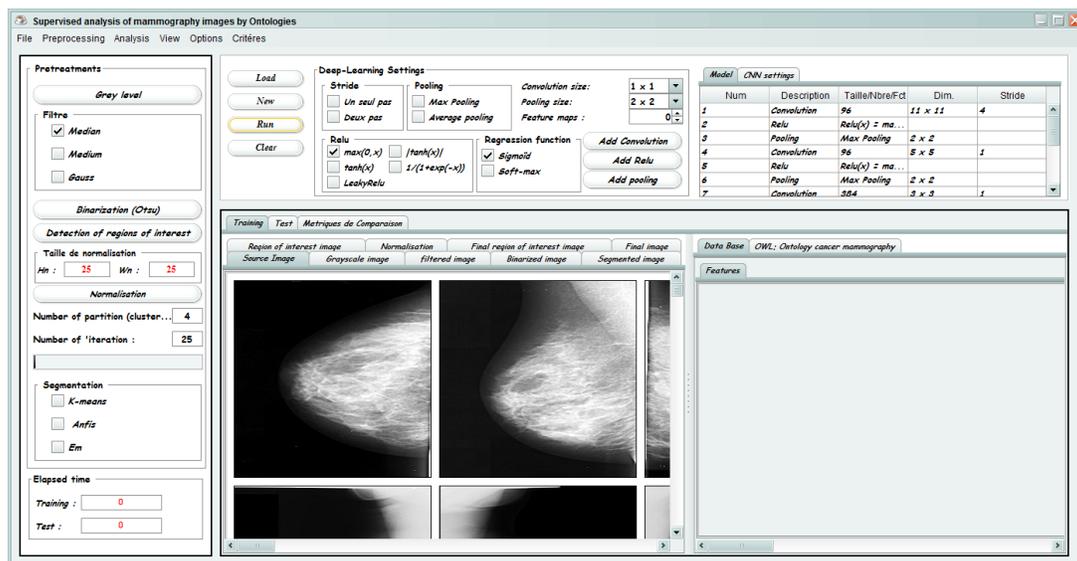


Fig. 7. Launching the CNN Algorithm for Learning.

Fig. 8 shows the architecture used in each model as well as the number of epochs. The results obtained are expressed in terms of learning accuracy, validation, and finally the error.

This comes down to the large size of the base which requires the use of a GPU instead of a CPU.

After analyzing the results obtained, the following remarks are noted:

The accuracy of training and testing increases with the number of epochs, this reflects that with each epoch the model learns more information. If the precision is reduced then we will need more information to teach our model and therefore we must increase the number of epochs and vice versa.

Likewise, the learning and validation error decreases with the number of epochs.

Model 2 VGG presented the best results found. The number of epochs and convolution layers reflect these good results; however the execution time was very expensive (due to the number of epochs). Our results improved as we deepened our network and increased the number of epochs. The learning base is also a determining element in convolutional neural networks; it takes a large learning base to achieve better results.

In general, a large and deep convolutional neural network performs well, and our network performance degrades if a

convolutional layer is removed. For example, from the table removing one of the two middle layers results in a loss in network performance. Therefore, depth is essential to achieve good results.

Our results improved as we deepened our network and increased the number of epochs. The learning base is also a determining element in convolutional neural networks; it takes a large learning base to achieve better results.

In order to show the contribution of ontologies for the automatic manipulation of information at the semantic level with the use of the SWRL language which enriches the semantics of an ontology defined in OWL based on the BIRADS characterization system (multi-class classification).

The construction of the ontology is a complex task, even to implement a small ontology, this one will take several lines of code and requires a great effort and time. In particular, if this ontology is coded directly by the developer in ontology language without using any tool. To do this, PROTEGE is designed to free the ontologist from this complexity and automatically generate the structure of the ontology created in OWL-DL.

The results presented in Fig. 9 show the characteristics of the tumor using our Mammocancer ontology as a classifier, which is based on semantic reasoning on an ontology enriched with SWRL rules.

	Architecture used			epoch number	Accuracy obtained on the basis of learning	Accuracy obtained on the basis of validation	error
	convolution layer	pooling layer	Fully connected				
AlexNet	05	02	03	15	91.29%	89.10%	60.05%
VGGNet	04	03	03	10	93.85%	87.44%	50.47%
RestNet	03	02	02	16	92.56%	84.03%	56.86%

Fig. 8. Experimental Results.

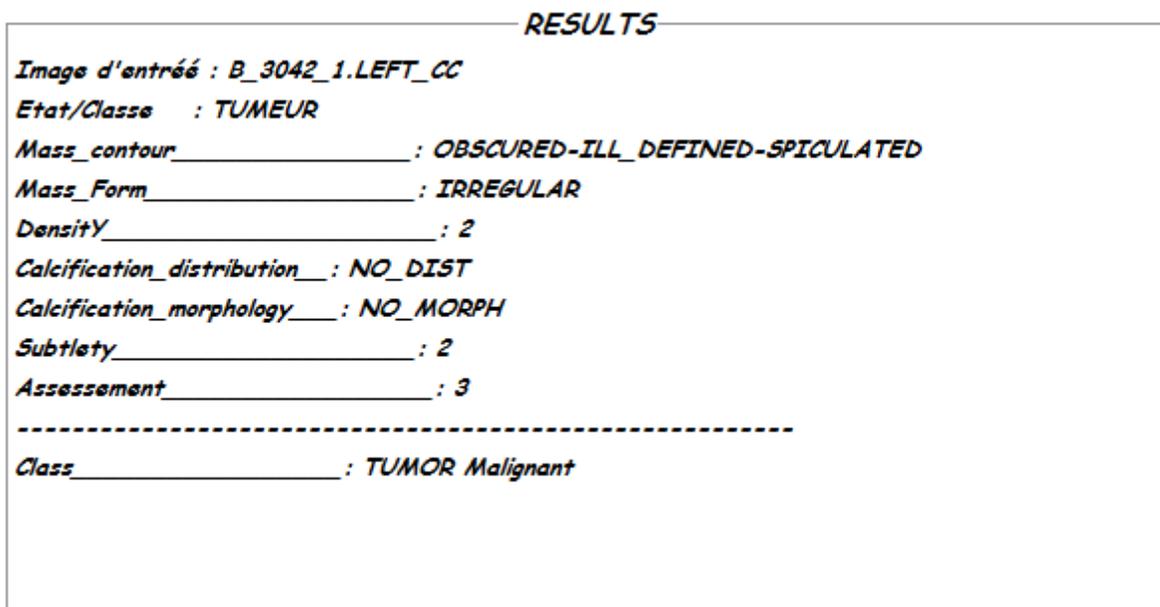


Fig. 9. Result of the Classification of Tumors by Ontology.

V. CONCLUSION

All of the work we have done is based on two phases. While the first is devoted to the classification of mammograms into two categories normal or suspicious (binary classification) based on a deep neural network, for this, we used three models with different architectures and we showed the different results obtained in terms of precision and error. Comparison of the results found showed that the epoch number, the size of the base and the depth of networks, are important factors for obtaining better results.

The network parameters are difficult to define a priori. It is for this reason that we have defined different models with different architectures in order to obtain the best results in terms of precision and error.

The second phase aims to add a semantic level to our classification through a specialized ontology developed for this purpose. The objective of the second phase is to show the contribution of ontology for the automatic manipulation of information at the semantic level with the use of the SWRL language, which enriches the semantics of an ontology defined in OWL based on the system of BI-RADS characterization (multi-class classification).

Finally, we evaluated and tested the performance of each phase of our approach in terms of accuracy and error.

The comparison of the results found showed that the epoch number, the size of the base and the depth of networks, are important factors in obtaining better results.

The network parameters are difficult to define a priori. It is for this reason that we have defined different models with different architectures in order to obtain the best results in terms of precision and error. We encountered some problems in the implementation phase, the use of a CPU made the execution time too expensive. In order to solve this problem one must use deeper convolutional neural networks deployed on a GPU instead of a CPU on larger bases.

In order to improve the classification rate and to have more detail (multi-class classification), we modeled knowledge in the form of ontology to attribute a semantic aspect to information based on the BI-RADS characterization system.

The results of the data classification obtained by our approach are very conclusive and prove the effectiveness of our approach. However, in order to improve our approach and increase the classification rate, we propose to make the following improvements:

- Extension of the database: we could consider validating it on other types of images such as histopathological images.
- Integration of the notion of interoperability of ontologies by hybridizing their classification techniques with the fuzzy approach, for example.

REFERENCES

- [1] Bethany, T. Samuelson Erik, K. Fromme Charles, R. Thomas "Changes in Spirituality and Quality of Life in Patients Undergoing Radiation Therapy", *The American journal of hospice & palliative care* 29(6):449-54, November 2011 Edition, DOI: 10.1177/1049909111428607.
- [2] N. Benamrane, Contribution à la vision stéréoscopique par mise en correspondance de régions, Phd Thesis, University of Valenciennes, France, 1994.
- [3] N. Benamrane, A. Fekir : Medical images segmentation by neuro-genetic approach, *The Ninth International Conference on Information Visualisation (IV'05)*, 981-986, 2005.
- [4] Belgrana Fatima Zohra, Benamrane Nacéra, Detection of tumor in mammographic images by rbf neural network and multi population genetic algorithm, *International Journal of Applied Information Systems (IJAIS)* 6 (3), 2013.
- [5] F. Boutaouche, N. Benamrane, Diagnosis of breast lesions using the local Chan-Vese model, hierarchical fuzzy partitioning and fuzzy decision tree induction, *Iranian Journal of Fuzzy Systems* 14 (6), 15-40, 2017
- [6] Rahli Hamida Samiha, Benamrane Nacéra « Interprétation des images de mammographie par l'algorithme search harmony », *Anale. Seria Informatică. Vol. X fasc. 2 – Année 2012*.
- [7] Hrich Ilyass ; Farss Sidi Mohamed ; Idy Diop ; Jahid Tarik : "Ontology-based mammography annotation for breast cancer diagnosis", 2nd World Symposium on Web Applications and Networking (WSWAN), Tunisia, 2015.
- [8] Ahlem Othmani, Carole Meziat, Nicolas Loménie : *Ontology-driven Image Analysis for Histopathological Images. ISVC 2010 : 6th International Symposium on Visual Computing*, Nov 2010, Las Vegas, United States. 2010.
- [9] Benmarouf Meriem, Tlili Yamina: « Interpretation breast cancer imaging by using ontology », *Cyber Journals: Multidisciplinary Journals in Science and Technology, Journal of Selected Areas in Bioengineering (JSAB)*, March Edition, 2012.
- [10] Oshani Seneviratne, Sabbir M. Rashid, Shruthi Chari, James P. McCusker, Kristin P. Bennett, James A. Hendler, and Deborah L. McGuinness: "Knowledge Integration for Disease Characterization: A Breast Cancer Example", *The Semantic Web – ISWC (2018)* pp 223-238.
- [11] Edson F. Luque, Daniel L. Rubin, Dilvan A. Moreira: « Automatic Classification of Cancer Tumors using Image Annotations and Ontologies », *International Symposium on Computer-Based Medical Systems, São Carlos e Ribeirão Preto*, 2015.
- [12] M. Arfan Jaffar: « Deep Learning based Computer Aided Diagnosis System for Breast Mammograms », (*IJACSA*) *International Journal of Advanced Computer Science and Applications*, Vol. 8, No.7, 2017.
- [13] Chijun Li, Xiang Ren, Yule Huang, Kai Yang, Peiying Liang, Hui Cao, "Multi-software-hybrid-programming digital image processing for high definition single lens digital imaging system", *proceedings of the 2016 5th International Conference on Measurement, Instrumentation and Automation (ICMIA 2016)*, <https://doi.org/10.2991/icmia-16.2016.127>.
- [14] Daniel Lévy, Arzav Jain « Breast Mass Classification from Mammograms using Deep Convolutional Neural Networks », 30th Conference on Neural Information Processing Systems, Barcelona, Spain, 2016.
- [15] Hackenberger, Branimir K. "Tensors all around us." *Croatian medical journal* vol. 60,4 (2019): 369-374. doi:10.3325/cmj.2019.60.369.
- [16] A. Krizhevsky, I. Sutskever, G.E. Hinton, *Imagenet classification with deep convolutional neural networks*, in, *Adv. Neural Inform. Process. Syst.* (2012). 1097–1105.
- [17] Dobrilovic, D.; Brtko, V.; Stojanovic, Z.; Jotanovic, G.; Perakovic, D.; Jausevac, G. A Model for Working Environment Monitoring in Smart Manufacturing. *hppl. Sci.* 2021, 11, 2850. <https://doi.org/10.3390/app11062850>.

- [18] Simonyan, K., & Zisserman, A. (2014). Very deep convolutional networks for large-scale image recognition. arXiv 1409.1556.
- [19] Ridha Ilyas Bendjillali, Mohammed Beladgham, Khaled Merit, Abdelmalik Taleb-Ahmed, "Illumination-robust face recognition based on deep convolutional neural networks architectures", Indonesian Journal of Electrical Engineering and Computer Science Vol 18(No 2): December 2019, DOI: 10.11591/ijeecs.v18.i2.pp1015-1027.
- [20] Jesus Gonzalez. "Symbolic One-Class Learning from Imbalanced Datasets: Application in Medical Diagnosis." International Journal on Artificial Intelligence Tools (2009).
- [21] B H. Nagarajasri, "Design of Mass Detection Algorithm using Hyper Analytical Wavelet Transform in Digital Mammography", International Journal of Engineering Research & Technology (IJERT), Vol. 10 Issue 07, July-2021.
- [22] <http://techblog.cognitum.eu/2015/08/using-swrl-built-ins-in-cnl-ontology.html>.

Electronic Commerce Product Recommendation using Enhanced Conjoint Analysis

Andrew Brian Osmond, Fadhil Hidayat, Suhono Harso Supangkat

School of Electrical Engineering and Informatics

Center of Smart City Community and Innovation, Institut Teknologi Bandung, Indonesia

Abstract—While finding any product, there are many identical products sold in the marketplace, so buyers usually compare the items according to the desired preferences, for example, price, seller reputation, product reviews, and shipping cost. From each preference, buyers count subjectively to make a final decision on which product is should be bought. With hundreds of thousands of products to be compared, the buyer may not get the product that meets his preferences. To that end, we proposed the Enhanced Conjoint Analysis method. Conjoint Analysis is a common method to draw marketing strategy from a product or analyze important factors of a product. From its feature, this method also can be used to analyze important factors from a product in the marketplace based on price. We convert importance factor percentage as a coefficient to calculate weight from every attributes and summarize it. To evaluate this method, we compared the ECA method to another prediction algorithm: generalized linear model (GLM), decision tree (DT), random forest (RF), gradient boosted trees (GBT), and support vector machine (SVM). Our experimental results, ECA running time is 6.146s, GLM (5.537s), DT (1s), RF (10,119s), GBT (45.881s), and SVM (11.583s). With this result, our proposed method can be used to create recommendations besides the neural network or machine learning approach.

Keywords—Enhanced conjoint analysis; marketplace; e-commerce

I. INTRODUCTION

e-Commerce, in its first form, was established 40 years ago. Since then, new technology, advances in internet connectivity and security, payment gateways, and widespread consumer and business model acceptance have all aided e-growth. Commerce's Michael Aldrich launched electronic shopping in 1979 by connecting a customized television to a transaction-processing computer through a telephone line. Amazon was one of the earliest e-commerce sites for books, and PayPal followed it as an e-commerce payment system in 1995. Alibaba was founded in 1999 as an online e-commerce platform. It transforms the company model from single-store e-commerce to a multistore marketplace.

In the 2000s, Shopify and BigCommerce have launched a cloud e-commerce platform that helps retailers to have their e-commerce shop. Previously our system had been built from scratch, but Shopify and Bigcommerce allow us to have our e-commerce store by renting their platform. Since 2010, numerous payment systems have arisen, including stripe, apple pay, Samsung Pay, and other payment method. Now, there is a social commerce, where people can buy or sell something from

social media like Facebook, Instagram, and even messenger applications like WhatsApp, telegram, and signal.

In Indonesia, Bhinneka and Sanur are the first ecommerce in Indonesia in 1996. Then Doku as payment gateway system is introduced in 2007. New era of ecommerce starts from 2010 as Tokopedia and Bukalapak launch as e-commerce marketplace. Later, there are a lot of marketplace launched such as: Blibli, JD.ID, Lazada, qoo10, and many more. e-Commerce is a new way in business transaction through internet with cover of lease or the auction goods [1]. e-Commerce marketplace in Indonesia are commonly act as mediator. Marketplace platform act as bridge between customer and seller, they obtained data generated by all its participant [2]. Author [3] formulate e-commerce as integrated platform from upstream supplier (individual industry, cooperative, and production) into end customer. This platform consists of intermediate channel provider (distributor, importer), one or few categories of product, called vertical e-commerce, and O2O (online-to-offline) model where customer can browse the product through e-commerce and buy it in physical store.

e-Commerce today is not only a rigid platform for interaction between buyers and sellers, where information received by buyers only comes from the platform but provides direct access between buyers and sellers to create an interactive environment [4]. Even e-commerce offers transactions in one country and more than one country; it is called cross border e-commerce, a new concept about resource integration, supply and demand matching, joint operation, and supply chain logistics between countries [5]. People buy some items at online stores for a variety of reasons: They can buy at any time. They save time by not having to go to the store. They can easily compare prices. They do not have to bargain because the price of the product is fixed. More information and chances to compare goods and prices among thousands of products are available to customers in an online shop, and better product selection, convenience, and simplicity of discovering desired products [6]. In the marketplace, consumers usually search the products and filter them according to the needs of consumers, for example, location, price, discount, delivery courier. All sellers with their products will appear based on appropriate keywords. After choosing the product, consumers will choose the delivery courier and payment method. Finally, after payment is completed, consumers can wait for their product to come. Consumers can finish their order when the product comes, and the fund can be released to the seller. Flow of e-commerce transaction is shown in Fig. 1.

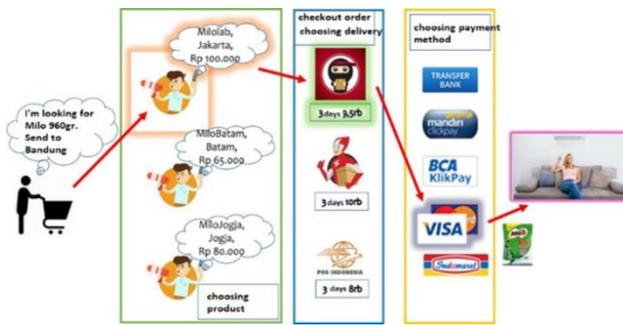


Fig. 1. Flow of e-commerce Transaction.

Currently, transactions in a marketplace are determined by many factors:

- 1) Location of buyers and sellers. The location of the buyer and seller usually becomes one of the things that are considered for buying goods because relating to shipping cost.
- 2) Delivery services that the seller activates. Every buyer has an opinion or experience using certain shipping services.
- 3) Price. One of the essential aspects for purchasers is the pricing of goods. Buyers hunt for the best deal on everyday items.
- 4) Review. Reviews about products, services, and shipping from certain transactions of previous buyers.
- 5) Promotion. Promotions are provided by sellers, such as discounts, cashback, or free shipping.

Indonesia is regarded as one of Asia's most developed e-commerce markets. Several reasons contribute to Indonesia's e-commerce sector's fast growth. To begin with, smartphone and Internet development continue to accelerate. Second, Indonesia has a large population with rising purchasing power due to the country's macroeconomic solid growth. Third, Indonesia's populace is young and tech-savvy. [2]. There are 175.4 million active Internet users in January 2020 [3]. With 2.201 start-ups, Indonesia can adjust and develop product based new technology rapidly [4]. Besides, the support from the government by opening the large scale of investment from domestic or overseas to participate in developing Micro, Small and Medium Enterprises and e-commerce have made e-commerce grow very fast. This growth gives chances to e-commerce practitioners to grow their business, such as Tokopedia, Bukalapak, Blibli, and others [5]. In Indonesia, buyers usually spend an average of 4 minutes in a marketplace to have a look at some products before deciding to buy an item or not. In general, there are many identical products sold in the marketplace, so buyers usually compare the items according to the desired preferences, for example: price, seller reputation, product reviews, and shipping cost. From each preference, buyers count subjectively to make a final decision which product is should be bought. With so many products in e-commerce, there is a problem finding the optimal product because buyers have to manually compare products one by one.

Motivated by the problem, the following research the question arises and will be discussed in this paper: what types of consumer strategy should be implemented to get the optimal product?

To answer the question above, we proposed a method for helping buyer finds optimal product from price, shipping cost, and insurance cost. An enhanced conjoint analysis method is chosen to recommend optimally product. Conjoint analysis is a well-known research technique in marketing and consumer research. This the approach has been used to address a wide range of marketing challenges, including predicting product demand, developing a new product line, and calibrating pricing sensitivity/elasticity. The approach entails presenting respondent consumers with a carefully crafted collection of hypothetical product profiles (defined by the necessary levels of relevant qualities) and gathering their preferences for those profiles in the form of ratings, rankings, or selections [6].

Conjoint analysis usually is used to identify some variables that important for a product. For example: [7] using adaptive choice-based conjoint analysis to identify surcharge for outdoor apparel, [8] evaluate domestic express coach service using conjoint analysis, [9] identify the critical attribute of smartphones using conjoint 3 analyses. Widely conjoint analysis is used to evaluate essential attributes for a product. By knowing the critical attribute of the product, a company can create a new marketing strategy, new version of the product, or new product that is close to what consumer needs. In this research, a conjoint analysis is proposed to get essential attributes from a consumer's product. Value from attribute is converted as attribute weight. Later multiply the value of each product attribute and its weight to get a score and choose the minimum score as a recommendation. Assumed that there exists e-commerce. When the consumer chooses the product, our system can recommend what the consumer should choose.

The following is a breakdown of the paper's structure. The second section examines research in a similar field. We introduce notations, assumptions, formulations, and the system that will be used to answer the problems in Section 3. To identify the performance of our method, we create simulation, test, and analyze it. Section 4 contains the conclusion and future works of this research.

II. LITERATURE REVIEW

Identify applicable sponsor/s here. If no sponsors, delete this text box (sponsors). Some study has been done on pricing strategies in the marketplace: [10] offers an empirical analysis and analytical a model that shows how an online shop may achieve a competitive advantage by designing an optimal mix of product price and shipping price. In [11], has proposed a unique algorithmic approach for estimating optimal prices in e-commerce scenarios using noisy and sparse data. Their structure is broad and can be tailored to a particular issue. Experiments have demonstrated that using their methodology in practice can result in significant increases in profit and revenue. In [12], recommends a multi-armed bandits algorithm for dynamic pricing using a customer-centric strategy, based on the notion that systems track client behavior and price impacts whether or not a purchase is made. In the e-commerce recommender system, there is some research about it. Collaborative filtering, knowledge-based reasoning, content-based filtering, demographic-based filtering and hybrid technique are still become a favorite primary method to be explored. In [13], improve recommender system using previous

search information, user behavior analysis, and current search information. The proposed method by combining content and web usage mining technique then measure the accuracy of the system. In [14], improving collaborative filtering to recommend trendy items to a customer to demonstrate the performance of their algorithm, they took the system to an actual retail mall. They claim that their system outperforms traditional collaborative filtering in terms of efficiency. In [15], developed and implemented a recommender system based on web mining. Their complicated recommendation engine takes data from web mining as input. For the implementation of a recommender system, [16] employed demographic data from the client registration form as an essential source of data mining algorithm. They proposed four-phase in their recommender system workflow: 1) acquire information implicitly and explicitly, 2) information processing, 3) recommendation processing, Moreover, 4) indicating the outcome to the clients. They also employed a data diversity such as online market data, query data, server log data, hyperlink inside web pages, client registration data, and web pages. From the research, the author concludes that the proposed approach improves the quality of recommendation efficiently. To construct their recommendation system, [17], [18], [19] used a knowledge-based filtering strategy. In [19], Using KBF to help a customer make a decision. They used the length of time spent shopping and the kind of things purchased by the consumer as input to choose the most important product. It was discovered that KBF could improve decision-making by reducing the length of shopping and the effort required to choose the right product. In [18], using data clustering analysis results to develop a web mining framework. It is used to deliver recommendations for e-commerce recommender systems. He also stores knowledge rules using pattern analysis on acceptable media and learns the recommender engine from web mining. The author concluded that the suggested method could manage massive data quantities while increasing reaction time substantially and scalability. There is also some research about recommender systems in e-commerce using content-based filtering methods. In [20], suggest content analysis for improving the recommender system. The proposed method will recommend sample websites to meet user requirements. However, it has a high operation cost and response time because many websites have different structures, naming tags, and information. In [21], introduced BPR (Bayesian Personalized Ranking) to explore user preferences by ranking. They employed a global score function to determine the user's preference for various goods. In [22], proposed a strategy that used CF and CBF to achieve excellent recommendation accuracy. The author proposes a three-part weighted combination filtering recommender system: gathering required data, creating recommendations, and communicating findings to the user. Moreover, one of the most popular recommender system research techniques is a hybrid technique by joining various algorithms and methods. Several different algorithms are used for collecting and processing information that improves the quality of recommendations. In [23], developed a weighted parallel technique for developing an e-commerce recommender system in Indonesia. The author uses a combination of CF and CBF approaches. While in [24] uses a personalized hybrid way to evaluate standard algorithms to

enhance user interest modelling, variety, and scale. As we know so far, there is no research about using the Conjoint Analysis method to create a recommender system, especially in e-commerce. So, we assess CA as a base method to create recommendations, especially for e-commerce in Indonesia.

III. NOTATION, FORMULATION, AND SYSTEM DESIGN

For convenience, we summarize the notation adopted in this paper is in Table II. In this research, we do preliminary study to determine what kind of attribute to use in this research. We investigate three of e-commerce in Indonesia: Tokopedia (<https://www.tokopedia.com>), bukalapak (<https://www.bukalapak.com>), and shopee (<https://shopee.co.id>). Each explicit product attribute is shown in Table I.

TABLE I. PRODUCT ATTRIBUTES

	Tokopedia	Bukalapak	Shopee
Product Name	✓	✓	✓
Sold	✓	✓	✓
Weight	✓	✓	✓
Tags		✓	
Percentage of satisfaction consumer		✓	
Order processing time		✓	
Insurance Cost		✓	
Price	✓	✓	✓
Free shipping badge	✓		✓
Delivery courier	✓	✓	✓
Buyer Location	✓	✓	✓
Stock	✓	✓	✓
Description	✓	✓	✓
Categories	✓	✓	✓
Brand	✓	✓	✓
Seller Location	✓	✓	✓
Review score	✓	✓	✓

In addition to determining the essential qualities, the examinable performance level for each attribute must be defined using the following [25] criteria: 1) attribute levels should be as similar to the real-life experience of the customer as feasible, 2) attribute levels should be related to the product that is accessible to the consumer, and 3) contain characteristics that are regarded to be essential competences. Then determine that the primary attributes that will be used for this method should be numeric.

Product score, sold, price, shipping cost, and insurance cost are chosen as our method's primary attributes. When not all preferences are satisfied, the customer must make a trade-off between all primary attributes during the selection process. We try to solve it using Multi Attributes Decision Making (MADM) problem formulation. The problem formulation for MADM is as follows [26]:

- 1) There is a set of X attributes, where $X = \{X_1, X_2, \dots, X_n\}$
- 2) a set of domain values $D = \{D_1, D_2, \dots, D_n\}$: each $D_i (1 \leq i \leq n)$ represents a collection of possible values for attribute X_i . To prevent confusion, we use D to represent the space of all possible outcomes.

3) a set of restrictions $C = \{C_1, C_2, \dots, C_m\}$: where each $C_j(1 \leq j \leq m)$ is a constraint function that limits the possible values for a subset of the characteristics X.

4) a list of available outcomes $O = \{O_1, O_2, \dots, O_l\}$: where each $O_j(1 \leq j \leq l)$ is an element of the possible result space D, and O is a subset of D. Although the size of O is usually smaller than that of D, it is still too large for the decision maker to choose one at a time. This set must contain the solution(s) that the decision maker ultimately chooses.

5) a set of statements expressing the decision maker's preferences $P = \{P_1, P_2, \dots, P_t\}$: this piece of data must be elicited from the decision maker prior to or during the encounter. Different decision makers may have different preference statements, and during the process of searching for the best answer, certain preferences may be violated for tradeoff purposes.

In this paper, consider there are i product ($i = 1, 2, 3, \dots, N$). Every product i has their attributes product score (c_i), sold (d_i), price (p_i), shipping cost (s_i), and insurance cost (u_i). Each of attributes has a weight coefficient denoted by K, L, M, N, O . Notation is shown in Table II.

Conjoint analysis is a well-known research technique in marketing and consumer research. This methodology, which allows for the understanding of consumer preferences, has been used to solve a wide range of marketing challenges, including forecasting product demand, creating a new product line, and calibrating pricing sensitivity/elasticity. Respondent customers are presented with a well-crafted collection of hypothetical product profiles (defined by the stated levels of the necessary qualities), and their preferences are collected in the form of ratings, rankings, or selections for those profiles [6]. The technique of ordinary least square regression (OLS) is often used to estimate preference functions. According to research, this technique's efficiency (predictive power) is often relatively similar to more complex techniques, but the findings are easier to grasp. OLS equation is shown below:

$$S = \sum_{i=1}^n (y_i - \tilde{y}_i)^2 = \sum_{i=1}^n (y_i - b_1x_1 - b_0)^2 = \sum_{i=1}^n (E_i)^2 = \min$$

where,

\tilde{y}_i = predicted value for i observation,

y_i = actual value for i observation,

E_i = error / residual for i observation,

n = total number of observation.

Global utility of a given attribute is determined using the equation (2), where Op is the relative significance of the product attribute, $max up$ is the utility of the attribute's most preferred level. $Min up$ is the utility of the attribute's least chosen performance level. The operation is continually changing and based on a variety of factors.

$$Op = \frac{(max(u_p) - min(u_p))}{\sum_{p=1}^t (max(u_p) - min(u_p))} \quad (2)$$

TABLE II. NOTATION

Notation	Description
c_i	Review score for product i
d_i	Number of sold for product i
p_i	Price for product i
s_i	Shipping cost for product i
u_i	Insurance cost for product i
K	Weight for product score
L	Weight for number of sold
M	Weight for price
N	Weight for shipping cost
O	Weight for insurance cost

Here, define that

$$O_1 = K,$$

$$O_2 = L,$$

$$O_3 = N,$$

$$O_4 = O,$$

Then we construct an enhanced equation to calculate weight for all attributes from each product below (3) and find the minimum value for the weight of the i product as an enhanced conjoint analysis method to give a recommendation.

$$R = \min(\sum_{i=1}^n (Kc_i + Ld_i + Ns_i + Ou_i)) \quad (3)$$

A. Designed System

The designed recommender system is shown in Fig. 2. The flow of the recommendation process is described as follows:

1) User the product name as a keyword, then aggregator will collect the data from the marketplace and save it to the database.

2) Pre-processor will get the data from the database and clean it first (such as: removing NULL values, unused attributes) before it comes to the conjoint analyzer.

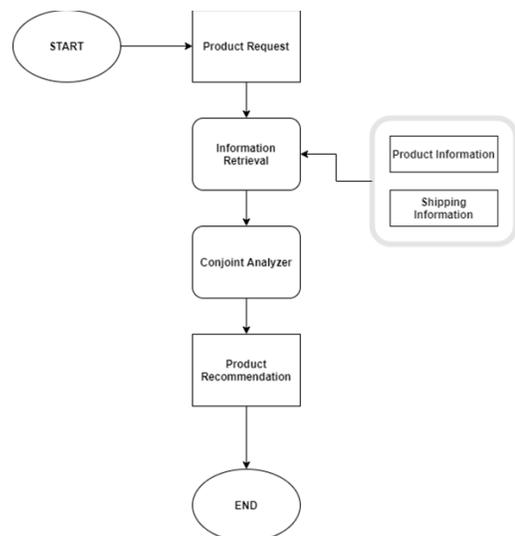


Fig. 2. Designed System.

3) In Conjoint Analyzer, equation (1) is implemented for each attribute ($c_i, d_i, p_i, s_i,$ and u_i) from product i . The result from this function is O of each attributes p .

4) Choosing the minimum value using equation (3) and recommend it to the user.

Table III shows how construct a table to store data from the marketplace.

TABLE III. PRODUCT TABLE

Field	Type	Length
<i>id</i>	<i>Integer</i>	11, PK
<i>Link</i>	<i>Varchar</i>	300
<i>ProductName</i>	<i>Varchar</i>	255
<i>Price</i>	<i>Integer</i>	11
<i>Sold</i>	<i>Integer</i>	11
<i>Reviews</i>	<i>Integer</i>	11
<i>Location</i>	<i>Varchar</i>	30
<i>Delivery Services</i>	<i>Varchar</i>	40
<i>ShippingCost</i>	<i>Integer</i>	11
<i>InsuranceCost</i>	<i>Integer</i>	11
<i>Eta</i>	<i>Varchar</i>	11
<i>etalInfo</i>	<i>Varchar</i>	11

B. Dataset Processing

There are some choices of Indonesian marketplace as data source, such as: Tokopedia, Shopee, Bukalapak, Lazada, Jakmall, or Blibli. Bukalapak has been chosen as our data source because Bukalapak provides API to get information about product delivery instead of product from their website. Assumed that users search for products using “gegep tekiro” to grab products related to “gegep tekiro.” A searching page for the keyword “gegep tekiro” is shown in Fig. 4. Later from the searching page, go to the detail of every product. Information on the detailed product is shown in Fig. 5. We retrieve product name, link, price, sold, reviews, location, delivery services, shipping cost, insurance cost, eta (estimated time arrival), and eta on the detailed product page info.

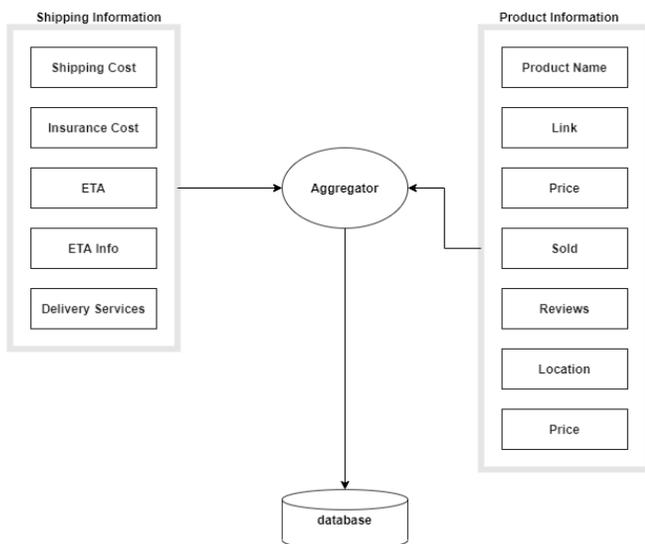


Fig. 3. Parameter Processing.

An aggregator is created to retrieve only needed information based on the HTML tag on the product detail page. Eliminating unessential parameters, then insert the value into the table on the database. Parameters processing is shown in Fig. 3.

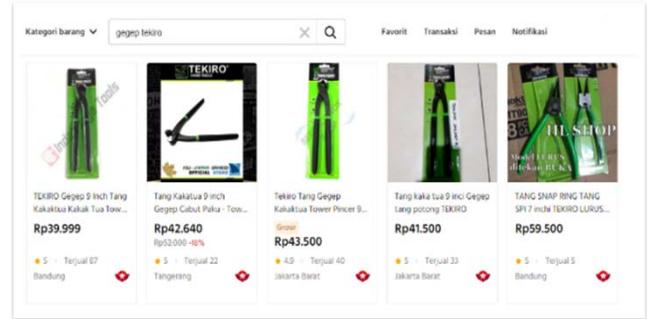


Fig. 4. Product Result Page.

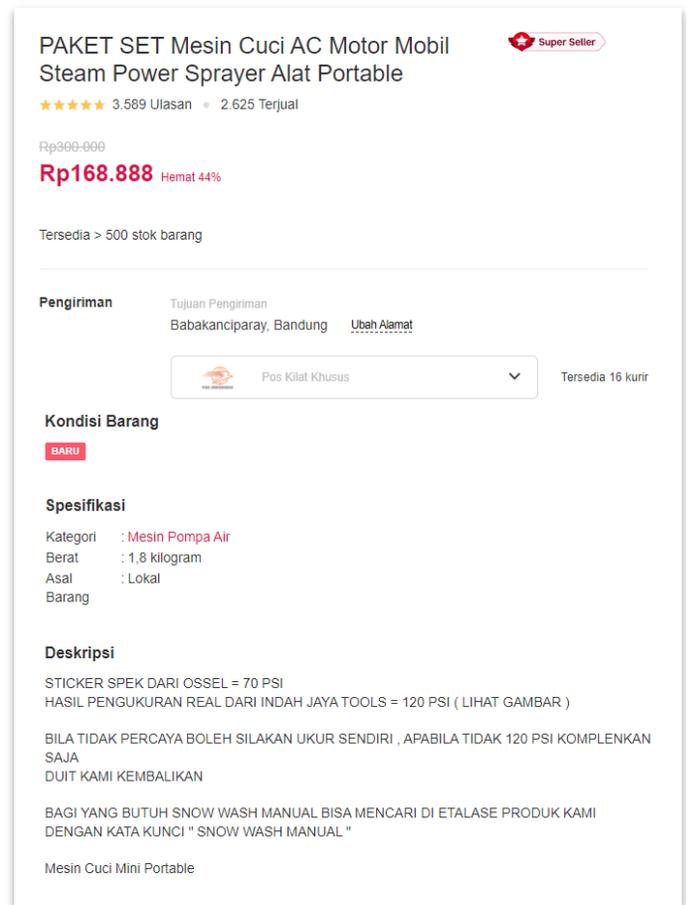


Fig. 5. Product Detail Page.

IV. SIMULATION

In this experiment, we limit data to 240 sellers. The five cheapest product is selected from the dataset. In this simulation, we will simulate the Enhanced Conjoint Analysis method compared to price. There are three scenarios with dynamic growth data starting from 80 data, 160 data, and 240 data. The five cheapest products are shown in Table IV.

TABLE IV. FIVE CHEAPEST PRODUCT BY PRICE

Name	Price (Rp)
tang gegep 9 inch kakatua tower pincer Tekiro	39.300
TEKIRO tang kakatua 9 tang gegep 9 tower pincer 9 inch	39.700
TEKIRO Gegep 9 Inch Tang Kakatua Kakak Tua Tower Pincer	39.999
TANG GESEP - KAKAKTUA 9 INCH TEKIRO - TOWER PINCER	40.000
Tang Kakatua Tang Gegep Tower Pincer 9 TEKIRO	41.000

Three different scenarios are implemented to get result from our method. The result is described as follows:

1) *Scenario 1*: Importance attribute from conjoint analysis process is shown in Table V. Here, the most important attribute is insurance cost, followed by shipping cost, sold, and reviews.

Keywords	Gegep tekiro
Total seller	80 seller
Location buyer	Bandung

TABLE V. IMPORTANCE ATTRIBUTES OF SCENARIO 1

Attributes	Importance Percentage
Insurance cost	63.1 %
Shipping cost	14.7 %
Sold	12.8 %
Reviews	9.3 %

Later, equation to create recommendation is:

$$R = \min(\sum_{i=1}^n (63.1c_i + 12.8d_i + 14.7s_i + 63.1u_i)) \quad (4)$$

TABLE VI. RESULT OF SCENARIO 1

Name	P	S	R	SC	IC	TW
TEKIRO Gegep 9 Inch ...	39.999	52	5.0	8000	216	1319.42
Tang Gegep Tekiro 9 inches ...	45.000	0	0	8000	238	1326.18
TEKIRO Gegep 9 Inch ...	39.999	52	5.0	8500	218	1394.18
Tang Gegep Tekiro 9 inches ...	45.000	0	0	8500	241	1401.57
Gegep Tekiro 9 in	45.000	12	5.0	8500	241	1403.57

Note: P: price, S: sold, SC: shipping cost, IC: insurance cost, TW: total weight.

In this scenario, the obtained result is different from the product in Table VI. Our system chooses a product with a price of Rp 39.999 with the combination of shipping cost Rp 8.000, insurance cost Rp 216, 52 sold, and have 5.0 reputation as show in Table VI.

2) *Scenario 2*: Importance attribute from conjoint analysis process is shown in Table VII. Here, the most important attribute is insurance cost, followed by shipping cost, sold, and reviews.

Keywords	Gegep tekiro
Total seller	160 seller
Location buyer	Bandung

TABLE VII. IMPORTANCE ATTRIBUTES OF SCENARIO 2

Attributes	Importance Percentage
Insurance cost	73.8 %
Shipping cost	13.1 %
Sold	8.5 %
Reviews	4.7 %

equation to create recommendation is:

$$R = \min(\sum_{i=1}^n (4.7c_i + 8.5d_i + 13.1s_i + 73.8u_i)) \quad (5)$$

TABLE VIII. RESULT OF SCENARIO 2

Name	P	S	R	SC	IC	TW
TEKIRO Gegep 9 Inch ...	39.999	52	5.0	8000	216	1212.06
Tang Gegep Tekiro 9 inches ...	45.000	0	0	8000	238	1223.64
TEKIRO Gegep 9 Inch ...	39.999	52	5.0	8500	218	1279.04
Tang Gegep Tekiro 9 inches ...	45.000	0	0	8500	241	1291.36
Gegep Tekiro 9 in	45.000	12	5.0	8500	241	1292.61

In this scenario, using twice data more than scenario one, the obtained result is the same as scenario one, but the equation to create a recommendation is different. Numbers of data makes different results for importance factor value and affected variable, used in (5). Our system chooses a product with a price of Rp 39.999 with the combination of shipping cost Rp 8.000, insurance cost Rp 216, 52 sold, and have a 5.0 reputation as show in Table VIII.

3) *Scenario 3*: Importance attribute from conjoint analysis process is shown in Table IX. Here, the most important attribute is insurance cost, followed by shipping cost, sold, and reviews.

Keywords	Gegep tekiro
Total seller	240 seller
Location buyer	Bandung

TABLE IX. IMPORTANCE ATTRIBUTES OF SCENARIO 3

Attributes	Importance Percentage
Insurance cost	73.4 %
Shipping cost	12.9 %
Sold	8.8 %
Reviews	5.0 %

Equation to create recommendation is:

$$R = \min(\sum_{i=1}^n (5.0c_i + 8.8d_i + 12.9s_i + 73.4u_i)) \quad (6)$$

In this scenario, using three times more data than in scenario 2, our systems still choose products with combinations the same as indicated by scenario 2 as show in Table X. For each scenario, our system will calculate the coefficient of every preference depending on the number of data, and the result can be different. The most interesting is that insurance cost is the most critical factor in a product besides price.

TABLE X. RESULT OF SCENARIO 3

Name	P	S	R	SC	IC	TW
TEKIRO Gegep 9 Inch ...	39.999	52	5.0	8000	216	1195.15
Tang Gegep Tekiro 9 inches ..	45.000	0	0	8000	238	1206.09
TEKIRO Gegep 9 Inch ...	39.999	52	5.0	8500	218	1261.11
Tang Gegep Tekiro 9 inches ..	45.000	0	0	8500	241	1273.39
Gegep Tekiro 9 in	45.000	12	5.0	8500	241	1274.48

For choosing a product in the marketplace, we need more than one attributes to determine which one is optimal in price. We also compared it with another method to observe its performance, relativity error, correlation, and root mean square error. Another method we try to compare is the Generalized Linear Model (GLM), Decision Tree (DT), Random Forest (RF), Gradient Boosted Tree (GBT), and Support Vector Machine (SVM).

From Fig. 6, our method outperforms another method in relative error results. Our experimental results, ECA relative error is 0.0001, GLM (0.008), DT (0.018), RF (0.048), GBT (0.014), and SVM (0.031). Compared to another method, ECA does not need training and test data. Using OLS regression, we obtain an equation and then apply it to the dataset, while another method still needs to predict using training and test data. A relative error has a relation with correlation. With the smallest relative error, the correlation of the ECA method is the highest as show in Fig. 7. ECA correlation is 0.998, GLM (0.994), DT (0.987), RF (0.975), GBT (0.992), and SVM (0.979).

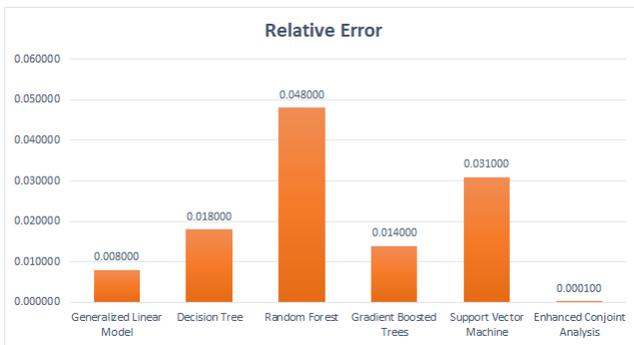


Fig. 6. Relative Error.



Fig. 7. Correlation.

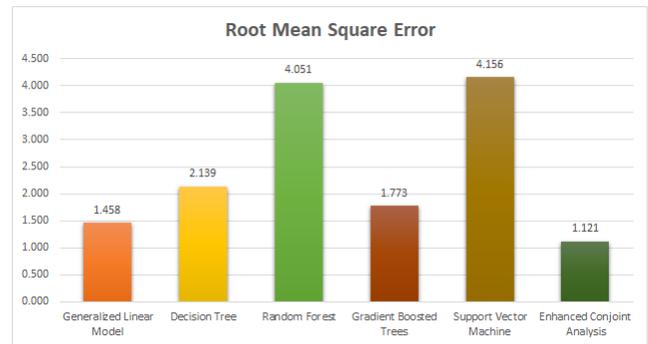


Fig. 8. Root Mean Square Error.

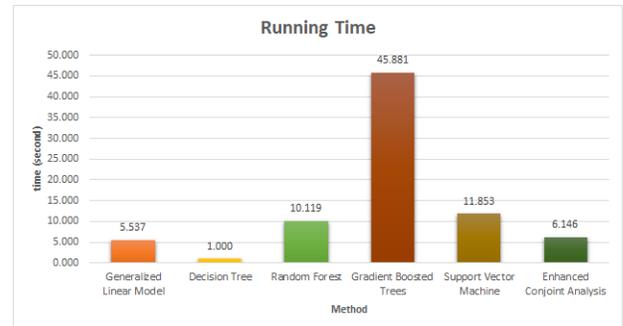


Fig. 9. Running Time.

Since ECA has the slightest relative error, it also has the smallest value for RMSE as show in Fig. 8. ECA RMSE value is 1.121, GLM (1.458), DT (2.139), RF (4.051), GBT (1.773), and SVM (4.156). Although the ECA method has a small error, the decision tree has the best running time as show in Fig. 9. ECA running time is 6.146s, GLM (5.537s), DT (1s), RF (10.119s), GBT (45.881s), and SVM (11.583s). The ECA method has a small difference value from the GLM method because both ECA and GLM are extended linear models. ECA method use Ordinary Least Square as a linear model and GLM using linear regression.

Since we do not have many features in this dataset, the Decision Tree does not have to create a big tree so it can do the deep search faster into the branch, while our method, though it has a regression equation, we still need to calculate a value for each data then sort it. The larger the data, the more time it is needed to calculate.

V. LIMITATIONS AND CONCLUSION

Conjoint Analysis is a standard method to draw marketing strategy from a product or analyze essential factors of a product. This method can also analyze critical factors from a product in the marketplace based on its price. We convert importance factor percentage as a coefficient to calculate weight from every attribute. The simulation results show how that conjoint analysis network works well in choosing a product from multiple attributes to get the best price.

Although our method has good performance, there are some limitations to this method. ECA needs time to calculate a value for each data then sort it. If the data becomes more significant than before, our method needs more time because ECA will calculate all data. We can reduce computing time by

sampling some data to be calculated, but it also can reduce the accuracy result. Another approach is by using a parallel computing approach in calculating value, but it needs observations.

Since ECA uses OLS regression to create an equation, it will choose the optimal value for each attribute. Optimal value can be the biggest or the smallest value in an attribute. In a real-world implementation, if one online shop has a lot of sales, reviews, and low prices, it will be recommended continuously by our method.

Besides its limitation, ECA gives optimal recommendation because all attributes processed using OLS regression give optimal coefficient for every attribute. ECA has the slightest relative error (0.0001) and good correlation and RMSE. The accuracy and the optimization are traded off with computing time. ECA has a running time of 6.146s meanwhile decision tree method has the best time in 1s. With this result, ECA can be used as one alternative recommendation system besides a neural network or machine learning approach.

REFERENCES

- [1] P. Butler and J. Peppard, "Consumer purchasing on the Internet: Processes and prospects," *Eur. Manag. J.*, vol. 16, no. 5, pp. 600–610, 1998.
- [2] A. V. Gunawan, L. Linawati, D. Pranandito, and R. Kartono, "The Determinant Factors of E-Commerce Purchase Decision in Jakarta and Tangerang," *Binus Bus. Rev.*, vol. 10, no. 1, pp. 21–29, 2019.
- [3] S. Kemp, "DIGITAL 2020: INDONESIA," 2020. [Online]. Available: <https://datareportal.com/reports/digital-2020-indonesia>.
- [4] Startup ranking, "Startups per Country," 2020. [Online]. Available: <https://www.startupranking.com/countries>.
- [5] H. Harsono, "Indonesia will be Asia's next biggest e-commerce market," 2017. [Online]. Available: <https://techcrunch.com/2016/07/29/indonesia-will-be-asias-next-biggest-e-commerce-market/>.
- [6] J. Agarwal, W. S. DeSarbo, N. K. Malhotra, and V. R. Rao, "An Interdisciplinary Review of Research in Conjoint Analysis: Recent Developments and Directions for Future Research," *Cust. Needs Solut.*, vol. 2, no. 1, pp. 19–40, 2015.
- [7] B. M. Brand and T. M. Rausch, "Examining sustainability surcharges for outdoor apparel using Adaptive Choice-Based Conjoint analysis," *J. Clean. Prod.*, no. January 2021, p. 125654, 2020.
- [8] M. Walter, F. Haunerland, and R. Moll, "Heavily regulated, but promising prospects: Entry in the German Express Coach Market," *Transp. Policy*, vol. 18, no. 2, pp. 373–381, 2011.
- [9] A. Anand, G. Bansal, and D. Aggrawal, "Choice based diffusion model for predicting sales of mobile phones using conjoint analysis," *J. High Technol. Manag. Res.*, vol. 29, no. 2, pp. 216–226, 2018.
- [10] Y. Yao and J. Zhang, "Pricing for shipping services of online retailers: Analytical and empirical approaches," *Decis. Support Syst.*, vol. 53, no. 2, pp. 368–380, 2012.
- [11] J. Bauer and D. Jannach, "Optimal pricing in e-commerce based on sparse and noisy data," *Decis. Support Syst.*, vol. 106, pp. 53–63, 2018.
- [12] M. Castronovo et al., "Learning Exploration/Exploitation Strategies for Single Trajectory Reinforcement Learning," *Conf. Proc.*, vol. 24, no. 2002, pp. 1–9, 2012.
- [13] V. Bajpai and Y. Yadav, "An Improved Dynamic E-Commerce Recommendation System," *SSRN Electron. J.*, 2019.
- [14] H. Hwangbo, Y. S. Kim, and K. J. Cha, "Recommendation system development for fashion retail e-commerce," *Electron. Commer. Res. Appl.*, vol. 28, pp. 94–101, 2018.
- [15] Y. K. Choi and S. K. Kim, "An auxiliary recommendation system for repetitively purchasing items in E-commerce," 2014 Int. Conf. Big Data Smart Comput. BIGCOMP 2014, pp. 96–98, 2014.
- [16] Y. Fan, Y. Shen, and J. Mai, "Study of the model of e-commerce personalized recommendation system based on data mining," *Proc. Int. Symp. Electron. Commer. Secur. ISECS 2008*, pp. 647–651, 2008.
- [17] M. I. Martín-Vicente, A. Gil-Solla, M. Ramos-Cabrera, Y. Blanco-Fernández, and M. López-Nores, "Avoiding fake neighborhoods in e-commerce collaborative recommender systems: A semantic approach," *SMAP '09 - 4th Int. Work. Semant. Media Adapt. Pers.*, pp. 9–14, 2009.
- [18] Y. Luo, "An analysis of web mining-based recommender systems for E-commerce," *Proc. 2012 Int. Conf. Comput. Appl. Syst. Model. ICCASM 2012*, pp. 0167–0170, 2012.
- [19] F. Huseynov, S. Y. Huseynov, and S. Özkan, "The influence of knowledge-based e-commerce product recommender agents on online consumer decision-making," *Inf. Dev.*, vol. 32, no. 1, pp. 81–90, 2016.
- [20] P. Gatchalee and Z. Li, "Ontology Development for SMEs E-commerce website based on Content Analysis and its Recommendation System," pp. 7–12, 2013.
- [21] C. Chen, D. Wang, and Y. Ding, "User actions and timestamp based personalized recommendation for E-commerce system," *Proc. - 2016 16th IEEE Int. Conf. Comput. Inf. Technol. CIT 2016, 2016 6th Int. Symp. Cloud Serv. Comput. IEEE SC2 2016 2016 Int. Symp. Secur. Priv. Soc. Netwo*, pp. 183–189, 2017.
- [22] J. F. Miao, "Design and implementation of personalization recommendation system in mobile e-commerce," *Adv. Mater. Res.*, vol. 989–994, pp. 4506–4509, 2014.
- [23] M. Aprilianti, R. Mahendra, and I. Budi, "Implementation of weighted parallel hybrid recommender systems for e-commerce in Indonesia," 2016 Int. Conf. Adv. Comput. Sci. Inf. Syst. ICACSIS 2016, pp. 321–326, 2017.
- [24] F. Dong, J. Luo, X. Zhu, Y. Wang, and J. Shen, "A personalized hybrid recommendation system oriented to E-commerce mass data in the cloud," *Proc. - 2013 IEEE Int. Conf. Syst. Man, Cybern. SMC 2013*, pp. 1020–1025, 2013.
- [25] A. Gustafsson, F. Ekdahl, and B. Bergman, "Conjoint analysis: A useful tool in the design process," *Total Qual. Manag.*, vol. 10, no. 3, pp. 327–343, 1999.
- [26] J. Zhang and P. Pu, "Survey of Solving Multi-Attribute Decision Problems," *EPFL Tech. Rep. No IC/2004/54*, no. July 2010, pp. 1–14, 2004.

Normalisation of Indonesian-English Code-Mixed Text and its Effect on Emotion Classification

Evi Yulianti, Ajmal Kurnia, Mirna Adriani
Faculty of Computer Science
Universitas Indonesia
Indonesia

Yoppy Setyo Duto
Faculty of Economy and Business
Universitas Mercu Buana
Indonesia

Abstract—Usage of code-mixed text has increased in recent years among Indonesian internet users, who often mix Indonesian-language with English-language text. Normalisation of this code-mixed text into Indonesian needs to be performed to capture the meaning of English parts of the text and process them effectively. We improve a state-of-the-art code-mixed Indonesian-English normalisation system by modifying its pipeline modules. We further analyse the effect of code-mixed normalisation on emotion classification tasks. Our approach significantly improved on a state-of-the-art Indonesian-English code-mixed text normalisation system in both the individual pipeline modules and the overall system. The new feature set in the language identification module showed an improvement of 4.26% in terms of F_1 score. The combination of machine translation and ruleset in the lexical normalisation module improved BLEU score by 25.22% and lowered WER by 62.49%. The use of context in the translation module improved BLEU score by 2.5% and lowered WER by 8.84%. The effectiveness of the overall pipeline normalisation system increased by 32.11% and 33.82%, in terms of BLEU score and WER, respectively. Code-mixed normalisation also improved the accuracy of emotion classification by up to 37.74% in terms of F_1 score.

Keywords—Code-mixed normalisation; Indonesian; English; emotion classification

I. INTRODUCTION

One common form of the phenomenon of multilingualism is code-mixing. It is a linguistic phenomenon that mixes two or more language variations in one utterance [1]. This phenomenon can be found in various contexts, including social media [2], news articles [3], lectures [4], and even sermons [5].

Indonesia is highly multilingual, with more than 700 languages spoken across the nation. A 2015 report noted that 57.5% of Indonesian people are bilingual and 17.4% are trilingual, among whom the most popular language combination is Indonesian, English and Javanese.¹ Multilingualistic phenomena such as code-mixing have recently become increasingly common due to more widespread usage of the internet, especially social media.

Recently, code-mixing of Indonesian and English has become popular in Indonesia and has become widely known as “Bahasa Anak JakSel”. JakSel stands for “Jakarta Selatan” (“South Jakarta”); thus “Bahasa Anak JakSel” essentially means “a language of South Jakarta teenagers”, so named

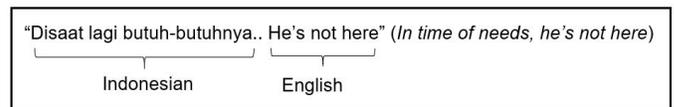


Fig. 1. Example of Indonesian-English Code-mixed Text.

because combining English and Indonesian words or phrases first become popular amongst teenagers in South Jakarta.

A previous linguistic study found there are four main reasons why Indonesian-English code-mixing (i.e. “Bahasa Anak JakSel”) has become a trend today [6]. The first is language pride: people in Indonesia who can speak or write English are considered prestigious, since not all Indonesians have mastered English. The second is social status and style: some groups frequently use some English words in their conversations because of social demands that arise if many people in the group are also used to speaking English. The third is the existence of English words that can not be translated into Indonesian: some topics are much more familiar and easier to discuss using English terms instead of the equivalent Indonesian expressions. The fourth is the desire to increase English vocabulary use: practicing using English words in conversation or writing helps people master English.

There are no noticeable differences in how code-mixing occurs for Indonesian-English versus other language pairs. English words that are mixed with the other language may be nouns, verbs or adverbs, among other parts of speech (POSS). Like code-mixing in other language pairs, Indonesian-English code-mixing can happen within a sentence (intra-sentential), across different sentences (inter-sentential) or even within a word (intra-lexical/sub-word). The distinction between Indonesian-English code-mixed text and code-mixed text in other language pairs mainly involves the syntactic and semantic aspects of the languages themselves. Fig. 1 illustrates an example of an Indonesian-English code-mixed tweet.

The increase of code-mixed text in social media has invoked research interest in studying various forms of processing such text. However, code-mixed text is more difficult to analyse than monolingual text. Analysing code-mixed text using only one language means that information written in other languages cannot be analysed effectively. On the other hand, analysing code-mixed text using two languages increases the complexity of the model due to the larger amount of vocabulary that needs to be processed and the different

¹<https://www.inlingua-edinburgh.co.uk/how-multilingual-is-your-country/>

language characteristics that need to be taken into account. A simple alternative option is to translate the code-mixed text to monolingual text. Translation of code-mixed text has been done previously for various language pairs, including Hindi-English [7], Chinese-English [8], Arabic-English [9] and Indonesian-English [10].

Barik et al. [10] built a system pipeline to normalise and translate Indonesian-English code-mixed tweets. The system pipeline consists of four modules: tokenisation, language identification, lexical normalisation, and translation. We see some potential points of improvement for Barik et al.'s code-mixed normalisation pipeline. First, in the language identification module, the features used in the language identification process could be expanded to improve the identification results. Second, in the lexical normalisation module, Barik et al.'s method – which only relies on a ruleset and a lexicon – was unable to determine whether an ambiguous word was a formal word or slang; their method always considered the word slang if it appeared in the lexicon. To overcome this issue, we propose combining a machine translation (MT) approach with a ruleset to perform lexical normalisation. Finally, in the translation module, Barik et al.'s method translates each token separately, meaning that the system lacks context when performing the translation. This research tackles this problem by translating neighboring tokens simultaneously.

Although extensive research has been performed on code-mixed text normalisation, very few studies have actually investigated the effect of this normalisation on text processing. Goot and Çetinoğlu [11] studied the effect of code-mixed normalisation on a POS-tagging task for Turkish-German text and obtained significant improvement in task performance as a result of normalisation. Singh et al. [12] investigated the effect of code-mixed text normalisation on sentiment analysis and POS-tagging for several language pairs, including Bengali-English, Hindi-English, and Tamil-English. Their results showed that code-mixed normalisation improved performance on both tasks.

No research has yet investigated the effect of Indonesian-English code-mixed text normalisation on a specific text-processing task. Therefore, in this research we also analysed the effects of code-mixed normalisation on an emotion classification task using social media data. Emotion classification tasks often rely on detecting certain phrases or words that signify emotions. Therefore, performing this task on code-mixed data is difficult when the emotion phrases or words are written in different languages. We argue that first normalizing code-mixed text into monolingual text may have benefits for emotion classification. In this work, we examine the extent to which code-mixed normalisation affects the accuracy of emotion classification systems. In general, our research questions are as follows:

- 1) To what extent the addition of some features to the language identification module, the combination of MT & rule-based approaches in the lexical normalisation module and the addition of context to the translation module can improve the state-of-the-art pipeline system for Indonesian-English code-mixed text normalisation?
- 2) Does the use of code-mixed text normalisation system affect the accuracy of emotion classification system?

II. RELATED WORK

A. Code-mixed Text Normalisation

The simplest way to normalise and translate code-mixed text is by using an existing MT system to translate the portion of the text that is in a foreign language. Patel and Parikh [13] translated Gujarati-English code-mixed text to Gujarati. The Gujarati token was transliterated using a handcrafted dictionary, whereas the English token was translated using an existing MT system. Dhar et al. [7] proposed using an existing monolingual translation system using the Matrix Language-Frame (MLF) model to translate Hindi-English code-mixed text. Their approach was adapted from the MLF linguistic theory developed by Myers-Scotton [14], which involves first determining the matrix language (dominant language) and embedding language (non-dominant language), then translating the token in the embedding language to the matrix language and finally translating the text to a desired language, if needed.

Another way to translate code-mixed text is by using a parallel corpus of code-mixed and normalised text to train an MT system. Menacer et al. [9] used this approach to translate Arabic-English code-mixed text into English. Mahata et al. [15] used deep learning for Bengali-English code-mixed normalisation, employing a character-level long-short term memory network to perform language identification. Next, the English text was translated using a neural MT system, whilst the Bengali text was transliterated back to its Devanagiri form. Finally, bigram and trigram language models were used to reorder the tokens to fix grammatical errors.

Relatively very few studies have explored code-mixed normalisation for Indonesian-English text. The only work that we could find on Indonesian-English code-mixed normalisation was Barik et al.'s study [10], which performed code-mixed normalisation using a pipeline system consisting of four modules: tokenisation, language identification, lexical normalisation, and translation. They used the condition random field (CRF) sequence labelling model for the tokenisation and language identification modules; rule-based, spelling correction and word embedding for the lexical normalisation module; and MLF (as in [7]) for the translation module. In this work, we wanted to improve Barik et al.'s code-mixed normalisation system by modifying its pipeline modules.

B. Emotion Classification

Emotion classification is a specific task in natural language processing to identify emotion contained in a particular document. The dataset used for emotion classification can be in a variety of forms, including video [16], speech [17], text [18], or even electroencephalography signals [19]. Classes or categories for emotion classification tasks are usually limited to basic emotions as defined based on research in the field of psychology. The emotion theory developed by Ekman [20] proposed six basic emotions: anger, joy, sadness, fear, disgust, and surprise. There are also Shaver's [21] six basic emotions, according to which love is categorized as a basic emotion instead of disgust. Another popular emotion theory is Plutchik's [22] eight basic emotions, which are the same as in Ekman's theory but with the addition of anticipation and trust.

A popular approach to performing emotion classification based on textual data is to utilise an emotion lexicon containing

TABLE I. THE STATISTIC OF CODE-MIXED TEXT DATASET FOR CODE-MIXED NORMALIZATION

Item	Value
#Tweet	825
#Token	22,725
#Character	105,955
#Indonesian Token	11,200
#English Token	5,608
Code Mixing Index (CMI)	19.4

a list of words and the emotion associated with each word. The lexicon can be either semi-automatically generated or manually handcrafted [23], [24]. The emotion label of a document can be determined by computing the point mutual information (PMI) value of affect words [25]. The lexicon can be used as a feature for supervised machine learning models in combination with other features, such as POS tags.

Saputri et al. [18] performed emotion classification on a dataset of Indonesian tweets. They classified each tweet as belonging to one of five emotion categories: angry, happy, sad, fear, and love. They explored various features, including emotion lexicon, sentiment lexicon, bag of words, word embedding, POS tags and morphological information. In this work, we use the five emotion labels used by Saputri et al. [18] in our emotion classification task.

III. DATASET

The dataset used in this research is taken from previous research [10]. It consists of 825 Indonesian-English code-mixed tweets along with annotations for all steps in their pipeline normalisation system (i.e. tokenisation, language identification, lexical normalisation and translation). The statistics of the dataset are presented in Table I. The data consist of 22,725 tokens and 105,955 characters. The average tweet lengths is 27.54 tokens and the average token length is 4.66 characters. There are 11,200 tokens in Indonesian (49.28% of overall tokens) and 5,608 in English (24.67% of overall tokens).

The code-mixing index (CMI) value for this dataset was 19.44. CMI is a metric used to measure how often code mixing occurs in a text [26]. This CMI value is rather high; almost 20% of the overall non-neutral language tokens in this dataset are code-mixed text.

To analyse the effect of code-mixed normalisation on emotion classification, we needed a ground truth of emotion labels for each Indonesian-English code-mixed tweet in our dataset. For this purpose, human annotation was performed to assign emotion labels to the tweets. This process was conducted by two annotators (both master's students in computer science who were familiar with the annotation tasks). Before performing the annotations, the annotators were given guidance on how to label the emotions for each tweet. Our annotation procedure followed previous research on emotion classification using Indonesian tweets [18]. Each tweet in the dataset was assigned to one of seven possible emotion labels: anger, joy, sadness, fear, love, mixed and neutral. Tweets labeled as mixed or neutral were filtered out and were not used in the emotion classification task; neutral tweets were those not associated with any emotion, whereas mixed label was assigned to tweets to which multiple emotion labels could be applicable, which is beyond the scope of this task. The annotators achieved a

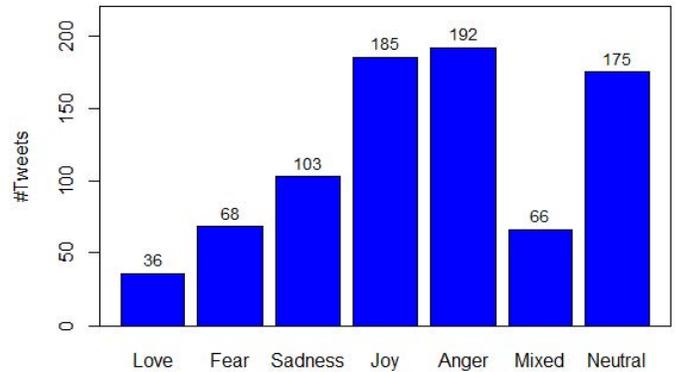


Fig. 2. The Distribution of Emotion Labels in Our Dataset.

TABLE II. THE STATISTIC OF CODE-MIXED TEXT DATASET FOR EMOTION CLASSIFICATION

Item	Value
#Tweet	584
#Token	16,939
#Character	77,041
#Indonesian Token	8,539
#English Token	4,289
Code Mixing Index (CMI)	24.26

Cohen's kappa coefficient of 64.72 before consolidating the final label for each tweet, representing substantial inter-rater agreement according to Landis and Koch [27]. Our code-mixed dataset for emotion classification has been made available for research purposes.²

The distribution of emotion labels after the annotation process is shown in Fig. 2. In total, 66 tweets were labelled as mixed and 175 as neutral, meaning that 241 of the 825 tweets from the original dataset could not be used in the emotion classification task. Fig. 2 also indicates imbalances in the emotion labels in the dataset. The emotion associated with the smallest number of tweets is love, with 36 tweets. In comparison, tweets expressing anger and joy were associated with the highest number of tweets (192 and 185, respectively). Meanwhile, 68 tweets were labelled as expressing fear and 103 as expressing sadness.

The summary statistics of the final dataset for emotion classification task are shown in Table II. The emotion classification dataset was reduced to 584 tweets with 16,939 tokens (including 8,539 Indonesian tokens and 4,289 English tokens) and 77,041 characters. The CMI value increased to 24.26, meaning that, on average, code-mixing occurred more often in this dataset compared to the original dataset (see Table I for comparison).

The other dataset used in this research was a corpus of Indonesian-English code-mixed tweets, consisting of 900,000 Indonesian-language tweets and 1.6 million English-language tweets. This corpus was taken from Barik et al.'s work and was used as training data to build word embedding for the emotion classification process.

²<https://github.com/ir-nlp-csui/CodeMixedEmotion>

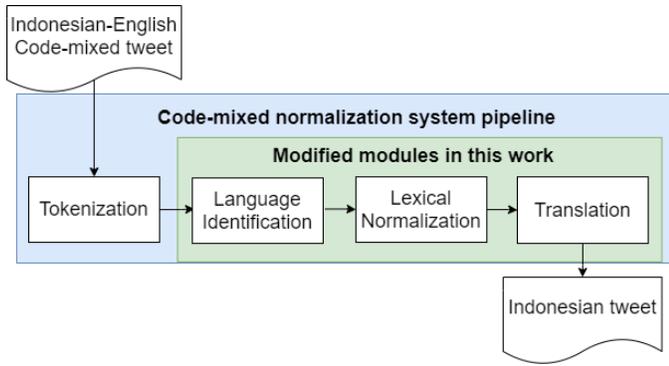


Fig. 3. The Framework of Indonesian-English Code-mixed Normalisation Pipeline.

IV. METHODS

A. Code-Mixed Normalisation

Given Indonesian-English code-mixed text, our normalisation system will transform the text into Indonesian. In general, our approach follows Barik et al.'s [10] pipeline system, which consists of four sequential modules: tokenisation, language identification, lexical normalisation, and translation. We choose to improve their pipeline because it is the most recent work in Indonesian-English code-mixed normalisation. They proposed the use of four modules in an attempt to perform comprehensive preprocessing (by adding dedicated tokenisation and lexical normalisation modules) before translating code-mixed text into one language. Some previous researchers have used simpler methods than Barik et al.'s, including Patel and Parikh [13], Dhar et al. [7], and Menacer et al. [9], who essentially omitted the special tokenisation (by tokenising simply using space characters), lexical normalisation, and/or language identification modules. We decided to use four modules in our system because Barik et al. has reported that the use of all four modules was more effective than using only some modules. Three of their modules are modified in this work with the aim to improve their system. Briefly, our modifications are as follows: (i) adding some features of the language identification module, (ii) using different approaches by combining rule-based and MT approaches in the lexical normalisation module, and (iii) adding context to the MLF approach in the translation module.

The flow of our system's pipeline is illustrated in Fig. 3. The modules of Barik et al.'s pipeline are shown in blue box. The modules modified in this work are shown in the green box. The following subsections explain the details of each module in our code-mixed normalisation pipeline system and how it differs from previous research.

1) *Tokenisation*: Tokenisation is the process of splitting text into tokens, which can be a single word or multi-word expression. Our tokenisation method follows the same procedure as Barik et al.; in other words, we did not make any changes to this module. The strategy is to classify each character in the text to a beginning-inside-outside (BIO) tag label. The label B (for "beginning") represents a character at the beginning of a token, the label I (for "inside") represents characters in the middle of a token, and the label O (for "outside") represents

characters not in any tokens. For example, the BIO tag label for the text "top text" is "BIIIOBII", so the sequence token result is "top" and "text". This approach has some advantages compared with the common tokenisation method of using whitespace as the delimiter of a token. This is supported by Barik et al.'s results, which showed that this approach was more effective than tokenisation using whitespace and a ruleset (e.g. the TweetTokenizer module from the nltk package) for informal text with high levels of noise. In total, there are 8 features used in this module.

2) *Language Identification*: This module identifies the language for each token. This process is important because, in this code-mixed normalisation work, the English part of the Indonesian-English code-mixed text will be translated into Indonesian. Therefore, we need to identify which tokens are in Indonesian and which are in English in the code-mixed text. The language identification method used by Barik et al. applied a sequence labelling approach. A CRF model is trained to identify the language for each token based on the tokenisation result. The language labels are "id", "en", and "un". The label "id" represents a token in Indonesian, "en" represents a token in English, and "un" refers to a language-neutral token (i.e. a token that cannot be identified as either Indonesian or English, such as punctuation, named entities, emoji, and tokens in other languages).

This research expands the language identification features from Barik et al.'s work. The window token feature was expanded to window size of 4 to capture more contextual information and it showed good performance in our early experimental results. Additional questions such as "is title case" and "has punctuation" were added to the token morphology feature to enrich the morphology information. The previous research only used the character n -gram feature with the size of 5. We believe that this restriction prevents the model from capturing the variety of unique character sequences and other sub-word information that is unique in each language, such as affixes. Affixes in English are very different from affixes in Indonesian. To capture this information, we decided to add more character n -grams to the feature set to add more sub-word information. Specifically, we used character n -grams ranging from unigram through 6-gram as features. Lastly, we added one feature, called morphology sequence, to better understand how the morphology of each character changed in a token. This feature is obtained by converting all lowercase and uppercase alphabet characters to "a" and "A" (respectively), all numeric characters to "0", all whitespace characters to " ", all punctuation to "-" and removing character repetition. In total, 19 features were used in this module.

3) *Lexical Normalisation*: Lexical normalisation is the process of transforming informal or slang words into their formal variants. The previous model by Barik et al. used a combination of rule-based and spelling-correction approaches for this process. Their ruleset was composed of six rules that normalise tokens containing specific language. Spelling correction normalises tokens that are not in the formal lexicon using edit distance and word embedding. Our model replaces the spelling-correction part of the model with an MT approach.

Our method for lexical normalisation combines rule-based and MT approaches. The rule-based method was applied as a pre-normalisation stage before the text was inputted into the

TABLE III. RULESET FOR LEXICAL NORMALISATION

No	Rule Description	Lang	Example
1	Reduce character repetition to maximum 2	id, en	" <i>aaamiin</i> " => " <i>aamiin</i> " (amen)
2	Reduplicate token ends with character "2"	id	" <i>baik2</i> " => " <i>baik-baik</i> " ("fine")
3	Add "-" in the middle of a duplicate token	id	" <i>baik baik</i> " => " <i>baik-baik</i> " ("fine")
4	Extend contracted words using Kooten	en	" <i>I m</i> " => " <i>I am</i> "
5	Delete prefix " <i>nge-</i> "	en	" <i>ngevote</i> " => " <i>vote</i> "
6	Delete suffix " <i>-nya</i> " and add "the" at the start of the token	en	" <i>jobnya</i> " => " <i>the job</i> "

MT stage. This idea is supported by previous work [28], [29], [30]. Veliz et al. [28] found that a ruleset could be used for lexical normalisation as a pre-normalisation step before the text was processed using MT. Kurnia and Yulianti [29] confirmed that a ruleset could be applied and proved to be useful for lexical normalisation. Yulianti et al. [30] applied rule-based MT (RBMT) before the text was inputted into statistical MT (SMT), and showed that the resulting hybrid MT was more effective than using RBMT or SMT alone.

The ruleset used in this work is taken from Barik et al.'s work. The details of the ruleset are listed in Table III. In total, six rules are used in our ruleset, which only applies to alphanumeric tokens with a minimum of one alphabet character. It does not apply to emoji, emoticons, URLs, hashtags, and user tags. This restriction was implemented to avoid transforming already-formal tokens, known as over-normalisation.

The goal of the first rule is to reduce the amount of character repetition variations of a token. This rule applies to all non-restricted tokens, regardless of language. The second and third rules normalise informal reduplicated words (applied only to tokens in the Indonesian language). The fourth rule extends contracted English words. The fifth and sixth rules normalise sub-word code-mixed tokens. For the Indonesian-English language pair, sub-word code-mixing occurs when combining English words with Indonesian affixes.

The MT approach to lexical normalisation works by translating text in informal language to formal language. This approach has been used to normalise text in various languages, such as English [31] Dutch [28], and Indonesian [32]. The MT model used in this research is SMT with a phrase translation unit, also known as phrase-based statistical MT (PBSMT). The PBSMT model was implemented with the Mosesdecoder tool [33]. The alignment model used for the PBSMT model is IBM Model 5 with MGIZA [34]. The language models (3-gram, 4-gram, and 5-gram) were trained with a normalised corpus on training data using KenLM [35]. Tuning was performed in batches with the margin-infused relax algorithm (MIRA) using bilingual evaluation understudy (BLEU) as a tuning metric [36]. Special tokens – such as URLs, hashtags, and user tags – were converted to "[URL]", "[HASHTAG]", and "[USER]" in the training and tuning process.

4) *Translation*: The translation module translates code-mixed text to monolingual text – here, Indonesian-English code-mixed text to Indonesian-language text. We slightly modified the MLF approach used by Barik et al. by grouping neighbouring tokens with the same language in the text as one language segment; thus the translation is not performed for

each token, but for each segment, similar to the approach taken in [15]. Because Barik et al. separately applied translation to individual tokens, it potentially produces incorrect translation results since it prevents the MT system to know the correct context of the token. In our method, we added context to the MT by translating a group of neighboring tokens together. The use of language partitions serves as context during translation to improve translation results.

Given the code-mixed text input, we first determine the text's matrix and embedding languages. Neighboring tokens with similar language are then grouped to form one segment. Using MLF method, each segment from the embedding language is translated to the matrix language. If the embedding language is English and the matrix language is Indonesian, translate the English segment into Indonesian. If the embedding language is Indonesian and the matrix language is English, first translate the Indonesian segment into English, then translate the overall text into Indonesian (This is important because the goal of this work is to normalise Indonesian-English code-mixed text into Indonesian).

The difference between the MLF method used in previous work by Barik et al. and that used in this work is illustrated in Fig. 4. Previous work separately applied translation to individual tokens, which may result in translation errors. In our method, we added context to the MT by translating a sequence of tokens together. As shown in the figure, using our modified MLF, the English text "It is not that hard" is translated as a unit and produces an accurate translation result in Indonesian, whereas the MLF used in previous work produces a translation error as a result of translating each token separately.

B. Emotion Classification

The emotion classification process begins by preprocessing data using a code-mixed normalisation system. In this research, we compared two different classification systems. The first uses a classic approach, following the research in [18]. The second is a more modern approach based on deep learning.

The first system uses word embedding as a feature to represent each sentence. We take the average word embedding of all the tokens in a sentence as a feature when training the classifier model. Based on the results of previous research, we used the word embedding Word2Vec: a dense representation of a word based on its context [37]. This representation is obtained using a neural network that attempts to predict a word based on its context or vice-versa. We chose a word embedding size of 300 based on our early experimental results. The emotion classifier for the first system is SVM, based on the results in [18] as well as our early experimental results.

The second system fine-tunes a deep pretrained language model on emotion classification task. The popularity of deep pretrained language model has been on the rise since the original release of BERT [38]. Such model has been extensively researched, and have become the state of the art for many text-processing tasks, including classification. Deep pretrained language models are deep learning models (usually transformers) trained on a large corpus with tasks that the dataset can easily generate. For example, BERT is pretrained on a masked language model task and a next sequence prediction task (see

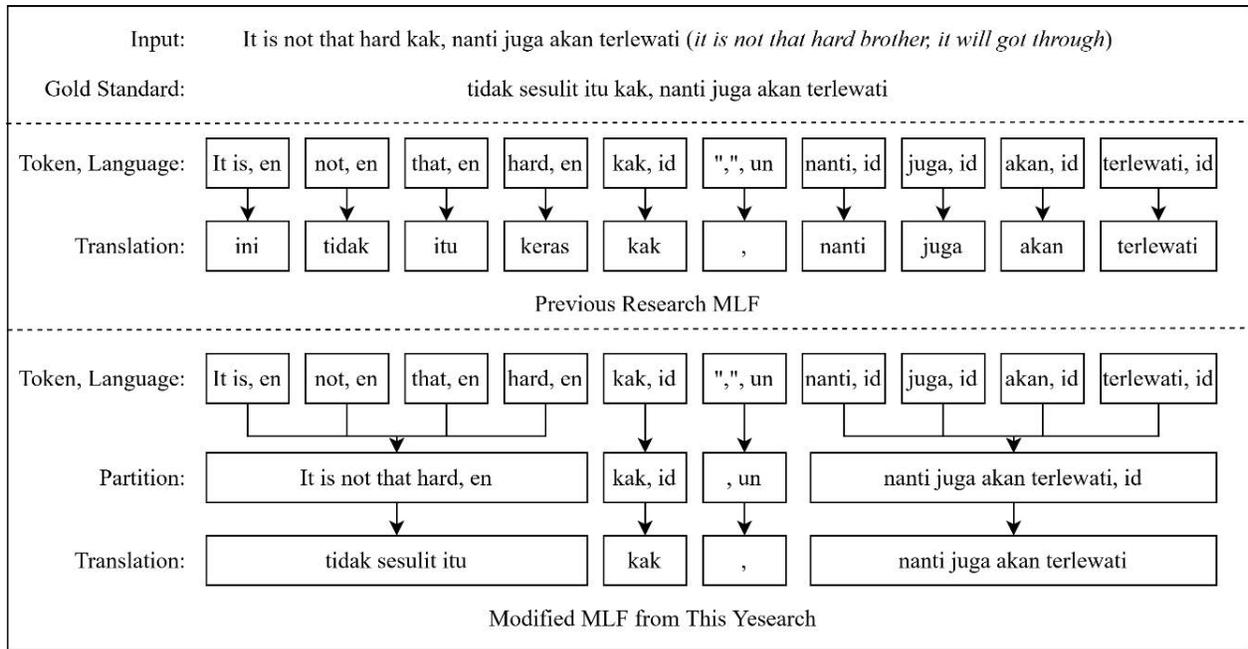


Fig. 4. Example of Indonesian-English Code-mixed Text.

TABLE IV. EXPERIMENT SCENARIO

No	Experiment	Baseline	Measure
1	Code-Mixed Normalisation (individual modules)		
	a. Language Identification	CRF [10], CNN, RNN, CNN+CRF	Accuracy, Precision, Recall, F_1 score
	b. Lexical Normalisation	raw data, ruleset + spell correction [10], SMT	BLEU, WER
	c. Translation	Direct translation, MLF[10]	BLEU, WER
2	Code-Mixed Normalisation (the whole pipeline)	raw data, Barik et al.'s system [10]	BLEU, WER
3	Using Code-mixed Normalisation for Emotion Classification	tokenisation-only, simple preprocessing	Accuracy, Precision, Recall, F_1 score

the original paper for a more in-depth explanation). The pre-trained language model used in this experiment is IndoBERT, a BERT-based model trained on Indonlu corpus (Indonesian corpus containing approximately four billion words) [39].

V. EXPERIMENT

Three experiments were performed in this research. All models in our experiments were trained with five-fold cross validation. Significance was measured using t-test with a 0.05 significance level. A summary of all of our experiments, including the baseline methods and evaluation measures, is presented in Table IV.

The **first experiment** separately tested the individual modules of the code-mixed text normalisation system. This experiment was performed to examine the effectiveness of our modifications to each module (except tokenisation, as we did not make any changes to the tokenisation module). During this experiment, the input for each module used gold-standard or reference data from the previous step in the pipeline. This

configuration makes it possible to safely assume that the input from the previous normalisation step is free of errors.

The modified language identification model is compared with four other models as baselines. They include the Conditional Random Field (CRF) model from Barik et al.'s work, Convolutional Neural Network (CNN) on character level [40], Recurrent Neural Network (RNN) [41], and CRF model using CNN as feature (CNN+CRF). The CNN architecture used in this work consist of one convolution layer and one fully connected layer. The CNN+CRF method replaces the fully connected layer with CRF.

Next, the modified lexical normalisation module is compared with three other models as baselines. They include using unprocessed input text (raw data), the combination of rule-based and spell correction model from Barik et al., and SMT model alone. We used SMT model alone as one of our baselines to analyse the effect of ruleset in our lexical normalisation module.

At last, the modified translation module is compared with two baselines: MLF method used by Barik et al., and direct translation method using machine translations. In direct translation method, we simply translate the Indonesian-English code-mixed text into Indonesian language using two popular machine translations: Microsoft³ and Google. Translate⁴

The **second experiment** tested the entire code-mixed text normalisation system to normalise the given Indonesian-English code-mixed text into Indonesian, which is the main goal of the system. The input for this experiment was code-mixed Indonesian-English tweets, which were put through the tokenisation, language identification, lexical normalisation,

³<https://translator.microsoft.com/>

⁴<https://translate.google.com/>

and translation modules, resulting in normalised Indonesian-language tweets. Baselines for this experiment included unprocessed input text (raw data), and the code-mixed normalisation pipeline system from Barik et al.'s work.

The **third experiment** performed emotion classification using a code-mixed text normalisation system to preprocess the data. The aim of this experiment was to analyse the effect of code-mixed normalisation on effectiveness in the emotion classification task. For this purpose, we compared the results of emotion classification methods that used code-mixed normalisation in the preprocessing step and the baseline methods that did not use code-mixed normalisation (tokenisation-only and simple preprocessing methods). In the tokenisation-only method, the tweets are simply tokenised before an emotion classification method is applied. We used Tweet-Tokenizer from NLTK library⁵ to perform this tokenisation. In the other baseline, i.e. simple preprocessing method, common preprocessing data methods including tokenisation, stopword removal, punctuation removal, and character repetition removal were performed. The stopword list for Indonesian and English languages were taken from NLTK library .

This research uses varieties of evaluation metrics to measure the system performance on each experiment. Accuracy, precision, recall, and F_1 score are common metrics to compare a set of labels between gold standard (reference) and the prediction from the model. In this work, they are used for evaluating language identification module in the first experiment, and emotion classification in the third experiment. Accuracy measures the rate of correct prediction over the entire test data. Precision measures how many predictions of a relevant classes that are actually correct. Recall measures how many relevant classes the model could find. F_1 score is a harmonic mean between precision and recall. The formula to calculate Accuracy, Precision, Recall, and F-1 measures are as follows:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \quad (1)$$

$$Precision = \frac{TP}{TP + FP} \quad (2)$$

$$Recall = \frac{TP}{TP + FN} \quad (3)$$

$$F_1 = \frac{2 * Precision * Recall}{Precision + Recall} \quad (4)$$

TP (True Positive) defines the correctly predicted positive values. TN (True Negative) defines the correctly predicted negative values. FP (False Positive) defines the value of incorrect positive predictions. FN (False Negative) defines the value of incorrect negative predictions.

Bilingual Evaluation Understudy (BLEU) and Word Error Rate (WER) are used to evaluate task that produce a correctness of a free form text compared to gold standard text. BLEU score measures the similarity of the text produced by the model and the gold standard. While this measure is

TABLE V. THE RESULTS OF LANGUAGE IDENTIFICATION EXPERIMENT

Model	Precision	Recall	F_1 score	Accuracy
CRF[10]	91.22	88.60	89.72	90.40
CNN	92.58	91.70	92.08	92.70
CNN+CRF	92.00	91.63	91.79	92.42
RNN	85.71	84.38	84.77	86.09
CRF++	94.56*†‡×	93.53*†‡×	93.98*†‡×	94.41*†‡×

Note: Significant differences of our method (CRF++) against CRF[10], CNN, CNN+CRF, and RNN are denoted by *, †, ‡, and ×, respectively.

commonly used for evaluating machine translation system, previous researches also use this metric to measure lexical normalisation performances that use machine translation [31], [42], [43]. Since there is translation task in our lexical normalisation module, translation module, and overall code-mixed text normalisation system, then we use BLEU for the experiments on these systems. WER measures how many edits (substitution, deletion, insertion) it takes from the predicted model to the gold standard with respect to the length of the gold standard text. In other words, WER measures the error of a system. This metric is commonly used on speech recognition task and expanded to measure performance on other task such as translation and lexical normalisation [42], [28]. The formula to calculate BLEU and WER are as follows:

$$BLEU = p * bp \quad (5)$$

$$WER = \frac{ed}{N} \quad (6)$$

BLEU score is computed by multiplying the geometric mean of the corpus precision scores (p) by the exponential brevity penalty factor (bp). For more detailed explanation, please refer to the original paper of BLEU metric [44]. WER is computed by taking the ratio between edit distance (ed) and the number of token in the reference text (N). Here, edit distance is measured by finding the minimum number of insertion, deletion, and substitution operations required to perform the alignment between the predictive text and the reference text.

VI. RESULTS AND ANALYSIS

A. Effectiveness of Individual Modules of Code-Mixed Normalisation System

1) *Results of Language Identification Module:* Table V shows the experimental results for the language identification module. The model created in this research achieved the highest score, outperforming the CRF model used by Barik et al. by 3.33% on precision, 4.92% on recall, 4.26% on F_1 score, and 4.01% on accuracy. This improvement comes from the new feature set for language identification. The deep learning baseline was unable to outperform our CRF++ model. The RNN model achieved the worst performance. One possible cause for this was the low amount of sequences in the training data. The data that the RNN processed included entire tweets or the whole sequence of a token, and there are only 825 tweets in the dataset. The same problem did not occur with the CNN model because CNN attempts to classify each token separately; thus the processed data are individual tokens. Note that there are 22,725 tokens available in the dataset.

⁵<https://www.nltk.org/>

TABLE VI. THE RESULTS OF LEXICAL NORMALISATION EXPERIMENT

Model	Precision	Recall
Raw Data	47.79	15.18
Ruleset+Spell Correction [10]	71.67	12.45
SMT	88.14	5.63
Ruleset+SMT	89.75*†‡	4.67*†‡

Note: Significant differences of our method (ruleset+SMT) against raw data, ruleset+spell correction [10], and SMT are denoted by *, †, and ‡, respectively.

Whilst the evaluation shows promising results, the CRF model in this research still has some difficulty classifying certain specific tokens (e.g. named entity tokens, such as a place or person) as either “id” or “en” when they should be labelled “un”. The model also often misclassifies Indonesian loan words that are taken from English words such as “stop” (“stop”). Loan words present ambiguity that makes it difficult for the model to correctly label the token. Another challenge for the model is sub-word code-mixing, which happens when Indonesian affixes are added to English words – for example, “gap-nya” (“the gap”). In this case, the correct label is the language of the root word, but sub-word code-mixed tokens are often misclassified as Indonesian rather than English.

2) *Results of Lexical Normalisation Module:* The results for the lexical normalisation module are shown in Table VI. The new model outperformed the Barik et al.’s model by 18.08 on BLEU score and 7.78 on WER. Raw data exhibited the worst performance, with 47.79 BLEU score and 15.18 WER. This result shows that our model is able to perform normalisation properly. Table VI also shows that the ruleset slightly helps the SMT model when performing lexical normalisation, increasing BLEU score by 1.61 higher and reducing WER by 1.04.

The SMT model can properly normalise ambiguous slang tokens that can serve as both a formal word and a slang word. This was a problem in Barik et al.’s model that relied on a formal lexicon to differentiate between formal and slang words. For example, the Indonesian word “aja” can serve as slang for the formal word “saja” (“only”), but may also be the formal word “aja”, an archaic way to refer to the daughter of a noble. The SMT model relies on the context of a word during the training process to normalise that word. Another problem in Barik et al.’s model is that the model was unable to properly normalise slang words that were very different from their formal versions. Their model normalised the slang word “ga” (“no”) into the letter “g”, but the actual formal version of this word is “tidak” (“no”). This occurred because Barik et al.’s model relied only on rules. However, our method, which uses SMT in addition to a ruleset, did not have this problem.

The problem with the SMT model is that it is fully supervised. Therefore, it is only able to normalise slang words that appear in the training phase and cannot process slang tokens that appear only during testing. This becomes a prominent issue in low-resource settings. However, the use of a ruleset enables our model to normalising some words that the SMT might have not encountered during training. This also explains why the combined model was able to achieve the best performances (see Table VI).

3) *Results of Translation Module:* Table VII presents the experimental results for the translation module. Google’s MT

TABLE VII. THE RESULTS OF TRANSLATION EXPERIMENT

Translation System	Model	BLEU	WER
Microsoft	Direct Translation	62.19	21.19
	MLF[10]	74.49	15.06
	MLF[10]+context	75.36*	14.36*
Google	Direct Translation	72.63	16.56
	MLF[10]	75.87	14.36
	MLF[10]+context	77.77*†	13.09*†

Note: Significant differences of our method (MLF[10]+context) against direct translation and MLF[10] are denoted by * and †, respectively.

TABLE VIII. THE RESULTS OF OVERALL CODE-MIXED NORMALISATION SYSTEM PIPELINE

Model	BLEU	WER
Raw Data	30.01	42.18
Barik et al.’s system [10]	48.86	28.18
Our System	64.55*†	18.65*†

Note: Significant differences of our method against raw data and Barik et al.’s system [10] are denoted by * and †, respectively.

system produced better translation results than Microsoft’s on every translation configuration. The modified MLF produced more accurate translation results than the baselines, achieving a BLEU score 1.9 higher and a WER 1.27 lower than the MLF method on Google’s MT system. Direct translation had the worst performance, with a BLEU score of 5.14 and WER of 3.47 on Google’s MT system. A similar result was observed when using Microsoft’s MT system.

This improvement shows that the use of a group of neighboring tokens or a language segment for translation process can produce more accurate translations than using individual token. The language segment provides sufficient context for the translation system to translate ambiguous words better than the original MLF used by Barik et al. However, our model still struggles to translate certain ambiguous words. For example, the English word “I” can be translated as either “saya” or “aku” in Indonesian; both have the same meaning, except that “saya” is often used in formal settings, whereas “aku” is often used in casual conversation.

B. Effectiveness of Overall Code-Mixed Normalisation System Pipeline

Table VIII shows the evaluation results for the code-mixed text normalisation system experiment. We used Google’s MT system for the translation module, following the results of the previous experiment. The new system demonstrated better code-mixed text normalisation performance compared with the Barik et al.’s system, increasing BLEU score by 15.69% absolute improvement or 32.11% relative improvement and lowering WER by 9.53% absolute improvement or 33.82% relative improvement. This indicates the effectiveness of our modifications on Barik et al.’s modules. Both code-mixed text normalisation systems outperformed the evaluation results for the raw data baseline, which highlight the merit of normalizing the code-mixed text.

To understand the contribution of each module modified in this work with regard to improving the code-mixed normalisation system pipeline proposed by Barik et al., we conducted an additional experiment using each of our individual modules in Barik et al.’s system. The increases or decreases resulting

TABLE IX. THE CONTRIBUTIONS OF EACH MODULE

Model	Δ BLEU	% Δ BLEU
Language Identification	2.03	4.15%
Lexical Normalisation	14.08	28.82%
Translation	15.69	32.11%

TABLE X. THE EXAMPLE OF RESULTS GENERATED BY OUR CODE-MIXED NORMALISATION SYSTEM AND BARIK ET AL.'S SYSTEM

Input	Argh gimana cara save gif nya. [URL] (Argh how to save the gif [URL])
Output from Barik et al.'s system [10]	
Tokenisation	Argh, gimana, cara, save, gif, nya, '.', [URL]
Language Identification	id, id, id, id, id, id, un, un
Lexical Normalisation	karuan, kenapa, cara, edit, klik, ya, '.', [URL]
Translation	karuan, kenapa, cara, edit, klik, ya, '.', [URL]
Output from our system	
Tokenisation	Argh, gimana, cara, save, gif, nya, '.', [URL]
Language Identification	id, id, id, en, en, id, un, un
Lexical Normalisation	argh, gimana, cara, save, gif, nya, '.', [URL]
Translation	argh, gimana, cara, simpan, gif, nya, '.', [URL]
Gold standard	argh, gimana, cara, menyimpan, gifnya, '.', [URL]

from this addition were then examined. For example, to see the contribution of our language identification module, we replaced Barik et al.'s language identification module with our module. The difference in BLEU scores (Δ BLEU) was calculated for the scores of Barik et al.'s system using our modules versus the original system. A positive contribution is indicated by a positive Δ BLEU score, whilst a negative contribution is indicated by a negative Δ BLEU score. The results are summarized in Table IX.

As shown in Table IX, all of our modules positively contributed to the Barik et al.'s code-mixed normalisation system pipeline, since all Δ BLEU scores are positive. The most important module is the translation module, which improved on Barik et al.'s system by 32.11%, followed by the lexical normalisation module (28.82% improvement) and the language identification module (4.15% improvement).

Table X compares the code-mixed text normalisation process for Barik et al.'s system and the new system implemented in this work. The former system detects the words "save" and "gif" as Indonesian words, whereas the latter properly detects them as English. Barik et al.'s system changes most tweets during lexical normalisation, leaving only "cara" ("method"), ".", and "[URL]" unchanged. The new system, however, did not perform any changes during lexical normalisation. Next, Barik et al.'s system does not perform any translation because all words are detected as Indonesian, whereas the new system translates "save gif" to "simpan gif". A comparison of both results indicates that the new system can produce results that are closer to the gold standard.

C. Effect of Code-Mixed Normalisation System on Emotion Classification

The result of emotion classification is presented in Table XI. The best overall result is achieved by using code-mixed normalisation in data preprocessing and the more modern approach with BERT. In terms of the results of using normalised code-mixed text, BERT is superior to Word2Vec by 16.56%

TABLE XI. THE RESULTS OF EMOTION CLASSIFICATION

Model	Preprocessing	Precision	Recall	F_1 Score	Accuracy
Word2Vec	TO	37.82	33.38	32.99	45.87
	SP	42.49	38.36	39.20	46.41
	CN	53.15* [†]	44.13*	45.44*	54.97* [†]
BERT	TO	45.85	43.98	43.92	50.33
	SP	47.82	45.21	45.92	50.34
	CN	54.06* [†]	51.44* [†]	51.93* [†]	56.84* [†]

Note: Significant differences of our emotion classification method using code-mixed normalisation (CN) as the preprocessing method against the methods that do not use code-mixed normalisation, but using tokenisation-only (TO) and simple preprocessing (SP) methods are denoted by * and [†], respectively.

TABLE XII. THE CLASSIFICATION RESULTS FOR EACH EMOTION CLASS

Class	Precision	Recall	F_1 score	Accuracy
Love	68.75	30.56	42.31	94.86
Anger	59.46	68.75	63.77	74.32
Sadness	46.84	35.92	40.66	81.51
Joy	54.58	70.81	61.64	72.09
Fear	37.04	14.71	21.06	87.16

according to F_1 score. In both models, the best performance is achieved when code-mixed normalisation is applied as a preprocessing step before classification. This demonstrates the advantage of normalizing the code-mixed text before a main text processing task is conducted. Two factors could explain this result: lexical normalisation and translation.

The tokenisation-only and simple preprocessing approaches did not have a robust lexical normalisation step. This may result in some key emotion words or phrases involving some informal token becoming out of vocabulary (OOV) or the words being incorrectly represented by both classification models. The performance gap between using versus not using code-mixed normalisation indicates that the classic method is more affected than the BERT model. This is because the BERT model uses a sub-word tokeniser and is able to handle OOV tokens to some degree. In this case, code-mixed normalisation improved the F_1 score and accuracy of the Word2Vec model by 37.74% and 19.77%, respectively. The improvement obtained by the BERT model is slightly lower: 18.24% for F_1 score and 12.93% for accuracy.

Some key emotion words are also written in English. This leads to better performance on classification systems which applied code-mixed text normalisation in the preprocessing step. It is because they translate these words into Indonesian and therefore enables us to capture their meanings.

Table XII presents a breakdown of classification results for each emotion class. Since our dataset has uneven class distribution, F_1 score is more representative than accuracy because the values of false positives and false negatives do not have similar cost. The highest F_1 score was obtained by the class "anger", followed by the class "joy". This can be understood because these classes have the highest number of tweets in our dataset. Consequently, the classifier can successfully learn the characteristics of tweets expressing the emotions anger and joy. Therefore, the ratios of correctly predicted labels for these classes to the total predicted labels and to the total actual labels for these classes are high.

To better illustrate the number of correct and incorrect classifications for each class, a confusion matrix is displayed in Fig. 5. The confusion matrix shows that imbalance in

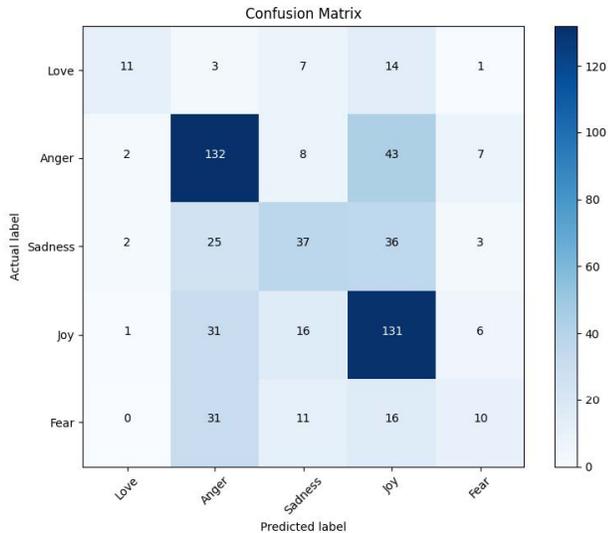


Fig. 5. Confusion Matrix of Emotion Classification Results.

TABLE XIII. EXAMPLE OF EMOTION CLASSIFICATION RESULTS

Input: Not good, not good.. Maag gue selalu kambuh sejak kerja di sini.. Setres (Not good, not good.. My ulcer always relapses since working here.. stress)
Gold standard class: Sad
Preprocessed input (TO): Not good , not good .. Maag gue selalu kambuh sejak kerja di sini .. Setres
Predicted class: Joy
Preprocessed input (SP): good good maag gue kambuh kerja setres
Predicted class: Fear
Preprocessed input (CN): tidak bagus , tidak bagus , . mag saya selalu kambuh sejak kerja di sini. setres
Predicted class: Sad

Note: TO, SP, and CN stands for "Tokenisation-Only", "Simple Preprocessing", and "Code-mixed Normalisation", respectively.

the dataset affects the emotion classification results. This can be seen from the two classes with the highest frequency of occurrence in our dataset, i.e. anger and joy, which showed a low proportion of false negatives and a high proportion of false positives relative to the total number of instances for these classes. The opposite happened for the emotion labels with the lowest frequency in our dataset, i.e. love and fear. Compared to other labels, both of these labels obtained the highest proportion of false negatives and the lowest proportion of false positives. The true positive values for these classes were also much lower than the false negative values.

In Table XIII, we demonstrate how different preprocessing methods may affect the classification results. Word2Vec was used to implement the classification model. According to the human annotation label, the input tweet expresses a sad emotion. This emotion is indicated by terms such as "not good", "selalu kambuh" ("always relapses"), "setres" ("stress").

A classification method using tokenisation-only preprocessing misclassifies the tweet's emotion as joy, presumably because the model cannot properly detect the emotion contained in the phrase "not good". Because this phrase is not translated into Indonesian and it may appear infrequently in the data, the Word2vec model is unable to learn the semantics of the phrase well, which may lead to an incorrect classification result. A classification method using simple preprocessing also

misclassifies the tweet's emotion as fear. This preprocessing method removes the term "not" from phrase "not good". This means that all tweets in the collection that contain the phrase "not [ADJECTIVE]" and "[ADJECTIVE]" will have similar preprocessing results for that phrase, even though they actually convey opposite emotions, since the term "not" indicates a contrast in meaning. We argue that this causes the model to be inaccurate in classifying the emotion. A classification method using a code-mixed text normalisation pipeline, on the other hand, can properly classify the tweet's emotion as sad. Translating the English phrase "not good" into the Indonesian phrases "tidak bagus" enables the Word2vec model to capture the semantics of the phrase since the translation phrase appears frequently in the collection.

VII. DISCUSSION AND FUTURE WORK

The number of code-mixed text used in this work is still relatively small when compared to the code-mixed text in other language pairs such as Bengali-English [45], Malayam-English [46], and Hindi-English [47]. Our dataset consists of 825 sentence pairs for our experiment on code-mixed normalisation and 584 sentences for our experiment on the effect of the code-mixed normalisation on emotion classification. Note that it is because a large dataset of Indonesian-English code-mixed text is still unavailable. The dataset from Barik et al. [10] that we use in this work is the only dataset of Indonesian-English code-mixed text that is available. Using this data also enables us to directly comparing our result with Barik et al. Therefore, further experiments using larger data may be useful to confirm the results reported in this work.

Our approach for code-mixed normalisation has some advantages compared to end-to-end deep learning approaches. Our approach does not require big data resources to achieve good results compared to deep learning methods. So, it is suitable for low-resource languages, such as Indonesian language. In addition, our approach is also more flexible in which users can easily add new rules or features in the individual modules of code-mixed normalisation system if needed.

The approach used in this task is aimed for code-mixed normalisation. However, each individual module in the pipeline can also be used separately for a specific task. For example, users can adopt the tokenisation module only if they just want to have more accurate tokenisation. Since our methods are mostly data driven (except the ruleset on lexical normalisation module), then with some tuning on the ruleset, we believe the individual modules as well as the overall system pipeline is applicable to other languages (or language pairs) as long as the data is available.

We are aware there are more modern methods that utilize Neural Machine Translation (NMT) model for lexical normalisation [48], [49]. However, we decided not to use this method because the dataset used in this research is too small for NMT to be able to learn an accurate model for this complex task. This effect has been demonstrated before by Matoz, et. al. [28] that utilizes RNN encoder-decoder to perform lexical normalisation on English-Dutch and Wibowo et. al.[32] that utilizes GPT-2 to normalise Indonesian text. Both of these research showed that on low resource settings, SMT model still gives on par performance if not better than the NMT model because of the insufficient amount of training data.

There are several avenues through which future research might improve on the results of our proposed system. The SMT model in the lexical normalisation module could be improved by using an additional corpus for the language model. A large dataset could be built containing formal Indonesian-English code-mixed text to improve the accuracy of the lexical normalisation module. Another possible improvement that could be made to the lexical normalisation module involves the ruleset. The ruleset used in this work are still limited for normalising informal Indonesian words that contain character repetitions and reduplication shortening; and informal English words that contain contractions and code-mixed prefixes / suffixes. Therefore, some extra rules can be added to improve the accuracy of the lexical normalization module in our system. An example of additional rules could be derived from informal affixes that are common in Indonesian, such as the informal suffixes “-ny” or “-x”, which can be converted to “-nya” and then prefix “ng-”, which can be converted to “meng-”.

Next, in this research, the effect of code-mixed normalisation was examined for an emotion classification task. Whilst the results showed a positive effect, this cannot be generalised to many other language processing tasks. Thus, similar analysis could be performed for other tasks – such as sentiment analysis, POS tagging and so on – to examine whether performing code-mixed normalisation can offer significant improvement for these tasks as well.

VIII. CONCLUSION

In this research, we improved a state-of-the-art code-mixed text normalisation system for Indonesian-English tweets. Specifically, we improved three modules of the original code-mixed normalisation system pipeline, including improving the feature set in the language identification module, combining an MT approach and a ruleset in the lexical normalisation module and adding some context in the translation module. Our experimental results show that our approach outperformed a state-of-the-art Indonesian-English code-mixed normalisation system. The new feature set in the language identification module showed an improvement of 4.26% in F_1 score. The use of an MT approach in the lexical normalisation module improved BLEU score by 25.22% and lowered WER by 62.49%. The addition of context to the translation process improved BLEU score by 2.5% and lowered WER by 8.84%. The overall effectiveness of the code-mixed text normalisation system was improved, with an increase of 32.11% in BLEU score and a decrease of 33.82% in WER.

This research also analysed the effect of code-mixed text normalisation process on emotion classification. Applying code-mixed normalisation process resulted in increased effectiveness of emotion classification systems. The systems that used code-mixed normalisation in the preprocessing step were more effective than those that did not. Compared with tokenisation-only preprocessing method, the code-mixed normalisation system achieved better evaluation results by up to 37.74% in F_1 score. The code-mixed normalisation system also outperformed a simple preprocessing method by up to 15.92% in F_1 score.

ACKNOWLEDGMENTS

This research is supported by the PUTI (Publikasi Terindeks Internasional) Q3 grant with number NKB-4379/UN2.RST/HKP.05.00/2020 from Universitas Indonesia.

REFERENCES

- [1] S. Poplack and J. A. Walker, “Pieter muysken, bilingual speech: a typology of code-mixing. cambridge: Cambridge university press, 2000. pp. xvi+ 306.” *Journal of Linguistics*, vol. 39, no. 3, pp. 678–683, 2003.
- [2] K. Bali, J. Sharma, M. Choudhury, and Y. Vyas, ““i am borrowing ya mixing?” an analysis of english-hindi code mixing in facebook,” in *Proceedings of the First Workshop on Computational Approaches to Code Switching*, 2014, pp. 116–126.
- [3] L. S. Kia, X. Cheng, T. K. Yee, and C. W. Ling, “Code-mixing of english in the entertainment news of chinese newspapers in malaysia,” *International journal of English linguistics*, vol. 1, no. 1, p. 3, 2011.
- [4] K. Ariffin and M. Susanti Husin, “Code-switching and code-mixing of english and bahasa malaysia in content-based classrooms: Frequency and attitudes.” *Linguistics Journal*, vol. 5, no. 1, 2011.
- [5] E. Syam *et al.*, “Code switching by an indonesian muslim preacher,” in *7th International Conference on English Language and Teaching (ICOELT 2019)*. Atlantis Press, 2020, pp. 18–22.
- [6] D. Rusydah, “Bahasa anak jaksel: A sociolinguistics phenomena,” *LITERA KULTURA*, vol. 8, no. 1, 2020.
- [7] M. Dhar, V. Kumar, and M. Shrivastava, “Enabling code-mixed translation: Parallel corpus creation and mt augmentation approach,” in *Proceedings of the First Workshop on Linguistic Resources for Natural Language Processing*, 2018, pp. 131–140.
- [8] Q. Zhang, H. Chen, and X. Huang, “Chinese-english mixed text normalization,” in *Proceedings of the 7th ACM international conference on Web search and data mining*, 2014, pp. 433–442.
- [9] M. A. Menacer, D. Langlois, D. Jouvet, D. Fohr, O. Mella, and K. Smaili, “Machine translation on a parallel code-switched corpus,” in *Canadian Conference on Artificial Intelligence*. Springer, 2019, pp. 426–432.
- [10] A. M. Barik, R. Mahendra, and M. Adriani, “Normalization of indonesian-english code-mixed twitter data,” in *Proceedings of the 5th Workshop on Noisy User-generated Text (W-NUT 2019)*, 2019, pp. 417–424.
- [11] R. van der Goot and Ö. Çetinoğlu, “Lexical normalization for code-switched data and its effect on pos tagging,” in *Proceedings of the 16th Conference of the European Chapter of the Association for Computational Linguistics: Main Volume*, 2021, pp. 2352–2365.
- [12] R. Singh, N. Choudhary, and M. Shrivastava, “Automatic normalization of word variations in code-mixed social media text,” *arXiv preprint arXiv:1804.00804*, 2018.
- [13] D. Patel and R. Parikh, “Language identification and translation of english and gujarati code-mixed data,” in *2020 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)*. IEEE, 2020, pp. 1–4.
- [14] C. Myers-Scotton, *Duelling languages: Grammatical structure in codeswitching*. Oxford University Press, 1997.
- [15] S. K. Mahata, S. Mandal, D. Das, and S. Bandyopadhyay, “Code-mixed to monolingual translation framework,” in *Proceedings of the 11th Forum for Information Retrieval Evaluation*, 2019, pp. 30–35.
- [16] J. Gao, Y. Fu, Y.-G. Jiang, and X. Xue, “Frame-transformer emotion classification network,” in *Proceedings of the 2017 ACM International Conference on Multimedia Retrieval*, 2017, pp. 78–83.
- [17] M. Grimm and K. Kroschel, “Rule-based emotion classification using acoustic features,” in *Proc. Int. Conf. on Telemedicine and Multimedia Communication*. Citeseer, 2005.
- [18] M. S. Saputri, R. Mahendra, and M. Adriani, “Emotion classification on indonesian twitter dataset,” in *2018 International Conference on Asian Language Processing (IALP)*. IEEE, 2018, pp. 90–95.
- [19] Y.-P. Lin, C.-H. Wang, T.-P. Jung, T.-L. Wu, S.-K. Jeng, J.-R. Duann, and J.-H. Chen, “Eeg-based emotion recognition in music listening,” *IEEE Transactions on Biomedical Engineering*, vol. 57, no. 7, pp. 1798–1806, 2010.

- [20] P. Ekman, "An argument for basic emotions," *Cognition & emotion*, vol. 6, no. 3-4, pp. 169–200, 1992.
- [21] P. Shaver, J. Schwartz, D. Kirson, and C. O'connor, "Emotion knowledge: further exploration of a prototype approach." *Journal of personality and social psychology*, vol. 52, no. 6, p. 1061, 1987.
- [22] R. Plutchik, "A general psychoevolutionary theory of emotion," in *Theories of emotion*. Elsevier, 1980, pp. 3–33.
- [23] J. Li, Y. Xu, H. Xiong, and Y. Wang, "Chinese text emotion classification based on emotion dictionary," in *2010 IEEE 2nd Symposium on Web Society*. IEEE, 2010, pp. 170–174.
- [24] S. M. Mohammad and P. D. Turney, "Crowdsourcing a word–emotion association lexicon," *Computational intelligence*, vol. 29, no. 3, pp. 436–465, 2013.
- [25] A. Agrawal and A. An, "Unsupervised emotion detection from text using semantic and syntactic relations," in *2012 IEEE/WIC/ACM International Conferences on Web Intelligence and Intelligent Agent Technology*, vol. 1. IEEE, 2012, pp. 346–353.
- [26] A. Das and B. Gambäck, "Identifying languages at the word level in code-mixed indian social media text," in *Proceedings of the 11th International Conference on Natural Language Processing*, 2014, pp. 378–387.
- [27] J. R. Landis and G. G. Koch, "The measurement of observer agreement for categorical data," *biometrics*, pp. 159–174, 1977.
- [28] C. M. Veliz, O. De Clercq, and V. Hoste, "Comparing mt approaches for text normalization," in *Proceedings of the International Conference on Recent Advances in Natural Language Processing (RANLP 2019)*, 2019, pp. 740–749.
- [29] A. Kurnia and E. Yulianti, "Statistical machine translation approach for lexical normalization on indonesian text," in *2020 International Conference on Asian Language Processing (IALP)*. IEEE, 2020, pp. 288–293.
- [30] E. Yulianti, I. Budi, A. N. Hidayanto, H. M. Manurung, and M. Adriani, "Developing indonesian-english hybrid machine translation system," in *2011 International Conference on Advanced Computer Science and Information Systems*. IEEE, 2011, pp. 265–270.
- [31] A. Aw, M. Zhang, J. Xiao, and J. Su, "A phrase-based statistical model for sms text normalization," in *Proceedings of the COLING/ACL 2006 Main Conference Poster Sessions*, 2006, pp. 33–40.
- [32] H. A. Wibowo, T. A. Prawiro, M. Ihsan, A. F. Aji, R. E. Prasoj, R. Mahendra, and S. Fitriany, "Semi-supervised low-resource style transfer of indonesian informal to formal language with iterative forward-translation," in *2020 International Conference on Asian Language Processing (IALP)*. IEEE, 2020, pp. 310–315.
- [33] P. Koehn, H. Hoang, A. Birch, C. Callison-Burch, M. Federico, N. Bertoldi, B. Cowan, W. Shen, C. Moran, R. Zens *et al.*, "Moses: Open source toolkit for statistical machine translation," in *Proceedings of the 45th annual meeting of the association for computational linguistics companion volume proceedings of the demo and poster sessions*, 2007, pp. 177–180.
- [34] F. J. Och and H. Ney, "A systematic comparison of various statistical alignment models," *Computational linguistics*, vol. 29, no. 1, pp. 19–51, 2003.
- [35] K. Heafield, "Kenlm: Faster and smaller language model queries," in *Proceedings of the sixth workshop on statistical machine translation*, 2011, pp. 187–197.
- [36] C. Cherry and G. Foster, "Batch tuning strategies for statistical machine translation," in *Proceedings of the 2012 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies*, 2012, pp. 427–436.
- [37] T. Mikolov, K. Chen, G. Corrado, and J. Dean, "Efficient estimation of word representations in vector space," *arXiv preprint arXiv:1301.3781*, 2013.
- [38] J. Devlin, M.-W. Chang, K. Lee, and K. Toutanova, "Bert: Pre-training of deep bidirectional transformers for language understanding," in *Proceedings of the 2019 Conference of the North American Chapter of the Association for Computational Linguistics: Human Language Technologies, Volume 1 (Long and Short Papers)*, 2019, pp. 4171–4186.
- [39] B. Wilie, K. Vincentio, G. I. Winata, S. Cahyawijaya, X. Li, Z. Y. Lim, S. Soleman, R. Mahendra, P. Fung, S. Bahar *et al.*, "Indonlu: Benchmark and resources for evaluating indonesian natural language understanding," in *Proceedings of the 1st Conference of the Asia-Pacific Chapter of the Association for Computational Linguistics and the 10th International Joint Conference on Natural Language Processing*, 2020, pp. 843–857.
- [40] X. Zhang, J. Zhao, and Y. LeCun, "Character-level convolutional networks for text classification," *Advances in neural information processing systems*, vol. 28, pp. 649–657, 2015.
- [41] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
- [42] D. Contractor, T. A. Faruque, and L. V. Subramaniam, "Unsupervised cleansing of noisy text," in *Coling 2010: Posters*, 2010, pp. 189–196.
- [43] B. Han and T. Baldwin, "Lexical normalisation of short text messages: Mkn sens a# twitter," in *Proceedings of the 49th annual meeting of the association for computational linguistics: Human language technologies*, 2011, pp. 368–378.
- [44] K. Papineni, S. Roukos, T. Ward, and W.-J. Zhu, "Bleu: a method for automatic evaluation of machine translation," in *Proceedings of the 40th annual meeting of the Association for Computational Linguistics*, 2002, pp. 311–318.
- [45] S. Mandal, S. K. Mahata, and D. Das, "Preparing bengali-english code-mixed corpus for sentiment analysis of indian languages," in *The 13th Workshop on Asian Language Resources*, 2018, p. 57.
- [46] B. R. Chakravarthi, N. Jose, S. Suryawanshi, E. Sherly, and J. P. McCrae, "A sentiment analysis dataset for code-mixed malayalam-english," *arXiv preprint arXiv:2006.00210*, 2020.
- [47] P. Makhija, A. Srivastava, and A. Gupta, "hinglishnorm-a corpus of hindi-english code mixed sentences for text normalization," in *Proceedings of the 28th International Conference on Computational Linguistics: Industry Track*, 2020, pp. 136–145.
- [48] M. Lusetti, T. Ruzsics, A. Göhring, T. Samardzic, and E. Stark, "Encoder-decoder methods for text normalization," in *Proceedings of the Fifth Workshop on NLP for Similar Languages, Varieties and Dialects (VarDial 2018)*, 2018, pp. 18–28.
- [49] B. Muller, B. Sagot, and D. Seddah, "Enhancing bert for lexical normalization," in *The 5th Workshop on Noisy User-generated Text (W-NUT)*, 2019.

Sign Language Gloss Translation using Deep Learning Models

Mohamed Amin, Hesahm Hefny, Ammar Mohammed
Department of Computer Science
FGSSR, Cairo University, Egypt

Abstract—Converting sign language to a form of natural language is one of the recent areas of the machine learning domain. Many research efforts have focused on categorizing sign language into gesture or facial recognition. However, these efforts ignore the linguistic structure and the context of natural sentences. Traditional translation methods have low translation quality, poor scalability of their underlying models, and are time-consuming. The contribution of this paper is twofold. First, it proposes a deep learning approach for bidirectional translation using GRU and LSTM. In each of the proposed models, Bahdanau and Luong’s attention mechanisms are used. Second, the paper experiments proposed models on two sign languages corpora: namely, ASLG-PC12 and Phoenix-2014T. The experiment conducted on 16 models reveals that the proposed model outperforms the other previous work on the same corpus. The results on the ASLG-12 corpus, when translating from text to gloss, reveal that the GRU model with Bahdanau attention gives the best result with ROUGE (Recall-Oriented Understudy for Gisting Evaluation) score 94.37% and BLEU (Bilingual Evaluation Understudy)-4 score 83.98%. When translating from gloss to text, the results also show that the GRU model with Bahdanau attention achieves the best result with ROUGE score 87.31% and BLEU-4 66.59%. On Phoenix-2014T corpus, the results of text to gloss translation show that the GRU model with Bahdanau attention gives the best result in ROUGE with a score of 42.96%, while the GRU model with Luong attention gives the best result in BLEU-4 with 10.53%. When translating from gloss to text, the results report that the GRU model with Luong attention achieves the best result in ROUGE with a score of 45.69% and BLEU-4 with a score of 19.56%.

Keywords—Sequence to sequence model; neural machine translation; sign language; deep learning; LSTM; GRU

I. INTRODUCTION

Sign languages is a visual-gesture based language considered to be the standard language for the deaf. This language operates through gestures and visual channels [1]. In sign languages, hand gestures, facial expressions, and body movements are used for communication. According to the World Health Organization¹, around 466 million people worldwide have hearing impairments, out of which 34 million are children. It is estimated that by 2050 over 900 million people will have hearing impairments or difficulties in communication [2].

Also, it is estimated that there are almost 121 types of sign language used worldwide today [3] with less than sufficient number of sign language interpreters to deal with the diversity of sign languages. Hence, there is a need for developing translation systems that make the translation process faster and

more accurate. The first step toward automating the translation is to formalize the sign language in standard form. There are existing several forms of sign languages including Stokoe [4], HamNoSys [5], SignWriting [6], and Gloss Notation [7]. Stokoe notation does not include facial expressions and body movements. Thus, this sign language is limited and is not suitable for translation to the deaf. Furthermore, the HamNoSys form is designed to formalize any sign language using 3D animated avatar. However, it does not provide any easy way for describing facial expressions and body movements. The SignWriting notation uses highly iconic symbols, but is difficult to analyze with a computer. Gloss notation [7] on the other hand is a formal sign language that is similar to Braille, finger-spelling, and Morse code. It is used to annotate, represent, and describe sequences of visual-gestural language sequences based on labels on natural language words. This form is a straightforward way that conveys the idea expressed in a natural language, in sign languages. For its simplicity, expressiveness, and formal representation of sign language, glossing has attracted considerable research attention in sign language translation [8], [9], [10], [3].

Several studies have been proposed to translate sign languages to natural languages. Those efforts can be categorized into rule-based [11], [12], example-based [13], [14], [15] and statistical-based approach [8], [9], [10], [3]. However, those previous forms are limited in terms of the translation quality and need extra human efforts. For example, the rule-based approach needs domain knowledge of linguistic experts that will be responsible for analyzing the sign language, performing natural language processing tasks, and generating translation rules. Also, natural language processing adds extra complexity as it has many exceptional cases needed to cover using rules. Hence, the number of generated rules is increased. In contrast, example-based machine translation relies on large parallel aligned corpora. It tries to match input sentences with relevant retrieved sentences in a specific corpus. The shortcomings of this translation approach is that it needs massive use-cases to match the input with similar retrieved cases. Also, retrieving similar cases is inefficient and time-consuming [16]. In the statistical approach, translations are generated based on a statistical-based model whose parameters are derived from the analysis of bilingual text corpora. However, this approach needs a large parallel aligned corpus. Moreover, building a corpus with preprocessing tasks is expensive and time-consuming, and it requires collaboration with computer scientists, translators, and linguists. The full process consumes much time. Additionally, the statistical-based approach is tedious to fix mistakes of the translation system, and the precision of translation might become superficial. [17].

¹<https://www.who.int/news-room/fact-sheets/detail/deafness-and-hearing-loss>

In contrast to traditional methods, machine and deep learning have shown great success in several application domains for years [18], [19], [20]. Several researchers have shown interest in the study of machine translation for translating sign languages using a neural network [21], [22], [23], [24], [25]. The recent translation approach based on neural networks is the Neural Machine Translation (NMT) [26], [27] It is an end-to-end learning approach for an automated translation [28]. It consists of two parts: encoder and decoder. To enhance the learning process, an attention mechanism [27] has been lately proposed to allow a neural network to pay attention to only a specific part of an input sentence while generating a translation similar to that of human translations. Although NMT approaches are successful compared to the traditional machine translation approaches, most neural-based studies ignore the sign language's linguistic properties. They assume that there is only a one-to-one mapping of sign-to-spoken words. Additionally, most of the current neural machines focus on the translation from the gloss sign language to the natural language. However, the second direction from natural language to gloss sign language is important to fully automate the translation systems in both directions.

The primary contributions of this paper can be summarized as follows: First, it proposes a sequence-to-sequence deep learning models using LSTM [29] and GRU [30] that translate gloss sign language to natural language text. Second, it introduces a sequence-to-sequence deep learning model that translates natural language text to sign language gloss. In both directions, deep learning models use Bahdanau [27] and Luong [31] attention mechanisms. Third, this paper experiments the proposed models on two different corpora: ASLG-PC12 [32], [33] and Phoenix-2014T [21]. The performance of the results is evaluated using different metrics, e.g., BLEU (Bilingual Evaluation Understudy) and ROUGE (Recall-Oriented Understudy for Gisting Evaluation) scores. Also, the best model of the experiments is compared to similar work on the same corpus.

The rest of the paper is organized as follows: Section II presents a brief background on sign languages. Section III discusses several related works. Section IV introduces the proposed approach. Section V discusses the experimental results. Finally, section VI concludes the paper.

II. BACKGROUND

This section briefly introduces the concept of sign language and machine translation.

A. Sign Language

Sign languages are languages that apply the visual-manual form to convey meaning [34]. The articulators of sign languages are different compared to spoken languages. The primary articulators in spoken languages are the throat, nose, and mouth, whereas the main articulators in sign languages are the fingers, hands, and arms. There are several linguistic features of sign language, and one of those common features is the so-called non-manual feature. The later feature is a parameter of a sign that has meaning. It is not made with hands. but with facial expression, eyebrow movement, movement of the eyes/cheeks, mouth patterns, tilting of the head, movement of the upper body, and shoulder movements. It should be noted

that without a non-manual feature, a sign language statement will be meaningless regardless of whether the syntax is in the proper order. Sign language relies on non-manual signals to convey the difference between declarative, imperative, and interrogative sentences.

Furthermore, sign language can be expressed using different ways like Stokoe [4], HamNoSys [5], SignWriting [6], and Gloss Notation [7]. Stokoe, HamNoSys, and SignWriting are iconic representations for a sign language that are hard to read and interpret by deaf people, as translation systems use them to generate 3D animations.

On the contrary, Gloss notation is used to annotate, represent, and describe sequences of signs in a visual-gestural language based on labels-words. It is an interlinear translation used by linguists for transcription. Also learners of sign languages for analysis also use it. The gloss notation is considered an effective way to focus on the grammar and word order, which separates it from the vocabulary. Also gloss notation is written above the natural words using CAPITAL letters. Table I shows pairs of (English, American sign language) sentences.

TABLE I. ENGLISH AND AMERICAN SIGN LANGUAGE PAIRS

English Sentences	ASL Gloss
What is your name?	NAME YOU WHAT ^{WH}
He doesn't like pizza.	PIZZA IX-boy DOESN'T-LIKE
Help me.	HELP-ME (one sign)
See you later.	SEE-YOU-LATER (one sign)
Don't know.	DON'T-KNOW (one sign)
Today is Friday, October 28th.	NOW+DAY FRIDAY fs-OCT 28

B. Machine Translation

Early work on machine translation used traditional approaches like rule-based, example-based, and statistical-based. However, these approaches are inefficient in terms of the quality of translation, the limitation of their underlying models, and the exerted efforts of human domain experts. Recently, NMT [26], [27] approach has achieved great progress in machine translation. It is an end-to-end learning approach for automated translation[26].

There are many factors that make NMT performance exceed other traditional approaches [28] First, NMT optimizes all the translation learning parameters simultaneously to automatically decrease network output loss. Second, it has distributed representations with many improvements by sharing statistical strengths among similar words or phrases. Third, it can exploit the context of translations better. The more source and target text, the bigger context that NMT can learn. Thus, NMT is more efficient and has better quality than other approaches.

One of the NMT approaches is a sequence-to-sequence model implemented as a coupled network of encoder and decoder with attention mechanism [27]. In this model, a source sentence $x = \{x_1, x_2, \dots, x_I\}$ of length I words is given, The model converts this sentence into a target sentence $y = \{y_1, y_2, \dots, y_J\}$.

The encoder network is responsible for converting source sequences into a list of vectors, one vector per input. whereas the decoder network is responsible for generating one symbol

at a time until the special end-of-sentence symbol. In what follows, we briefly describe the encoder and decoder network.

The encoder network can be encoded as a Recurrent Neural Network (RNN) function. It takes the input x_i and a previous hidden state h_{i-1} , and then generates a current hidden state h_i . Without an attention mechanism, the encoder generates a context vector representing the input sentence. The later context vector is fed to the decoder in the first-time step. However, in the consequent time steps, the decoder forgets the context vector. To remedy the forgotten part, either the context vector is copied to each time step in the decoder or to use an attention mechanism. The later mechanism is better as it focuses on the important part in the input sentence [35].

The decoder network, on the other hand, is represented by a function RNN, The RNN takes an input as the decoder hidden state s_{j-1} , the context vector c_j , and the output of the previous time step y_{j-1} , and then generates the current state s_j . Finally, to generate the output, the hidden states s_j are squashed by a non-linear function g , which is passed to the softmax function to calculate the probabilities.

III. RELATED WORKS

Recently, there have been many research efforts to automate sign language translations. Those efforts depend on several types of algorithms and machine translation approaches.

Similar to the work proposed in this paper, several authors used neural machine translation of sign languages. For example, the authors in [21] presented a neural sign Language translation that translates gloss sign language to natural language. In their work, they applied sequence-to-sequence neural model and experimented their results on phoenix-2014T² corpus. Their proposed GRU model with Luong attention mechanism achieved BLEU on the range of 1 to 4 grams with scores 44.13%, 31.47%, 23.89%, and 19.26% respectively, and ROUGE score 45.45%.

Another similar work that used sequence-to-sequence model was reported in [23]. The authors proposed to translate gloss sign language into text. They used ASLG-PC12 corpus on several network architectures for their experiments with three different attention functions: dot, general, and concat. The evaluation of BLEU score on the range of 1 to 4 gram achieved are 86.70%, 79.50%, 73.20%, and 65.90% using GRU with dot attention function hidden size 800 units.

Similarly, the authors in [24] proposed a sequence-to-sequence translation model based on human key point estimation. In their work, they build KETI sign language corpus [24], which consists of 14,672 videos of high resolution and quality with the corresponding gloss translation. The corpus was divided into 64% training set, 7% development set, 29% test set. Their model based on a sequence-to-sequence model based on GRU cells achieved an accuracy score of 55.28%, a BLEU score of 52.63%, and a ROUGE score of 63.53 on gloss level.

Furthermore, the authors in [36] proposed sign language transformers: joint end-to-end sign language recognition and translation. They experimented their proposed work

on Phoenix-2014T dataset, The evaluation of their proposed model with BLEU scores are 48.9%, 36.88%, 29.45%, 24.54%

Also, the authors in [22] proposed a translation system based on transformers models. They experimented their proposed work on Phoenix-2014T [21] and ASLG-PC12 [32], [33] corpora. The evaluation of their proposed model on Phoenix-2014T achieved BLEU on the range of 1 to 4 grams with scores 48.40%, 36.90%, 29.70% and 24.90% using Transformer on Phoenix-2014T dataset. Moreover, they achieved BLEU scores of 92.88%, 89.22%, 85.95% and 82.87% using Transformer on ASLG-PC12.

Also the author in [37] proposed Sign Language Semantic Translation System using Ontology and Deep Learning. Where CNN trained model used in the recognition process with adding the semantic layer. Collected signs of 10 Arabic gestures and their meanings in English and French sign languages used in training and testing the system.

Despite the success of the previous neural network translation approaches except this paper, most of these approaches, however, focus on one direction-translation, particularly from gloss sign language to natural language.

IV. PROPOSED APPROACH

This section shows the proposed approach that translates from natural language text to gloss sign language and vice versa. The proposed approach is divided into two directions. The first direction translates text to gloss notation, while the second direction translates from gloss notation to text. We describe the details of each direction as follows.

A. Text to Gloss Notation Approach

In the text to gloss notation approach, shown in Fig. 1, the input text is fed to the NMT, which translates the text to gloss notation. The NMT consists of two phases, preprocessing and encoding-decoding phase.

In the preprocessing phase natural language processing occurs as Convert natural language text to lowercase and convert gloss notation to uppercase, Stripe whitespaces, and remove numbers and punctuation. Then text is embedded into continuous vector space. The second phase consists of an encoder-decoder neural network model augmented with an attention mechanism that translates the embedded text into gloss notation language. The neural network of the last phase consists of an encoder and decoder. Generally, the encoder transforms a source sentence into a list of vectors, one vector per input symbol. Given this list of vectors, the decoder produces one symbol at a time until the special end-of-sentence symbol (EOS) symbol is produced. The encoder and decoder are connected through the attention model. The attention model allows a neural network to pay attention to only part of an input sentence while generating a translation, similar to the human translator.

B. Gloss to Text Approach

The second direction of the proposed approach is shown in Fig. 2.

²<https://www-i6.informatik.rwth-aachen.de/koller/RWTH-Phoenix-2014-T/>

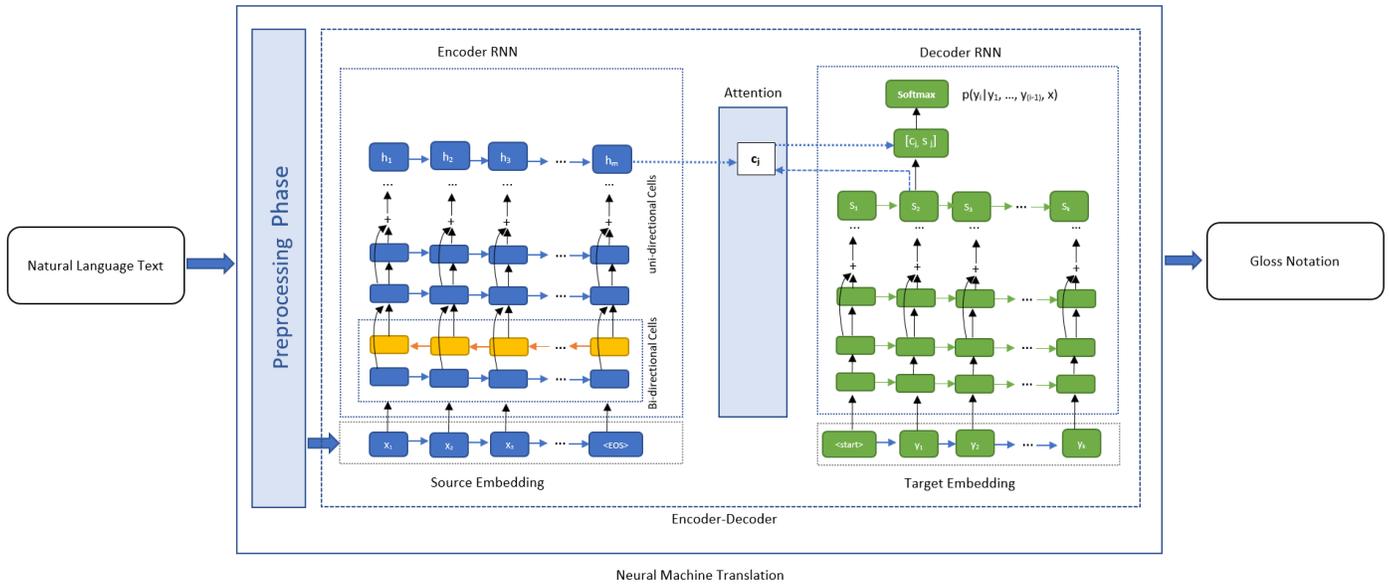


Fig. 1. Natural Language Text to Sign Language Gloss Model.

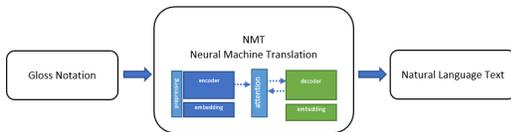


Fig. 2. Sign Language Gloss to Natural Language Text Model.

Here The main task is to translate gloss notation into text. First, the machine translation component receives a gloss notation and performs natural language preprocessing tasks on the gloss notation where the gloss is embedded on a continuous vector space. Second, the embedded gloss is then passed through an encoder-decoder neural network augmented with an attention mechanism that translates the embedded gloss into text. The architecture of the encoder and decoder is like the one in Fig. 1.

V. EXPERIMENTAL RESULTS

This section shows the experimental results of the proposed approach on two corpora: namely, ASL-PC12 and Phoenix-2014T. We begin by describing the details of each corpus before showing the results. In each corpus, we describe data splitting criteria that are used in the experiments. We described the criteria of each corpus using the following terms: sentence, Running words, vocabulary size, Singletons, and Out of Vocabulary (OOV). Sentences represents number of examples that exist in the corpus. The Running words stands for the number of words in the corpus. Vocabulary size is several tokens that measure how many words a particular model knows. Singletons represents the number of those words that occur only once in the training set. OOV expresses the number of words that occur in test data, but not in training data.

The first corpus, ASLG-PC12, was proposed in [32], [33]

as a big parallel corpus between English written texts and American Sign Language Gloss. The ASLG-PC12 is a bilingual corpus of 87,710 sentences. The total number of "running words" is 1,027,100 for English words and 906,477 for gloss words in addition to 4,662 singletons for English words and 6,561 singletons for gloss words. The vocabulary of both sign gloss annotation and spoken language are 16,788, and 12,344, respectively. In the experiments, we split the corpus into 52,626 sentences for training in the experiments, 17,542 sentences for validation, and 17,542 sentences for testing. Table II describes the statistics of the corpus.

TABLE II. KEY STATISTICS OF ASLG-PC12

	English			Gloss		
	Train	Dev	Test	Train	Dev	Test
Sentences	52,626	17,542	17,542	52,626	17,542	17,542
Running Words	610,129	207,760	209,211	538,681	183,242	184,554
Vocab Size	16,788	10,121	10,264	12,344	7,470	7,571
Singletons	4,662	-	-	6,561	-	-
OOV	-	2,671	3,027	-	1,949	2,330

The second corpus, Phoenix-2014T, is the German sign language of weather-forecast news. Phoenix-2014T [21] is an extended version of the continuous sign language recognition benchmark dataset found in [38]. It is a gloss annotation, video segments, and spoken language translations matching the sign language. It contains 8257 sequences with 9 different signers. The total running words is 113,717 for German words and 75,786 for gloss words. Additionally, it contains 1077 singletons for German words and 337 singletons for gloss words. The vocabulary of both sign gloss annotation and spoken language are 1236 and 2892 respectively. In the experiments, we split the corpus into 7,096 sentences for training in the experiments, 519 sentences for validation, and 642 sentences for testing. Table III describes the statistics of the corpus.

TABLE III. KEY STATISTICS OF PHOENIX-2014T

	German			Gloss		
	Train	Dev	Test	Train	Dev	Test
Sentences	7,096	519	642	7,096	519	642
Running Words	99,081	6,820	7,816	67,781	3,748	4,257
Vocab. Size	2,892	956	1006	1,236	397	415
Singletons	1077	-	-	337	-	-
OOV	-	57	60	-	19	22

A. Results

The experimental results are reported based on the two previous corpora on 4 types of encoder-decoder architectures with an attention mechanism. For this purpose, we applied two encoder-decoder architectures using GRU and LSTM. Also, we augmented each type of architecture with either Bahdanau or Luong’s attention mechanism. Two ways of training from text to gloss and from gloss to text for each combination of the attention mechanism with encoder-decoder architecture were applied. Thus, for both corpora, we totally perform 16 different models in the experiments. The hyper-parameters of the trained models are shown in Table IV.

TABLE IV. HYPERPARAMETERS

	ASLG-PC12	Phoenix-2014T
Number of Layers	1	4
Initial Learning Rate	10^{-4}	10^{-4}
Batch Size	128	128
Hidden units	1024	1024
Embedding units	1024	1024
Dropout	0.30	0.30
Gradient Clipping	5	5

To apply the proposed approach on ASLG-PC12, we created a deep network model with one layer of the encoder (unidirectional) layer, and one layer of the decoder layer. Also, we used GRU and LSTM cell for each type of network. We used an embedding layer of 1024 units with each recurrent layer containing 1024 hidden units of batch size 128. We also used Adam optimization with a learning rate of 10^{-4} as a default parameter and gradient clipping with a threshold of 5 and dropout connections with a drop probability of 0.3. The model was implemented the model using TensorFlow [39] with eager execution and we use evaluation metrics BLEU and ROUGE score. All our networks are trained in 70 epochs. Tables V and VI illustrate the full results of the proposed approach on ASLG-PC12 in two ways of translation, namely from text to gloss and from gloss to text.

TABLE V. ASLG-PC12 TEXT TO GLOSS MODEL RESULTS

	Test				
	Rouge	BLEU1	BLEU2	BLEU3	BLEU4
LSTM B	91.19	89.47	83.93	79.39	75.38
GRU B	94.37	93.26	89.64	86.68	83.98
LSTM L	88.88	89.98	81.14	74.82	69.55
GRU L	70.42	71.03	59.58	50.79	43.46

The results of the trained text to gloss models reveal that the encoder-decoder model with GRU of Bahdanau (B) attention achieves the best result with ROUGE score 94.37% and BLEU-4 score 83.98% when compared to other models. Also, the trained gloss-to-text models’ results reveal that the encoder-decoder model with GRU of Bahdanau attention achieves the best result with ROUGE score 87.31% and BLEU-4 66.59%.

TABLE VI. ASLG-PC12 GLOSS TO TEXT MODEL RESULTS

	Test				
	Rouge	BLEU1	BLEU2	BLEU3	BLEU4
LSTM B	80.59	81.88	70.99	62.76	55.98
GRU B	87.31	88.65	79.68	73.23	66.59
LSTM L	79.54	69.69	60.75	60.75	53.57
GRU L	62.78	63.90	51.63	42.66	35.52

To compare the results with other related work, Table VII summarizes our best results [*] against the best models in [23] concerning ASLG-PC12 gloss to text translation.

TABLE VII. COMPARISON TEST SCORE ASLG-PC12 FOR GLOSS TO TEXT WITH OTHER WORK

	Rouge	BLEU1	BLEU2	BLEU3	BLEU4
GRU L [23]	-	86.70	79.50	73.20	65.90
GRU B*	87.31	88.65	79.68	73.23	66.59

In the experiments for the proposed approach on Phoenix-2014T, we created the deep network model with four stacked layers of the encoder (1 bidirectional [40] and 3 unidirectional layers), and 4 stacked layers of the decoder that support residual connections to avoid exploding and vanishing gradient problems [41], [42]. Also, we used two GRU and LSTM cells for each type of network. Each recurrent layer contains 1024 hidden units and 1024 units of an embedding layer with batch size 128. Furthermore, we used Adam’s optimizer [43] with a learning rate of 10^{-4} as a default parameter. We are clipped the gradient with a threshold of 5 and dropout connections with a drop probability of 0.3. Likewise, for the models of ASLG-PC12 corpus, we implemented the models using TensorFlow [39] with eager execution. We equally applied BLEU and ROUGE score as the evaluation metric. All models are trained using 70 epochs. Table VIII and IX summarize the results of the proposed approach on Phoenix2014T for the two ways of the translation, i.e., text to gloss and from gloss to text, respectively.

TABLE VIII. PHOENIX-2014T TEXT TO GLOSS MODEL RESULTS

	Test				
	ROUGE	BLEU1	BLEU2	BLEU3	BLEU4
LSTM B	36.54	38.56	21.16	12.06	07.39
GRU B	42.96	43.90	26.33	16.16	10.42
LSTM L	40.21	42.60	24.24	15.34	10.55
GRU L	41.14	42.45	25.27	15.90	10.53

The results of trained text to gloss models show that the encoder-decoder model with GRU having Bahdanau (B) attention achieves the best result in ROUGE with a score of 42.96%, whereas GRU with Luong (L) attention achieves the best result in BLEU-4 with 10.53%. Also, the results of trained gloss-to-text models reveal that the GRU encoder-decoder model with Luong (L) achieves the best result in ROUGE and BLEU-4 with a score of 45.69% and 19.56% respectively.

To compare the results with other related work, Table X summarizes our best results against the best models in [21] concerning the gloss to text translation. In the evaluation comparison, we did not consider the text to gloss translation, as the authors of [21] focused only on the translation from gloss to text. Our GRU and LSTM models, marked with (*)

TABLE IX. PHOENIX-2014T GLOSS TO TEXT MODEL RESULTS

	Test				
	ROUGE	BLEU1	BLEU2	BLEU3	BLEU4
LSTM B	44.27	45.02	29.92	22.18	17.77
GRU B	45.45	45.38	31.26	23.34	18.64
LSTM L	44.60	44.47	29.55	21.72	17.38
GRU L	45.69	45.38	31.81	24.17	19.56

outperform the work of [21] in terms of ROUGE and BLEU evaluation metrics.

TABLE X. COMPARISON TEST SCORE PHOENIX-2014T FOR GLOSS TO TEXT WITH OTHER WORK

	Rouge	BLEU1	BLEU2	BLEU3	BLEU4
LSTM L	41.92	41.22	28.03	20.77	16.58
LSTM L*	44.60	44.47	29.55	21.72	17.38
GRU L	43.73	43.43	30.73	23.36	18.75
GRU L*	45.69	45.38	31.81	24.17	19.56
GRU B	42.61	42.76	29.55	22.00	17.40
GRU B*	45.45	45.38	31.26	23.34	18.64

VI. CONCLUSION

In this paper, we proposed an approach that translates sign language to natural language and vice versa. In particular, we proposed a deep learning approach based on sequence to sequence for bidirectional translation, from gloss notation to text and text to gloss for both directions of translation. We used encoder-decoder with attention to Bahdanau and Luong mechanism. In particular, two models of encoder-decoder network with GRU and LSTM were adopted. We have tested the proposed approach on both ASLG-PC12 and Phoenix-2014T corpora. We conducted four models of encoder-decoder with different attention mechanisms per each translation direction for the two corpora. We compared the results of the four models in each direction of translation. The overall experimental results on eight different models applied to the ASLG-PC12 corpus indicated that the GRU model with Bahdanau attention achieved the best performance using the ROUGE metric with an 87.31% score translating from gloss to text. Also, the GRU model with Bahdanau attention achieved the best performance with a ROUGE score of 94.37% when translating from text to gloss. Similarly, the overall experimental results on eight different models applied to the Phoenix-2014T corpus revealed that the GRU model with Luong attention achieved the best performance on ROUGE with a score of 45.69% when translating from gloss to text. In the other direction of translation, the GRU model with Bahdanau achieved the best performance on ROUGE with a score of 42.96%. Moreover, part of the results were compared to similar work on the same corpus in one direction of translation and showed the superiority of the proposed models. We think that one big enhancement of sign language translations is to use the so-called pose estimation[44], [45], [46]. In particular, the translation from text to pose estimation and vice versa is worth investigating as a future research direction.

REFERENCES

- [1] A. Othman and M. Jemni, "An xml-gloss annotation system for sign language processing," in *2017 6th International Conference on Information and Communication Technology and Accessibility (ICTA)*. IEEE, 2017, pp. 1–7.
- [2] B. O. Olusanya and V. E. Newton, "Global burden of childhood hearing impairment and disease control priorities for developing countries," *The Lancet*, vol. 369, no. 9569, pp. 1314–1317, 2007.
- [3] A. Othman and M. Jemni, "Statistical sign language machine translation: from english written text to american sign language gloss," *arXiv preprint arXiv:1112.0168*, 2011.
- [4] W. C. Stokoe Jr, "Sign language structure: An outline of the visual communication systems of the american deaf," *Journal of deaf studies and deaf education*, vol. 10, no. 1, pp. 3–37, 2005.
- [5] T. Hanke, "Hamnosys-representing sign language data in language resources and language processing contexts," in *LREC*, vol. 4, 2004, pp. 1–6.
- [6] M. Stuart, "A grammar of signwriting," Ph.D. dissertation, Thesis in Linguistics, University of North Dakota, 2011.
- [7] E. S. Klima and U. Bellugi, *The signs of language*. Harvard University Press, 1979.
- [8] J. Bungeroth and H. Ney, "Statistical sign language translation," in *Workshop on representation and processing of sign languages, LREC*, vol. 4. Citeseer, 2004, pp. 105–108.
- [9] V. López-Ludeña, R. San-Segundo, J. M. Montero, R. Córdoba, J. Ferreiros, and J. M. Pardo, "Automatic categorization for improving spanish into spanish sign language machine translation," *Computer Speech & Language*, vol. 26, no. 3, pp. 149–167, 2012.
- [10] R. San-Segundo, R. Barra, R. Córdoba, L. F. D'Haro, F. Fernández, J. Ferreiros, J. M. Lucas, J. Macías-Guarasa, J. M. Montero, and J. M. Pardo, "Speech to sign language translation system for spanish," *Speech Communication*, vol. 50, no. 11-12, pp. 1009–1020, 2008.
- [11] R. San-Segundo, R. Barra, L. D'Haro, J. M. Montero, R. Córdoba, and J. Ferreiros, "A spanish speech to sign language translation system for assisting deaf-mute people," in *Ninth International Conference on Spoken Language Processing*, 2006.
- [12] I. Marshall and É. Sáfár, "A prototype text to british sign language (bsl) translation system," in *The Companion Volume to the Proceedings of 41st Annual Meeting of the Association for Computational Linguistics*, 2003, pp. 113–116.
- [13] S. Morrissey and A. Way, "Lost in translation: the problems of using mainstream mt evaluation metrics for sign language translation," 2006.
- [14] —, "Joining hands: Developing a sign language machine translation system with and for the deaf community," 2007.
- [15] S. Morrissey, "Data-driven machine translation for sign languages," Ph.D. dissertation, Dublin City University, 2008.
- [16] P. Antony, "Machine translation approaches and survey for indian languages," in *International Journal of Computational Linguistics & Chinese Language Processing, Volume 18, Number 1, March 2013*, 2013.
- [17] C. K. Alexandris, *Issues in the Multilingual Information Processing of Spoken Political and Journalistic Texts*. Cambridge Scholars Publishing, 2020.
- [18] A. Mohammed and R. Kora, "Deep learning approaches for arabic sentiment analysis," *Social Network Analysis and Mining*, vol. 9, no. 1, pp. 1–12, 2019.
- [19] L. Deng and D. Yu, "Deep learning: methods and applications," *Foundations and trends in signal processing*, vol. 7, no. 3–4, pp. 197–387, 2014.
- [20] S. A. Abdelaziz Ismael, A. Mohammed, and H. Hefny, "An enhanced deep learning approach for brain cancer mri images classification using residual networks," *Artificial Intelligence in Medicine*, vol. 102, p. 101779, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0933365719306177>
- [21] N. Cihan Camgoz, S. Hadfield, O. Koller, H. Ney, and R. Bowden, "Neural sign language translation," in *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition*, 2018, pp. 7784–7793.

- [22] K. Yin and J. Read, "Attention is all you sign: Sign language translation with transformers," in *Proceedings of the European Conference on Computer Vision (ECCV) Workshop on Sign Language Recognition, Translation and Production (SLRTP)*, 2020.
- [23] N. Arvanitis, C. Constantinopoulos, and D. Kosmopoulos, "Translation of sign language glosses to text using sequence-to-sequence attention models," in *2019 15th International Conference on Signal-Image Technology & Internet-Based Systems (SITIS)*. IEEE, 2019, pp. 296–302.
- [24] S.-K. Ko, C. J. Kim, H. Jung, and C. Cho, "Neural sign language translation based on human keypoint estimation," *Applied Sciences*, vol. 9, no. 13, p. 2683, 2019.
- [25] S. Stoll, N. C. Camgoz, S. Hadfield, and R. Bowden, "Text2sign: towards sign language production using neural machine translation and generative adversarial networks," *International Journal of Computer Vision*, pp. 1–18, 2020.
- [26] I. Sutskever, O. Vinyals, and Q. V. Le, "Sequence to sequence learning with neural networks," in *Advances in neural information processing systems*, 2014, pp. 3104–3112.
- [27] D. Bahdanau, K. Cho, and Y. Bengio, "Neural machine translation by jointly learning to align and translate," *arXiv preprint arXiv:1409.0473*, 2014.
- [28] Y. Wu, M. Schuster, Z. Chen, Q. V. Le, M. Norouzi, W. Macherey, M. Krikun, Y. Cao, Q. Gao, K. Macherey *et al.*, "Google's neural machine translation system: Bridging the gap between human and machine translation," *arXiv preprint arXiv:1609.08144*, 2016.
- [29] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.
- [30] J. Chung, C. Gulcehre, K. Cho, and Y. Bengio, "Empirical evaluation of gated recurrent neural networks on sequence modeling," *arXiv preprint arXiv:1412.3555*, 2014.
- [31] T. Luong, E. Brevdo, and R. Zhao, "Neural machine translation (seq2seq) tutorial. 2017," URL: <https://www.tensorflow.org/tutorials/seq2seq>, 2017.
- [32] A. Othman and M. Jemni, "English-asl gloss parallel corpus 2012: Asl-gpc12," in *5th Workshop on the Representation and Processing of Sign Languages: Interactions between Corpus and Lexicon LREC*, 2012.
- [33] A. Othman, Z. Tmar, and M. Jemni, "Toward developing a very big sign language parallel corpus," in *International Conference on Computers for Handicapped Persons*. Springer, 2012, pp. 192–199.
- [34] T. Supalla, "The classifier system in american sign language," *Noun classes and categorization*, vol. 7, pp. 181–214, 1986.
- [35] A. Vaswani, N. Shazeer, N. Parmar, J. Uszkoreit, L. Jones, A. N. Gomez, Ł. Kaiser, and I. Polosukhin, "Attention is all you need," in *Advances in neural information processing systems*, 2017, pp. 5998–6008.
- [36] N. C. Camgoz, O. Koller, S. Hadfield, and R. Bowden, "Sign language transformers: Joint end-to-end sign language recognition and translation," in *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition*, 2020, pp. 10 023–10 033.
- [37] E. K. Elsayed and D. R. Fathy, "Sign language semantic translation system using ontology and deep learning," *International Journal of Advanced Computer Science and Applications*, vol. 11, 2020.
- [38] J. Forster, C. Schmidt, O. Koller, M. Bellgardt, and H. Ney, "Extensions of the sign language recognition and translation corpus rwth-phoenix-weather," in *LREC*, 2014, pp. 1911–1916.
- [39] M. Abadi, A. Agarwal, P. Barham, E. Brevdo, Z. Chen, C. Citro, G. S. Corrado, A. Davis, J. Dean, M. Devin *et al.*, "Tensorflow: Large-scale machine learning on heterogeneous distributed systems," *arXiv preprint arXiv:1603.04467*, 2016.
- [40] M. Schuster and K. K. Paliwal, "Bidirectional recurrent neural networks," *IEEE transactions on Signal Processing*, vol. 45, no. 11, pp. 2673–2681, 1997.
- [41] S. Hochreiter, Y. Bengio, P. Frasconi, J. Schmidhuber *et al.*, "Gradient flow in recurrent nets: the difficulty of learning long-term dependencies," 2001.
- [42] R. Pascanu, T. Mikolov, and Y. Bengio, "Understanding the exploding gradient problem. corr abs/1211.5063 (2012)," *arXiv preprint arXiv:1211.5063*, 2012.
- [43] D. P. Kingma and J. Ba, "Adam: A method for stochastic optimization," *arXiv preprint arXiv:1412.6980*, 2014.
- [44] Z. Cao, G. Hidalgo, T. Simon, S.-E. Wei, and Y. Sheikh, "Openpose: realtime multi-person 2d pose estimation using part affinity fields," *IEEE transactions on pattern analysis and machine intelligence*, vol. 43, no. 1, pp. 172–186, 2019.
- [45] S. Gattupalli, A. Ghaderi, and V. Athitsos, "Evaluation of deep learning based pose estimation for sign language recognition," in *Proceedings of the 9th ACM International Conference on Pervasive Technologies Related to Assistive Environments*, 2016, pp. 1–7.
- [46] M. Oberweger, P. Wohlhart, and V. Lepetit, "Hands deep in deep learning for hand pose estimation," *arXiv preprint arXiv:1502.06807*, 2015.

Swapping-based Data Sanitization Method for Hiding Sensitive Frequent Itemset in Transaction Database

Dedi Gunawan*, Yusuf Sulistyo Nugroho, Maryam
Informatics Engineering Department
Universitas Muhammadiyah Surakarta

Abstract—Sharing a transaction database with other parties for exploring valuable information becomes more recognized by business institutions, i.e., retails and supermarkets. It offers various benefits for the institutions, such as finding customer shopping behavior and frequently bought items, known as frequent itemsets. Due to the importance of such information, some institutions may consider certain frequent itemsets as sensitive information that should be kept private. Therefore, prior to handling a database, the institutions should consider privacy preserving data mining (PPDM) techniques for preventing sensitive information breaches. Presently, several PPDM methods, such as item suppression-based methods and item insertion-based methods have been developed. Unfortunately, the methods result in significant changes to the database and induce some side effects such as hiding failure, significant data dissimilarity, misses cost, and artificial frequent itemset occurrence. In this paper, we propose a swapping-based data sanitization method that can hide the sensitive frequent itemset while at the same time it can minimize the side effects of the data sanitization process. Experimental results indicate that the proposed method outperforms existing methods in terms of minimizing the side effects.

Keywords—Transaction database; data sanitization; data mining; sensitive frequent itemset; swapping-based method

I. INTRODUCTION

Retails and supermarkets are actively collecting their customers' data transactions. The collected data is then stored in a database, and it is referred to as a transaction database. A transaction database \mathcal{D} contains a set of transactions such as in Table I. In general, a set of transaction records T is a non-empty set where $T = \{t_1, t_2, t_3, \dots, t_x\}$. Each transaction t is composed of a transaction id Tid , customer name or id number $Cname$, and a set of items bought by the customer, IID . The transaction database provides various benefits for the business institutions when they perform data analysis, such as using data mining technology. Unfortunately, analyzing such a transaction database by using data mining techniques is not a trivial task for these institutions since many of them do not have sufficient resources, i.e., computation resources and human resources, to perform the data mining task. Therefore, they opt to handle the transaction database to other parties, for example, a data mining company to conduct the task. Even though this solution may solve the problem, sharing the transaction database may bring a hidden threat since there might be sensitive information resides the database.

One of the data mining tasks that are widely employed in

various domains is frequent itemset mining [1]. The frequent itemset mining is very useful to find the frequently bought items as well as to analyze customer buying patterns in transaction databases. Moreover, understanding such information allows the companies to enhance their marketing strategy as a way to increase business revenue. Referring to the Table I as an illustration, a company, defines that an itemset $\{1, 3\}$ has valuable information that should be learned by others. The table shows that item id 1, $iid = 1$ and item id 3, $iid = 3$, are frequently appear together in several transactions such as in t_1, t_5, t_7 , and t_{10} . Due to the importance of this information, the company does not want any other parties exploring such an itemset. Concealing sensitive information is mandatory prior to sharing databases [2]. Therefore, data sanitization methods should be taken into account by the database owner to enable database sharing while at the same time preserving sensitive frequent itemset from being disclosed by external parties during the data mining process.

Recently, various data sanitization methods have been proposed with different settings and assumptions. Most of them rely on item suppression-based and item insertion-based strategies to address the aforementioned problem. However, the methods that follow suppression-based strategy [3], [4] incur significant side effects such as hiding failure, significant data dissimilarity, misses cost, and artificial frequent itemset occurrence. Accordingly, the data utility of the sanitized one degrades drastically, leading to induce inaccurate information for data recipients. The term hiding failure represents the percentage of sensitive frequent itemset that fail to be hidden by the data sanitization algorithm. Meanwhile, data dissimilarity measures the difference between an original database and its anonymized version in terms of its items frequency. Misses cost indicates the percentage of non-sensitive frequent itemsets that cannot be discovered in a sanitized database. Simultaneously, artificial frequent itemset corresponds to any frequent itemset that previously do not exist in an original database; however, it newly appears as the frequent itemset in a sanitized database.

Therefore, in this paper, a distinct data sanitization method is proposed. The proposed method follows the swapping-based strategy to ensure privacy protection in a database while at the same time preventing excessive side effects of the data sanitization process. The method follows a recent data swapping method that has been developed in [5] to generate an anonymized database. The proposed method uses an item collision detection strategy, and it carefully selects a pair of

TABLE I. EXAMPLE OF CUSTOMER TRANSACTION DATABASE \mathcal{D}

Tid	Cname	IID
t_1	John	1,2,3,8,10
t_2	Alice	2,7,8,10
t_3	Mark	5,6,7,10,12
t_4	Martin	2,3,8,9
t_5	Amar	1,3,5,9,10
t_6	Felix	4,6,7,9,10,12
t_7	Nita	1,3,5,8,11
t_8	Marta	1,6,4,7,9
t_9	Ben	5,12
t_{10}	Doet	1,3

transaction records for swapping by evaluating item similarity in the transaction records. To the best of our knowledge, our proposed method is the first method which uses the swapping technique in PPDM to hide sensitive frequent itemset.

The rest of the paper is organized as follows: Section 2 explores related work. The proposed method is explained in Section 3. Section 4 and 5 describe the experimental result and conclusion, respectively.

II. RELATED WORK

A. Frequent Itemset Mining

Frequent itemset mining is a data mining task which aims to explore all combinations of itemset contained in transaction records under a certain number of occurrence frequency threshold [6], [7]. Prior to performing frequent itemset mining, a database owner needs to determine a minimum support threshold value. In addition, there is no certain fixed number of minimum support thresholds, and thus if a database owner sets the frequency threshold too low, the database may output a significant number of frequent itemset and vice versa.

Suppose we have a transaction database denoted as \mathcal{D} . Support $supp$ of an itemset X , is the total number of transactions in \mathcal{D} containing X . We denote the support of itemset X in a database \mathcal{D} as $supp(X, \mathcal{D})$. To compute the $supp(X, \mathcal{D})$, one can divide the frequency of itemset $X \in \mathcal{D}$, $f(X)$, over the total number of transaction records in the database $|\mathcal{D}|$. An itemset X is called frequent itemset FI if $supp(X, \mathcal{D})$ is greater or equal to the number of determined minimum support $minSupp$ [8]. Thus, any itemset having the support value below the $minSupp$ can be referred as FI . To compute the $supp$ of itemset X in \mathcal{D} we can refer to (1).

$$supp(X, \mathcal{D}) = \frac{f(X)}{|\mathcal{D}|} \quad (1)$$

B. Sensitive Frequent Itemset

Sensitive frequent itemset refers to any frequent itemset in which if such itemset are disclosed during the mining process conducted by other parties, and the database owner may lose their interest. In general, the database owners determine a set of a sensitive frequent itemset. Thus, if we formally denote the sensitive frequent itemset $F_s(X, \mathcal{D})$ as frequent sensitive itemset, then $F_s(X, \mathcal{D}) \subset FI$. Any other frequent itemset which is not considered as sensitive can be referred as non-sensitive frequent itemset F_n , where $F_s \neq F_n$ and $FI = F_s \cup F_n$. The relation between Sensitive frequent itemset and frequent itemset can be depicted in Fig. 1.

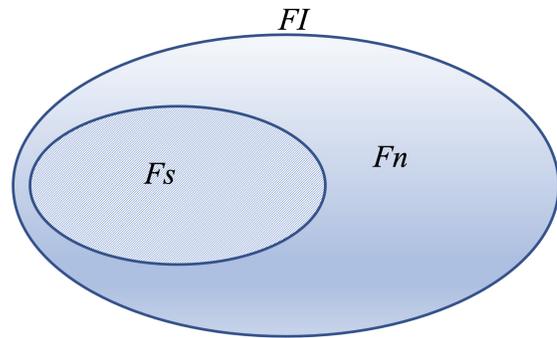


Fig. 1. Relation Among F_s , F_n and FI .

C. Data Sanitization Method

Data sanitization methods can be grouped into three main categories such as perturbation-based method, cryptographic-based method, and heuristics-based methods [9]. It has been proved that achieving a sanitized database that guarantees privacy protection and preserves maximum database utility is an NP-Hard problem [10], [11]. Therefore, various data sanitization methods with distinct parameters and settings have been proposed to address the issue. In addition, each proposed method is application-specific where it is designed for a particular problem, and it may not be adequate to work on another problem. For example, a data sanitization method that is intended for protecting sensitive frequent itemset mining is not suitable for privacy preserving data clustering. Thus, there is no one method fits all.

1) *Perturbation-based Method*: A perturbation-based method relies on a perturbing database either by removing items or inserting artificial items into transactions in the database. An initial data sanitization which follows the concept of the reconstruction-based to hide sensitive frequent itemset has been proposed in [4]. One of the solutions in the proposed method is called Naïve approach. It removes all the sensitive itemsets from a transaction database such that the sensitive information cannot be disclosed. While the technique effectively addresses the privacy problem, it causes significant item loss due to the removing process.

In reality, items in the transaction database may have a different level of importance. For example, item x is an item that is less important than item y since x generates low profit in a business process while item y is considered as an essential item due to its economic value. Therefore, a method that considers various threshold sensitivity has been proposed in [12]. The technique does not arbitrarily suppress all the sensitive frequent itemsets; instead, it creates a template containing possible victim items to disguise them. Another perturbation-based method has also been proposed in [13] namely rotation perturbation. However, the method is specifically designed to address sensitive information issues in clustering data mining. To solve the item loss issue, a technique that uses transaction insertion has been introduced in [14]. However, the method results in a significant difference between an original database and the sanitized one.

To optimize the performance of data sanitization, a method which based on particle swarm optimization (PSO) have been

proposed in [15]. The method achieves a sanitized database by removing sensitive items in specific transaction record while at the same time reducing the side effects. The size of database is also another challenge to solve. Concerning that issue a method called MR-OVnTSA have been proposed in [16]. The method hides frequent sensitive itemsets in big data environment by removing items and transactions that can balance the privacy and knowledge in the database.

2) *Cryptographic-based Method*: Realizing that transaction database is potentially analyzed by several geographically separated parties, another scenario of hiding frequent sensitive itemset in a distributed system has also been intensively studied. Pioneering work in this area is proposed in [17], [18]. The methods use a secure multi-party computation technique to where several parties perform data mining analysis. To improve the quality of the sanitized database, a more recent approach in [19] proposes a cryptographic technique to hide sensitive rules in transaction databases. The method successfully protects the transaction database from inference attacks. A recent method in [20] proposed employs a cryptographic technique where it improves the mining process by disjoining the encrypted transactions into a certain number of blocks and only uses bilinear pairs of ciphertexts from the blocks. Therefore, the approach becomes more applicable in real-life cases. Even though the cryptographic-based method provides a strong privacy guarantee, however, when it meets a huge-sized transactional database, the performance decreases drastically due to the encrypt and decrypt process.

3) *Heuristic-based Method*: As it has been mentioned that finding maximum privacy guarantee and maximum database utility is an NP-Hard problem, a close to an exact solution which is based on a heuristic approach needs to be devised to address the problems in a real-life scenario. Presently, various heuristic-based methods have been proposed under different settings and parameters. One of the pioneering works in this area, such as in [4], [21]. In literature, most of the heuristics-based methods apply either item pruning or artificial transaction insertion strategy to reduce the support of itemset, and therefore it successfully hides the sensitive frequent itemset in a database.

Distinct from the previous approach, [22] proposed a method which uses a unique strategy where it does not reduce the support of itemset to hide the sensitive frequent itemset; instead, it considers representative rules to remove the rules at the beginning. Another recent study proposed in [3] also adopts heuristic-based data sanitization method where the method performs item pruning strategy, and it successfully hides sensitive itemset in a database. To select the items for the pruning process, the method considers calculating the frequency of sensitive items and removing the one which causes a minimum item loss.

It is undoubtedly true that the heuristic-based method which uses either items pruning strategy or artificial transaction insertion can successfully hide sensitive frequent itemset in a database. Unfortunately, such strategies lead the database to lose its useful information due to some items are missing from the database. In addition, artificial transaction insertion strategy results in excessive changes to the database as a result, the item composition between an original database and the sanitized one differs significantly.

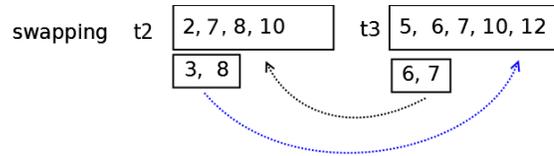


Fig. 2. Swapping Item from t_2 to t_3 and Vice Versa.

D. Swapping Techniques

The principle of data swapping technique is moving items from a certain transaction record to another record and vice versa. Therefore, it does not remove or add items in the transaction records, as a result, the database content can be well preserved. The data swapping techniques have been widely adopted for controlling statistical disclosure in micro dataset sharing. Pioneering work to protect sensitive information using the swapping technique was developed in [23], [24]. The method has successfully protects sensitive information in numerical and categorical attributes.

Regardless of a debate on its side effect, i.e., the techniques cause information incorrectness at a record level due to items of transaction records being swapped to another record. However, the techniques can successfully maintain items in the transaction database from loss. Thus, data recipients may perform data exploration to obtain all information of the items in the sanitized database.

The illustration of the swapping technique in transaction database is described in Fig. 2.

III. PROPOSED METHOD

To successfully hide sensitive frequent itemsets while at the same time maintaining the database utility, in this research, we propose a swapping-based data sanitization method. To the best of our knowledge, our proposal is the first data sanitization method that adopts swapping strategy. The swapping strategy does not remove items from a database and inserts new artificial transactions into the database; instead, it swaps items from one transaction to another. Accordingly, the side effect such as the number of artificial frequent itemset in the sanitized database can be minimized. An initial work in swapping strategy is firstly introduced in [25] to control data from disclosure. In this paper, the proposed method is distinct from the initial work which relies on a randomization strategy to protect the database. Our solution framework can be described in Fig. 3.

To evaluate whether an itemset is called a frequent itemset in \mathcal{D} , the data owner needs to determine a certain value called minimum support threshold, $minSupp$ and perform frequent itemset mining. All the obtained itemsets having support value greater than or equal to the $minSupp$ is called frequent itemsets, FI . The next step is the database owner defines a set of sensitive frequent itemsets F_s from the FI , where $F_s \subset FI$. The F_s is a non empty set containing sensitive frequent itemset si , thus $F_s = \{si_1, si_2, \dots, si_n\}$. Meanwhile, all the frequent itemsets that are not considered as F_s are called non-sensitive frequent itemset F_n , and it does not need to be hidden in a \mathcal{D} , such that $FI = F_s \cup F_n$.

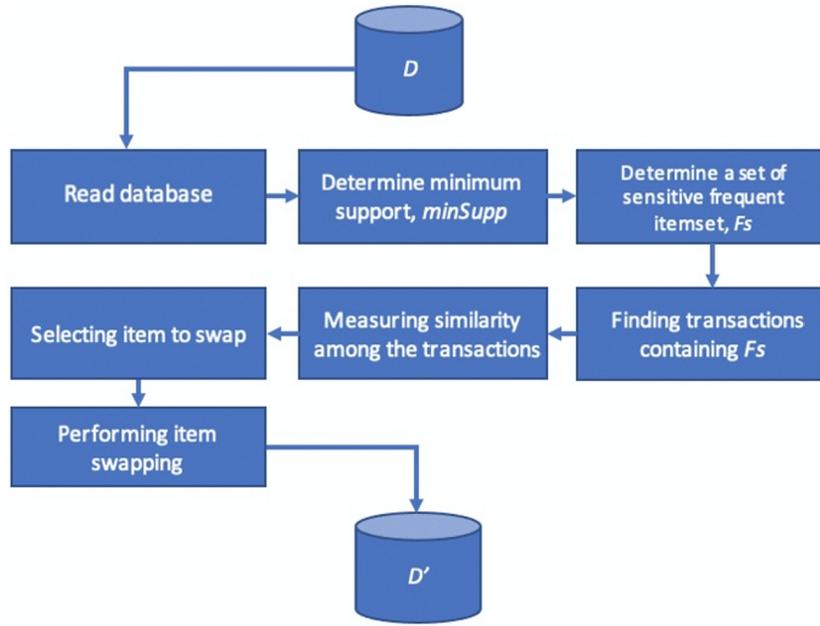


Fig. 3. Swapping-based Data Sanitization Framework.

In general, database owners can determine F_s in two ways. The first is database owners define F_s according to their intention from business perspective, and the second is customers can freely determine their purchased items as either sensitive or non-sensitive itemset [26]. In this research, we follow the first approach where the database owners determine a set of itemsets in which according to his/her point of view it is considered as sensitive information.

A. Reading and Segmenting Database

Initially, our proposed method scans a database \mathcal{D} and reads each transaction record $t_x \in \mathcal{D}$. During the reading process, the method identifies each t_x to check whether it contains sensitive frequent itemset si . For each t_x containing si , append the t_x to a bucket TF_s otherwise append it to another bucket TF_n . In this step, TF_s and TF_n have influence in separating the sensitive and non-sensitive transactions in database. Therefore, the TF_s only contains a set of transactions containing si , while TF_n is only containing a set of transactions not having si . The pseudo-code of this procedure is presented in the following Algorithm 1.

B. Measuring Transactions Similarity and Pairing the Transactions

Following the previous step, the proposed method measures similarity among transactions to obtain a pair of transactions for the swapping, P . P is used to simplify the pairing process of two transactions that will be used for swapping procedure. In this research, we follow the idea of [27] where the Jaccard coefficient is adopted to measure the similarity of transactions. In essence the Jaccard coefficient J_c computes the number of items that coexist in the two records over the number of the total item from those records. The formula of J_c measurement is depicted in (2).

$$J_c(t_x, t'_x) = \text{Max} \frac{(t_x \cap t'_x)}{(t_x \cup t'_x)} \quad (2)$$

Algorithm 1: Reading and segmenting database

Input: \mathcal{D} , $si \in SI$
Result: TF_s and TF_n

- 1 Scan \mathcal{D}
- 2 $\forall t_x \in \mathcal{D}$
- 3 **if** $si \subseteq t_x$ **then**
- 4 | add the t_x to TF_s
- 5 **else**
- 6 | add the t_x to TF_n
- 7 **end**

Algorithm 2: Measuring similarity and finding a pair

Input: TF_s
Result: P

- 1 $\forall t_x \in TF_s$
- 2 select a record $t_x \in TF_s$, randomly
- 3 select another record $t'_x \in TF_s$
- 4 **while** $si \subseteq t_x \neq si \subseteq t'_x$ **do**
- 5 | compute $J_c(t_x, t'_x) = \text{Min} \frac{(t_x \cap t'_x)}{(t_x \cup t'_x)}$
- 6 **end**
- 7 select a pair P having the minimum J_c

To avoid an item collision which may result in item loss and reduce the number of generated artificial frequent itemsets in a sanitized dataset, the proposed method implements two protocols. The first is our method only selects a pair of records that have the minimum similarity. Initially, the method selects a transaction $t_x \in TF_s$ randomly, and then it picks another transaction $t'_x \in TF_s$, selected transaction is referred as P .

The second step is our method ensures the sensitive itemsets si should not coexisting in both transactions, i.e., $si \in t_x \neq si' \in t'_x$ of P . While the si of both transaction are different, the algorithm computes the Jc . The next step is selecting a pair of records P which has the minimum Jc . Therefore, when the item $i \in si$ of the pair P are swapped to each other, the process does not cause item collision in both transactions significantly. In addition, such procedure can successfully ensure the hiding of sensitive frequent itemsets and minimize data dissimilarity. Algorithm 2 represents the pseudo-code of this procedure in detail.

1) *Selecting Item for Swapping*: Once the pair P have been determined, the following step is selecting items from the P to swap. In general, arbitrarily swapping items from these transactions may also hide the sensitive frequent itemset for both transactions. However, this action may distort item correlation in the transactions that result in significant changes in a sanitized database content [28]. To address this problem, in this research, the strategy in [5] is adopted. The key point of the strategy is checking whether items $i \in t_x$ that will be swapped are coexisting with that in t'_x .

Referring to Table I as an illustration, we aim to swap $si \in t_2$ with $si' \in t_3$. Let us denote item id as iid , for example, an item namely coffee has $iid = 7$ is a subset of sensitive frequent itemset si appears in t_2 and it also coexists in t_3 . Swapping the $iid=7$ from t_2 with another item such as bread i.e., an item with $iid = 6$ that presents in t_3 can successfully hides $si \in t_2$. However, due to the $iid = 7$ coexists in t_3 , while the $iid = 6$ does not present in t_2 , swapping the $iid = 7$ from t_2 causes an item collision in to the transaction t_3 , as a result, the t_3 loses one of its items i.e., $iid = 6$ and it is no longer exists in the t_3 . Accordingly, to successfully hide the $si \in t_x$ while at the same time reduce the number of items loss in the transactions, the proposed method selects items that do not cause item collision.

In addition, to minimize the amount of data utility loss, the proposed method also selects the sensitive items $i \in si$ that have the minimum support Pr in the \mathcal{D} . Selecting items $i \in si$ with the lowest Pr can minimize the changes of item correlation in t_x . For example, suppose we have a sensitive itemset with $iid = 2$ and $iid = 3$, $\{2, 3\}$. Referring to the Table I, the Pr of $iid = 2$ is $3/10=0.33$ while the Pr of $iid = 3$ is $5/10=0.50$. To hide the sensitive itemset we would like to swap either $iid = 2$ or $iid = 3$. Suppose we select $iid = 3$ as the item to swap, the item correlation of $iid = 2$ with other items is significantly distracted since it appears five times in the \mathcal{D} . On the other hand, when $iid = 2$ is selected to swap, its item correlation with other items is not significantly reduced due to its appearance in the \mathcal{D} is lower than that of the $iid = 3$, as a result, only small parts of the transactions in the \mathcal{D} experience changes.

Thus, to be selected as the items for the swapping process, the items $i \in si$ have to satisfy these two conditions. Firstly, the items $i \in si$ should not collide with any other items $i \in t'_x$. Secondly, it should have the lowest probability distribution in \mathcal{D} . Thus, it can successfully minimize the number of artificial frequent itemsets in the sanitized database \mathcal{D}' . The detail of item selection is described in Algorithm 3.

Algorithm 3: Procedure of items selection for swapping

Input: P
Result: i'

- 1 calculate the Pr of $i \in si$ of t_x
- 2 select $i \in si$ of t_x that has the minimum Pr
- 3 check whether the i exist in t'_x
- 4 **if** $i \neq i_j \in t'_x$ **then**
- 5 | select the i as the item for swapping
- 6 **else**
- 7 | repeat step 4
- 8 **end**
- 9 return i' ;
- 10 **end;**

Algorithm 4: Procedure of items swapping

Input: P, TFN
Result: \mathcal{D}'

- 1 create Buffer br_{t_k} and $br_{t'_k}$;
- 2 $br_{t_k}.add(i \in si \text{ of } t_k)$;
- 3 $br_{t'_k}.add(i \in si \text{ of } t'_k)$;
- 4 append $br_{t'_k}$ to t_k ;
- 5 append br_{t_k} to t'_k ;
- 6 merge $P' + TFN$;
- 7 save to \mathcal{D}' ;
- 8 **end;**

2) *Swapping the Selected Items*: Once the items for the swapping process have been determined, the next step is performing item swapping between that of t_x and t'_x . To swap the items, the proposed method creates two buffers for storing the items $i \in t_x$ and $i' \in t'_x$. At first, the item from t_x is stored in buffer br_{t_k} and that of t'_x is stored in $br_{t'_k}$. In this stage, br is a buffer to temporarily store the modified transaction records in swapping process. The second step is taking the items in $br_{t'_k}$ and appending it to the t_x . Following that, items in br_{t_k} is appended to t'_x . The procedure is performed until all i' from the pairs of records P have been swapped. Once the swapping process is finished, the algorithm can combine all the transaction records from TFN to successfully generate a sanitized database \mathcal{D}' . Algorithm 4 represents the pseudo-code of item swapping in detail.

IV. EXPERIMENTAL RESULTS

To evaluate the effectiveness of the proposed method, we conduct several extensive experiments using several real datasets such as the foodmart dataset [29]. The properties of the dataset are described in Table II, while the testing parameters are presented in Table III. We implement the algorithm in JAVA code and run it in UNIX operating system with memory of 8 GB and storage of 256 GB. An additional tool, namely SPMF [30] is also adopted to generate frequent itemset by utilizing FP-Growth algorithm [31].

A. Evaluation Metrics

To verify the performance of the proposed method, we compare the proposed method, SW with several existing sen-

TABLE II. DATASETS PROPERTIES

Properties	Datasets
	<i>FoodMart</i>
# transactions	4,141
# items	18,319
# distinct items	1,559
Average tuple length	11.75

TABLE III. TESTING PARAMETERS

Parameter	Dataset
	<i>FoodMart</i>
<i>minSupp</i>	0.03% - 0.1%
$ F_s $	$ FI *0.5$
Avg. <i>si</i> length	4

sitive frequent itemset methods, i.e., heuristic method, *HEU* [3] and naïve method, *NV* [4]. Testing parameters are also determined in this experiment, and the detail is presented in Table III. Several metrics are adopted to evaluate the performance of the proposed method, such as hiding failure, misses cost, dissimilarity, and artificial frequent itemset [32].

1) *Hiding Failure*: Hiding failure, *HF* is a metric to evaluate the percentage of sensitive frequent itemsets that fail to be hidden. Ideally, a data sanitization method should be able to hide all the sensitive frequent itemsets in a database, i.e., the *HF* is 0. However, in some cases because of the data sanitization method's inaccuracy, several sensitive frequent itemsets are failed to hide. The metric to evaluate *HF* is presented in (3), where $\#F_s(\mathcal{D})$ represents the number of sensitive frequent itemsets in an original database and $\#F_s(\mathcal{D}')$ refers to that of the sanitized one.

Referring to Fig. 4, we can observe that the proposed method results in the lowest percentage of hiding failure. Even though *SW* fails to hide some *si*, the percentage of the failure is insignificant compared to that of other methods. The percentage of *HF* induced by the *SW* is around 7.143%, while the percentage of *HF* resulted from *HEU* and *NV* are 47.619% and 66.667%, respectively. The method successfully achieves the results since it takes a pair of records and swaps the items in *si* of the records.

$$HF = \frac{\#F_s(\mathcal{D}')}{\#F_s(\mathcal{D})} \quad (3)$$

2) *Misses Cost*: The term misses cost, *MC* refers to the percentage of non-sensitive frequent itemsets F_n that are accidentally hidden when performing data sanitization. Ideally, the percentage of *MC* is 0%. The formula to compute *MC* is described in equation 4, where $\#F_n(\mathcal{D})$ and $\#F_n(\mathcal{D}')$ represent a set of frequent itemset that can be explored in \mathcal{D} and a set of non-sensitive itemset that cannot be discovered in \mathcal{D}' .

As can be observed in Fig. 5, when the sanitized database resulted from *SW* is mined under *minSupp* = 0.03%, our proposal induces a slightly higher percentage of *MC* compared to that of *HEU*. However, as the *minSupp* value increases to *minSupp* = 0.1% the proposed scheme achieves the same results as *HEU*. In addition, the *SW* successfully achieves better results compared to that of *NV* in terms of minimizing

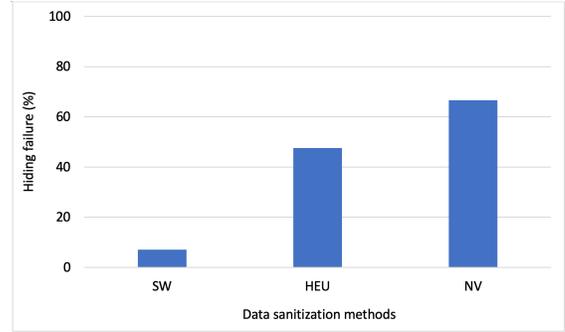


Fig. 4. Hiding Failure.

TABLE IV. NUMBER OF *MC* OF \mathcal{D}'

Methods	<i>minSupp</i>			
	0.03%	0.05%	0.07%	0.10%
<i>SW</i>	0.064	0.006	0.006	0
<i>HEU</i>	0.034	0.005	0.005	0
<i>NV</i>	0.276	0.029	0.029	0.034

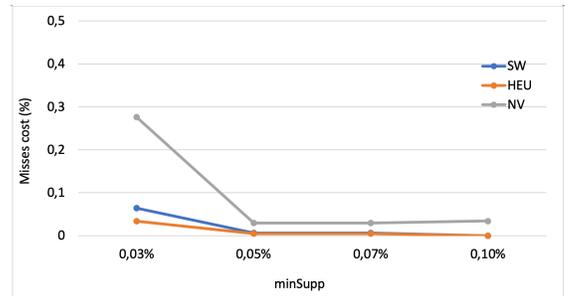


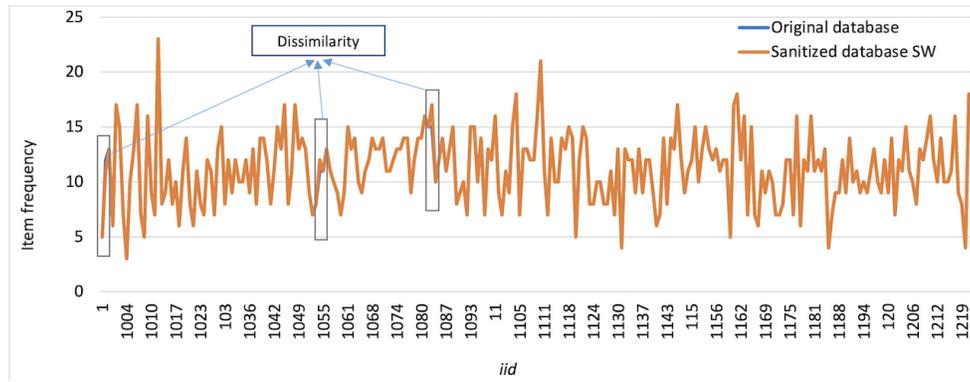
Fig. 5. Misses Cost.

MC in all the varying *minSupp* values. The detail values of *MC* among the methods are described in Table IV.

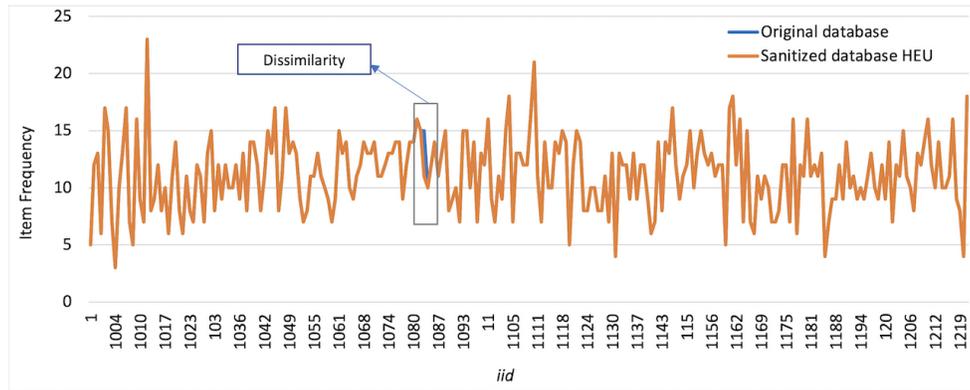
The main motivation of such results is due to the proposed method does not limit the number of modified records like in *HEU*. The *HEU* leaves some records containing *si* are kept unmodified to reduce the *MC*. However, such a strategy allows the *si* remain discoverable when data recipients perform frequent itemset mining using a lower confidence value than the *minSupp* value. As our goal is designing strong data sanitization, the proposed method does not apply the same strategy in *HEU*.

$$MC = \frac{\#F_n(\mathcal{D}) - \#F_n(\mathcal{D}')}{\#F_n(\mathcal{D})} \times 100\% \quad (4)$$

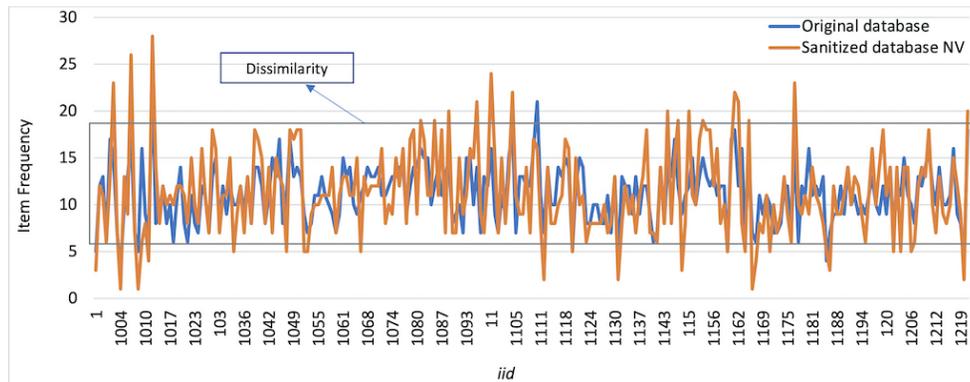
3) *Dissimilarity*: Applying data sanitization methods to a database always results in some changes to the database content. The changes in database content are considered as a side effect of the data sanitization methods, and it is referred to as dissimilarity. To evaluate the dissimilarity between an



(a) Histogram of item frequency between \mathcal{D} and generated \mathcal{D}' by SW



(b) Histogram of item frequency between \mathcal{D} and generated \mathcal{D}' by HEU



(c) Histogram of item frequency between \mathcal{D} and generated \mathcal{D}' by NV

Fig. 6. Histogram of Item Frequency Comparison.

original database and its sanitized version, one can compare the items' frequency in both databases. The formula to evaluate the dissimilarity $Diss$ is presented in (5), where $f^{\mathcal{D}}(i)$ represents the frequency of item i in an original database \mathcal{D} and $f^{\tilde{\mathcal{D}}}(i)$ refers to that of the sanitized one.

$$Diss(\mathcal{D}, \tilde{\mathcal{D}}) = \frac{1}{\sum_{i=1}^d f^{\mathcal{D}}(i)} \times \left| \sum_{i=1}^d f^{\mathcal{D}}(i) - \sum_{i=1}^{\tilde{d}} f^{\tilde{\mathcal{D}}}(i) \right| \quad (5)$$

As can be observed from Fig. 6a, the item frequency of the

sanitized database \mathcal{D}' generated by our proposed method SW is almost the same as that of the original database \mathcal{D} . Even though there are some differences in certain item frequency between the two databases, it does not significantly deviate. Referring to Fig. 6b, the item frequency in the sanitized database \mathcal{D}' generated by HEU also experiences a small dissimilarity. Meanwhile, in Fig. 6c we can see that the item frequency in \mathcal{D}' obtained from NV has a significant difference compared to the item frequency in the original database \mathcal{D} .

The summary of data dissimilarity of those databases is presented in Fig. 7. According to the figure, we can observe that the proposed method results in the lowest $Diss$ value

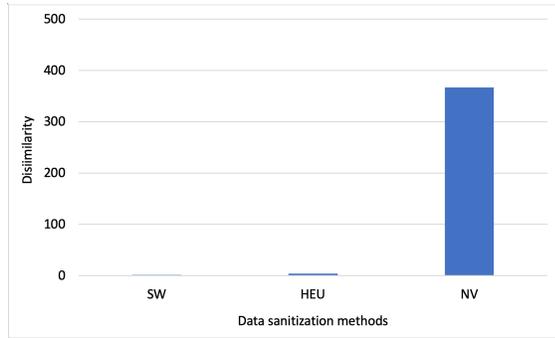


Fig. 7. Dissimilarity Value.

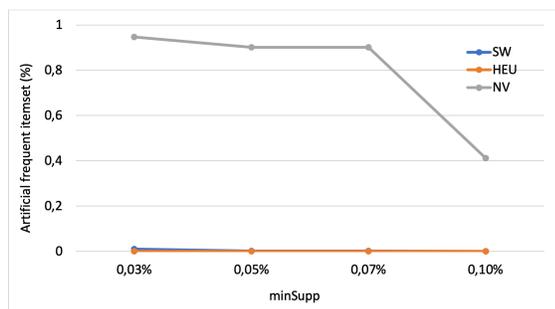


Fig. 8. Artificial Frequent Itemset.

compared to that of other methods. The *Diss* value resulted from the proposed method is 1.372, while that of the *HEU* and *NV* are 4.327 and 366.436, respectively. The result is achieved because the proposed method can minimize the number of item losses in the sanitized database. Meanwhile, since the other two methods adopt a suppression strategy that removes items from a database, their dissimilarity values are higher than that of our proposed method.

4) *Artificial Frequent Itemset*: Artificial frequent itemsets, *AFI* is defined as a percentage of all frequent itemsets that do not present in an original database. However, it newly appears in the sanitized one. Ideally, the percentage is 0. The formula to compute the *AFI* is stated in equation (6).

$$AFI = \frac{|\widetilde{FI}| - |\widetilde{FI} \cap FI|}{|\widetilde{FI}|} \quad (6)$$

The notations $|\widetilde{FI}|$ and $|FI|$ represent the cardinality of frequent itemset in a sanitized database and that of the original database, respectively. As can be seen in Fig. 8, the sanitized database resulted by *SW* results in considerably lower *AFI* than that of *NV*. While, it has the same *AFI* as the *HEU*, when the *minSupport* value is more than 0.03%. The proposed method, *SW* can minimize the *AFI* due to it does not remove or add items to a database. Therefore, the frequent itemset in \widetilde{D} remain the same as that of the original one. The detail values of the *AFI* is presented in Table V.

TABLE V. NUMBER OF *AFI* IN \mathcal{D}'

Methods	<i>minSupp</i>			
	0.03%	0.05%	0.07%	0.10%
<i>SW</i>	0.009	0.001	0.001	0
<i>HEU</i>	0	0	0	0
<i>NV</i>	0.947	0.902	0.902	0.411

V. THREATS TO VALIDITY

Threats to the *construct validity* relates to the proposed method's performance in handling various database with different properties. In our study, we only used one transaction database as described in the Table II. Even though we only used single database, however, it has more complex data properties compared to other databases that are usually used in PPDM areas such as *BMS – WebView1* and *BMS – WebView2* [33], specifically in the number of distinct items and the average of tuple length. Thus, we consider that the impact of using various database is not significant.

The second threats to validity is related to the performance of the proposed method compared to other more recent methods. Even though *NV* is not considered as the recent one, however, recent researches in PPDM [34], [35] still consider the method as the benchmark to evaluate the performance of their proposed method. Therefore, the impact of using other recent methods is small.

VI. CONCLUSION

In this paper, a data sanitization method based on a swapping approach called *SW* have been proposed. The main property of the proposed method is that it does not add or remove items in the database. The method has several steps to obtain a sanitized database. The main idea of the proposed method is finding transactions containing frequent sensitive itemset, measuring their similarity to determining a pair of records, and deciding items in the sensitive frequent itemset for the swapping process.

Experimental results show that in general the proposed method has a better performance compared to some existing methods. The method successfully hides the sensitive frequent itemsets with the lowest *HF* compared to that of several existing methods, indicating it provides stronger privacy protections in the sanitized database. In addition, since the method does not remove or add items in a database, the dissimilarity value between the original database and the sanitized one resulted from our method is lower than that of *HUE* and *NV*. In terms of data utility preservation, our method has a similar performance with *HEU* where the percentage of *AFI* is close to zero.

In the future, a more deeper analysis to the proposed method needs to be conducted, specifically in handling various transaction databases that have different properties and also evaluating the algorithm complexity. The proposed method *SW* also needs to be compared to more recent existing works in the same field to evaluate its performance.

ACKNOWLEDGMENT

This research is funded by Hibah Integrasi Tridharma (HIT) Universitas Muhammadiyah Surakarta under the grand number

015/A.3-III/FKI/I/2021.

REFERENCES

- [1] D. Apiletti, E. Baralis, T. Cerquitelli, P. Garza, F. Pulvirenti, and L. Venturini, "Frequent Itemsets Mining for Big Data: A Comparative Analysis," *Big Data Research*, vol. 9, pp. 67–83, 2017. [Online]. Available: <http://dx.doi.org/10.1016/j.bdr.2017.06.006>
- [2] J. C.-W. Lin, T.-Y. Wu, P. Fournier-Viger, G. Lin, J. Zhan, and M. Voznak, "Fast algorithms for hiding sensitive high-utility itemsets in privacy-preserving utility mining," *Engineering Applications of Artificial Intelligence*, vol. 55, pp. 269–284, 2016. [Online]. Available: <http://linkinghub.elsevier.com/retrieve/pii/S0952197616301282>
- [3] D. Gunawan and L. Guanling, "Heuristic Approach on Protecting Sensitive Frequent Itemsets in Parallel Computing Environment," in *The 1ST UMM International Conference on Pure and Applied Research (UMM-ICOPAR 2015)*, Malang, East Java, Indonesia, 2015, pp. 41–49.
- [4] S. Oliveira and O. Zaiane, "Privacy preserving frequent itemset mining," *Proceedings of the IEEE international conference on Privacy, security and data mining-Volume 14*, vol. 14, pp. 43–54, 2002. [Online]. Available: <http://portal.acm.org/citation.cfm?id=850782.850789>
- [5] D. Gunawan and M. Mambo, "Set-valued data anonymization maintaining data utility and data property," in *ACM International Conference Proceeding Series*. Association for Computing Machinery, jan 2018.
- [6] J. Han, M. Kamber, and J. Pei, *Data Mining: Concepts and Techniques*, 2012.
- [7] I. H. Witten, E. Frank, M. A. Hall, and C. J. Pal, *Data Mining: Practical Machine Learning Tools and Techniques*, 2016.
- [8] X. Cheng, S. Su, S. Xu, P. Tang, and Z. Li, "Differentially private maximal frequent sequence mining," *Computers and Security*, 2015.
- [9] D. Gunawan, "Classification of Privacy Preserving Data Mining Algorithms : A review," *Jurnal Elektronika dan Telekomunikasi (JET)*, vol. 20, no. 2, pp. 36–46, 2020.
- [10] R. Agrawal and R. Srikant, "Privacy-preserving Data Mining," in *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data*, ser. SIGMOD '00. New York, NY, USA: ACM, 2000, pp. 439–450. [Online]. Available: <http://doi.acm.org/10.1145/342009.335438>
- [11] C. C. Aggarwal, J. Pei, and B. Zhang, "On privacy preservation against adversarial data mining," in *Proceedings of the ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, 2006.
- [12] Y. P. Kuo, P. Y. Lin, and B. R. Dai, "Hiding frequent patterns under multiple sensitive thresholds," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5181 LNCS, pp. 5–18, 2008.
- [13] K. Chen and L. Liu, "Privacy preserving data classification with rotation perturbation," in *Fifth IEEE International Conference on Data Mining (ICDM'05)*, 2005, pp. 4 pp.–.
- [14] L. Chun-Wei, H. Tzung-Pei, C. Chia-Ching, and W. Shyue-Liang, "A Greedy-based Approach for Hiding Sensitive Itemsets by Transaction Insertion," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 4, no. 4, pp. 201–2014, 2013.
- [15] S. Jangra and D. Toshniwal, "VIDPSO: Victim item deletion based PSO inspired sensitive pattern hiding algorithm for dense datasets," *Information Processing and Management*, vol. 57, no. 5, p. 102255, 2020. [Online]. Available: <https://doi.org/10.1016/j.ipm.2020.102255>
- [16] S. Sharma and D. Toshniwal, "MR-OVnTSA: a heuristics based sensitive pattern hiding approach for big data," *Applied Intelligence*, vol. 50, no. 12, pp. 4241–4260, 2020.
- [17] Y. Lindell and B. Pinkas, "Privacy preserving data mining," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 2000.
- [18] —, "Privacy preserving data mining," *Journal of Cryptology*, 2003.
- [19] N. Rajesh and A. A. L. Selvakumar, "Association rules and deep learning for cryptographic algorithm in privacy preserving data mining," *Cluster Computing*, vol. 22, no. s1, pp. 119–131, 2019. [Online]. Available: <https://doi.org/10.1007/s10586-018-1827-6>
- [20] C. Ma, B. Wang, K. Jooste, Z. Zhang, and Y. Ping, "Practical Privacy-Preserving Frequent Itemset Mining on Supermarket Transactions," *IEEE Systems Journal*, vol. 14, no. 2, pp. 1992–2002, 2020.
- [21] A. HajYasien and V. Estivill-Castro, "Two new techniques for hiding sensitive itemsets and their empirical evaluation," *Data Warehousing Knowledge Discovery, Proc.*, vol. 4081, pp. 302–311, 2006.
- [22] D. Jain, P. Khatri, R. Soni, and B. K. Chaurasia, "Hiding sensitive association rules without altering the support of sensitive item(s)," *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering, LNICST*, vol. 84, no. PART 1, pp. 500–509, 2012.
- [23] S. P. Reiss, M. J. Post, and T. Dalenius, "Non-reversible privacy transformations," in *Proceedings of the 1st ACM SIGACT-SIGMOD Symposium on Principles of Database Systems*, ser. PODS '82. New York, NY, USA: ACM, 1982, pp. 139–146. [Online]. Available: <http://doi.acm.org/10.1145/588111.588134>
- [24] S. P. Reiss, "Practical data-swapping: The first steps," *ACM Trans. Database Syst.*, vol. 9, no. 1, pp. 20–37, Mar. 1984. [Online]. Available: <http://doi.acm.org/10.1145/348.349>
- [25] T. Dalenius and S. P. Reiss, "Data-swapping: A technique for disclosure control," *Journal of Statistical Planning and Inference*, vol. 6, no. 1, pp. 73–85, 1982. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/0378375882900581>
- [26] T. P. Hong, C. W. Lin, K. T. Yang, and S. L. Wang, "Using TF-IDF to hide sensitive itemsets," *Applied Intelligence*, vol. 38, no. 4, pp. 502–510, 2013.
- [27] J. Wicker and S. Kramer, "The best privacy defense is a good privacy offense: obfuscating a search engine user's profile," *Data Mining and Knowledge Discovery*, vol. 31, no. 5, pp. 1419–1443, 2017.
- [28] D. Gunawan and M. Mambo, "Data anonymization for hiding personal tendency in set-valued database publication," *Future Internet*, vol. 11, no. 6, 2019.
- [29] P. Fournier-Viger, "Foodmart dataset," 2020. [Online]. Available: <http://www.philippe-fournier-viger.com/spmf/index.php?link=datasets.php>
- [30] P. Fournier-Viger, J. C. W. Lin, A. Gomariz, T. Gueniche, A. Soltani, Z. Deng, and H. T. Lam, "The SPMF open-source data mining library version 2," *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 9853 LNCS, pp. 36–40, 2016.
- [31] G. Grahne and J. Zhu, "Fast algorithms for frequent itemset mining using FP-trees," *IEEE Transactions on Knowledge and Data Engineering*, vol. 17, no. 10, pp. 1347–1362, 2005.
- [32] L. Zhang, W. Wang, and Y. Zhang, "Privacy Preserving Association Rule Mining: Taxonomy, Techniques, and Metrics," *IEEE Access*, vol. 7, pp. 45 032–45 047, 2019.
- [33] KDD-CUP, "KDD CUP 2000: Online Retailer Website Clickstream Analysis ," <https://www.kdd.org/kdd-cup/view/kdd-cup-2000>, 2000, [Online; accessed 7-June-2019].
- [34] W. Wu, M. Xian, U. Parampalli, and B. Lu, "Efficient privacy-preserving frequent itemset query over semantically secure encrypted cloud database," *World Wide Web*, vol. 1, pp. 607–629, 2021.
- [35] H. Chen, A. A. Heidari, X. Zhao, L. Zhang, and H. Chen, "Advanced orthogonal learning-driven multi-swarm sine cosine optimization: Framework and case studies," *Expert Systems with Applications*, vol. 144, p. 113113, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S0957417419308309>

Software Security Static Analysis False Alerts Handling Approaches

Aymen Akremi

College of Computer and Information Systems
Umm Al-Qura University (UQU)
Makkah, Saudi Arabia

Abstract—False Positive Alerts (FPA), generated by Static Analyzers Tools (SAT), reduce the effectiveness of the automatic code review, letting them be underused in practice. Researchers conduct a lot of tests to improve SAT accuracy while keeping FPA at a lower rate. They use different simulated and production datasets to validate their proposed methods. This paper surveys recent approaches dealing with FPA filtering; it compares them and discusses their usefulness. It also studies the used datasets to validate the identified methods and show their effectiveness to cover most program defects. This study focuses mainly on the security bugs covered by the datasets and handled by the existing methods.

Keywords—Software security; static analysis; false alert reduction; source code dataset; security bugs

I. INTRODUCTION

Software coding and implementation have grown fastly during the last years. This is due to the rapid migration towards bits and the extensive use of digital technologies. The more software applications become relevant, the more security assurance of programs gets essential. However, software security defects increased due to implementation failures regarding security best coding practices. Escaping software faults into later stages of software development will increase the maintenance cost[1],[2]. Also, after application deployment, cyberhackers will try to detect these coding vulnerabilities and exploit them to achieve their goals. Thus, coding review and auditing is a primordial task before software use.

Static Analysis Tools (SAT) play an essential role in automatically detecting these vulnerabilities and alerting the programmer, which reduces the auditing time, effort, and cost. SAT automatically examines the code for any programming defects without executing the code and generates alerts about possible errors. Alerts provide the auditor with useful information such as the location of the purported defect in the source code, the nature of the fault, and additional contextual information. However, the SAT still suffers from several issues, letting them underused in practice. Among them, this study focuses on the large number of warnings generated by SAT; most of them are false positives, which is a time-consuming and painstaking task to review them all.

One approach to deal with a large number of FPAs is by unsoundly processing source code. Almost all existing SATs are uniformly unsound [3]. Loops and unknown external libraries call, for instance, are a significant source of imprecision. Unsound SAT considers only a fixed number of loops while ignoring the rest and assumes any unknown external library

call as predefined behaviors such as skip[3]. This unsoundness regarding loops and unknown external libraries causes the analysis to miss a significant amount of real bugs and reduce false-positive alerts.

In this study, any paper that sacrifices SAT soundness to reduce false-positive alerts is ignored. Ideally, an SAT must be precise and scalable while avoiding false positives.

Existing efforts dealing with the false-positive alert reduction face several challenges, mainly are:

- Handling of a large code base will decrease SAT precision; most of them perform better in a small set of problems. Besides, processing a significant codebase causes the SAT over-approximation of the input program behavior, which may consider correct program properties as errors.
- Increasing SAT precision raises much more false-positive alerts. The challenge is how to keep a high detectability rate without throwing FPAs.
- The inability of the SAT to get knowledge about the software architecture, its dependencies, and the manner of how data flows through the system, which may result in throwing FP alerts considered as potential errors [4].

So researchers are trying to solve one challenge or some of them to reduce false-positive alerts.

To our best knowledge, these different approaches have not been studied rigorously and comprehensively. Thus, the objective of this paper is the investigation of current methods dealing with false alert elimination. It mainly presents the most significant efforts in this field and their scalability in the last ten years. It defines new criteria to compare different approaches. Also, this study focuses on showing the most effective dataset used in the literature and provides statistics about them. Finally, the paper discusses the advantages and shortcomings of FPA handling approaches and presents recommendations to improve the SAT.

This paper is divided into eight parts; after introducing the research subject in Section 1, it presents the related works in Section 2. The paper shows the research methodology for selecting the relevant articles in Section 3 and existing approaches identified categories in Section 4. The paper compares, in Section 5, the different methods used to reduce false alerts. Section 6 provides an overview of the used datasets, then discusses the shortcomings and proposes recommendations to

deal with these limitations in Section 7. Finally, the paper is concluded in Section 8.

II. RELATED WORKS

In paper [5], authors studied the existing efforts aiming at combining static analysis and dynamic quality assurance techniques to improve SAT bugs detection with reduced false alerts. They finally selected 51 articles for their mapping study. Thus, they include only papers that consist of the integration of combined technologies so that the output of one method is the input of the second. However, this paper shows the different approaches categories and any possible combination used to improve SAT precision or reduce FP alerts.

Heckman et al in [6] investigates 18 research effort to identify actionable alert identification techniques. They categorize the approaches as classification or ranking methods. The authors also conducted a comparative study to identify the approaches having the best accuracy. In this effort, articles that improve SAT precision to reduce FP alerts, not only improving the bugs detection rate, are also studied.

Similar as [5], authors in the paper [7] identified 51 papers for their mapping study. They focus on the study of the existing static analysis tools and techniques to reduce false alerts. However, this article covers only methods handling false alerts.

The paper [8] surveys 79 articles that handle the enormous amount of FP alerts after their generation. The authors focus on the methods dealing with the reduction of SAT alert reports. While, this study considers all kinds of unique approaches that help minimize FP alerts, whether the method is for the refinement of the software source code, the improvement of SAT precision, or the post-handling of SAT alerts report.

It is worthy to note that all the reviewed papers by the above surveys were published four years ago since the last study [8] at our best knowledge published in 2016. Thus, this effort focuses on the recent papers fitting the selection requirement as maximum to provide researchers with a recent and accurate literature review.

This study outperforms the above surveys by:

- the selection and presentation of relevant datasets to test and validate the SAT tools. It collects the different open source datasets along with information about their size and features (see Section VI).
- the presentation of the features used by the identified methods for their model training and alerts prediction or classification(see Section V).
- providing the reader with the different types of security bugs handled by the identified approaches alongside with the paper reference (see Section VI-B).
- the comparison of the different false alert handling techniques according to their scalability in order to study their ease of integration and application (see Section V).
- depicting ongoing projects and competition aiming at boosting the researches to improve SATs and at providing accurately labeled datasets (more details in VI).

TABLE I. SEARCH KEYWORDS CATEGORIES

Category Number	Keywords
1	defects, bugs, faults
2	false alerts, false warnings, false alarms
3	static analysis, source code analysis, automatic static bugs detection
4	filtering, elimination, reduction, handling

Several other existing studies, such as [9], [10], [11], [12], [13], evaluate the SAT in terms of precision and alert handling and conduct a comparison study between them. This paper has a different objective by only presenting the approaches that improve SAT alerts handling, not testing their precision.

III. RESEARCH METHODOLOGY

This survey starts by identifying relevant papers that deal with false alert reduction. Fig. 1 depicts the main steps to select pertinent articles and extract information from them.

A. Research Questions

The process of relevant paper selection goes through the precise definition of the research topic, enabling identifying the keywords used for the scientific database search. This study aims at answering the following questions:

- **RQ.1:** What are the different techniques used to reduce FPAs?
- **RQ.2:** How extend human effort is required to execute the proposed approach?
- **RQ.3:** Are the proposed approaches scalable?
- **RQ.4:** Are security bugs considered during the FPAs reduction?
- **RQ.5:** What are the datasets used to validate the different methods?

B. Used keywords and Search Engine Configuration

The relevant keywords are determined based on the research questions identified in Section III-A. Keywords could be classified into four categories representing the most used terms and their synonyms. Then for each search round, a combination of keywords taken from each set is used. The used keywords are listed in Table I.

The first category encompasses the most used names of program errors. The second category contains the different terms of alerts; more specifically, it focuses on false-positive alerts. The third category includes possible static analysis names that different researchers may use, and finally, the last category contains the used keywords to describe alert reductions.

So, this study makes $108 = 3 \times 3 \times 3 \times 4$ separate search strings rounds at Google scholar, which ranks research papers based on their relevance. It refines the search by showing only articles published after 2010 to ensure that the selected documents consider recent programming technologies and new trends of SATs. The first 50 papers that match all the searched keywords combinations are chosen. So, this paper identified 540 articles before proceeding with the selection process.

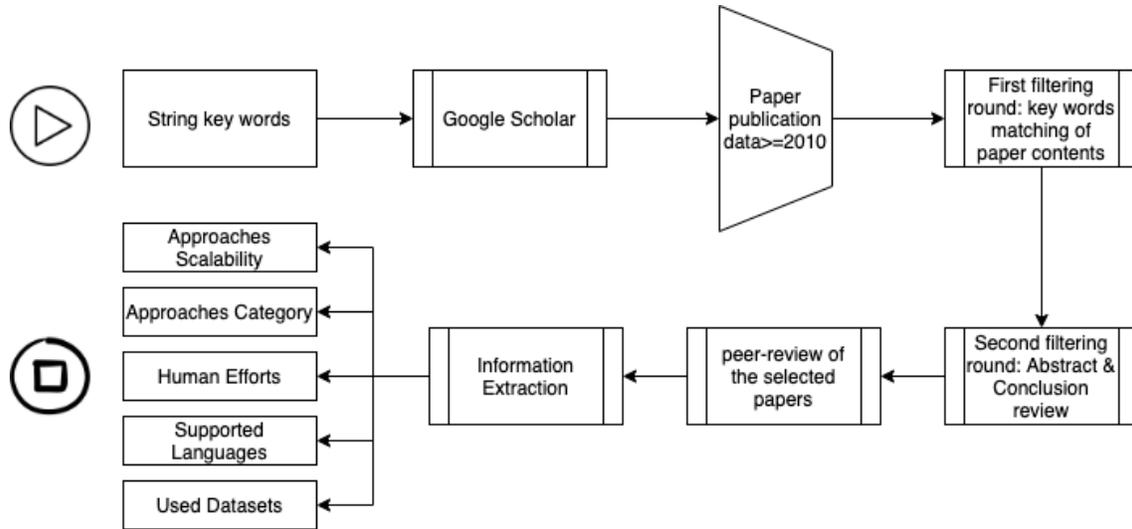


Fig. 1. Research Methodology Diagram.

C. Relevant Papers' Selection Process

This section presents the paper selection process that consists mainly of the quick and peer review of the candidate articles from the previous steps. Papers are filtered quickly at the second filtering round based only on the title, abstract, evaluation, and conclusion. Only papers satisfying the following criteria are included in the final peer review:

- papers that explicitly aim to reduce false alerts. Thus, any effort based on improving the precision of the static analyzer or modifying the software source code, or post handling of SAT alert reports is included.
- papers that have an evaluation and test of their approach.

Also, this study excludes papers that:

- sacrifices the soundness of the SAT to reduce false-positive alerts.
- aims only to detect true positive alerts without reducing FPAs.
- only surveys existing efforts without providing any new technique or approach to reduce FPAs.
- mostly uses similar techniques and datasets to another already selected paper. The aim is to keep the uniqueness and originality of each chosen article.

After this process, 30 relevant articles that summarize almost all approaches and efforts dealing with SAT false alert handling are finally selected. The distribution number of chosen papers according to the Scientific publisher databases are shown in Table II

D. Information Extraction Process

In this step, this study proceeds for peer review of the identified papers to extract the relevant and targeted information, which are:

TABLE II. DISTRIBUTION OF THE SELECTED PAPERS ACCORDING TO THE PUBLISHERS

Publisher	# of papers	Journal/Conference name
hal.archives-ouvertes.fr	1	10th European Congress on Embedded Real Time Software and Systems 2020
ScienceDirect	2	Journal of Systems and Software 137 (2018): 766-783 Information and Software Technology 52.2 (2010): 210-219
Springer	6	Asian Symposium on Programming Languages and Systems. Springer, Cham, 2014 IFIP Int. Conference on Open Source Systems. Cham, 2018 Int. Static Analysis Symposium. Berlin, Heidelberg, 2016 Int. Conference on Software Analysis, Testing, and Evolution. Cham, 2018 Int. Symposium on Formal Methods. Cham, 2015 OTM 2017 Conferences, Part II, LNCS 10574, pp. 99-106, 2017
ACM	8	ACM Transactions on Programming Languages and Systems, Vol. 39, No. 4, 2017 15th Int. Symposium on Open Collaboration. 2019. 33rd Annual Computer Security Applications Conference. 2017 27th ACM SIGSOFT international symposium on software testing and analysis. 2018 27th Annual ACM Symposium on Applied Computing. 2012 ACM on Programming Languages 1.GOPSLA (2017): 1-30-journal 40th Int. Conference on Software Engineering: Companion Proceedings MAPL'17, June 18, 2017, Barcelona, Spain - conference
IEEEEXPLOR	13	26th Int. Symposium on Software Reliability Engineering (ISSRE) 12th IEEE Conference on Software Testing, Validation and Verification (ICST).2019 27th Int.Symposium on Software Reliability Engineering.2016 6th Int.Workshop on Software Engineering Research and Industrial Practice. 2019 41st Int. Conference on Software Engineering: Software Engineering in Practice.2019 10th Int. Conference on Fuzzy Systems and Knowledge Discovery (FSKD). 2013 15th Int.Conference on Computer Systems and Applications (AICCSA). 2018 Formal Methods in Computer Aided Design., 2010 39th Int.Conference on Software Engineering (ICSE). 2017 Int. Conference on Big Data (Big Data),2018 1st Int. Workshop on Software Qualities and their Dependencies (SQUADE). 2018. 38th Int. Conference on Software Engineering Companion (ICSE-C).2016. 2014 21st Asia-Pacific Software Engineering Conference

- the used approaches or techniques.
- the application level of the approach. It means if the proposed method deals with improving the precision of SAT or modifying the software source code before analyzing it, or post handling of SAT reports.
- the coverity of the approaches to detect most programming bugs since several articles only reduce false alerts generated by specific bugs.
- the human intervention effort during the false alert filtering.
- the FPAs reduction percentage, whether explicitly mentioned or could be deduced from the other metrics presented in the paper. In some articles, it is not possible to extract the FPA reduction rate due to the

lack of specific measures.

- the programming language of the examined application.
- the SAT used for code examination.
- the dataset used to evaluate the proposed approach.

All gathered information is carefully saved in an Excel sheet database created to facilitate their mining. The extracted data contains the required information to answer this study's research questions.

IV. FALSE ALERTS HANDLING APPROACHES: A CLASSIFICATION

To answer RQ1, the paper starts by identifying the used approach of each article and categorizes them based on the similarities of the used techniques. This study distinguishes mainly seven categories, as shown in Fig. 2, which are: Machine Learning (ML) based approaches, Root Causes (RC) based approaches, Model Checking (MC) based approaches, Data Mining (DM) based approaches, and Semantics (SM) based approaches, Rule(RU) based approaches, and Slicing (SG)Based approaches.

A. Machine Learning-based Approaches

Machine Learning is the science of teaching a computer how to learn from data and create a model used after that to predict/classify new data[14]. It works mainly with algorithms, not raw data. ML is widely used in the field of static analysis to improve the SAT precision or post-handle the SAT-generated alarms and predict their truthness (resp. falseness).

Authors in [15], [16] have similar works that consist of establishing a new classifier based on additional learning features, which is the program structure patterns that correlate similar false alarms. They use mainly Naïve Bayes, LSTM (long-short term memories), and SVM to predict new alerts. In [17]and [18], the authors propose a clustering-based approach to classify and correlate similar alerts generated from the SAT. They formalize new methods to find dependencies between alarms caused by the buffer overflow error. Then, they cluster dependent warnings in the same cluster. After that, they tag the groups based on the dominant sound alerts. In [19], authors train a decision tree ML technique using ensemble learning (i.e.training several weak classifiers to form a new combined stronger model; authors use AdaBoost for ensemble learning) to classify alerts. They labeled the training dataset generated from multiple SATs to train the created model. Their approach is based only on the SAT reports, which provide their solution better scalability(no code pre-processing is required to try their approach) Authors in [20] proposed an approach that merges several SAT alerts to extract features used in the prediction model. They use four machine learning techniques to identify the best reducing false alarms. The paper [3] tries to deal with unsoundness static analysis and the tradeoff between False Negative rate (FNR) and False Positive Rate (FPR). Since reducing FPR increases the FNR, which is more critical and vise versa. They proposed to selectively learn their SVM model by only harmless codeset structures used to predict only FPAs. In [21] and [22] authors uses ML techniques to reduce false

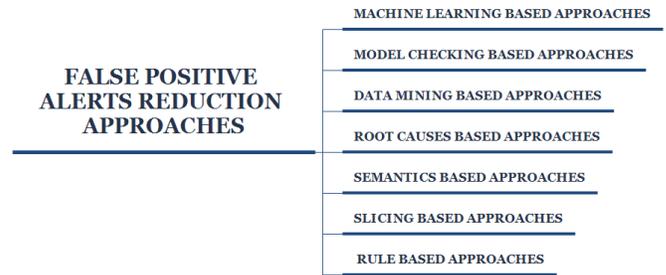


Fig. 2. False Positives Alerts Reduction Approaches.

alarms. They use tystate variables and software engineering metrics to learn their model and predict false alerts.

Authors in [23] use lexical tokenization labeled by the human to learn their CNN classifier to reduce false alerts. They propose a continuous mechanism for code integration after review.

B. Root Causes based Approaches

Root causes analysis is the process of identifying and investigating the causes of events occurrences. Therefore, investigators could specify effective corrective measures [24]. This technique is used to identify SAT false alerts root causes to eliminate or filter them. In [25], authors conduct a manual inspection of 30 javascript web application alerts generated by the static analyzer, and they conclude seven root causes of alarms. Then they use a different technique for each identified root cause to eliminate any generated alert. Authors[26] aims to reduce false alerts by reporting to the SAT user the alarm root causes to be inspected instead of the alarm itself. Also, they ask the user to answer questions related to the root causes to fix the error until no more alarm is triggered. Their approach requires extensive interaction with humans to validate root causes and define the corrective measures. The paper [27] aims to overcome the issues of the alert propagation technique. It consists of inserting new alerts before or after their causes location and removing original alarms generated by the SAT. However, the number of warnings may increase in several cases. Their paper overcomes this issue by repositioning alerts to their causes instead of creating new alerts and removing the original alert after that.

C. Model Checking based Approaches

Model Checking is a formal verification technique that investigates all possible states of a given system based on a model that defines the system behavior properties. The MC verification technique is as proper as the model representing the system [28]. SATs widely use MC techniques to reduce false-positive alerts by verifying their correctness according to the predefined model. The paper [29] aims at implementing a software analyzer that could process large-scale lines of codes with high precision at the expense of completeness and possible missing of potential defects. Their main idea is the use of specialized abstraction based on both data and predicate abstraction bounded on several model checkers. Similarly, Microsoft uses MC based static analyzer to review its software codes. Their product SLAM2 uses a model checking approach

over abstract C program statements to identify program defects and eliminate false warnings[30]. In [31], authors made a benchmark using the LABMC model checking for false alert reduction. They add loop abstraction before the use of the LABMC model checker. Authors in [32] aim to detect FPAs via the use of deductive checking to verify the conforms of source code position reported by the alert with a standard coding protocol such as Sei Cert C and ANSI/ISO. Authors in [33] aim to improve the scalability of model checking to handle the massive amount of generated SAT false positive alerts. They introduce a new variable named complete-range non-deterministic values (cnv) to reduce and avoid redundant verification calls of the model checker, mostly responsible for generating false-positive alerts. Another use of system verification techniques is the employment of Satisfiability modulo theories (SMT) solvers to identify the true/false alerts. In paper [34], authors use first abstract based analysis to fastly review codes, then link alarms to the related code snippet. After transforming alerts to SMT acceptable formulae, they use it to check the properness of such warnings.

D. Data Mining based Approaches

Data Mining (DM) techniques are used to identify hidden, potential, and valuable patterns from extensive data [35]. It is designed to extract the rules from a vast amount of data to be used by the human or other automated techniques [36]. Frequently, DM is used in combination with ML techniques that use DM-generated patterns as features to learn ML model [37]. SAT uses DM techniques to identify false-positive alert patterns for further filtering. Authors in [38] use a frequency-based algorithm to discover similar warnings patterns of SAT alerts. They transform generated warnings to composed traces and then compute their similarity using a DM-based technique that calculates similar patterns' frequencies. Then they use the patterns to filter false alerts. In [39], the authors use the Stochastic gradient descent (SGD) DM technique to reduce the complexity of finding patterns from important alerts set of several SAT's reports. Then, the authors use the Adaboost ML-based technique to create a stronger classifier trained from the SGD output.

E. Rule based Approaches

Rule-based approaches are used to manipulate knowledge to interpret information in a useful way. Rules are provided by a human or automatically generated using machine learning algorithms [38]. The latter is called Rule-based machine learning, considerably used in SAT precision enhancement and FPA reduction. Authors in [40] design and implement a bug detection software based on a set of rules extracted from manual inspection of software patches. They refine rules using a feedback-based approach by iteratively improving them each time their SAT reports a false alert. In [41], authors propose a new extension to the industrial static analyzers to fix the multiple locations of frequent warnings using experts' knowledge in the form of rules. Their expansion reduces only one false alert type by detecting the alert's name and applying a rule-based knowledge algorithm to check its truth. Authors in [4] propose a new algorithm to distinguish true positive from false-positive alerts. They try to identify the connection between the CWE and false positives to extract new rule-based patterns.

F. Semantics based Approaches

Semantic approaches refer to the meaning of language constructs. It "provides the rules for interpreting the syntax which does not provide the meaning directly but constrains the possible interpretations of what is declared," according to Euzenat [42]. The semantic approach uses mathematical logic to build rules describing constructs and relations identified in the program code. In [43] use logic programming language named DataLog to build their declarative static analyzer called URSA with the help of interactive user questions to identify alarm root causes. This tool augments the semantics of DataLog to control its over-approximation. Authors in [44] define new abstract domains that specify software violations. They apply the finite state machine technique to determine these domains and use them with a semantic-based static analyzer. In paper [45], authors propose an algorithm to generate a program graph that is used along with a static analyzer report to prioritize true bugs and reduce false alerts. Their main contribution is extracting semantic information to calculate the severity level of warnings and then using the graph algorithm to prioritize SAT alerts.

G. Slicing based Approaches

The program slicing approach is mainly used to avoid the complexity analysis of codes by reducing the original program to its minimal form called slice while keeping the same program behavior [46]. It consists of the computation of a program statement set, called program slices, that may affect the values at some point of interest. The slicing approach is used widely in program debugging to locate errors more easily [47]. There exist two types of Slicing techniques: static program slicing and dynamic slicing. The first, according to the original definition of Weiser, consist of all statements in a program that may affect the value of a specific variable in a certain statement [46]. In contrast, dynamic program slicing "contains all statements that actually affect the value of a variable at a program point for a particular execution of the program rather than all statements that may have affected the value of a variable at a program point for any arbitrary execution of the program" [48].

The main idea of the slicing approach proposed by [49] is the decomposition of the program into several executable slices and run dynamic analysis over each of them, which will reduce the processing time and complexity and consequently reduce the false alarms. Authors in [50] aim to focus directly on the sliced code generated by the alarm and verify its correctness. After applying static analysis over JAVA EE code, they slice the code based on the linked alert, transform it into executable slices and verify the code again while filtering any false alarm.

V. COMPARISON AND ANALYSIS OF RECENT EXISTING EFFORTS

This section provides the different extracted data from the 30 selected papers after several rounds of peer-reviewing depicted in Table III.

This effort starts by depicting the papers processed bugs called **bugs coverity** aiming at knowing whether the proposed approach deals with all security bugs or just focuses on some types. According to the Table III, 53.3% of the approaches

filter all kinds of defects in general. However, a considerable effort, about 46%, focuses only on specific types of defects, and therefore they could not be used without combining with other methods. Also, only 43% of papers explicitly aim to reduce false-positive alerts while maintaining high accuracy in detecting true security bugs.

Then, the paper show the *categorization* of the different approaches as detailed in S IV. The extensive use of *ML based approaches* to reduce false alerts is very observable, which is very expected since ML techniques outperform other methods when treating big data. However, the main issue of ML-based approaches is the need for a large amount of labeled data to obtain satisfactory accuracy. ML-based techniques are combined with model checking methods to verify source code properties better, extract features, and predict or classify the alerts. All identified papers that use ML techniques are applied to the source code or SAT alert reports.

Data mining-based approaches are used in four papers to reduce false-positive alerts. Also, none of the identified articles using DM methods are applied to the SAT source code level. It is explained by the SAT use of verification techniques based on knowledge rules to check software source code rather than ML or DM based models.

Model Checking based approaches used logical rules to verify source code properties or alerts truthiness. MC methods are applied and used for all integration levels.

Root causes based approaches as well are used to identify the location of alert causes from the examined software source code. Thus, all papers using root causes-based approaches apply their methods to both software source code and SAT alert reports.

Semantic based approaches is generally used to extract source code properties used further as patterns and features by SAT.

Slicing based approaches most times used to reduce source code complexity by decomposing it into small slices having the same behavior then run SAT over reduced programs which improve its soundness without throwing a large number of false alerts. *Rule based approaches* are only used with software source code for rule patterns extraction used after that by ML or DM based techniques to predict or classify alerts.

The *supported languages* feature aims to understand the research direction focus on the handled languages. Since C language is unsafe, most SAT analyzers are dedicated to analyzing C codes. Consequently, most approaches dealing with FP alert handling are generated from the static analysis of C implemented applications.

The *Scalability* feature seeks to depict the extend of a proposed approach to easily being used by most users. In Fig. 3, this article distinguishes three application levels of false alert handling approaches, which are *Software source code level*, *Static analyzer source code*, and *Static analyzer alerts report*. Also, Fig. 3 summarizes each application level's most used approach categories.

This paper consider approaches dealing false alert handling only from SAT reports as the most scalable. It is explained

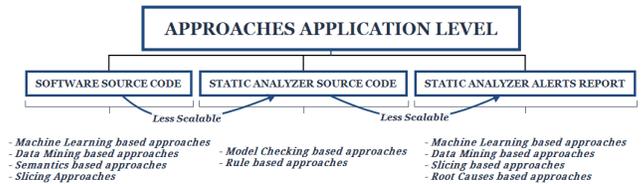


Fig. 3. Approaches Application Levels.

by the direct processing of SAT reports without any pre-processing, which will avoid any inconvenience when trying to adopt the approach. Meanwhile, approaches already integrated with SAT tools are also easy to use since the difficulty is only in the integration step already made by the approach's authors.

The *human effort* feature shows the approach reliance extend of human intervention. Of course, each time the proposed method does not require human interaction, it is considered more effective, scalable, and time/cost-saving. Almost all ML and DM-based approaches require moderate to extensive human intervention. This is due to the labeling effort required to train the created models. Few ML-based approaches require reduced human efforts explained by using a clustering approach to label the dataset then use it to lean an ML model. It is observable from the Table III that almost proposed approaches, that do not require human intervention, are applied to the SAT alerts report.

The *False Alerts Reduction Rate* feature extracts the reduction rate of false alerts, as mentioned by the paper authors. Some papers explicitly present the reduction rate while, in other articles, the FPA reduction rate is deduced. Almost approaches do not exceed 90% of reduction rate except one paper [41] that reaches a 100% reduction rate but for only one type of alert.

VI. AN OVERVIEW OF THE USED DATASETS

Finding or creating an effective dataset that reflects the real issues and complexity of software source code analysis to validate SATs is of paramount importance. To facilitate the identification of valuable datasets, this study extracts the relevant datasets used by the selected papers and shows their related information. It is worthy to note that several papers do not explicitly provide the used dataset, while others use an anonymous dataset for privacy issues. Thus, this article presents only the papers providing open datasets. The Table IV provides the dataset name or the paper reference using it. All the programs are available through quick Google searching.

This study depicts if provided by the paper's authors, the features extracted from the dataset used to train their models that has the potential to predict or classify the alerts. The number of Lines Of Code (LOC) for each program to better know the used dataset's size is also depicted. It is very observable that almost all datasets are not labeled, and authors do not share their manual labeling of SAT alert reports. Only two datasets from NIST and OWASP provide guidelines to label SAT alerts.

TABLE III. COMPARISON OF THE IDENTIFIED APPROACHES

Paper/ Criteria	Security Bugs coverage		Categories							Supported Languages	Scalability			Human label- ing effort				False alert reduction rate
	Most Bugs coverage	Only Spe- cific kind of bugs	Machine learning	Data Mining	Model Checking	Root causes	Semantics based	Slicing based	Rule based		Software source code level	Analyzer source code level	Report Directly	None	Few	Moderate	High	
[15][2017]										Java							81.3%– 85%	
[39][2017]	✓									Java							not specified	
[16][2014]		✓		✓						Java						✓	37.33% – 86.79%	
[29][2014]		✓				✓				C++						✓	84% – 84%	
[31][2015]		✓				✓				C						✓	70% – not specified	
[33][2015]	✓					✓				C		✓				✓	76% – 97.3% (precision)	
[17][2017]		✓								C							45%	
[40][2018]	✓								✓	OOP Languages	✓						not specified	
[19][2019]	✓									C/C++						✓	61% – 80%	
[43][2017]	✓						✓		✓	Java							74%	
[25][2016]	✓						✓			JavaScript							36%	
[20][2018]	✓									Java/C/C++						✓	not specified	
[23][2019]	✓									C/C++							66% – 79%	
[4][2018]	✓								✓	Php/Java/C/C++						✓	not specified	
[45][2018]		✓								C						✓	prioritization approach	
[26][2016]	✓						✓			C							42%	
[3][2017]		✓								C						✓	80%	
[18][2016]	✓									C						✓	not specified	
[34][2010]		✓				✓				C		✓				✓	68%	
[49][2012]		✓								C						✓	82%–86%	
[50][2018]		✓								Java EE						✓	not specified	
[21][2017]		✓								C/C++						✓	81%	
[27][2018]		✓						✓		C						✓	6%	
[30][2010]	✓									C						✓	96% *	
[32][2019]	✓									C						✓	90%	
[51][2018]	✓									C						✓	not specified	
[44][2020]	✓									C						✓	not specified	
[22][2018]	✓									C/C++						✓	not specified	
[41][2019]		✓							✓	Java EE						✓	100% **	
[38][2013]		✓								C						✓	23.2%	

* for only microsoft codes.
** for only one false alert type

A. Interesting Dataset Projects and Competitions

This section presents interesting community projects aiming to provide accurate datasets and enhance static analysis verification research.

1) *Juliet Dataset*: The National Institute of Standards and Technology (NIST) provides the Software Assurance Reference Dataset (SARD) ¹ to users, researchers, security assurance developers to evaluate SAT and test their methods. SARD includes a set of well-known security flaws as test cases covering all software development lifecycles. Also, it covers a large variety of vulnerabilities, languages, platforms, and compilers. The dataset fits all user’s needs since it includes wild, synthetic, and academic test cases. It is intended to be a broad effort contributed from many sources².

Juliet ³, one of the SARD provided datasets, is a collection of test cases dedicated to C, C++, and Java languages. Juliet’s first version 1.0 appeared in December 2010, and its last release, 1.3 delivered in October 2017. It contains examples organized under 118 different CWEs for C/C++ and 112 different CWEs for Java. NIST labels through the methods nominations bad and good codes.

2) *OWASP Benchmark Project*: OWASP Benchmark Project ⁴ aims to address the difficulties of testing software defects detection tools and study their weakness, strengths, and analysis time. OWASP provides a Java test suite designed to investigate and evaluate the accuracy, coverage, and speed of Software vulnerabilities analysis and detection tools. OWASP benchmark provides the users with test cases covering all kinds of vulnerabilities and a scoring tool to score the SAT-generated alert and compute the True Positive, False Negative, True Negative, and False Positive alerts percentages.

3) *Competition on Software Verification*: The European Joint Conferences on Theory & Practice of Software, ETAPS⁵ organizes each year, starting from 2012, an international competition on software verification to boost the invention of new methods, technologies, and tools to improve the software analysis process.

In the training phase, they provide several benchmark programs, each covering a wide range of CWEs weaknesses to SAT developers. Then, the submitted verifiers’ tool will be executed in the evaluation phase, and the number of solved instances and runtime is measured. Researchers could find valuable programs to use as a dataset within the ETAPS website and competition results of each year.

B. Papers’ Identified Security Bugs

Table V presents the security bugs handled on different papers to enhance SAT precision to detect potential security bugs without increasing the FPA rate. The paper [19] is the only one that considers almost security bugs during the FPA reduction process.

This section answered the research questions RQ4 and RQ5 by presenting the used datasets, the identified bug types, and the relevant projects and competitions.

VII. DISCUSSION: SHORTCOMINGS AND RECOMMENDATIONS

In the review of the identified approaches, this study depicted several shortcomings that decrease the effectiveness of false alert handling methods. We cite mainly:

- almost cited papers use open programs labeled by themselves without providing their alerts labeling datasets. Which will prohibit other researchers from reproducing the papers’ proposed method.

¹ <https://samate.nist.gov/index.php/SARD.html>
² https://samate.nist.gov/index.php/Software_Assurance_Reference_Dataset.html
³ <https://samate.nist.gov/SRD/testsuite.php>
⁴ <https://owasp.org/www-project-benchmark/>

⁵ <https://etaps.org/about/conferences>

TABLE IV. SELECTED SAT DATASETS

Dataset Name	Provider	Type	Language	Labeled	Programs Name	LOC	Extracted Features
Open source code	[16]	projects	Java		axiom	57,650	# of conditional statements
					guava	64,629	# of loop statements
					ivy	64,629	# of return statements
					jenkins-core	77,157	# of break or continue statements
					mahout	264,374	# of exit or assert method invocations
					maven-core	32,322	# of null expressions
					opennlp	36,151	# of comparisons with a null value
					poi	292,967	# of null assignments
					rav	30,762	# statements that return a null value
					tika	15,037	
Open Source	[18]	programs	C	-	brutefir-1.0f	103	-
					consolcalculator-1.0	298	
					id3-0.15	512	
					mp3rename-0.6	2,466	
					irmp3-0.5.3.1	3,797	
					httptunnel-3.3	6,174	
					e2ps-4.34	6,222	
					less-382	23,822	
					bison-2.5	56,361	
					pies-1.2	66,196	
					icecast-server-1.3.12	68,564	
					raptor-1.4.21	76,378	
					dico-2.0	84,333	
lsh-2.0.4	110,898						
Open source	[3]	libraries	C	-	BIND-1	-	is the loop condition contains nulls or not
					BIND-2		is the loop condition contains constants or not
					BIND-3		is the loop condition contains array accesses or not (
					BIND-4		is the loop condition contains && or not
					SM-1		is loop condition contains an index for a single array
					SM-2		is loop condition contains an index for multiple arrays
					SM-3		is the loop condition contains an array index outside the loop
					SM-4		is an index is initialized before the loop
					SM-5		# of exits in the loop
					SM-6		the (normalized) size of the loop
					SM-7		# of array accesses in the loop
					FTP-1		# of arithmetic increments in the loop
					FTP-2		# of pointer increments in the loop
FTP-3		is the loop condition prunes the abstract state or not					
Industrial application	[20]	Applications	Java/C++/C	-	Not provided	-	name of the codebase where the alert was detected
							audit determination
							full path to the file where the alarm occurs
							line number in the file where the alert occurs
							name of the CERT rule associated with the alert
							title of the CERT rule associated with the alert
							severity field of the CERT rule
							likelihood field of the CERT rule
							remediation field of the CERT rule
							priority field of the CERT rule
							level field of the CERT rule
							name of the function where the alert occurs
							#of lines of code in the function
		cyclomatic complexity of the function					
		#of significant lines of code in the function					
		cyclomatic complexity of the function					
		# of parameters to the function					
		# of lexical tokens in the function					
		line number where the function definition starts					
		line number where the function definition ends					
		# of alert that occur in this function					
		Filename					
		# of significant lines of code in the file					
		# of functions/methods in the file					
		average significant lines of code in functions in the file					
		average number of tokens in functions in the file					
		# of alerts that occur in the file					
		depth of the file where the alert occurs					
Juliet 1.0 – 1.3	NIST	Test cases	C/C++/JAVA	✓	test cases covering 118 C/C++ CWEs and 112 Java CWEs	-	-
Owasp benchmark	Owasp	Test cases	Java	✓	2,371 data points 1,193 false positive 1,178 true positive error	-	-
Juliet version 1.2	[19]	Test case + Alarms	C	✓	-	-	Name of the tool generating the warning # alerts in the same file Category of the warning # alerts triggered for the same line by any tool # of alerts less than 4 lines away from the triggered alert is the tool triggered an alert for that location
Open Source	[21]	programs	C/C++	-	bitlbee 4.2	68,413	-
					nghttp2 1.6.0	71,387	
					mupdf 1.2.337	122,481	
					h2o 1.7.2	517,731	
					xserver 1.14.3	568,964	
					php 5.6.7	709,356	

TABLE V. SOFTWARE CODING SECURITY BUGS

Paper reference	Language	Bug name
[16]	Java	General null dereference Dereferencing of an unchecked null value Dereferencing of a returned null value
[27][17]	C	Buffer overflow
[19]	C	Buffer overflow related issues Integer overflow and underflow Divisions by zero Uninitialized variable Unused variable Pointer issues (e.g.: Null pointer dereference) Misused operators (e.g.: i f (myVar = bu f [i])fg) Issues with function parameter Expression is either always true or always false Memory issues (e.g., Memory leak, Double free)
[3]	C	Format-string vulnerabilities Buffer-overflow
[15]	C	SQL inject flaw

- only a few papers consider the combination of more than one technique to handle alerts.
- almost proposed methods deal with the software source code refinements and analysis, which is not scalable as handling the SAT report directly.
- machine learning-based techniques require labeling efforts to examine and validate the proposed approach, which inhibits several researchers from using ML techniques.
- most of the proposed SAT false alert reduction approaches cover C, C++, and Java languages. However, languages such as Python used extensively with big data are rarely focused on by researchers.

To address these shortcomings, this study recommends focusing more on:

- combining several techniques parallelly or sequentially to get better accuracy and lower FPA rate. Existing studies on methods combination shows promising results [5].
- focusing more on the slicing approach to decompose extensive application on small slices is highly encouraged since SATs are very useful with small programs.
- focusing on the processing of SAT report directly to provide better scalability and testing easiness. The significant size of the alerts report is a suitable dataset to examine through deep learning techniques.
- thinking on labeling SAT alert report using active learning techniques to reduce the human effort [52].

VIII. CONCLUSION

This paper studied the recent efforts dealing with SAT alerts handling. It provides a new categorization of the used techniques as well as a comparison between the proposed methods. Then, it presents the datasets used to test and validate the different approaches along with information about their

size, features, and contained bugs. It summarizes the shortcomings of existing approaches and cites recommendations for future research to improve SAT false alerts handling.

As future plans, profoundly investigating the slicing approach of SAT alert reports and their processing using ML-based techniques will help preserve the SAT scalability and benefit from the high classification accuracy of ML-based methods.

REFERENCES

- [1] P. Copeland, "Google's innovation factory: Testing, culture, and infrastructure," in *2010 Third International Conference on Software Testing, Verification and Validation*. IEEE, 2010, pp. 11–14.
- [2] R. C. Seacord, D. Plakosh, and G. A. Lewis, *Modernizing legacy systems: software technologies, engineering processes, and business practices*. Addison-Wesley Professional, 2003.
- [3] K. Heo, H. Oh, and K. Yi, "Machine-learning-guided selectively unsound static analysis," in *2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE)*. IEEE, 2017, pp. 519–529.
- [4] F. Cheidari and G. Karabatis, "Analyzing false positive source code vulnerabilities using static analysis tools," in *2018 IEEE International Conference on Big Data (Big Data)*. IEEE, 2018, pp. 4782–4788.
- [5] F. Elberzhager, J. Münch, and V. T. N. Nha, "A systematic mapping study on the combination of static and dynamic quality assurance techniques," *Information and Software Technology*, vol. 54, no. 1, pp. 1–15, 2012.
- [6] S. Heckman and L. Williams, "A systematic literature review of actionable alert identification techniques for automated static code analysis," *Information and Software Technology*, vol. 53, no. 4, pp. 363–387, 2011.
- [7] V. R. L. de Mendonca, C. L. Rodrigues, F. A. A. de MN Soares, and A. M. R. Vincenzi, "Static analysis techniques and tools: A systematic mapping study," *ICSEA*, 2013.
- [8] T. Muske and A. Serebrenik, "Survey of approaches for handling static analysis alarms," in *2016 IEEE 16th International Working Conference on Source Code Analysis and Manipulation (SCAM)*. IEEE, 2016, pp. 157–166.
- [9] B. Aloraini, M. Nagappan, D. M. German, S. Hayashi, and Y. Higo, "An empirical study of security warnings from static application security testing tools," *Journal of Systems and Software*, vol. 158, p. 110427, 2019.
- [10] J. Herter, D. Kästner, C. Mallon, and R. Wilhelm, "Benchmarking static code analyzers," *Reliability Engineering & System Safety*, vol. 188, pp. 336–346, 2019.
- [11] P. Nunes, I. Medeiros, J. C. Fonseca, N. Neves, M. Correia, and M. Vieira, "Benchmarking static analysis tools for web security," *IEEE Transactions on Reliability*, vol. 67, no. 3, pp. 1159–1175, 2018.
- [12] M. Beller, R. Bholanath, S. McIntosh, and A. Zaidman, "Analyzing the state of static analysis: A large-scale evaluation in open source software," in *2016 IEEE 23rd International Conference on Software Analysis, Evolution, and Reengineering (SANER)*, vol. 1. IEEE, 2016, pp. 470–481.
- [13] A. Arusoae, S. Ciobăca, V. Craciun, D. Gavrilit, and D. Lucanu, "A comparison of open-source static analysis tools for vulnerability detection in c/c++ code," in *2017 19th International Symposium on Symbolic and Numeric Algorithms for Scientific Computing (SYNASC)*. IEEE, 2017, pp. 161–168.
- [14] S. Heckman and L. Williams, "A model building process for identifying actionable static analysis alerts," in *2009 International Conference on Software Testing Verification and Validation*. IEEE, 2009, pp. 161–170.
- [15] U. Koc, P. Saadatpanah, J. S. Foster, and A. A. Porter, "Learning a classifier for false positive error reports emitted by static code analysis tools," in *Proceedings of the 1st ACM SIGPLAN International Workshop on Machine Learning and Programming Languages*, 2017, pp. 35–42.
- [16] J. Yoon, M. Jin, and Y. Jung, "Reducing false alarms from an industrial-strength static analyzer by svm," in *2014 21st Asia-Pacific Software Engineering Conference*, vol. 2. IEEE, 2014, pp. 3–6.

- [17] W. Lee, W. Lee, D. Kang, K. Heo, H. Oh, and K. Yi, "Sound non-statistical clustering of static analysis alarms," *ACM Transactions on Programming Languages and Systems (TOPLAS)*, vol. 39, no. 4, pp. 1–35, 2017.
- [18] K. Heo, H. Oh, and H. Yang, "Learning a variable-clustering strategy for octagon from labeled data generated by a static analysis," in *International Static Analysis Symposium*. Springer, 2016, pp. 237–256.
- [19] A. Ribeiro, P. Meirelles, N. Lago, and F. Kon, "Ranking warnings from multiple source code static analyzers via ensemble learning," in *Proceedings of the 15th International Symposium on Open Collaboration*, 2019, pp. 1–10.
- [20] L. Flynn, W. Snaveley, D. Svoboda, N. VanHoudnos, R. Qin, J. Burns, D. Zubrow, R. Stoddard, and G. Marce-Santurio, "Prioritizing alerts from multiple static analysis tools, using classification models," in *2018 IEEE/ACM 1st International Workshop on Software Qualities and their Dependencies (SQUADE)*. IEEE, 2018, pp. 13–20.
- [21] H. Yan, Y. Sui, S. Chen, and J. Xue, "Machine-learning-guided tpestate analysis for static use-after-free detection," in *Proceedings of the 33rd Annual Computer Security Applications Conference*, 2017, pp. 42–54.
- [22] E. A. Alikhashshneh, R. R. Raje, and J. H. Hill, "Using machine learning techniques to classify and predict static code analysis tool warnings," in *2018 IEEE/ACS 15th International Conference on Computer Systems and Applications (AICCSA)*. IEEE, 2018, pp. 1–8.
- [23] S. Lee, S. Hong, J. Yi, T. Kim, C.-J. Kim, and S. Yoo, "Classifying false positive static checker alarms in continuous integration using convolutional neural networks," in *2019 12th IEEE Conference on Software Testing, Validation and Verification (ICST)*. IEEE, 2019, pp. 391–401.
- [24] J. J. Rooney and L. N. V. Heuvel, "Root cause analysis for beginners," *Quality progress*, vol. 37, no. 7, pp. 45–56, 2004.
- [25] J. Park, I. Lim, and S. Ryu, "Battles with false positives in static analysis of javascript web applications in the wild," in *2016 IEEE/ACM 38th International Conference on Software Engineering Companion (ICSE-C)*. IEEE, 2016, pp. 61–70.
- [26] T. Muske and U. P. Khedker, "Cause points analysis for effective handling of alarms," in *2016 IEEE 27th International Symposium on Software Reliability Engineering (ISSRE)*. IEEE, 2016, pp. 173–184.
- [27] T. Muske, R. Talluri, and A. Serebrenik, "Repositioning of static analysis alarms," in *Proceedings of the 27th ACM SIGSOFT international symposium on software testing and analysis*, 2018, pp. 187–197.
- [28] C. Baier and J.-P. Katoen, *Principles of model checking*. MIT press, 2008.
- [29] M. Valdiviezo, C. Cifuentes, and P. Krishnan, "A method for scalable and precise bug finding using program analysis and model checking," in *Asian Symposium on Programming Languages and Systems*. Springer, 2014, pp. 196–215.
- [30] T. Ball, E. Bounimova, R. Kumar, and V. Levin, "Slam2: Static driver verification with under 4% false alarms," in *Formal Methods in Computer Aided Design*. IEEE, 2010, pp. 35–42.
- [31] B. Chimdyalwar, P. Darke, A. Chavda, S. Vaghani, and A. Chauhan, "Eliminating static analysis false positives using loop abstraction and bounded model checking," in *International Symposium on Formal Methods*. Springer, 2015, pp. 573–576.
- [32] T. T. Nguyen, P. Maleehuan, T. Aoki, T. Tomita, and I. Yamada, "Reducing false positives of static analysis for sei cert c coding standard," in *2019 IEEE/ACM Joint 7th International Workshop on Conducting Empirical Studies in Industry (CESI) and 6th International Workshop on Software Engineering Research and Industrial Practice (SER&IP)*. IEEE, 2019, pp. 41–48.
- [33] T. Muske and U. P. Khedker, "Efficient elimination of false positives using static analysis," in *2015 IEEE 26th International Symposium on Software Reliability Engineering (ISSRE)*. IEEE, 2015, pp. 270–280.
- [34] Y. Kim, J. Lee, H. Han, and K.-M. Choe, "Filtering false alarms of buffer overflow analysis using smt solvers," *Information and Software Technology*, vol. 52, no. 2, pp. 210–219, 2010.
- [35] M. Bharati and M. Ramageri, "Data mining techniques and applications," 2010.
- [36] D. J. Hand, "Principles of data mining," *Drug safety*, vol. 30, no. 7, pp. 621–622, 2007.
- [37] S. Dua and X. Du, *Data mining and machine learning in cybersecurity*. CRC press, 2016.
- [38] D. Zhang, D. Jin, Y. Xing, H. Zhang, and Y. Gong, "Automatically mining similar warnings and warning combinations," in *2013 10th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*. IEEE, 2013, pp. 783–788.
- [39] F. Cheidari and G. Karabatis, "On the verification of software vulnerabilities during static code analysis using data mining techniques," in *OTM Confederated International Conferences "On the Move to Meaningful Internet Systems"*. Springer, 2017, pp. 99–106.
- [40] J. Nam, S. Wang, Y. Xi, and L. Tan, "Designing bug detection rules for fewer false alarms," in *Proceedings of the 40th International Conference on Software Engineering: Companion Proceedings*, 2018, pp. 315–316.
- [41] J. Yang, L. Tan, J. Peyton, and K. A. Duer, "Towards better utilizing static application security testing," in *2019 IEEE/ACM 41st International Conference on Software Engineering: Software Engineering in Practice (ICSE-SEIP)*. IEEE, 2019, pp. 51–60.
- [42] J. Euzenat, P. Shvaiko *et al.*, *Ontology matching*. Springer, 2007, vol. 18.
- [43] X. Zhang, R. Grigore, X. Si, and M. Naik, "Effective interactive resolution of static analysis alarms," *Proceedings of the ACM on Programming Languages*, vol. 1, no. OOPSLA, pp. 1–30, 2017.
- [44] D. Kästner, L. Mauborgne, S. Wilhelm, and C. Ferdinand, "High-precision sound analysis to find safety and cybersecurity defects," in *10th European Congress on Embedded Real Time Software and Systems (ERTS 2020)*, 2020.
- [45] H. Wang, M. Zhou, X. Cheng, G. Chen, and M. Gu, "Which defect should be fixed first? semantic prioritization of static analysis report," in *International Conference on Software Analysis, Testing, and Evolution*. Springer, 2018, pp. 3–19.
- [46] M. Weiser, "Program slices: formal, psychological, and practical investigations of an automatic program abstraction method," *PhD thesis, University of Michigan*, 1979.
- [47] B. Korel and J. Laski, "Dynamic slicing of computer programs," *Journal of Systems and Software*, vol. 13, no. 3, pp. 187–195, 1990.
- [48] H. Agrawal and J. R. Horgan, "Dynamic program slicing," *ACM SIGPlan Notices*, vol. 25, no. 6, pp. 246–256, 1990.
- [49] O. Chebaro, N. Kosmatov, A. Giorgetti, and J. Julliand, "Program slicing enhances a verification technique combining static and dynamic analysis," in *Proceedings of the 27th Annual ACM Symposium on Applied Computing*, 2012, pp. 1284–1291.
- [50] J. Thome, L. K. Shar, D. Bianculli, and L. Briand, "Security slicing for auditing common injection vulnerabilities," *Journal of Systems and Software*, vol. 137, pp. 766–783, 2018.
- [51] A. Ribeiro, P. Meirelles, N. Lago, and F. Kon, "Ranking source code static analysis warnings for continuous monitoring of floss repositories," in *IFIP International Conference on Open Source Systems*. Springer, 2018, pp. 90–101.
- [52] B. Mozafari, P. Sarkar, M. Franklin, M. Jordan, and S. Madden, "Scaling up crowd-sourcing to very large datasets: a case for active learning," *Proceedings of the VLDB Endowment*, vol. 8, no. 2, pp. 125–136, 2014.

CDRA: A Community Detection based Routing Algorithm for Link Failure Recovery in Software Defined Networks

Muhammad Yunis Daha¹, Mohd Soperi Mohd Zahid², Babangida Isyaku³, Abdussalam Ahmed Alashhab⁴

Department of Computer and Information Sciences,
Universiti Teknologi PETRONAS, Seri Iskandar, Malaysia^{1,2,4}
Department of Mathematics and Computer Science,
Sule Lamido University, Kafin Hausa, Nigeria³

Abstract—The increase in size and complexity of the Internet has led to the introduction of Software Defined Networking (SDN). SDN is a new networking paradigm that breaks the limitations of traditional IP networks and upgrades the current network infrastructures. However, like traditional IP networks, network failures may also occur in SDN. Multiple research studies have discussed this problem by using a variety of techniques. Among them is the use of the community detection method is one of the failure recovery technique for SDN. However, this technique have not considered the specific problem of multiple link multi-community failure and inter-community link failure scenarios. This paper presents a community detection-based routing algorithm (CDRA) for link failure recovery in SDN. The proposed CDRA scheme is efficient to deal with single link intra-community failure scenarios and multiple link multi-community failure scenarios and is also able to handle the inter-community link failure scenarios in SDN. Extensive simulations are performed to evaluate the performance of the proposed CDRA scheme. The simulation results depicts that the proposed CDRA scheme have better simulations results and reduce average round trip time by 35.73%, avg data packet loss by 1.26% and average end to end delay 49.3% than the Dijkstra based general recovery algorithm and also can be used on a large scale network platform.

Keywords—Software Defined Network (SDN); community detection methods; CDRA; link failure

I. INTRODUCTION

The complexity, uncontrollability, and the increasing demand of the Internet has led to low utilization of network resources [1]. To address this problem, a new concept of Software Defined Network (SDN) technology has been introduced. The SDN technology decouples the control plane from the data plane and makes the IP networks programmable [2]. However, like traditional IP networks, SDN technology may also have network failure problems. Unlike other network failure problems, link failure is considered to be the most prevalent network failure in both traditional and SDN networks [3]. Link failures must be rectified as soon as possible, as they

can cause network congestion and decrease network efficiency. However, unlike traditional IP networks, the SDN can heal the link failure issue by setting up the controller to shift to another alternate shortest path assigned with OpenFlow [4], [5]. Recovery from link failure can be accomplished either through the proactive failure recovery approach or through the reactive failure recovery approach. In the proactive failure recovery method, backup resources are pre-reserved before the occurrence of the failure scenario. On the other hand, in the reactive failure recovery method, backup resources are reserved after the failure scenario [2]. Both the proactive and the reactive failure recovery approaches have their own benefits and limitations. Based on proactive and reactive failure recovery approaches a variety of research studies have been conducted to make the link failure recovery process more fast and efficient. Among the existing work, the use of a community detection scheme for the failure recovery process of SDN is one of the reactive approaches. The existing work [6], [7] shown good performance, however, they have not addressed the multiple link failure and inter-community link failure problem.

This paper presents a reactive failure recovery approach based CDRA scheme for link failure recovery in SDN. The proposed CDRA scheme is efficient and capable to address the single link intra-community failure scenario and multiple link multi-community failure scenario and also able to handle the inter-community link failure scenarios in SDN. This research study has the following primary contribution:

- The CDRA scheme is proposed which deals with both single and multiple link failure scenarios.
- This CDRA scheme is efficient to deal with intra-community, inter-community and multi-community link failure scenarios.
- The CDRA scheme implemented the Louvain and Infomap community detection methods along with the previous study Girvan and Newman method.

- Lastly this study presents a comparative analysis of all three community detection approaches in term of their performance after failure scenarios in SDN.

The rest of the paper is organized as follows. Section II will discuss the literature review part. Section III talks about the community detection methods used for the proposed CDRA scheme. Section IV discussed the Proposed CDRA scheme for single and multiple link community and inter-community link failure scenarios in SDN. Section V and Section VI present the mathematical explanation of the proposed CDRA scheme and also discuss an example case study respectively. Simulation setup and result discussion are presented in Section VII. Finally, Section VIII delivers an overall conclusion and future direction based on the result analysis and discussion.

II. LITERATURE REVIEW

Based on the link failure scenarios in SDN, failure recovery approaches are classified into two categories, the first one is the proactive failure recovery approach and the second one is the reactive failure recovery approach [2], [8]. The processing time of proactive failure recovery is fast however, in proactive mechanism, flow entries are installed along with the TCAM (ternary content-addressable memory) which is limited in size, expensive and power-hungry [9], [10].

However, on the other hand, the reactive recovery mechanism is cheaper than the proactive mechanism. But, the reactive failure recovery approach has the latency problem as the network controller will first need to calculate an alternative path and then install the flow entries in the relevant switches [3].

Many researchers have discussed their works by using the proactive and reactive failure recovery approaches to overcome the failure scenarios in SDN. This section presents some of the research studies relevant to the proposed CDRA scheme conducted on the basis of the reactive failure recovery approach for link failure recovery scenarios in SDN.

Sharma et al. [11] describe the reactive failure recovery mechanism in which the controller adjusts the topology and determines a new path for each failure-affected flow after failure detection. After pushing new flow entries and deleting original functioning path flow entries, the redirection will be complete. The results demonstrate that the reactive recovery strategy has larger recovery latency, making it impossible to achieve the carrier-grade requirement. The author [12] demonstrates the restoration based link failure scenario in SDN but the conducted study is performed over small network topology and only discuss the performance of link failure scenarios in SDN. The authors of [13] developed a novel technique for rapid restoration by lowering the processing time, which is normally paid by the controller, by identifying an alternate path (from end-to-end) with a low

operation demand. One major flaw in this research is that it does not ensure that the health nodes in the impacted path will be in the same sequence on the alternate path. Furthermore, there is a scarcity of information on the simulation technology that was utilized.

Research work proposed in [14] demonstrated how a quick restoration may be achieved, however, the experimental topologies in both studies were small scale. In addition, the processing time for setting up the selected path was neglected, which is a need in SDNs to re-route traffic from the impacted primary path to the backup way.

Author in [15] suggested a reactive link failure recovery approach based on the shortest path first algorithm. Each path's packets are classified as high or low priority. For high-priority packets, the suggested approach assures the shortest possible delay. The method, however, can only be used on a small-scale network and is not suitable for large-scale SDNs. By spreading traffic evenly among the available paths, the method also reduces congestion. As a result, as the network grows larger, the algorithm's complexity grows. Another flaw in the suggested solution is that the implementation mechanism is given insufficient information. Furthermore, the method has not been validated using conventional internet topology datasets.

Unlike previous studies, the approach developed by [6], [7] used the community detection technique for failure recovery in SDN. In their study, the authors first divide the whole network into cliques. When a link failure occurs, instead of correcting the whole network from the beginning, it is possible to correct only the path in that clique. Thus, the path recovery works faster. But on the other hand, they have not considered the specific problem of multiple link failure and inter-community link failure problem scenarios in SDN and their used community detection method is relatively slow and time costing [16].

In comparison with the previous research studies, this paper proposed a community detection-based routing algorithm for link failure recovery in SDN. The proposed CDRA scheme is capable to deals with both single and multiple link failure scenarios. Moreover, the proposed CDRA scheme is efficient to deal with both the inter and the intra-community failure problem as well. Unlike previous studies, this paper implies Louvain and Infomap community detection methods. Both community detection algorithms accuracy is comparable to other community detection algorithms and also have better scalability [17]–[19]. A summary of the related work to reactive failure recovery relevant to the proposed CDRA scheme is presented in Table I.

III. COMMUNITY DETECTION METHODS

The community detection methods can increase the speed and efficiency with which networked data is processed, analyzed, and stored. Various types of network-related problems, such as routing and data forwarding, have been solved using community detection [20]

TABLE I. SUMMARY OF THE RELATED WORK

Author	Year	Recovery Approach	Link Failure Type	Community Detection Method	Limitations
Sharma [11]	2011	Reactive	Single Link Failure	No	Large Recovery Time Delay
Sharma [14]	2013	Reactive and proactive	Single Link Failure	No	The experimental topologies were small scale. In addition, the processing time for setting up the selected path was neglected.
Astaneh [13]	2016	Reactive	Multiple Link Failure	No	Does not ensure the health nodes in the impacted path, and there is a scarcity of information on the simulation technology.
Malik [6]	2017	Reactive	Single Link Failure	Girvan and Newman	Not consider addressing Inter community failure and multiple failure.
Muthuma-[15]	2017	Reactive	Single and Multiple Link Failure	No	Can only be used on a small-scale network. Secondly, When network grows larger, the algorithm's complexity grows.
Malik [7]	2020	Reactive	Single Link Failure	Girvan and Newman	Not consider Inter community failure and multiple failure. Used relatively Slow community detection Method.
Yunis [12]	2021	Reactive	Single&multi Link Failure	No	Studied link failure performance over small network topology in SDN.

[21]. Many algorithms have been developed to recognise communities like structures in networks such as Girvan and Newman, 2002 [22], Clauset, 2004 [23], Louvain, 2008, [24] Infomap, 2008 [25]. This section presents a comparative analysis between Louvain, Infomap, and the Girvan and Newman community detection algorithms. Fig. 1 shows the network communities obtained from Cost266 network topology [26] by implementing the Louvain, Infomap and Girvan and Newman community detection methods.

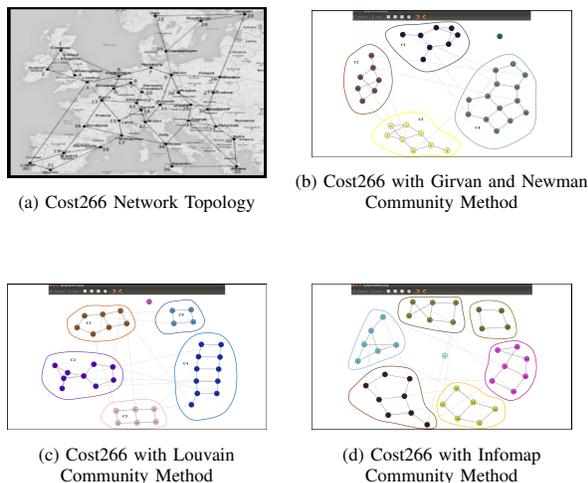


Fig. 1. Implementation of Community Detection Methods over Cost266 Network Topology.

In a previous study, [6], [7] author, used the Girvan and Newman community detection approach for partitioning the network graph into different network communities. The Girvan and Newman community detection

algorithm identifies edges that lie between communities in a network and removes them thereby allowing for the identification of distinct communities in the network.

However, on the other hand, when dealing with a large network graph, this algorithm is not particularly efficient and not recommended for large data sets. Moreover, the Girvan and Newman algorithm has time complexity $\mathcal{O}(m^2n)$ which make this algorithm relatively slow and time costing as compared to the Louvain and Infomap community detection method [16], [24], [27], [28].

Unlike the previous study, based on the concept of modularity, this paper used the Louvain and Infomap community detection method along with the previous study community detection method for partitioning the network graph. High modularity networks feature extensive connections between nodes inside communities, but sparse connections between nodes in different communities [16]. The Louvain community detection algorithm is a hierarchical technique that combines communities into one node repeatedly and performs the modularity clustering on the condensed network. The Louvain algorithm efficiently detects large-scale communities and achieves high modularity. This optimizes for each community the modularity score, where the modularity quantifies the quality of node assignment to the groups. The time complexity of Louvain community detection method is $\mathcal{O}(n \log n)$ [16], [24].

Similar to the Louvain community detection method, the Infomap is another community detection method that allows for the creation of high-quality communities. Infomap method figures out communities by employing random walks to analyze the information flow through a network. The smaller the number of candidates, the more information about the original network has been

transferred. Furthermore, it also tries to minimize the cost function of a network graph. The Infomap community detection method runs on time complexity of $\mathcal{O}(m)$ which make this method more efficient [16], [25].

Both algorithm's accuracy is comparable to other community detection algorithms and also have better scalability [17]–[19].

Fig. 2 represents that the modularity obtained by the Louvain and Infomafop community detection methods of different network topologies before and after failure scenarios are higher than the modularity obtained by Girvan and Newman community detection method.

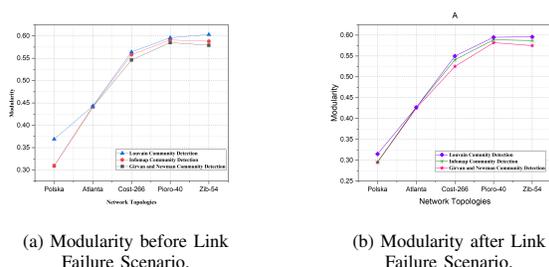


Fig. 2. Modularity of Different Network Communities for Different Community Detection Methods.

IV. CDRA: A PROPOSED FAILURE RECOVERY SCHEME IN SDN

Based on this principle of community detection algorithms, a community detection-based routing algorithm is proposed. The proposed CDRA scheme efficiently deals with both single and multiple link failure scenarios. The proposed CDRA scheme divides a network graph into a small number of different network communities by implementing the community detection algorithms as mentioned in the previous section. Once the network graph is split into different small communities, a data packet is sent from the source node to the destination node. Data packet passes through different network communities that belong to that primary path.

During this data transmission process, once failure happened, most probably either inside the single community or inside two different communities or even between two different communities belonging to that affected path, then instead of searching and correcting throughout the entire graph the proposed CDRA scheme only considered the failure affected communities for treatment. Through this proposed CDRA scheme, only the failure-affected communities are required to install a new path, and the rest of the communities are not disturbed and carry on their duties. This helps the controller to directly deal with that particular community switches and assigned new flow entries instead of searching through the entire network graph. Partitioning the

network graph through community detection approaches and directly dealing only with failure affected network communities instead of treating the entire network graph, makes the CDRA scheme more efficient and productive as compared to the general recovery algorithm which considers the complete graph in the failure recovery scenario.

Fig. 3, represents the research framework of the proposed CDRA scheme which is composed of SDN controller, topology analyzer, community producer and route finder. The POX controller used as a remote controller that communicate with application plane and data plane through Northbound API and Southbound API respectively. The topology analyzer is used to analyze the network topology graph through POX OpenFlow-discovery. The community producer and route finder, are the two main components of this research framework and our contribution lies in these two components.

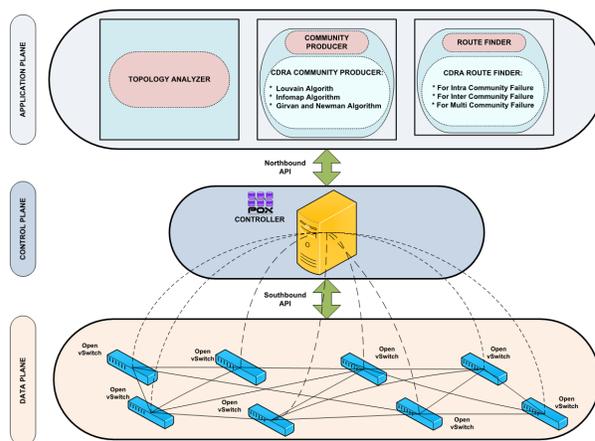


Fig. 3. Research Framework for the Proposed CDRA Scheme.

A. Proposed CDRA Scheme for Community Producer and Reroute Finder

The proposed CDRA scheme implies the community detection methods to determine link failure recovery in SDN. The CDRA scheme can be classified into the following two steps:

The first step of the proposed CDRA scheme is the community producer. The community producer split the network topology graph into different sizes of small network communities by using the Louvain, Infomap, and Girvan and Newman community detection methods. The obtained network communities after implementing the community detection methods can have a different number of nodes and links. Different colors are used for different network communities to make them easy identifiable. The second step of the proposed CDRA scheme is to determine the shortest path from the source node to the destination node passing through different network communities before and after the occurrence

of link failure scenarios. Two algorithms have been developed for the second step of the router finder.

The first algorithm is known as the Dijkstra based general recovery algorithm. The general recovery algorithm is based on the simple Dijkstra algorithm that describes the default action which is done through the SDN controller when link failure happens. Algorithm 1 eliminates the flow entries of failure effected path and then install the rules for back-up path from source node to destination node after the occurrence of link failure scenarios. Algorithm 1, finds the shortest path without using the community detection method. The pseudocode of this general recovery algorithm is presented in Algorithm 1.

Algorithm 1 Dijkstra based general recovery algorithm to find the shortest path from network graph N_G

- 1: **Input:** Implementing the Dijkstra based Recovery Algorithm for Network Graph:= N_G
 - 2: **Output:** Getting Shortest path based on the Dijkstra based Recovery Algorithm
 - 3: **Start**
 - 4: Setting-up the Dijkstra based Recovery Algorithm for Network Graph:= N_G
 - 5: When Link is up:
 - 6: Set Primary path as short path
 - 7: $P_p \in P_{short}(S_n, D_n)$
 - 8: When Link is down:
 - 9: Set Secondary path as short path
 - 10: $S_p \in P_{short}(S_n, D_n)$
 - 11: $P_{short}(S_n, D_n) := P_{short}(S_n, D_n) - P_p$
 - 12: $S_p := D_g[P_{short}(S_n, D_n)]$
 - 13: **End**
-

Algorithm 2 CDRA: Community based routing algorithm for network graph N_G

- 1: **Input:** Implementing the CDRA approach for Network Graph:= N_G
 - 2: **Output:** Getting Shortest path based on the CDRA approach
 - 3: **Start**
 - 4: Setting-up the CDRA approach for Network Graph:= N_G
 - 5: When Link is up:
 - 6: Set Primary path as short path
 - 7: $P_p \in P_{short} \{(S_n, N_{cs}), (D_n, N_{cd})\}$
 - 8: When Link is down:
 - 9: Set Secondary path as short path
 - 10: $S_p \in P_{short}$
 - 11: $P_{short} \{(S_n, N_{cs}), (D_n, N_{cd})\}$
 - 12: $P_{short} \{(S_n, N_{cs}), (D_n, N_{cd})\} - P_p$
 - 13: $S_p := D_{N_c}[P_{short} \{(S_n, N_{cs}), (D_n, N_{cd})\}]$
 - 14: **End**
-

The second algorithm is known as the proposed community detection-based routing algorithm. The proposed CDRA scheme is discussed in Algorithm 2. Algorithm

2 is compared with the Dijkstra based general recovery algorithm 1 and set-up it as a meaningful and appropriate benchmark based on the previous research study [6], [7]. Algorithm 2 shows the proposed CDRA scheme that find the shortest path from source node to destination node of a network graph before and after the occurrence of link failure scenarios. Algorithm 2 implies the community detection methods for finding the shortest path after the occurrence of link failure scenarios. The contribution of the proposed CDRA scheme lies in Algorithm 2. The pseudocode of the proposed CDRA scheme is presented in Algorithm 2.

V. MATHEMATICAL EXPLANATION OF COMMUNITY DETECTION METHOD FOR THE PROPOSED CDRA SCHEME

Mathematically a network graph G is a combinational set of vertices "V" and edges "E" as $G = (V, E)$. Both vertices and edges connect different set nodes in the network graph. By implementing the community detection approach a network graph can be split into the different numbers of communities and every network community defined the subset of the network graph as $N_c \subseteq G$. Where the network community is the combination set small network communities $N_c = (N_{c1}, N_{c2}, \dots, N_{cn})$. Every small network community is also the combination of different set of nodes and links presented in equation 1.

$$N_{c1} = (v_1, e_1) | v_1 \subseteq V \wedge e_1 \subseteq E \quad (1)$$

A path "P" is a set of distance that start from a source node "Sn" of a network community and ends at the destination node "Dn" of an other network community, passes through different set of different small network communities as presented in equation 2.

$$P = \{S_{n1}, N_{c1}, S_{n1+n}, N_{c1+n}, \dots, D_n, N_{cd}\} \quad (2)$$

Once the path "P" is set up between a source node and the destination node the concept of link failure is introduced and failure recovery scenarios are presented as follows:

The first failure recovery scenario represents the single link intra community failure scenario, when link link is down between two node which belongs to the same network community N_{c1} .

Equation 3, define the first failure recovery scenario, when failed link between two different node $(S_{n1}, N_{c1}, S_{n1+n}, N_{c1})$ belongs to to the same network community N_{c1} .

$$F_{N_{c1}} = (S_{n1}, N_{c1}, S_{n1+n}, N_{c1}) | \exists(N_{c1} : N_{c1}) \\ = (v_1, e_1) \subseteq F_{N_{c1}} \in e_1 \quad (3)$$

Unlike, first failure recovery scenario, the second failure recovery scenario is about the inter community link failure where the failed link belongs between two different nodes present inside two different network communities.

Equation 4, shows the inter community link failure scenario between node (S_{n_1}, N_{c_1}) present inside network community N_{c_1} and node (S_{n_1+n}, N_{c_2}) present inside network community N_{c_2} .

$$F_{N_{c_1-2}} = (S_{n_1}, N_{c_1}, S_{n_1+n}, N_{c_2}) | \exists (N_{c_1} : N_{c_2}) \\ |(N_{c_1} = (v_1, e_1), N_{c_2} = (v_2, e_2)) | (N_{c_1} = N_{c_2}) \\ \Rightarrow (S_{n_1}, N_{c_1}) \in v_1 \wedge (S_{n_1+n}, N_{c_2}) \in v_2 \\ \subseteq F_{N_{c_1-2}} \in (e_1, (N_{c_1} - N_{c_2})) \quad (4)$$

Lastly, the third failure recovery scenario shows the multiple link multi-community failure recovery scenario, when the failed links belong to four different nodes present inside two different network communities (i.e. node $(S_{n_1}, N_{c_1}, S_{n_1+n}, N_{c_1})$ belongs to network community N_{c_1} and nodes $(S_{n_n}, N_{c_2}, S_{n+n}, N_{c_2})$ belongs to network community N_{c_2} . Multiple link failure scenario inside two network community N_{c_1} and N_{c_2} is shown in equation 5.

$$F_{N_{c_1}} - F_{N_{c_2}} = \{(S_{n_1}, N_{c_1}, S_{n_1+n}, N_{c_1}), (S_{n_n}, N_{c_2}, \\ S_{n+n}, N_{c_2})\} | \exists (N_{c_1} : N_{c_1}, N_{c_2} : N_{c_2}) | (N_{c_1} = (v_1, e_1) \\ , N_{c_2} = (v_2, e_2)) \subseteq F_{N_c} (F_{N_{c_1}} - F_{N_{c_2}}) \\ \in (e_1 N_{c_1}, e_2 N_{c_2}) \quad (5)$$

The contribution of the proposed CDRA scheme is explained in equation 4 and equation 5.

The path obtained by applying the general recovery algorithm without community detection approach implementation from the source node to the destination node is presented in equation 6.

$$P_{D_g} = \{P | \forall (S_n, D_n) \in V : P = D_g(P(S_n, D_n))\} \quad (6)$$

Unlike equation 6, equation 7, represents the shortest path formula for the proposed CDRA scheme after implementing the community detection approach.

$$P_{D_{N_c}} = \{P | \forall (S_n, N_{c_s}, D_n, N_{c_d}) \in V : \\ P = D_{N_c}(P(S_n, N_{c_s}, D_n, N_{c_d}))\} \quad (7)$$

A set of notations used for the explanation of the proposed CDRA scheme and algorithms are presented in Table II.

TABLE II. LIST OF NOTATIONS

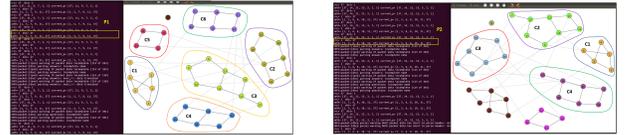
Symbol	Description
P_p / P_s	Primary path / Secondary path
S_n / D_n	Source node / Destination node
N_c	Network community
N_{c_s}	Network community based on source
N_{c_d}	Network community based on destination
F_{N_c}	Failure in network community
D_g	Dijkstra algorithm based on graph
D_c	Dijkstra algorithm based on community
P_{D_g}	Path obtained by Dijkstra algorithm
$P_{D_{N_c}}$	Dijkstra-based on community path

VI. CDRA: AN EXAMPLE CASE STUDY

This section, explains the functionality of the proposed CDRA scheme by using the COST266 network topology [26] as an example case study. The Cost266 network topology is made up of 37 nodes and 57 links that connect them. Following the implementation of the community detection algorithms, different colors were utilized to represent the various network communities. Fig 4(a) represents the network topology graph after the implementation of the proposed CDRA scheme before happening link failure scenario. In which a primary path named P1 pass through three different network communities (i.e. N_{c_1} , N_{c_2} and N_{c_3} . The single link intra-community, inter-community and multiple link multi-community failure recovery cases are explained in following three scenarios:

- Single link intra-community failure recovery scenario:

Let suppose the link between nodes 5 and 7 is down. It's worth noting that this is the first failure scenario in which both nodes node 5 and node 7 are members of the same network community N_{c_1} as shown in Fig. 4(a). After happening failure, the network controller calculates a new path "P2" and updates the network topology graph. This time the second path passes through four different network communities (i.e. N_{c_1} , N_{c_2} , N_{c_3} , and N_{c_4} as shown in Fig 4(b).



(a) CDRA before Intra Community Link Failure Scenario. (b) CDRA after Intra Community Failure Scenario.

Fig. 4. Single Link Intra Community Failure Recovery Scenario Through CDRA Scheme.

- Inter-community link failure recovery scenario:

In the inter-community link failure recovery scenario, suppose the link between two nodes, node 7 and node 9 fails. It should be noticed that this time both nodes belong to two separate network communities as node 7 belongs to N_{c_1} and node 9 belongs to N_{c_2} as shown in Fig. 5(a). After the occurrence of inter-community link failure scenario the network controller updates the network topology and determine a new path "P3" that passes through three network communities (i.e. N_{c_1} , N_{c_2} and N_{c_3} as shown in Fig 5(b).

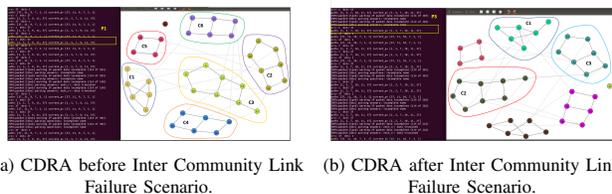


Fig. 5. Inter Community Link Failure Recovery Scenario through CDRA Scheme.

- Multiple link multi-community failure recovery scenario:

Lastly, in the multiple link multi-community failure recovery scenario, imagine a multi-link failure that occurred simultaneously between four separate nodes. This time suppose the first failure occurred between nodes 5 and node 7, which belong to a network community one N_{c_1} , and the second failure occurred between nodes 9 and node 11, both nodes are present inside the network community two N_{c_2} . This time, all four nodes are members of two different network communities N_{c_1} and N_{c_2} as shown in Fig. 6(a). After the occurrence of multiple failures inside two different network community, the network controller creates a new path, "P4", and this time path that passes through two network communities (i.e. N_{c_1} , and N_{c_2} as shown in Fig 6(b).

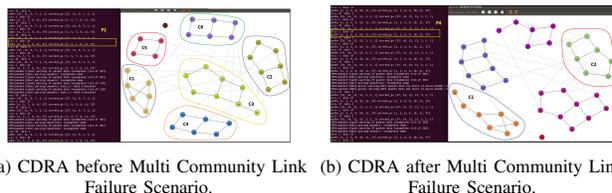


Fig. 6. Multiple Link Multi-community Failure Recovery Scenario through CDRA Scheme.

This example study indicates that after failure scenarios only a limited number of affected network communities need to be evaluated. The controller just needs to replace and update a few listed nodes that belong to affected communities and have been adopted by new pathways to update the rules. The rest of the nodes, which are dispersed among the various communities, keep their configuration and order. This is how the proposed CDRA scheme makes the failure recovery process more efficient by directly dealing with the failure affected communities and installing a new path, instead of searching through the entire network graph.

VII. SIMULATION SETUP AND RESULT DISCUSSION

To simulate the proposed CDRA scheme the following software tools and programming language is used on the experimental platform: Ubuntu 14.04 LTS is a long-term support version of Ubuntu, Mininet 2.2 developed by Nick McKeown from Stanford University, POX Controller (carp branch), NetworkX, Python 2.7.9 version. The hardware environment includes a PC a 64-bit operating system, x64- based processor DESKTOP-851QV1U that has an Intel(R) Core(TM) i7-4770 CPU @ 3.40GHz 3.40 GHz as a CPU, 16.0 GB DDR3 1600 of internal user memory. Summary of the simulation setup along with the software tools is presented in Table III.

TABLE III. SUMMARY OF THE SIMULATION SETUP ALONG WITH THE SOFTWARE TOOLS

Operating system	Ubuntu 14.04 LTS
System Specification	x64-Intel(R)-Core(TM) i7-4770 CPU
simulation Tool	Mininet 2.2
Remote Controller	POX Controller
POX Branch	Carp
OpenFlow Support	OpenFlow v1.0
Programming Language	Python 2.7.9
Network Topology	Atlanta , Cost-266
Bandwidth	10 Mbit/sec
Delay	1 ms
Packet Size (byte)	64

Furthermore, a system work flowchart is presented in Fig. 7, which depicts the simulation setup for the proposed CDRA recovery scheme and the general recovery scheme.

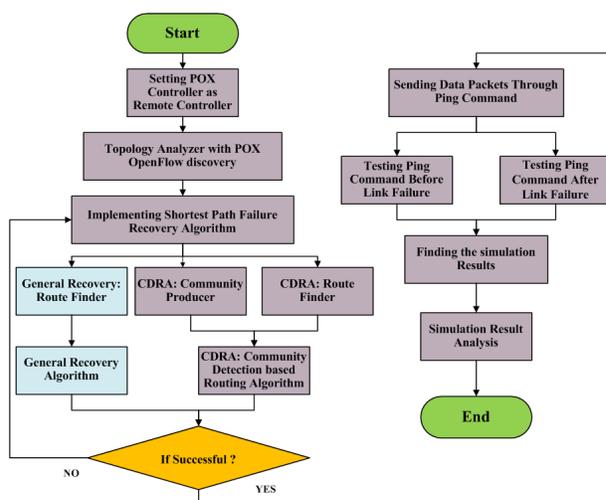


Fig. 7. System Work Flowchart for the Proposed CDRA Scheme and the General Recovery Algorithm.

A. Performance Evaluation

This paper examines the performance of the general recovery algorithm and the proposed CDRA scheme after the occurrence of link failure scenarios. We chose two topologies from SNDlib [26] to function as experimental topologies (Atlanta and Cost266), with the scale increasing from Atlanta to Cost266. To simulate these topologies, we utilize Mininet, and the Pox controller to monitor and operate the network. Both recovery algorithms are implemented in the POX controller and studied and measured by the average round trip time (RTT), average data packet loss rate and the average end-to-end delay as performance metrics. Furthermore, this study conducted the simulation results multiple times and calculated their average results with a possible 95 percent confidence interval. The performance metrics simulation results study for both recovery algorithms is discussed in the next section.

B. Average Round-Trip Time (RTT)

The RTT (round trip time) refers to the time that an ICMP (internet control message protocol) data packet takes to travel from source to destination, as well as the time it takes for the destination to acknowledge receipt of the packet. The average RTT can be measured by dividing the complete amount of time by the sum of total RTT by the network server and the client. The average RTT measurements for both the general recovery algorithm and the proposed CDRA scheme after the occurrence of single link intra-community failure, inter-community link failure, and multiple link multi-community failure events are shown in Fig. 8, Fig. 9, and Fig. 10, respectively.

Simulation results show that the values of average RTT after the occurrence of the single link intra-community failure, inter-community link failure, and multiple link multi-community failure scenarios are lower for the proposed CDRA scheme. However, the values of average RTT after the occurrence of link failure scenarios are higher for the general recovery algorithm. In a small network topology like Atlanta, the average RTT difference is not as much but when it comes to large network topologies like Cost266 the the performance difference of average RTT after failure scenarios for both algorithms is clearly visible. This is because the proposed CDRA scheme is more optimized and efficient for path-finding after failure scenarios in the large network than the general recovery algorithm. Because the proposed CDRA scheme split the whole network graph into small communities and hunt for the special the failure affected communities. But on the other hand, the general recovery algorithm search throughout the network graph for path-finding after the occurrence of failure scenarios which is time costing.

Furthermore, simulation results also reflects the community detection methods comparison in term of the average RTT after happening link failures for intra-community, inter-community, and multi communities.

Simulation results also show that the Louvain and Infomap community detection approaches perform slightly better than the Girvan and Newman community detection approaches. This is because the Girvan and Newman community detection approach is a bit time-consuming and not a preferred approach over a large network. Unlike the Girvan and Newman community detection approach, the Louvain and Infomap community detection approaches are mostly considered to be more optimized approaches for community detection. Research the study supports our results as the Girvan and Newman community detection approach consumes slightly larger time and Louvain community detection approach is more favorable while considering large network graphs [17]–[19].

C. Average Data Packet Loss

Data Packet loss happens when one or more data packets roaming over a computer network do not arrive at their required destination. Network congestion, hardware difficulties, and software faults are all major causes of data packet loss. The ping command is used to send a large number of ICMP data packets from the source node to the destination node, and collect the unsuccessful responses to compute the average data packet loss. Figure 11, Figure 12, and Figure 13 respectively shows the average data packet loss rate readings after the occurrence of intra-community, inter-community, and multi-community link failure scenarios for both the general recovery algorithm and the proposed CDRA scheme.

Simulation results depict that the average value of data packet loss for the general recovery algorithm is higher than the average value of data packet loss achieved by the proposed CDRA recovery scheme. The reason behind this phenomenon is that the general recovery algorithm is not as time-efficient as compared to the proposed CDRA scheme. Because, after happening link failure scenarios, the general recovery algorithm takes longer to search across the whole graph for data packet re-transmission after the event of a link failure. On the other hand, the proposed CDRA scheme, which works only with a small number of failures affected tiny communities in big network graphs and takes less time. Taking a longer time for data packet transmission result in more data packet loss.

In addition, simulation results also reveal that when compared to the Girvan and Newman community techniques, the Infomap and Louvain community methods have a lower or equivalent average data packet loss rate. This is because the Louvain and Infomap community techniques are faster and more efficient than the time-consuming Girvan and Newman method.

D. Average End-to-End Delay

The time it takes for a packet to go from source to destination via a network is referred to as end-to-end delay. The end-to-end delay is determined by dividing the time when data is received by the time it

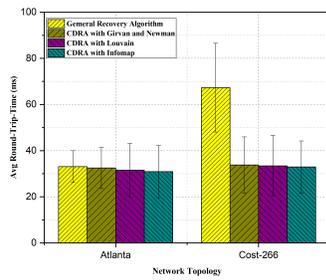


Fig. 8. Average RTT after Occurrence of Single Link Intra-community Link Failure Scenario.

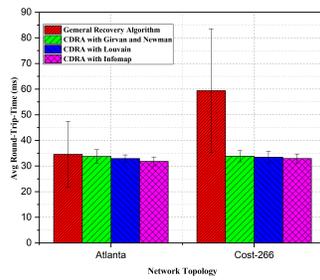


Fig. 9. Average RTT after Occurrence of Inter-community Link Failure Scenario.

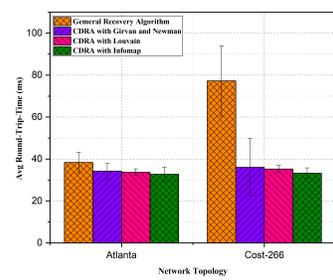


Fig. 10. Average RTT after Occurrence of Multiple Link Multi-community Link Failure Scenario.

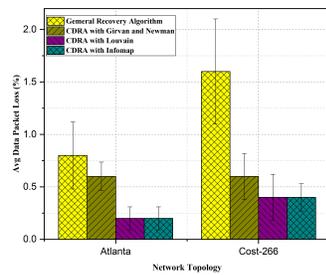


Fig. 11. Average Data Packet Loss after Occurrence of Single Link Intra-community Link Failure Scenario.

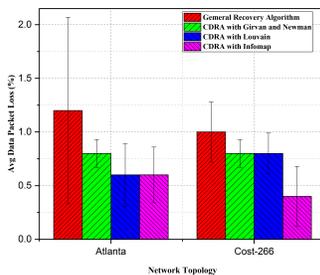


Fig. 12. Average Data Packet Loss after Occurrence of Inter-Community Link Failure Scenario.

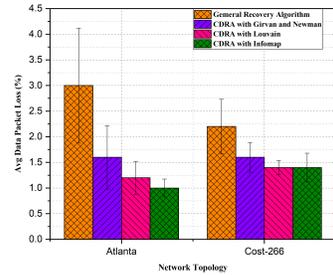


Fig. 13. Average Data Packet Loss after Occurrence of Multiple Link Multi-community Link Failure Scenario.

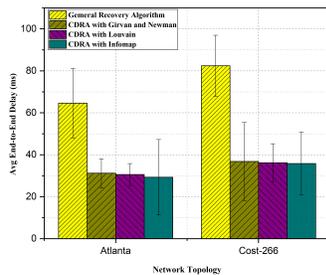


Fig. 14. Average End-to-end Delay after Occurrence of Single Link Intra-community Link Failure Scenario.

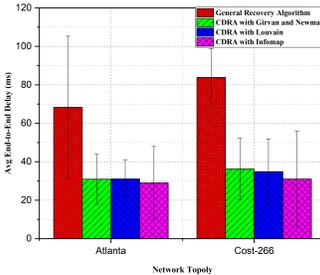


Fig. 15. Average End-to-end Delay after Occurrence of Inter-Community Link Failure Scenario.

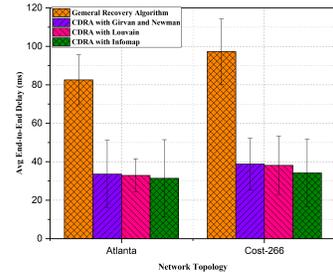


Fig. 16. Average End-to-end Delay after Occurrence of Multiple Link Multi-community Link Failure Scenario.

takes to transmit data by the number of data packets received. This paper measured the average end-to-end delay for both the general recovery algorithm and the proposed CDRA scheme after the occurrence of the link failures scenarios for intra-community, inter-community, and multi communities.

Simulation results of Fig. 14, Fig. 15, and Fig. 16, respectively shows that average end-to-end delay results obtained by the general recovery, algorithm are higher than the average end-to-end delay results obtained by the proposed CDRA scheme. The reason behind these

simulations results is the same as we discussed earlier for the average RTT and average data packet loss that the general recovery algorithm takes more time than the proposed CDRA recovery scheme. Because the proposed CDRA recovery scheme split the network graph into small network communities and in case of failure CDRA approach deals only with the failure affected community and the rest of the network graph is not disturbed.

However, on the other hand, the general recovery algorithm considers the entire graph for correction after the occurrence of failure scenarios which make it time

cost which result in larger end-to-end delay.

Furthermore, simulation results also shows that due to the time complexity of the Girvan and Newman community detection method, the proposed CDRA scheme shows higher end-to-end delay results as compared to Louvain and Infomap community detection methods which are more effective and time-efficient community detection methods.

VIII. CONCLUSION AND FUTURE WORK

Due to the increasing complexity and demand of Internet usage, a new notion of Software Defined Network (SDN) technology has emerged. SDN technology eliminates the limitations of traditional networks and allows IP networks to be programmed. SDN, like traditional networks, is vulnerable to network failures. Link failure is the most prevalent network failure in both traditional networks and SDN. Several studies have been undertaken to improve the speed and efficiency of the link failure recovery procedure. One of these research studies is the use of a community detection mechanism for SDN failure recovery.

However, several specific difficulties, such as multiple link failure and inter-community link failure, were not addressed in these studies.

This work developed a community detection-based routing algorithm (CDRA) method that can handle intra-community, inter-community, and multiple-community connection failure scenarios. Using community detection methods, the suggested CDRA scheme partitioned the network graph into smaller communities. In the event of similar failure scenarios, the proposed CDRA system only deals with the failure-affected communities, and the failure-affected nodes present in that failure-affected community are replaced by rules are replaced the failure affected nodes present in that failure affected community and the rest of the communities will remain on their working phenomena. This makes the proposed CDRA recovery scheme more time-efficient than the general recovery algorithm.

Simulation results show that the proposed CDRA scheme shows better performs than the general recovery algorithm. Furthermore, this study also presents the comparative analysis of different community detection methods such as Girvan and Newman, Louvain, and Infomap community detection methods. Simulation results show that the Louvain and Infomap community detection methods have better performance when they are compared with the Girvan and Newman community detection approach. Because the Girvan and Newman community detection approach is slow and time costing and not recommended for a large network. However, the Louvain and Infomap community detection is more efficient and capable of dealing with large network graphs.

The proposed CDRA approach has broad prospects for further development. The next step of this research

study is to imply machine learning techniques in proposed CDRA scheme to provide a fast routing solution for SDN restoration.

REFERENCES

- [1] D. Kreutz, F. M. Ramos, P. E. Verissimo, C. E. Rothenberg, S. Azodolmolky, and S. Uhlig, "Software-defined networking: A comprehensive survey," *Proceedings of the IEEE*, vol. 103, no. 1, pp. 14–76, 2014.
- [2] A. Rehman, R. L. Aguiar, and J. P. Barraca, "Fault-tolerance in the scope of software-defined networking (sdn)," *IEEE Access*, vol. 7, pp. 124474–124490, 2019.
- [3] J. Ali, G.-M. Lee, B.-h. Roh, D. K. Ryu, and G. Park, "Software-defined networking approaches for link failure recovery: A survey," *Sustainability*, vol. 12, no. 10, p. 4255, 2020.
- [4] P. C. Fonseca and E. S. Mota, "A survey on fault management in software-defined networks," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2284–2321, 2017.
- [5] B. Isyaku, K. A. Bakar, M. S. Mohd Zahid, E. H. Alkhamash, F. Saeed, and F. A. Ghaleb, "Route path selection optimization scheme based link quality estimation and critical switch awareness for software defined networks," *Applied Sciences*, vol. 11, no. 19, p. 9100, 2021.
- [6] A. Malik, B. Aziz, C.-H. Ke, H. Liu, and M. Adda, "Virtual topology partitioning towards an efficient failure recovery of software defined networks," in *2017 International Conference on Machine Learning and Cybernetics (ICMLC)*, vol. 2. IEEE, 2017, pp. 646–651.
- [7] A. Malik, R. de Fréin, and B. Aziz, "Rapid restoration techniques for software-defined networks," *Applied Sciences*, vol. 10, no. 10, p. 3411, 2020.
- [8] B. Isyaku, M. S. Mohd Zahid, M. Bte Kamat, K. Abu Bakar, and F. A. Ghaleb, "Software defined networking flow table management of openflow switches performance and security challenges: A survey," *Future Internet*, vol. 12, no. 9, p. 147, 2020.
- [9] C. Wang, D. Zhang, L. Zeng, E. Deng, J. Chen, and W. Zhao, "A novel mtj-based non-volatile ternary content-addressable memory for high-speed, low-power, and high-reliable search operation," *IEEE Transactions on Circuits and Systems I: Regular Papers*, vol. 66, no. 4, pp. 1454–1464, 2018.
- [10] Y. Wang, S. Feng, H. Guo, X. Qiu, and H. An, "A single-link failure recovery approach based on resource sharing and performance prediction in sdn," *IEEE Access*, vol. 7, pp. 174750–174763, 2019.
- [11] S. Sharma, D. Staessens, D. Colle, M. Pickavet, and P. Demeester, "Enabling fast failure recovery in openflow networks," in *2011 8th International Workshop on the Design of Reliable Communication Networks (DRCN)*. IEEE, 2011, pp. 164–171.
- [12] M. Y. Daha, M. S. M. Zahid, K. Husain, and F. Ousta, "Performance evaluation of software defined networks with single and multiple link failure scenario under floodlight controller," in *2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS)*. IEEE, 2021, pp. 959–965.
- [13] S. A. Aastaneh and S. S. Heydari, "Optimization of sdn flow operations in multi-failure restoration scenarios," *IEEE Transactions on Network and Service Management*, vol. 13, no. 3, pp. 421–432, 2016.
- [14] S. Sharma, D. Staessens, D. Colle, M. Pickavet, and P. Demeester, "Openflow: Meeting carrier-grade recovery requirements," *Computer Communications*, vol. 36, no. 6, pp. 656–665, 2013.
- [15] V. Muthumanikandan and C. Valliyammai, "Link failure recovery using shortest path fast rerouting technique in sdn," *Wireless Personal Communications*, vol. 97, no. 2, pp. 2475–2495, 2017.

- [16] S. Rahiminejad, M. R. Maurya, and S. Subramaniam, "Topological and functional comparison of community detection algorithms in biological networks," *BMC bioinformatics*, vol. 20, no. 1, pp. 1–25, 2019.
- [17] F. R. Khawaja, J. Sheng, B. Wang, and Y. Memon, "Uncovering hidden community structure in multi-layer networks," *Applied Sciences*, vol. 11, no. 6, p. 2857, 2021.
- [18] S. Emmons, S. Kobourov, M. Gallant, and K. Borner, "Analysis of network clustering algorithms and cluster quality metrics at scale," *PLoS One*, vol. 11, 2016.
- [19] Y. L. Youngho Lee, A. S. Jeong Seong, and C. S. Hwang, "A comparison of network clustering algorithms in keyword network analysis: A case study with geography conference presentations," *International Journal of Geospatial and Environmental Research*, vol. 7, no. 3, 2020.
- [20] Z. Lu, J. Wahlström, and A. Nehorai, "Community detection in complex networks via clique conductance," *Scientific reports*, vol. 8, no. 1, pp. 1–16, 2018.
- [21] V. Rosset, M. A. Paulo, J. G. Cespedes, and M. C. Nascimento, "Enhancing the reliability on data delivery and energy efficiency by combining swarm intelligence and community detection in large-scale wsns," *Expert Systems with Applications*, vol. 78, pp. 89–102, 2017.
- [22] M. Girvan and M. E. Newman, "Community structure in social and biological networks," *Proceedings of the national academy of sciences*, vol. 99, no. 12, pp. 7821–7826, 2002.
- [23] A. Clauset, M. E. Newman, and C. Moore, "Finding community structure in very large networks," *Physical review E*, vol. 70, no. 6, p. 066111, 2004.
- [24] V. D. Blondel, J.-L. Guillaume, R. Lambiotte, and E. Lefebvre, "Fast unfolding of communities in large networks," *Journal of statistical mechanics: theory and experiment*, vol. 2008, no. 10, p. P10008, 2008.
- [25] M. Rosvall and C. T. Bergstrom, "Maps of random walks on complex networks reveal community structure," *Proceedings of the national academy of sciences*, vol. 105, no. 4, pp. 1118–1123, 2008.
- [26] S. Orłowski, R. Wessälly, M. Pióro, and A. Tomaszewski, "Sndlib 1.0—survivable network design library," *Networks: An International Journal*, vol. 55, no. 3, pp. 276–286, 2010.
- [27] K. Mkhitarian, J. Mothe, and M. Haroutunian, "Detecting communities from networks: comparison of algorithms on real and synthetic networks," *International Journal Information Theories and Applications*, vol. 26, 2019.
- [28] R. George, K. Shujaee, M. Kerwat, Z. Felfli, D. Gelenbe, and K. Ukuwu, "A comparative evaluation of community detection algorithms in social networks," *Procedia Computer Science*, vol. 171, pp. 1157–1165, 2020.

A Reliable Lightweight Trust Evaluation Scheme for IoT Security

Hamad Aldawsari, Abdel Monim Artoli

Department of Computer Science, College of Computer and Information Sciences,
King Saud University, Riyadh 11543, Saudi Arabia

Abstract—The rapid development of smart devices and the consequent demand their reliability have posed many challenges limiting their versatility. One of the most significant challenges is safeguarding the widespread network of sensors and devices within harsh remote environments. Numerous trust schemes have been proposed to overcome related IoT security concerns. However, most of these schemes are not lightweight and consequently are not energy-efficient. This paper proposes a reliable lightweight trust evaluation scheme (RTE) to mitigate the malicious behavior of the nodes within IoT networks. The nodes are grouped into a set of clusters each having a cluster head while cluster members are categorized by evaluating their associated residual energy. Nodes with residual energy lower than the threshold (which is determined by the base station) are suspended until they recover and regain their activity. The computations are handled by the CH which is elected by an algorithm according to its energy and coverage degree in order to optimize the energy consumption in the network. For validation and performance evaluation, the proposed RTE scheme was compared to three of the recent schemes in its category. The obtained results have revealed that the proposed RTE scheme outperforms all of them in terms of detection rate, trust evaluation time, and energy efficiency.

Keywords—IoT security; clustering; trust; energy efficient algorithm

I. INTRODUCTION

The Internet of Things (IoT) is cumulatively improving the way of our life at a stunning pace. Basically, IoT can be referred to as the technology that provides a network allowing people, things, applications, and data to connect with each other through the Internet. This enables remote control, management, and interactive integrated services to be done easily, smoother, faster, and more reliable. IoT benefits several applications in different fields such as, but not restricted to, medical care, agriculture, and economics. IoT can be viewed as the smart infrastructure enabling numerous advantages while saving costs and ensuring efficiency. IoT things (Devices) should be able to control their resource access policy, for example, which device can gain access to its humidity resource. The hurdle is that the connected devices have limited resources that restrict their ability for storing and processing access policy information [1]. Another critical issue is that devices are dynamically added and deleted from IoT networks thus as a consequence, requiring the devices to update their access policy. Moreover, with this enormous number of connected devices, a highly scalable, secure, and reliable IoT management system is needed. Another crucial issue is the attacks which maybe initiated by some nodes participated in the network. One of the well-known attacks in this area is the brute force attack. This attack can be viewed as an attacker submitting

numerous passwords or passphrases with the desire for in the long run speculating a blend accurately. In other words, the attacker is methodically checking every single imaginable password until the right one is caught. Then again, the attacker can endeavor to figure the key which is commonly made from the secret key utilizing a key inference work. This process is referred to as an exhaustive key search. Several attempts have been done in this direction but, however, they are based on centralized architecture assuming that devices are distributed statically. Specifically, most current IoT systems are built on a centralized client/server model, which requires all devices to be connected and authenticated through a centralized server. This model, however, would not be able to provide the need to disseminate the IoT system in the future which contradicts the real situations where devices are mobile like such as in IoT vehicle-to-vehicle scenarios which prevent IoT scalability. In this context, we provide a reliable light-weight trust evaluation (RTE) scheme able to maintain the trust between communicating devices to alleviate the risky effects of security-related issues. The main interesting point about RTE is its ability to achieve trust while consuming a very little amount of network energy which makes it a promising choice for scalable IoT-networks.

It is worth noting that IoT-WSN is paving its way as promising market segments [2]. The problem with IoT-WSN, however, is that all the involved sensor nodes have the permission to send data directly to BSs. This leads to consuming a large amount of stored energy, especially, with the nodes located far away from BSs. Clustering can be a solution to this problem with each cluster contains a set of sensor nodes while setting one of them as the cluster head (CH); aka coordinator. In this manner, CH is responsible for collecting the sensed data in its cluster and sends it to BS, while being the only permitted node to send to BS in its cluster. However, despite the phenomenal development of IoT-WSN, a number of issues still need more research work. The most hazardous issue, that comes in the first place, facing IoT-WSN is the security that threatens the deployment of IoT applications. In the second place, IoT is facing an energy efficiency issue. This is due to the usage of resource-constrained wireless sensors in several applications [3].

Despite the fact that there exists a large number of security techniques, it is indeed challenging to apply these technologies directly in IoT systems. This is due to following reasons [4]. First, the energy-sources limitation of sensor node which hamper the implementation of the security algorithms on the sensor node side [5]. Second, the potential physical risk due to installing the sensor node in harsh remote areas [6]. Third,

the security concerns as the sensor-people may have direct interaction with humans and the environment [7]. Finally, the heterogeneous of IoT network in which several types of sensor nodes are integrated in the IoT system [8]. This heterogeneity hinders the cooperative behavior between the sensor nodes [9]. These deficiencies deteriorate the performance of the IoT system which, in turn, exposes the system to serious attacks [10].

In literature, cryptography techniques made great efforts in mitigating security issues, for which the cryptographic-based systems are considered more effective with respect to the security concerns. However, these cryptography techniques depend on public-key schemes with powerful computing capabilities which lead, in turn, to higher energy consumption. This restricts the usage of such technique for achieving security in limited-resources sensor nodes. Still, the cryptographic technique requires a fixed infrastructure with centralized administration which, to some extent, contradicts with IoT concept of scalability; aiming to achieve a decentralized nature. This raises another security aspect known as internal attacks [11], where the attacks come from inside the network. As per the literature, trust-based technique [12] is considered the alternative that is able to resolve the security issue in IoT systems. Formally, trust is the level of confidence in a person or thing. In IoT systems, trust reflects the degree of belief or confidence about other nodes based on their past interaction and observation. Recently, it has been widely agreed that trust mitigates the problem of access control, providing reliable routing path and security mechanisms. Therefore, communication between nodes in the IoT system should be done under the supervision of trust. The problem with the trust technique, however, is twofold. First, the misleading information communicated from malicious nodes negatively impact the trust computation. This problem is exacerbated strongly if the network contains numerous illegitimate sensor nodes. To elaborate further, such nodes provide fake recommendations that confuse the task of CHs in evaluating trust. This problem, also, hurts the CH of BSs. Second, not all the involved sensor nodes provide recommendations to CH which results in an inaccurate trust computation. To elaborate further, sensor nodes with either low bandwidth or limited energy may prefer to preserve their resources; i.e., do not send recommendations, for actual data transfer. This results in a non-cooperative behavior among sensor nodes. Such bad-behavior not only compromises the network security but also deteriorates its limited resources and results in unbalanced energy consumption among nodes in the network.

Several studies have been devoted to optimization of trust computation based on different methods and theories such as game theory [17], matrix theory [14], beta distribution [16], weighting [13], and Bayesian statistics [15]. However, it is worth mentioning that all attempts of the aforementioned studies results in increasing the energy consumption and network complexity. This, in turn, makes the network vulnerable to several attacks [18]. Thus, the idea is to design a less complex attestable lightweight trust evaluation scheme that alleviates the consequences of non-cooperative behavior of the nodes. Specifically, in this work we design a reliable trust evaluation (RTE) scheme for lightweight security, energy-efficient, free of the current trust evaluation schemes limitations. Several experiments were carried out to assess the performance of

RTE. The end result is a promising security framework. For further validation, a case study was carried out assessing the ability of RTE to ban the brute force attack. The results show its superiority.

The rest of this article is organized as follows. Section II covers related work. Section III describes the proposed Model. In Section IV, experimental work is presented to validate the approach and evaluate its performance. Finally, concluding remarks are presented in Section V.

II. RELATED WORK

Trust evaluation is one of the prominent research directions in the IoT security, and it is characterized by two key issues: trust metrics and trust computational methods, [20]. Researchers in this field are challenged to achieve a balance between security requirements and energy efficiency in variant IoT environments. This section reviews the related attempts that have been done in the context of trust evaluation schemes in IoT networks. Khalil et al. [21] presented a framework based on a Fuzzy Logic model to evaluate the security trust level for each IoT node. The node is trusted if its trust level is greater than a threshold defined by the user. Only the trusted nodes are permitted to collect the critical information. Chen et al. [22] presented a trust architecture called IoTrust, integrating SDN with a cross-layer authorization protocol, and used two reputation evaluation schemes for node and organization. These schemes are efficient in defending against modification, replay, and message dropping attacks, with high detection accuracy. However, one of the main drawbacks of this technique is disregarding malicious user and organization behaviors, which could generate fake reputation values. Another research has been done to evaluate trust among devices in SDN-enabled home networks using a blockchain-based trust assessment framework. Boussard et al. [23] proposed such a system called STeward which computes the trust score for each connected device based on its historical behavior. Then, this score is used to judge whether the node is permitted to connect to the crowd or not if it meets the required trust level assigned by the user. One drawback of this framework is that it has not yet proven the convergence of the underlying reputation system. However, it is still under development and its scalability problems should be solved. Other frameworks were conducted in the field of edge computing, Gao et al. [24] proposed a service-driven collaboration mechanism among IoT edge devices using multidimensional trust evaluation, in addition to a double-filtering design to filter the feedback from malicious devices in an efficient way. This mechanism applied low-overhead algorithms, which had an excellent performance in defeating malicious behaviors and improved the reliability of the IoT edge environment. However, the flexibility should be improved by optimizing the data aggregation technique. Another attempt was implemented for the security of Industrial IoT. Wang et al. [25] proposed an intelligent mobile edge computing-based trust evaluation scheme (MTES). The trustworthiness of sensor nodes has been evaluated by the mobile edge nodes which had relatively strong computation and storage ability. This mechanism could distinguish compromised and malicious nodes and decrease the energy consumption of the entire network. Dass et al. [26] proposed a trust evaluation model to compute the trustworthiness of the data generated from the participating nodes in an intelligent transport system. They

considered direct and indirect trust mechanisms for each of the sensor nodes and update their trust measures at regular intervals of time. They achieved a high detection rate and a low false detection rate. However, as all the operations are performed at the cloud server, it causes a delay in trust assessment, which do not suit real time scenarios. Recently, the deployment of machine learning algorithms in trust evaluation for IoT devices were widely investigated. Jayasinghe et al. [27] proposed a quantifiable trust assessment model based on machine learning principles. The model is consisted of three sub-models that classify the extracted trust features and combine them to produce a final trust value to be used for decision making. While Ma et al. [28] used a deep learning algorithm and adopted trust metrics based on comprehensive network behaviors in trust evaluation, to build a behavioral model for a given IoT device, and predict the trust status of this device which is used for decision making. These algorithms are still in their elementary stages, and need to be more flexible and practical, also the privacy issue of the training datasets needs to be considered. These algorithms consume are applicable for dedicated applications where the number of IoT devices is limited. They provide a high degree of security in the network, while consuming power heavily, and causing delay to the system due to complex computations. Therefore, the accomplishment of lightweight security algorithms is strongly demanded. Sedjelmaci et al. [29] proposed a light weight hybrid intrusion detection system, in which the game theory concept is employed to overcome the challenge of high-energy consumption in HIDS. For this purpose, the anomaly detection algorithm is activated just when a pattern of new attack is likely to happen. This technique achieved a good detection rate with a reduction of energy consumption. However, it still had many false positives. Therefore, Sedjelmaci et al. [30] enhanced the latter technique by adding an improved model on the basis of game theory to alleviate the rates of false positives. Another game theoretic approach has been used by Duan et al. [19] to establish an energy-aware trust derivation scheme to ensure sufficient security of WSNs by deriving the optimal number of recommendations. By using this scheme, the performance of the network has improved in terms of security, but it has still been affected by the increased overhead due to the trust requests. In view of the same, an energy efficient trust evaluation scheme (known as EETE) is introduced by Rani et al. [31].proposed another approach for trust evaluation in WSN-enabled IoT networks using game theory techniques for cluster creation. This scheme enabled the detection of malicious nodes while decreasing the needed communications between nodes. These algorithms will be compared to our proposed algorithm in Section IV. Lately, in a 2021 study, Rao et al. [32] proposed a novel method to attain security in wireless body area network based on fuzzy logic and considering the residual energy as the trust factor, and their results show that this metric has successfully improved the lifetime of the network. The study of the contemporary research in the trust evaluation for IoT systems illustrates the persistent need to obtain a reliable and lightweight algorithm that is flexible and applicable in different environments.

III. THE PROPOSED RTE SCHEME

In this section, we propose the RTE model as a tool for applying trust between communicating nodes in an IoT

network. The contribution of the RTE model is twofold. First, it applies trust management in intra-cluster and inter-cluster modes. Second, it is a light-weight model with an energy-efficient schema.

A. Network Model

Here, we consider an IoT sensor-network having M sensor nodes with limited energy sources along with limited radio range. A BS exists in the network with an unlimited energy source. The M nodes are grouped into N clusters. Each cluster has a different number of nodes. Each node m_i , $i = 1, \dots, M$ is classified to either CH or CM. The hurdle is that these sensor nodes are operating in an open remote environment which makes it vulnerable to attacks. Additionally, some of the nodes may be initiating malicious attacks classified to either internal attacks like collusion attacks or external attacks like denial of service (DOS). In this context RTE model is used to observe the behavior of each node then evaluates the degree of trust in this node. The general components of the RTE scheme are depicted in Fig. 1.

B. Trust Model

Leaks of internal data of a specific organization may originate from its practitioners. It can be difficult sometimes to believe that a practitioner will intentionally sabotage their own business, and while it happens willfully often, it is strictly unintentional much of the time. Such behavior is referred to as internal attacks. The present work is an attempt to secure the network against such type of attacks. It should be noted that the RTE is controlled using a time slot S parameter; a user-defined parameter. Specifically, if the time slot is set to 60 seconds, then the RTE calculations, discussed below, are invoked every 60 seconds. Each time slot represents an iteration t in the algorithm. Therefore, we can say that iteration 1 starts at second 1 and iteration 2 starts at second 61, and so on.

1) *Cluster Formation:* At the very top level, RTE clusters the involved sensor nodes into N clusters as follows. Initially, the sensor nodes are deployed in a random manner while being kept static. Once the node starts up, it transmits a beacon signal to the BS. Afterward, the distance between each pair of sensor nodes is computed. The BS is responsible for computing the distance through evaluating the receiving signal strength which, in turn, can be translated into the distance. Let us comment on how the distance is computed. First, receive signal strength indicator (RSSI) is used to determine the signal strength measured in dBm. Note that higher dBm indicates higher signal strength. Second, according to the RSSI, the BS can calculate the distance to each node, for example, is the BS beacon signal broadcast range is 15 meters, it is widely known that if the RSSI is -50 dBm, then the distance is 1 meter. The task now is to find the N CHs. When a group of M sensor nodes runs in a network with a BS, naturally some nodes will perform better than others, basically by better aggregating data from neighboring nodes and transmit it to the BS. Let us call the few that excel at round $t = 1, 2, \dots$ CHs, denote that \mathbb{H}_t , and the rest are CMs. The good thing about RTE is that at every round $t = 1, 2, \dots$, the M nodes will share some information (discussed briefly below) with the BS who, in turn, uses this information to adjust the CHs. Accordingly, in the

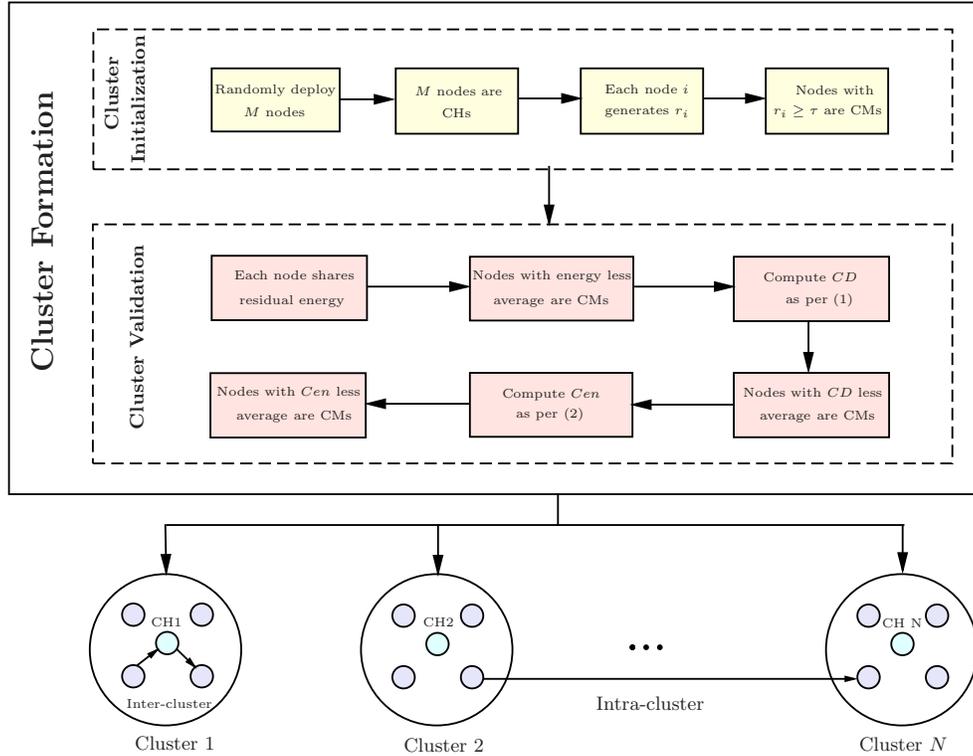


Fig. 1. The Main Components of RTE Scheme.

next round, the node that was a CM in the last round may become a CH. Each node has a number $i = 1, 2, \dots, M$ and a tag: CH or CM. The numbers are permanent, but the tags may change from round to round. The BS transmits a threshold τ to all the sensor nodes to guide the task of electing the CHs. Each node m_i , $i = 1, 2, \dots, M$ generates a random number r_i . Then r_i is compared against τ , if $r_i \geq \tau$, then node m_i is considered CH. Otherwise, it is an ordinary CM. Now, it is the BS turn to evaluate the validity of the elected CHs. The BS evaluates the CHs $\mathcal{H}_j \in \mathbb{H}_t$ according to three metrics. First, the residual energy of each CH is computed. This parameter must be high for a competitor CH. Second, the CH coverage degree (CD) is evaluated. This parameter indicates the ratio of the neighboring nodes (nbr) of the CH to the total number of nodes M . Neighboring nodes to a CH are those nodes that are located in either 1-hop or 2-hop from that CH. The CD of a given CH is evaluated by:

$$CD(\mathcal{H}_j) = \frac{|nbr(\mathcal{H}_j)|}{M}, \quad (1)$$

Where $|\mathcal{X}|$ is the cardinality of set \mathcal{X} . This parameter must be high for a competitor CH. Third, the CH centrality CH_Cen is evaluated. Contradicting with the other two metrics, CH centrality should be of low value. This parameter indicates energy consumption of a CH during the data aggregation and is given by:

$$CH_Cen(\mathcal{H}_j) = \frac{\sqrt{\frac{\sum_{k \in nbr(\mathcal{H}_j)} d^2(\mathcal{H}_j, m_k)}{|nbr(\mathcal{H}_j)|}}{A}}, \quad (2)$$

Where $d(\mathcal{H}_j, m_k)$ is the distance between the CH \mathcal{H}_j and node m_k and A is the area of the network. The CHs that pass the three metrics are considered confirmed ones while the others are considered CMs.

2) *RTE Intra-cluster Evaluation:* After electing the CHs, it is now the responsibility of each CH $\mathcal{H}_j \in \mathbb{H}_t$ to maintain the trust of the CMs $m_{i_j} \in \mathcal{H}_j$ in its cluster. To this end, the trust is represented as a continuous number in the interval $[0,1]$, in which 0 indicates malicious, 1 indicates complete trust, and 0.5 indicates suspicious. For achieving trust in the case of intra-cluster, two direct and indirect trust concepts are employed. The degree of belief of CH \mathcal{H}_j in a node m_{i_j} represents the direct trust (DT) which is computed according to the direct communication between node m_{i_j} with its CH \mathcal{H}_j . On the other hand, indirect trust (IT) is the degree of belief in node m_{i_j} from its neighbors. The idea is that each CM m_{i_j} preserves the trust of its neighbors and transmits these values to the CH \mathcal{H}_j . Both the DT and IT withstand against internal attacks. The trust T_t of a CM m_{i_j} with respect to its CH \mathcal{H}_j . at round $t = 1, 2, \dots$ is given by:

$$T_t(\mathcal{H}_j, m_{i_j}) = \alpha DT_t(\mathcal{H}_j, m_{i_j}) + \beta \frac{\sum_{k \in nbr(m_{i_j})} IT_t(m_{k_j}, m_{i_j})}{|nbr(m_{i_j}) - 1|}, \quad (3)$$

where $\alpha > 0$ and $\beta > 0$, chosen afresh at each round, are weight factors such that $\alpha + \beta = 1$. $DT_t(\mathcal{H}_j, m_{i_j})$ represents the direct trust of CH \mathcal{H}_j in node m_{i_j} at round t and $IT_t(m_{k_j}, m_{i_j})$ is the indirect trust of node m_{k_j} in node m_{i_j} . Before elaborating on computing both the DT and

IT, we provide some preliminaries. Given a node m_{i_j} , let us define the positive well-behaved $P(m_{i_j})$ activity and the negative malicious $N(m_{i_j})$ activity. Consider that $E_{\max}(m_{i_j})$ is the maximum energy attained by node m_{i_j} , $\Delta_t(m_{i_j})$ is the residual energy of node m_{i_j} after communications in round t and $E_{th} \in [0, 1]$ is an energy threshold chosen by the BS. If the node is doing some malicious communications at round t , then it is expected that by the end of the round, the node would consume a lot of energy. Therefore, the strategy is as follows. If $\Delta_t(m_{i_j})/E_{\max}(m_{i_j}) < E_{th}$, then node m_{i_j} well-behaved at round t , i.e. $P(m_{i_j}) = \Delta_t(m_{i_j})/E_{\max}(m_{i_j})$ and $N(m_{i_j}) = 0$. Otherwise, node m_{i_j} maliciously-behaved at round t , i.e. $N(m_{i_j}) = \Delta_t(m_{i_j})/E_{\max}(m_{i_j})$ and $P(m_{i_j}) = 0$. Each node m_{i_j} starts out at round 1 by a suspended direct trust, i.e. $DT_1(\mathcal{H}_j, m_{i_j}) = 0.5$. In the next round $t + 1$, the node m_{i_j} updates its direct trust as follows.

$$DT_t(\mathcal{H}_j, m_{i_j}) = P(m_{i_j})DT_{t-1}(\mathcal{H}_j, m_{i_j}) - N(m_{i_j})DT_{t-1}(\mathcal{H}_j, m_{i_j}). \quad (4)$$

It should be noted that if $\alpha \geq \beta$, it means that node n_i has a higher trust of *DT* than that of *IT*. Otherwise, node n_i has a higher trust of *IT* than that of *DT*.

Finally, with the above in mind, the indirect trust of node m_{i_j} is given by:

$$IT_t(m_{k_j}, m_{i_j}) = P(m_{i_j}) \sum_{k \in nbr(m_{i_j}), k \neq i} DT_{t-1}(m_{k_j}, m_{i_j}) - N(m_{i_j}) \sum_{k \in nbr(m_{i_j}), k \neq i} DT_{t-1}(m_{k_j}, m_{i_j}). \quad (5)$$

3) *RTE Inter-cluster Evaluation*: A satisfactory observation about the RTE model is its ability to evaluate the trust between two different clusters using the inter-cluster evaluation schema. This is achieved with the employment of CHs $\mathcal{H}_j \in \mathbb{H}_t$ and BS. Specifically, the trust value T between two nodes belonging to different clusters ($\mathcal{H}_j, \mathcal{H}_k$) is basically established by the trust between the two cluster heads, i.e. $T_t(\mathcal{H}_j, \mathcal{H}_k)$. The inter-cluster trust evaluation between node m_{i_j} from CH \mathcal{H}_j and node m_{l_k} from CH \mathcal{H}_k is expressed mathematically by:

$$T_t(m_{i_j}, m_{l_k}) = T_t(\mathcal{H}_j, \mathcal{H}_k) \times T_t(\mathcal{H}_k, m_{l_k}). \quad (6)$$

The RTE model shown in Algorithm 1 employs the above calculations.

IV. EXPERIMENTAL WORK

In this section, the performance of the proposed algorithm RTE is evaluated in IoT sensor-based network using the NS-3 simulator. This network has a number of nodes behave in a malicious manner. We compute and compare the detection rate, energy consumption, and trust evaluation time of RTE with three benchmark schemes TDDG [19], LHIDS [30] and EETE [31]. Then, to verify the resilience of RTE we measured the detection rate under brute force attack. The simulation keeps running for 50 iterations, which was good enough for accurate results.

Algorithm 1: reliable lightweight trust evaluation scheme (RTE)

```

Input :  $N$  //Number of sensor nodes
           $S$  //Time slot
Output:  $T$  //Trust of the sensor nodes
1  $t := 1$  //Iteration number representing the number of
  the time slot  $S$ 
  //Cluster the nodes
2 Deploy the  $N$  sensor nodes randomly.
3 foreach node  $m_i \in N$  do
4   | Transmit beacon signal to the BS.
5   | Compute the distance to the BS.
6 end
7 do
8   | BS transmits a threshold  $\tau$  to the  $N$  sensor nodes.
9   |  $\mathbb{H}_t := \emptyset$ . //Set of all CHs.
10  foreach node  $m_i \in N$  do
11    | Generate random number  $r_i$ .
12    | if  $r_i \geq \tau$  then
13      | Node  $m_i$  declares it self a temporary CH.
14      | Node  $m_i$  is added to  $\mathbb{H}_t$ .
15    | else
16      | Node  $m_i$  is declared as a CM.
17    | end
18  end
19 end
  //Evaluation of the permanent CHs
20 foreach CH  $\mathcal{H}_j \in \mathbb{H}_t$  do
21   | Compute the residual energy of CH  $\mathcal{H}_j$ .
22   | Compute  $CD(\mathcal{H}_j)$  of CH  $\mathcal{H}_j$  as per (1).
23   | Compute  $CH\_Cen(\mathcal{H}_j)$  of  $\mathcal{H}_j$  as per (2).
24 end
25 BS generates a CH threshold  $C\tau$  in the interval
   $[0, N]$ .
26 Keep the best performing  $C\tau$  CHs in  $\mathbb{H}_t$  and
  switch the rest to CMs.
27 BS transmits the energy threshold  $E_{th} \in [0, 1]$ .
28 foreach Ch  $\mathcal{H}_j \in \mathbb{H}_t$  do
29   | foreach node  $m_{i_j} \in \mathcal{H}_j$  do
30     | Compute  $E_{\max}(m_{i_j})$  of node  $m_{i_j}$ .
31     | Compute  $\Delta_t(m_{i_j})$  of node  $m_{i_j}$ .
32     | if  $\Delta_t(m_{i_j})/E_{\max}(m_{i_j}) < E_{th}$  then
33       |  $P(m_{i_j}) := \Delta_t(m_{i_j})/E_{\max}(m_{i_j})$ .
34       |  $N(m_{i_j}) := 0$ .
35     | else
36       |  $N(m_{i_j}) := \Delta_t(m_{i_j})/E_{\max}(m_{i_j})$ .
37       |  $P(m_{i_j}) := 0$ .
38     | end
39   | end
40   | Compute the DT of node  $m_{i_j}$  as per (4).
41   | Compute the IT of node  $m_{i_j}$  as per (5).
42   | Compute the trust  $T$  as per (3).
43   end
44 end
45 Wait until the end of the time slot.
46  $t := t + 1$ .
47 while the network is running;

```

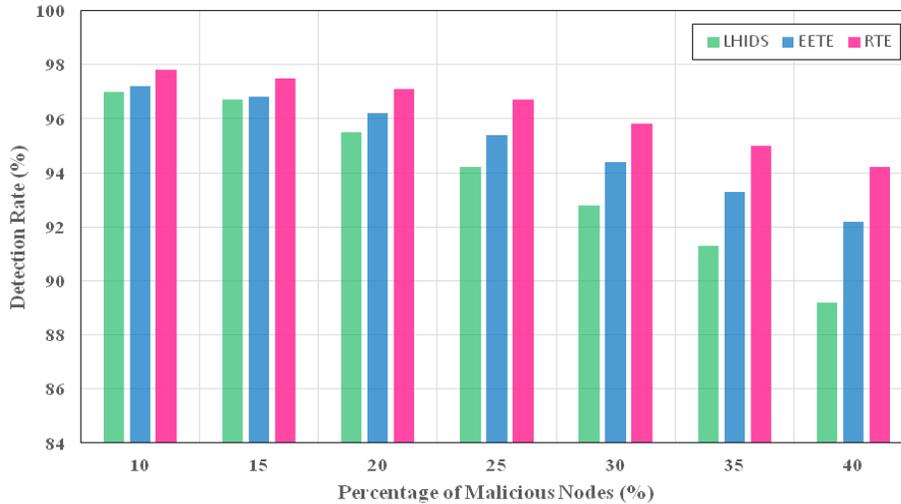


Fig. 2. Detection Rate Comparison between RTE Algorithm and other 2 Algorithms, while Increasing the Number of Misbehaving Nodes in the Network.

TABLE I. SIMULATION PARAMETERS

Parameter	Value
Network area, A	$500 \times 500 \text{ m}^2$
Node number, N	300
Number of iterations, R	50
Packet size	1024-bits
Communication range	100 m
Percentage of malicious nodes	10 – 40%
Hop limit	2
Initial DT	0.5 (suspend)
Max. number of nodes in a cluster, K	10
Initial energy	10J
Node transmission range	25m

A. Experimental Setup

We consider that we have a network of $500 \times 500 \text{ m}^2$, with 300 nodes randomly deployed. The propagation delay is calculated using constant speed propagation. Moreover, the radio energy model are utilized for initial energy distribution. We assume that we have a 1024-bits packet length. In all the experiments, we use the following values in Table I, which proved good enough for accurate and fast results:

B. Evaluation Metrics

For validating the proposed RTE algorithm, the following validation measures are employed.

- 1) Detection rate, $D_t(W)$: Given an IoT-network W , the detection rate ($D_t(W)$) is the ratio between the number of correctly detected malicious nodes \mathbb{M}_t at iteration t to the total number of predefined malicious nodes \mathcal{M} and is given by

$$D_t(W) = \frac{\mathbb{M}_t}{\mathcal{M}}.$$

- 2) Average energy consumption, $Avg(C_i)$: Given a cluster C_i with K sensor nodes, the average energy consumption ($Avg(C_i)$) is the average consumed energy, in Joule (J), by the active nodes in Cluster C_i , and is given by

$$Avg(C_i) = \frac{\sum_{j=2}^K E_j}{K},$$

where E_j is the consumed energy by node j in cluster i . The reason why the summation start by 2 is that the CH is not considered while computing the average consumed energy.

- 3) Trust Evaluation time: It is the time taken by the algorithm to evaluate the trust since receiving the request to computing the direct and indirect trust of the node. This is computed using the concept of elapsed seconds.

C. Experiment 1: Detecting Malicious Nodes and Detection Rate

In this experiment, the detection rate of our proposed algorithm RTE was tested to validate its reliability, this metric is important and should be as high as possible. The experiment is run several times in a nested format according to varying percentages of malicious nodes start from 10% to 40%, with a step of 5%. Figure 2 illustrates the comparison of detection rate between LHIDS, EETE, and RTE. The detection rate decreases when the number of malicious nodes increases. However, the detection rates of LHIDS and EETE start decreasing significantly when the ratio of misbehaving nodes exceeds 20%, while the chart of RTE keeps decreasing slightly and never falls below 94.6%, this value is in the worst case when 40% of the nodes in the network behaving illegitimately, which shows a reliable performance unaffected by the high numbers of malicious nodes. The results show the superiority of RTE clearly which is justified by the two following reasons. The first one is the accurate calculations carried out by RTE, specifically, RTE inter-cluster and intra-cluster trust evaluation

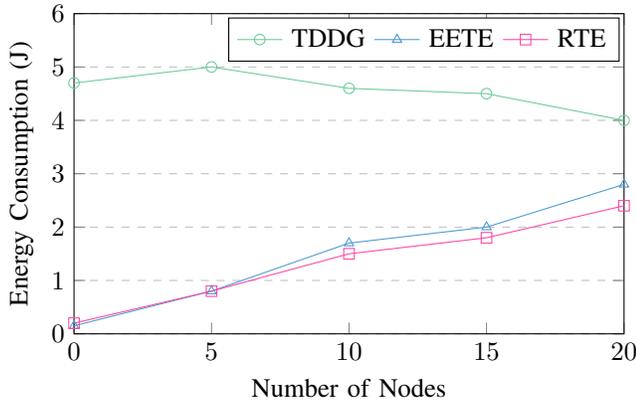


Fig. 3. Average Energy Consumption Comparison between RTE Algorithms and other 2 Algorithms, while Increasing the Number of Nodes in the Network.

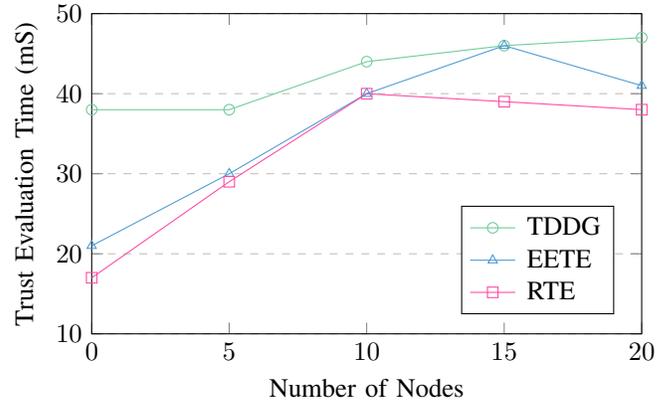


Fig. 4. Trust Evaluation Time Comparison between RTE Algorithm and other 2 Algorithms, while Increasing the Number of Nodes in the Network.

by the CHs. For which, the nodes are classified upon their past behaviors into trusted, suspicious, or malicious. Moreover, the malicious nodes are immediately excluded from the network which helps efficiently in mitigating the malicious behavior in the network. The second reason is the consistent validation of the clusters by the BS each iteration, which provides an additional monitoring to the network and improves the security by keeping the CHs trusted.

D. Experiment 2: Average Energy Consumption ($Avg(C_i)$)

In this experiment, the efficiency of the proposed algorithm is validated by the measurement of the average energy consumed by the algorithm to evaluate the trust of the participating nodes in the network. As mentioned earlier, the nodes in the IoT environment are power constrained, so the trust evaluation algorithm should be as light as possible and consume the minimum amount of energy. The experiment is run several times with a varying number of participating nodes starting from 0 to 20, with a step of 5. Fig. 3 shows the results of this experiment for three lightweight algorithms TDDG, EETE, and RTE. At the beginning of the chart EETE and RTE consume similar amount of energy. However, when the number of nodes increases, our algorithm needs less energy than the other two models. When the number of nodes is 20, it consumes 0.40J less than the EETE algorithm. It is observed that RTE gives the best performance. This optimization in energy consumption is resulted from the reduction of the trust calculations in the network, where only the CHs are responsible for the trust computations while the other CMs concentrate in the process of packets transmission. Another reason for the efficiency of our algorithm, is the role of BS in evaluation the clusters each iteration and elect the appropriate CHs, which helps in maintaining a steady amount of energy in the network.

E. Experiment 3: Trust Evaluation Time

In this experiment, we assess the robustness of the algorithm by investigating the required time for trust evaluation of the participating nodes. The algorithm should be performed as fast as possible to protect the network from the dangerous consequences of the presence of misbehaving nodes. The experiment is run several times with a varying number of

nodes from 0 to 20 nodes, with a step of 5. Fig. 4 We can see that RTE's curve is the least deviating curve from the others, but this ideal behavior is practically hard to attain due to nodes interaction overhead in computing the indirect trust. However, we can observe that the curve of RTE is the least deviating curve from the others, and this algorithm requires the least amount of time to evaluate the trust between nodes. This results rationally match the results of the previous experiment, as the proposed algorithm limits the computations and implement them only in the CHs and BS, which also reduces the needed communication overhead for the process. Therefore, we can say that RTE is unaffected by increasing the number of participating nodes in the network.

F. Case Study: RTE Performance under Brute Force Attack

To prove the efficiency of the RTE algorithm, it was tested for computing the trust of the involved nodes in an IoT sensor-based network, while assuming the presence of some malicious nodes behaving badly and initiating brute force attack. This section is dedicated mainly for analyzing the performance of RTE under brute force attack. RTE was run several time slots. Each time slot takes number of second that vary from slot to another. The time slot ends when all nodes sense and transmit the data, along the path, to the BS. In each slot, we categorize the nodes as follows: normally behaving nodes, malicious nodes, attacked nodes, and dead nodes. The node is considered dead when its energy is less than threshold (user-defined value), in our case it is assumed 60% of the average energy of the nodes in the slot. On the other hand, malicious nodes are those initiating brute force attack. Fig. 5 illustrates the performance of RTE under brute force attack in terms of False Positive Rate (FPR) and False Negative Rate (FNR), while increasing the percentage of malicious nodes in the network. The graph shows that when the percentage of malicious node is 10%, the FPR is 11%. By increasing the number of malicious nodes, the performance of the RTE will not be highly affected. We observe that if half of the network is infected, the FPR approaches 21%. The FPR has increased 10% when the percentage of malicious nodes has increased 40%. This proves the highly efficient performance of the proposed algorithm in such highly malicious environment.

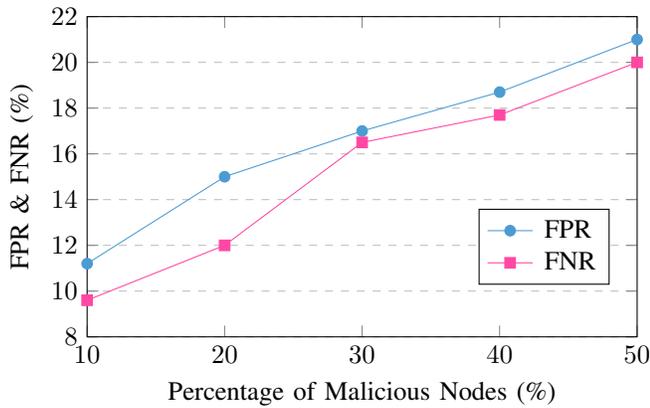


Fig. 5. Performance (2 metrics) of RTE with Respect to Varying Ratio of Misbehaving things under Brute Force Attack.

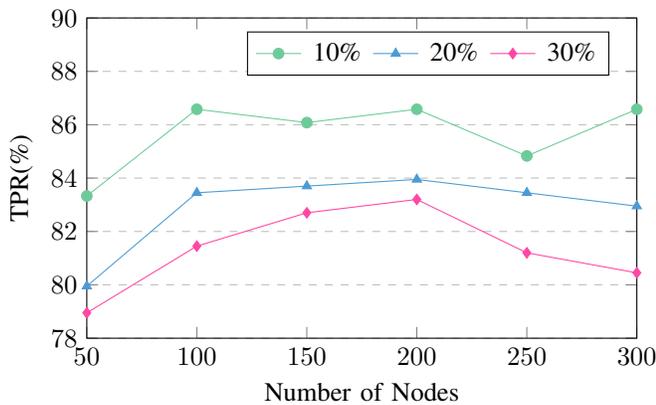


Fig. 6. Performance (TPR) of RTE under Brute Force Attack.

G. Performance Investigation

The performance results of RTE would have been greatly affected with varying percentages of malicious nodes. In other words, as the percentage of malicious node in the network increases, the performance of RTE, or any competitor algorithm for that matter, naturally affected. With this in mind, to the end of the experiment, we validate RTE performance with respect to three scenarios, each with a different percentage of malicious nodes. Specifically, scenario 1 assumes 10% malicious nodes, scenario 2 assumes 20% malicious nodes, and scenario 3 assumes 30% malicious nodes. That is to expose the operational range of RTE.

The TPR results of RTE with respect to the three scenarios is depicted in Fig. 6. It gives a vivid picture on the evolution of the algorithm with respect to the three scenarios. It can be easily noticed that as the number of nodes increase, the RTE performance, TPR, increases. This is attributed mainly to the accurate design of the algorithm in computing the trust.

V. CONCLUSION

This paper proposes a novel reliable lightweight trust evaluation (RTE) scheme to improve the security of clustered-sensor IoT-network in presence of some malicious illegitimate nodes. The model considers both the trustworthiness of nodes

and network energy efficiency thus differentiating it from peers in the literature. In contrast with other trust evaluation schemes, RTE reduces the needless transmissions. RTE aggregates the nodes in a set of clusters, controlled by a set of CHs. Two scenarios are used to evaluate trust. First, intra-cluster evaluation is carried out by the CH to trust any communication between nodes in its cluster. Second, inter-cluster evaluation is carried out to trust any communication between nodes in different clusters. The CHs are responsible for evaluating the trust while CMs send/receive data which, in turn, increases the network lifetime. Simulation results of the RTE scheme show its superiority over current trust evaluation schemes in terms of detection rate and time of malicious nodes, energy efficiency, and trust evaluation time. What is more, RTE is abilities are tested in detecting brute force attack with varying percentage of attack and varying number of nodes. As the number of attacks increases, RTE detection rate for malicious nodes increases. This reflected RTE ability in achieving promising results for FPR, TPR, TNR and FNR. In future works, our goal is to extend the RTE scheme to be able to detect several kinds of external attacks like DoS, black-hole attack, and wormhole attack.

ACKNOWLEDGMENT

The authors would like to thank Deanship of scientific research for funding and supporting this research through the initiative of DSR Graduate Students Research Support (GSR), King Saud University

ABBREVIATIONS

The following abbreviations are used in this manuscript:

RTE	Reliable lightweight trust evaluation scheme
CH	Cluster head
CM	Cluster member
IoT	Internet of thing
BS	Base station
FPR	False Positive Rate
TPR	True Positive Rate
FNR	False Negative Rate
DR	Detection Rate

REFERENCES

- [1] Lim, J.; Keum, D.; Ko, Y. B. A Stepwise and Hybrid Trust Evaluation Scheme for Tactical Wireless Sensor Networks. *Sensors* 2020, 20(4), 1108.
- [2] Chitanya, M. Robustness, Security and Privacy in Location-Based Services for Future IoT. *Research and Reviews: Advancement in Robotics* 2018, 1(2), 1-5.
- [3] Bhushan, B.; Sahoo, G. Requirements Protocols, and Security Challenges in Wireless Sensor Networks: An Industrial Perspective. In *Handbook of Computer Networks and Cyber Security*, Springer, Cham, 2020; pp. 683–713.
- [4] Um, T. W.; Lee, E.; Lee, G.M.; Yoon, Y. Design and Implementation of a Trust Information Management Platform for Social Internet of Things Environments. *Sensors* 2019, 19(21), 4707.
- [5] Ram, M.; Kumar, S.; Kumar, V.; Sikandar, A.; Kharel, R. Enabling Green Wireless Sensor Networks: Energy Efficient T-MAC Using Markov Chain Based Optimization. *Electronics* 2019 8(5), 534.
- [6] Halder, S.; Ghosal, A.; Conti, M. LiMCA: an optimal clustering algorithm for lifetime maximization of internet of things. *Wireless Networks* 2019, 25(8), 4459–4477.

- [7] Derder, A.; Moussaoui, S.; Doukha, Z.; Boualouache, A. An online target tracking protocol for vehicular Ad Hoc networks. *Peer-to-Peer Networking and Applications* **2019**, 12(4), 969–988.
- [8] Rani, R.; Katti, C.P. End-to-end security in delay tolerant mobile social network. In International Conference on Application of Computing and Communication Technologies, 2019; pp. 45–54.
- [9] Bica, I.; Chifor, B.C.; Arseni, Ş.C.; Matei, I. Multi-Layer IoT Security Framework for Ambient Intelligence Environments. *Sensors* **2019**, 19(18), 4038
- [10] Fu, H.; Liu, Y.; Dong, Z.; Wu, Y. A Data Clustering Algorithm for Detecting Selective Forwarding Attack in Cluster-Based Wireless Sensor Networks. *Sensors* **2020**, 20(1), 23.
- [11] Bypour, H.; Farhadi, M.; Mortazavi, R. An Efficient Secret Sharing-based Storage System for Cloud-based Internet of Things. *International Journal of Engineering* **2019** 32(8), 1117–1125.
- [12] Alnumay, W.; Ghosh, U.; Chatterjee, P. A Trust-Based predictive model for mobile ad hoc network in internet of things. *Sensors* **2019** 19(6), 1467.
- [13] Ullah, I.; Youn, H.Y. A novel data aggregation scheme based on self-organized map for WSN. *The Journal of Supercomputing* **2019**, 75(7), 3975–3996.
- [14] Vijayan, R.; Jeyanthi, N. Trust Management Approaches in Mobile Adhoc Networks. In Ubiquitous Computing and Computing Security of IoT, 2019; pp. 69-99.
- [15] Yin, X.; Li, S. Trust evaluation model with entropy-based weight assignment for malicious node's detection in wireless sensor networks. *EURASIP Journal on Wireless Communications and Networking* **2019**, 198.
- [16] Wu, X.; Huang, J.; Ling, J.; Shu, L. BLTM: beta and LQI based trust model for wireless sensor networks. *IEEE Access* **2019**, 7, 43679–43690.
- [17] Mohsenzadeh, A.; Bidgoly, A.J.; Farjami, Y. A novel reward and penalty trust evaluation model based on confidence interval using Petri Net. *Journal of Network and Computer Applications* **2020**, 102533.
- [18] Malik, N.A.; Rai, M. Enhanced Secure and Efficient Key Management Algorithm and Fuzzy With Trust Management for MANETs. Available at SSRN 3565898
- [19] Duan, J.; Gao, D.; Yang, D.; Foh, C. H.; Chen, H. H. An energy-aware trust derivation scheme with game theoretic approach in wireless sensor networks for IoT applications. *IEEE Internet of Things Journal* **2014**, 1(1), 58–69.
- [20] Koliass, C.; Kambourakis, G.; Stavrou, A.; Voas, J. DDoS in the IoT: Mirai and other botnets. *Computer* **2017**, 50(7), 80-84.
- [21] Khalil, A.; Mbarek, N.; Togni, O. Fuzzy Logic based security trust evaluation for IoT environments. In *2019 IEEE/ACS 16th International Conference on Computer Systems and Applications (AICCSA)*, 2019; (pp. 1-8).
- [22] Chen, J.; Tian, Z.; Cui, X.; Yin, L.; Wang, X. Trust architecture and reputation evaluation for internet of things. *Journal of Ambient Intelligence and Humanized Computing* **2019**, 10(8), 3099–3107.
- [23] Boussard, M.; Papillon, S.; Peloso, P.; Signorini, M.; Waisbard, E. STeward: SDN and blockchain-based Trust evaluation for Automated Risk management on IoT Devices. In IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2019; pp. 841–846.
- [24] Gao, Z.; Zhao, W.; Xia, C.; Xiao, K.; Mo, Z.; Wang, Q.; Yang, Y. A Credible and Lightweight Multidimensional Trust Evaluation Mechanism for Service-Oriented IoT Edge Computing Environment. In 2019 IEEE International Congress on Internet of Things (ICIOT), 2019; pp. 156–164.
- [25] Wang, T.; Luo, H.; Jia, W.; Liu, A.; Xie, M. MTES: An intelligent trust evaluation scheme in sensor-cloud enabled industrial Internet of Things. *IEEE Transactions on Industrial Informatics*.
- [26] Dass, P.; Misra, S.; Roy, C. T-safe: Trustworthy service provisioning for IoT-based intelligent transport systems. *IEEE Transactions on Vehicular Technology* **2020**, 69(9), 9509-9517.
- [27] Jayasinghe, U.; Lee, G. M.; Um, T. W.; Shi, Q. Machine learning based on trust computational model for IoT services. *IEEE Transactions on Sustainable Computing* **2018**, 4(1), 39-52.
- [28] Ma, W.; Wang, X.; Hu, M.; Zhou, Q. Machine Learning Empowered Trust Evaluation Method for IoT Devices. *IEEE Access* **2021**, 9, 65066-65077.
- [29] Sedjelmaci, H.; Senouci, S. M.; Al-Bahri, M. A lightweight anomaly detection technique for low-resource IoT devices: A game-theoretic methodology. In *2016 IEEE international conference on communications (ICC)* **2016** (pp. 1-6).
- [30] Sedjelmaci, H.; Senouci, S. M.; Taleb, T. An accurate security game for low-resource IoT devices. *IEEE Transactions on Vehicular Technology* **2017**, 66(10), 9381–9393.
- [31] Rani, R.; Kumar, S.; Dohare, U. Trust evaluation for light weight security in sensor enabled internet of things: game theory oriented approach. *IEEE Internet of Things Journal* **2019**, 6(5), 8421–8432.
- [32] Rao, J. D.; Sridevi, K. Novel security system for wireless body area networks based on fuzzy logic and trust factor considering residual energy. *Materials Today: Proceedings* **2021**, 45, 1498-1501.

Multi-Criteria Decision-Making Approach for Selection of Requirements Elicitation Techniques based on the Best-Worst Method

Abdulmajeed Aljuhani

College of Computer Science and Engineering
Taibah University
Medina 41411, Saudi Arabia

Abstract—During requirements elicitation stage, requirements engineers gather system requirements and drive stakeholders to convey needs and desired software functionality. The elicitation techniques used to acquire software requirements significantly impact the quality of elicited requirements. Several elicitation techniques have been proposed for the Requirement Engineering (RE) process; however, these techniques are rarely used in reality due to a lack of empirical and relative appraisals to assist software team members in deciding on the most appropriate technique. Requirement engineers encounter difficulty in deciding the suitable elicitation technique to adopt for a certain software project. This difficulty is due to a lack of knowledge regarding the available elicitation techniques, their efficacy, and how appropriate they are for a certain project. According to the literature, requirements engineering processes benefit from the use of Multi-Criteria Decision-Making (MCDM) approaches within particular contexts. An optimal structure is constitutionally presented within the area of the requirements engineering process; hence, the demonstration of a robust decision-making method in the requirements engineering process should motivate a higher level of satisfaction with software projects developed in this way. This study proposes an approach for using the MCDM method in the requirements engineering process. The study contains a model for investigating the selection of an appropriate elicitation technique based on a decision-making method, namely, the Best-Worst Method (BWM). The findings of the proposed model demonstrate the BWM's power in solving complex decision problems involving several criteria and alternatives.

Keywords—Requirements elicitation; elicitation techniques; decision support methods; Best-Worst Method; BWM

I. INTRODUCTION

In Software Engineering (SE), the software requirements are the services that the software provides to customers to satisfy their needs. Additionally, the software requirements are constraints on its functionality [1]. Requirements engineering is the process of analyzing and determining these software services and constraints. Often, a focused investigation takes place as a pre-step at the RE stage. The focused investigation seeks to answer general queries, such as: does the software contribute to the goals of the company? Is the implementation plan appropriate considering the budget and schedule [1]? RE activities are introduced at the initial phase of the Software Development Life Cycle (SDLS), which allows the development team to draw a clear view of the functionalities and benefits that the system could provide.

The process of RE consists of activities such as communicating with software stakeholders to discover requirements (elicitation), creating a specification document based on the discovered requirements, and validating the requirements against the stakeholders' needs [2]. The requirements elicitation activity allows developers to better understand the stakeholders' needs and how they can benefit from using the new system. This is achieved by working with both stakeholders and developers in order to analyze the problem domain and the current limitations, along with the services and work activities that stakeholders needs.

However, gathering requirements from stakeholders is a difficult task due to system stakeholders' lack of knowledge about what they want. In addition, developers may have a lack of stakeholders' domain, which might lead to a misunderstanding regarding what customers need during the elicitation process. Furthermore, several stakeholders might emphasize the same requirements in different ways, which may result in requirements conflicts. Despite the dynamic environment of the analysis stage, new customers will bring about changes to the project's initial requirements and the addition of new requirements. Also, political and environmental issues might affect the system requirements and the requirements gathering process.

Generally, the activities in the requirements elicitation process include requirements finding and understanding, requirements categorisation, requirements ranking, and requirements documentation. The requirements elicitation process is based on several iterations with ongoing feedback between these activities. There are several requirements elicitation techniques that can be used to assist developers in discovering and gathering the system requirements, which results in delivering satisfactory software to stakeholders [3]. Increasing the number of requirements elicitation techniques makes it difficult for the development team to select the most appropriate technique for a certain software project. Several challenges accompany the selection of the appropriate elicitation technique, such as the type of software methodology, developers experience, customer knowledge, and available technologies. There is no elicitation technique that is appropriate for all projects; however, each software project has its circumstances that affect the selection of an appropriate requirements elicitation technique. The selection of an elicitation technique might be affected by various criteria that influence the software project, making it important for the development team to be aware of this. These

criteria include, for example, the diversity of customers and their availability, and customers' skills and experiences.

This paper investigates the incorporation of a MCDM—specifically, the BWM—into requirement elicitation activity in order to select the appropriate requirement elicitation technique. The BWM framework consists of a set of elicitation techniques that serve as alternatives that are weighted against each other with respect to several criteria that influence the software project. Each elicitation technique is evaluated with respect to these criteria, and the final selection is made based on the overall weight of all techniques.

This paper is organized as follows: Section 2 describes the work related to this research topic. Section 3 introduces the BWM method. Sections 4 describes the proposed criteria and alternatives. Section 5 shows the BWM structure in the requirement elicitation process. Section 6 presents the results and discussion. Finally, Section 7 offers a conclusion and suggests possible future work

II. RELATED WORK

Tiwari and Rathore sought to enhance the requirement elicitation process by introducing an approach in order to choose a subset of requirement elicitation methods [4]. The authors identified several criteria with respect to three dimensions—namely, the people, the project, and the software process development—and constructed the three p matrix for the three dimensions and their relationship with the elicitation methods. The selection decision is made based on the analyst's experience and the three p matrix mapping mechanism [4]. Ribeiro et al. [5] introduced a method for determining the acceptability and effectiveness of a web collaborative tool whose primary goal is to gather requirements from stakeholders. As a development tool, the six thinking hats technique and gamification were applied. The primary objective of this research is to strengthen stakeholder collaboration by discussing findings and their impacts [5]. The requirements elicitation activity can be viewed from a behavioral and social perspective, which requires equally collaborative communication by all stakeholders. Chakraborty et al. [6] introduced a model based on a conceptualized method in order to provide a road map for the requirements elicitation activity. In their model, the authors addressed interaction dynamics between future system users and requirements engineers. Their study is focused on the four states, and it highlights potential variables that are likely to cause movement from one stage to the next [6].

A prototype was suggested by Vijayan and Raju to be used for requirement elicitation in order to avoid system errors caused by a lack of communication between users and requirements engineers [7]. Domain knowledge acquisition, system understanding, requirements elicitation, prototype validation, and requirements stabilization are the five processes in this prototype method. Such a method is appropriate for small to medium-sized projects, but it adds to the project's cost and time is also required to build a prototype model of the project. Requirements ambiguity has a negative influence on several significant factors, such as quality and cost [8]. There are difficulties in defining the complete and correct requirements in the early stages. Thus, having a prototype model of how the system should look can assist customers in understanding

the system's layout and structure. Poorly stated requirements, according to Jain and Ingle [9], are due to inconsistencies in the choosing of requirements elicitation techniques, the amount of information, and missing requirements on standard security solutions. Mulla and Girase [10] stated that eliciting requirements is a difficult undertaking, particularly in large software projects with a wealth of details and several stakeholders with various perspectives. Moreover, Zhang et al. [11] suggested that a lack of requirements elicitation activity is the main cause of software project failure besides inadequate project scope.

The significance of the human factor at the requirements elicitation stage has been studied by different researchers [12], [13], [14], [15], [16], [17], [18]. For example, Fuentes et al. [12] presented a comprehensive Unified Modeling Language (UML) schemata for social issues, providing patterns in order to reconcile stakeholder conflicts. In addition, it is believed that the elicitation process should involve any factor that might impact the developed system or its use in terms of meeting the customers' needs [12]. Dragicevic and Celar [13] presented a method for requirement elicitation, documentation, and validation called MeDoV. Even-driven process (EPC) and UML activity diagrams were used to model requirements. The high acceptance of EPC by business users made it the preferred method of the authors. Additionally, the authors introduced the adoption of the MoDeV framework for requirement engineering [13].

Yousuf et al. [19] proposed a method for selecting appropriate elicitation techniques based on a variety of parameters, including system and requirements type, stakeholder involvement, schedule, and team skills and experience. Abbasi et al. [20] compared the strength of several requirement elicitation methods and requirement tools with respect to numerous factors. In addition, the authors addressed the disadvantages of using a single requirement elicitation technique. Factors such as project environment and stakeholder characteristics were specified by Anwar and Razali [21] as requiring consideration in order to develop a step-by-step strategy to decide the best requirements elicitation techniques for a specific project. Furthermore, Hickey and Davis' [22] mathematical model of requirement elicitation discussed what requirements engineers need to consider during requirement elicitation activity, how to select the appropriate elicitation techniques, and how to enhance the likelihood that the system will fulfill stakeholders' needs.

Darwish et al. [23] investigated the selection of requirements elicitation techniques based on an artificial neural network (ANN) model in order to minimize human engagement in the selection stage. The introduced model can recommend appropriate techniques for gathering information. In addition, the model depends on a set of features representing past requirement elicitation scenarios, such as project complexity.

Li et al. [24] studied the selection of requirement elicitation techniques based on the Analytic Network Process (ANP). The ANP has the ability to structure complex decision problems in a network containing several criteria that affect the selection of elicitation techniques. The authors identified 14 criteria, such as stakeholder availability, reusable requirements availability, project schedule constraints, financial constraints, stakeholder relationship, stakeholder diversity, existing system maintenance, etc. [24]. Moreover, Li et al. evaluated six elicitation

techniques as alternatives: interview, surveys, task analysis, introspection, questionnaire, and document analysis [24].

III. THE BEST WORST METHOD

The best–worst method (BWM), introduced by Rezaei [25], is a new approach that, since its presentation, has stood out for researchers from different disciplines. Its ease of use, the more modest number of comparisons, and the steadier judgments, in contrast with comparable techniques such as the Analytic Hierarchy Process (AHP) and ANP, have made the BWM a trustworthy and attractive approach. The BWM can assist decision makers in deciding criteria weights by distinguishing the best (i.e., generally positive or generally significant) and the worst (i.e., least significant) criteria. Moreover, pairwise comparisons are then completed based on each of the two criteria (i.e., best and worst) and other criteria. After that, the criteria weights are dictated by tackling a minimax problem. Despite prioritization in BWM being demonstrated to be sensible, it can be enhanced to catch the decision makers’ uncertainty. Two vectors of comparison (best-to-other criteria and other criteria-to-worst) are equally significant in the BWM. In addition, the decision maker’s confidence in the best-to-others and others-to-worst judgments are treated as equally significant. Moreover, the BWM expects decision makers to be completely sure about the best and worst criteria, along with the corresponding pairwise comparisons [26]. The decision-makers use the AHP fundamental scale introduced by Saaty [27] to obtain their judgments.

TABLE I. FUNDAMENTAL SCALE [27].

Value	Level of Importance
1	Equal importance
2	Weak or slight
3	Moderate importance
4	Moderate plus
5	Strong importance
6	Strong plus
7	Very strong
8	Very, very strong
9	Extreme importance

Similar to the AHP and the ANP, the BWM uses pairwise comparisons, yet the BWM is a more effective method in some ways than the AHP and the ANP, which has made it more common lately. For example, the BWM requires fewer pairwise comparisons than the AHP. Furthermore, the BWM involves less complex pairwise comparisons as, in the BWM, decision makers only need to fill the up part of the pairwise comparison with no need to use the reciprocal of the 1-9 scale, which makes it easier for the decision makers to measure.

Several researchers have investigated incorporating the BWM into software development. For example, Aljuhani and Alhubaishy [28] adopted the BWM in Mobile-D development, identifying nine insertion points that can benefit from the adoption of the BWM in order to reconcile conflicting perspectives among the team members. Furthermore, Alhubaishy and Aljuhani [29] investigated the use of the BWM in cloud computing in order to manage resource allocation and prioritize several tasks.

A. Steps of BWM

As stated by Rezaei [25], the BWM consists of five main steps, which are as follows:

Step 1. The decision criteria $\{c_1, c_2, \dots, c_n\}$ that impact the proposed solutions or alternatives are specified.

Step 2. The best and the worst criteria are specified by the decision makers without making a comparison at this step.

Step 3. A series of judgments of the other criteria are made with respect to the best criterion, based on the proposed fundamental scale in table I and what the outcome vector would be [25]:

$$A_B = (a_{B1}, a_{B2}, \dots, a_{Bn}),$$

Where a_{Bj} reflects the comparison of criterion j with respect to the best criterion B .

Step 4. A series of judgments are made on the worst criterion in relation to the other criteria based on the proposed fundamental scale in table I and what the outcome vector would be [25]:

$$A_W = (a_{1W}, a_{2W}, \dots, a_{nW}),$$

Where a_{1W} reflects the comparison of criterion j with respect to the worst criterion W .

Step 5. The criteria optimum weights $w^*_{1}, w^*_{2}, \dots, w^*_{n}$ are identified, and it is the weight where, we have $w_B/w_j = a_{Bj}$ and $w_j/w_w = a_{jw}$ for each pair of w_B/w_j and w_j/w_w [25]. Also, in order to determine the solution, the maximum absolute differences $\left| \frac{w_B}{w_j} - a_{Bj} \right|$ and $\left| \frac{w_j}{w_w} - a_{jw} \right|$ should be minimized to be to satisfy these conditions for all j as stated by [25]. This leads to the following problem:

$$\begin{aligned} \min \max_j \left\{ \left| \frac{w_B}{w_j} - a_{Bj} \right|, \left| \frac{w_j}{w_w} - a_{jw} \right| \right\} \\ \text{s.t.} \\ \sum_j w_j = 1 \\ w_j \geq 0, \text{ for all } j \end{aligned} \quad (1)$$

Thus, problem 1 has been transferred to the next problem:

$$\begin{aligned} \min \xi \\ \text{s.t.} \\ \left| \frac{w_B}{w_j} - a_{Bj} \right| \leq \xi, \text{ for all } j \\ \left| \frac{w_j}{w_w} - a_{jw} \right| \leq \xi, \text{ for all } j \\ \sum_j w_j = 1 \\ w_j \geq 0, \text{ for all } j \end{aligned} \quad (2)$$

We obtain the ideal weights and ξ^* by solving problem 2.

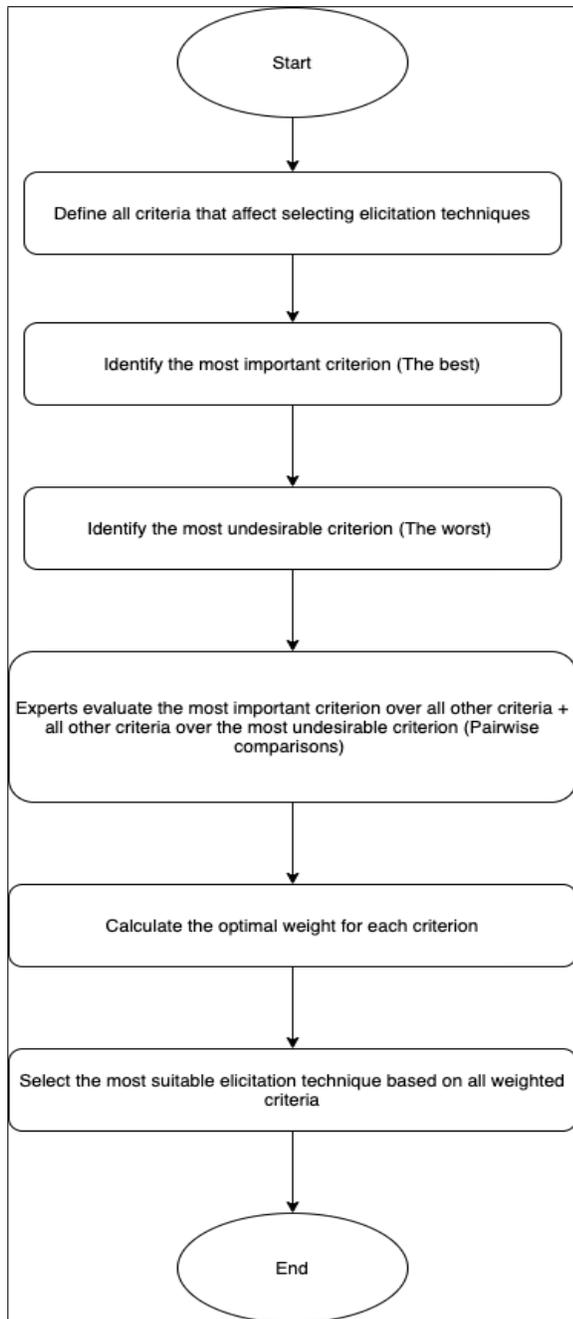


Fig. 1. BWM Steps to Select the Best Elicitation Technique.

Moreover, the consistency ratio is obtained based on the following problem:

$$\text{Consistency Ratio} = \frac{\xi^*}{\text{Consistency Index}}$$

Where the consistency index depends on the number of criteria included in the decision problem as shown in [25]. While the consistency ratio value should be < 0.10 as the comparisons would otherwise be considered inconsistent. The BWM steps are visually represented in Fig. 1.

IV. PROPOSED CRITERIA FOR SELECTING PROCESS

Technique selection for the elicitation process is greatly affected by project environment criteria (attributes). It may be appropriate to use one technique for eliciting requirements with respect to one attribute, but not for the rest of them. Identifying the factors that influence the selection process is essential for choosing the right elicitation technique. To show their inter-dependencies, these criteria are compared with each other and compared in relation to each alternative or elicitation technique. Criteria are used to compare the elicitation techniques, allowing for a better understanding of how the selection process is affected by each criterion. Therefore, to select a suitable elicitation technique, this paper proposes nine criteria, which are taken from [24], [30], [18], and [31]. It is valuable to address how different studies use the same methodology with different criteria. The studied criteria are as follows:

- Analysts and User's Cultural Diversity (AUCD)
- Availability of Key Stakeholders (ASTK)
- Availability of Reusable Requirements (RQ)
- Availability of Communication Technology (ACT)
- Availability of Resources (AR)
- Degree of Financial Constraints (FCO)
- Geographical Distribution of the Stakeholders (DSTK)
- User's Cooperation and Motivation (UCM)
- User's Expressiveness (EXP)

V. BWM STRUCTURE FOR SELECTING ELICITATION TECHNIQUES

Similar to the ANP and AHP, the BWM structure for selecting the appropriate elicitation technique consists of three levels. The first level explains the goal of the adoption of the BWM, which in this paper is selecting the best elicitation technique. The second level describes the selection criteria, which are introduced in the previous section. The third level contains the alternatives, which are the elicitation techniques that are evaluated against each other in order to select the most appropriate one with respect to various attributes. Eliciting requirements can be done using a variety of methods; however, in this paper, six traditional elicitation techniques are selected to evaluate in the BWM model. These techniques are [20], [24], [32]:

- Interview (IV)
- Questionnaire (QN)
- Survey (SV)
- Document Analysis (DA)
- Task Analysis (TA)
- Introspection (IS)

Fig. 2 shows the BWM structure for selecting the best elicitation technique.

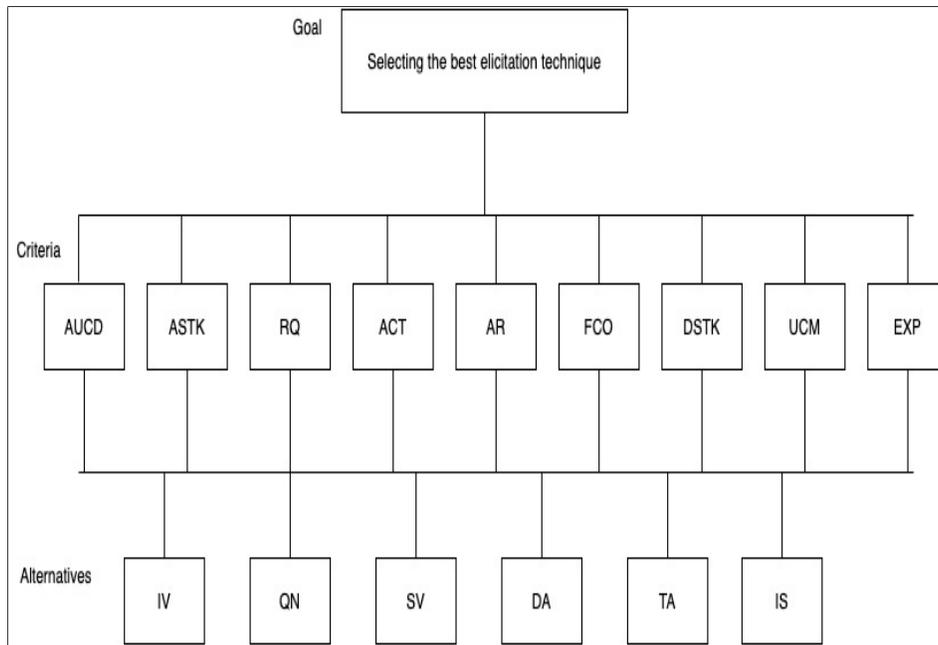


Fig. 2. BWM Structure for the Elicitation Techniques.

A. BWM Model Evaluation Based on Expert's Opinion

In this paper, the main objective is to investigate the adoption of the BWM for selecting the appropriate requirement elicitation technique during software project development. The chosen research methodology is the case study methodology, which is described in [11]. In this regard, two research questions are raised in order to better focus the case study: 1) how can the BWM help in selecting the appropriate requirement elicitation technique, and 2) how can the BWM affect the team members' communication and productivity? The units of analysis for the proposed study are derived from these questions. Evaluating and selecting are two units of analysis that are appropriate to use, as well as the experts' opinion of the BWM in selecting the suitable elicitation technique.

Criteria that affect the selection of elicitation techniques were identified as a first step in BWM evaluation in order to highlight the BWM's abilities and benefits. The source of the collected data was 27 domain experts, and the data collection tool was a questionnaire distributed among these experts. The experts were asked to evaluate the proposed criteria in order to weight each criterion in the model. By following the BWM steps, the experts first determined the best criterion and made a pairwise comparison to specify the weight of the best chosen criterion over all of the other criteria, as shown in Table II. The pairwise comparison in Table II can be read as follows: the ASTK criterion is 4, 9, 8, 4, 8, 5, 4 and 5 times more important than the AUCD, RQ, ACT, AR, FCO, DSTK, UCM and EXP criteria, respectively. In other words, the ASTK should be given preference over the EXP criterion, for example, as it is 5 times more important.

Then, the experts made judgments based on the pairwise comparison among all of the other criteria over the worst selected criterion. In table III FCO should be given preference over RQ, for example, but the judgement between the two

criteria indicates that there is a weak level of preference of FCO over RQ, as FCO is only 2 times as important as RQ. In addition, ASTK is given preference over RQ as it is 9 times more important, which means that there is an extreme preference for ASTK over RQ.

VI. RESULTS AND DISCUSSION

The aggregated result based on 27 domain experts shows that the ASTK criterion was evaluated as the most significant attribute for selecting the appropriate elicitation technique. The AR criterion was ranked in the second position, followed by EXP and UCM. The AUCD criterion was ranked in the fifth position. ACT and RQ were ranked in the sixth and seventh positions, respectively. FCO was ranked in the eighth position, while DSTK was the least important. The overall weights of all criteria are shown in Table IV.

Furthermore, based on the BWM, the IV technique is evaluated as the most appropriate elicitation technique. The results also show that TA is ranked in the second position, followed by the DA technique. Moreover, SV was ranked in the fourth position, followed by QN and IS. The final weights for all techniques are shown in Table V.

The domain experts addressed some benefits they gained from this study. For example, the BWM reconciled conflicting opinions among the team members using a scientific approach. The power of the BWM helps the development team to easily solve complex and unstructured problems. In addition, the structure of the presented method allows every member to participate in the decision process based on his/her experience. This way, a high level of satisfaction among these members is ensured, which might be reflected in the project's quality. The BWM assists in making decisions with respect to several attributes affecting the decision-making process. Moreover, the BWM provides team members or managers with a better

TABLE II. PAIRWISE COMPARISON OF ASTK CRITERION WITH RESPECT TO OTHER CRITERIA

Best to Others & AUCD & ASTK & RQ & ACT & AR & FCO & DSTK & UCM & EXP
ASTK & 4 & 1 & 9 & 8 & 4 & 8 & 5 & 4 & 5

TABLE III. PAIRWISE COMPARISON OF CRITERIA WITH RESPECT TO RQ CRITERION

Others to the Worst	RQ
AUCD	3
ASTK	9
RQ	1
ACT	2
AR	3
FCO	2
DSTK	3
UCM	5
EPX	4

TABLE IV. THE IMPORTANCE OF CRITERIA

Ranking	Criteria	Weights (%)
1	ASTK	18.08%
2	AR	13.60%
3	EXP	12.70%
4	UCM	12.04%
5	AUCD	11.67%
6	ACT	11.06%
7	RQ	8.50%
8	FCO	7.01%
9	DSTK	5.30%

understanding about the most significant criteria to consider when selecting the suitable elicitation technique. The BWM also produces highly consistent findings for the consistency ratio value for each paired comparison. Here, the consistency ratio was 0.08, which is less than the maximum acceptable consistency ratio of 0.10.

These results demonstrate that the BWM can be integrated into requirement elicitation activities, as shown in Table IV and Table V, thereby validating the method’s viability. Regarding the decision model presented here, there is a key issue. At least one team member (such as a project leader) would involve significant BWM training, since it is an integral part of the requirement elicitation activities. The BWM can be applied to impromptu decision crises not covered by the presented model. After all, the cost of integrating the BWM into the requirement elicitation stage is included in this.

VII. CONCLUSION

It is essential to use the most appropriate selection approach in order to elicit relevant requirements. The most appropriate technique will gather the most relevant requirements, increasing productivity and ensuring more successful software projects within the planned budget and schedule. The requirement elicitation activity was contextualized in this paper by applying the BWM decision-making method. In particular, this study concentrates on selecting the appropriate elicitation technique for a certain project with respect to multiple attributes affecting the selection process. The requirements engineering stage is a critical stage in the software life-cycle; therefore, selecting the most suitable requirement elicitation technique is important in order to ensure project success. A total of 27 domain experts participated in this

TABLE V. THE IMPORTANCE OF ELICITATION TECHNIQUES

Ranking	Criteria	Weights (%)
1	IV	28.72%
2	TA	15.92%
3	DA	14.62%
4	SV	14.21%
5	QN	13.71%
6	IS	12.81%

investigation by adopting the BWM for selecting the best elicitation technique. The participants entered their judgments in BWM pairwise comparisons, and the final results were obtained based on the aggregated results of all experts. The BWM results addressed the importance of the ASTK criterion during gathering requirements. The interview was selected as the best elicitation technique based on the BWM results. The research findings showed the power of the BWM for solving complicated problems in less time as compared to similar approaches, such as the AHP and the ANP. The introduced method requires $2n-3$ comparisons, while AHP requires $n(n-1)/2$ comparisons, where n is the number of elements in the model.

The following are some of the advantages of using the model presented in this paper:

- A formalized decision-making process is established to help improve the structure and adaptability of the selection of the requirement elicitation technique.
- Based on a scientific approach, it is possible to reconcile different perspectives when selecting the most suitable elicitation technique.

In the future, the BWM can be integrated into other approaches in order to enhance the accuracy of its outputs. For example, it can be integrated with a fuzzy set to provide better results in handling subjective assessments and roughness when evaluating a model’s items. Building an automated BWM tool to meet the RE process and its values is another future project that could be undertaken. However, the adoption of a multi-decision support approach at the requirement elicitation stage requires comprehensive knowledge of the problem area, to ensure that the most effective attributes are identified and techniques to avoid intensive computations are put to use.

REFERENCES

- [1] I. Sommerville, *Software Engineering GE*. Pearson Australia Pty Limited, 2016.
- [2] I. Board, “Ieee standard glossary of software engineering terminology,” *New York Inst. Electr. Electron. Engineers*, 1990.
- [3] N. Garg, P. Agarwal, and S. Khan, “Recent advancements in requirement elicitation and prioritization techniques,” in *2015 International Conference on Advances in Computer Engineering and Applications*. IEEE, 2015, pp. 237–240.
- [4] S. Tiwari and S. S. Rathore, “A methodology for the selection of requirement elicitation techniques,” *arXiv preprint arXiv:1709.08481*, 2017.

- [5] C. Ribeiro, C. Farinha, J. Pereira, and M. M. da Silva, "Gamifying requirement elicitation: Practical implications and outcomes in improving stakeholders collaboration," *Entertainment Computing*, vol. 5, no. 4, pp. 335–345, 2014.
- [6] S. Chakraborty, S. Sarker, and S. Sarker, "An exploration into the process of requirements elicitation: A grounded approach," *Journal of the association for information systems*, vol. 11, no. 4, p. 1, 2010.
- [7] J. Vijayan and G. Raju, "A new approach to requirements elicitation using paper prototype," *International Journal of Advanced Science and Technology*, vol. 28, pp. 9–16, 2011.
- [8] K. Pohl, *Requirements engineering fundamentals: a study guide for the certified professional for requirements engineering exam-foundation level-IREB compliant*. Rocky Nook, Inc., 2016.
- [9] S. Jain and M. Ingle, "Software security requirements gathering instrument," *International Journal*, vol. 2, 2011.
- [10] N. Mulla and S. Girase, "A new approach to requirement elicitation based on stakeholder recommendation and collaborative filtering," *International Journal of Software Engineering & Applications*, vol. 3, no. 3, p. 51, 2012.
- [11] Y. Zhang, M. Harman, A. Finkelstein, and S. A. Mansouri, "Comparing the performance of metaheuristics for the analysis of multi-stakeholder tradeoffs in requirements optimisation," *Information and software technology*, vol. 53, no. 7, pp. 761–773, 2011.
- [12] R. Fuentes-Fernández, J. J. Gómez-Sanz, and J. Pavón, "Understanding the human context in requirements elicitation," *Requirements engineering*, vol. 15, no. 3, pp. 267–283, 2010.
- [13] S. Dragicevic and S. Celar, "Method for elicitation, documentation and validation of software user requirements (medov)," in *2013 IEEE Symposium on Computers and Communications (ISCC)*. IEEE, 2013, pp. 000956–000961.
- [14] S. T. Acuña, J. W. Castro, and N. Juristo, "A hci technique for improving requirements elicitation," *Information and Software Technology*, vol. 54, no. 12, pp. 1357–1375, 2012.
- [15] G. N. Aranda, A. Vizcaíno, and M. Piattini, "A framework to improve communication during the requirements elicitation process in gsd projects," *Requirements engineering*, vol. 15, no. 4, pp. 397–417, 2010.
- [16] A. S. Bojnord, R. B. Ahmad, and H. S. Bojnord, "Webstuire: web-based support tool for user interface requirements elicitation," in *ICCKE 2013*. IEEE, 2013, pp. 52–58.
- [17] J. Fernandes, D. Duarte, C. Ribeiro, C. Farinha, J. M. Pereira, and M. M. da Silva, "ithink: A game-based approach towards improving collaboration and participation in requirement elicitation," *Procedia Computer Science*, vol. 15, pp. 66–77, 2012.
- [18] D. Carrizo, O. Dieste, and N. Juristo, "Systematizing requirements elicitation technique selection," *Information and Software Technology*, vol. 56, no. 6, pp. 644–669, 2014.
- [19] M. Yousuf, M. Asger, and M. Bokhari, "A systematic approach for requirements elicitation techniques selection: a review," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, no. 4, pp. 1399–1403, 2015.
- [20] M. A. Abbasi, J. Jabeen, Y. Hafeez, D. Batool, and N. Fareen, "Assessment of requirement elicitation tools and techniques by various parameters," *Software Engineering*, vol. 3, no. 2, pp. 7–11, 2015.
- [21] F. Anwar and R. Razali, "A practical guide to requirements elicitation techniques selection-an empirical study," *Middle-East Journal of Scientific Research*, vol. 11, no. 8, pp. 1059–1067, 2012.
- [22] A. M. Hickey and A. M. Davis, "Requirements elicitation and elicitation technique selection: model for two knowledge-intensive software development processes," in *36th Annual Hawaii International Conference on System Sciences, 2003. Proceedings of the*. IEEE, 2003, pp. 10–pp.
- [23] N. R. Darwish, A. A. Mohamed, and A. S. Abdelghany, "A hybrid machine learning model for selecting suitable requirements elicitation techniques," *International Journal of Computer Science and Information Security*, vol. 14, no. 6, pp. 1–12, 2016.
- [24] J. Li, A. Ullah, J. Li, S. Nazir, H. U. Khan, H. Ur Rehman, and A. U. Haq, "Attributes-based decision making for selection of requirement elicitation techniques using the analytic network process," *Mathematical Problems in Engineering*, vol. 2020, 2020.
- [25] J. Rezaei, "Best-worst multi-criteria decision-making method: Some properties and a linear model," *Omega*, vol. 64, pp. 126–130, 2016.
- [26] A. Vafadarnikjoo, M. Tavana, T. Botelho, and K. Chalvatzis, "A neutrosophic enhanced best-worst method for considering decision-makers' confidence in the best and worst criteria," *Annals of Operations Research*, vol. 289, no. 2, pp. 391–418, 2020.
- [27] T. L. Saaty, "How to make a decision: the analytic hierarchy process," *European journal of operational research*, vol. 48, no. 1, pp. 9–26, 1990.
- [28] A. Aljuhani and A. Alhubaishy, "Incorporating a decision support approach within the agile mobile application development process," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2020, pp. 1–6.
- [29] A. Alhubaishy and A. Aljuhani, "The best-worst method for resource allocation and task scheduling in cloud computing," in *2020 3rd International Conference on Computer Applications & Information Security (ICCAIS)*. IEEE, 2020, pp. 1–6.
- [30] Y. Ayalew and A. Masizana-Katongo, "A multi-criteria group decision support approach for requirements elicitation techniques selection," *Asian Journal of Information Technology*, vol. 7, no. 2, pp. 40–52, 2008.
- [31] L. C. Ronoh, G. M. Muchiri, and F. Wabwoba, "Factors affecting requirements elicitation for heterogeneous users of information systems," 2015.
- [32] M. Tariq, S. Farhan, H. Tauseef, and M. A. Fahiem, "A comparative analysis of elicitation techniques for design of smart requirements using situational characteristics," *International Journal of Multidisciplinary Sciences and Engineering*, vol. 6, no. 8, pp. 30–38, 2015.

e-Business Model to Optimise Sales through Digital Marketing in a Peruvian Company

Misael Lazo-Amado, Leoncio Cueva-Ruiz, Laberiano Andrade-Arenas
Facultad de Ciencias e Ingeniería
Universidad de Ciencias y Humanidades

Abstract—The COVID-19 pandemic has affected the Peruvian market, generating a great loss in sales in Peruvian companies. The objective of the research is to develop a model to optimize sales with the use of digital marketing in a Peruvian company, the chosen methodology is DesingScrum, which is a hybrid of Scrum and Desing Thinking, with 10 phases (empathize, define. It has 10 phases (empathise, define, ideate, planning meeting, sprint backlog, daily meeting, sprint review, sprint retrospective sprint, prototype and testing) and the MarvelApp tool was used to create the prototype. The results are obtained after the completion of the review of each sprint, showing in detail how it was progressing in each sprint, and through the retrospective evaluated the development of the project for the realization of continuous improvement in the next product. Further prototype was made, with the application MarvelApp, which shows the model of e-business. Then testing was done through a survey that customers gave their opinions about the prototype and finally the digital marketing proposal was made by a model, which explains the interconnected tools to attract new customers. The conclusion is the construction of the digital marketing model according to the needs of the context to improve the sales of the company through e-business.

Keywords—Design thinking; desingScrum methodology; digital marketing; e-Business; scrum

I. INTRODUCTION

The trade and economic impact of the pandemic on large and small businesses and organisations around the world has had an impact on their financial statements, and Pakistan's analysis indicates that 184 MIPYMES (small and medium-sized enterprises), 83%, did not have a strategic plan in place to deal with the impact of the pandemic [1], MIPYMES were severely affected and face several problems such as reduced sales, supply chain disruption, decreased demand and financial problems [2].

In Latin America, the Argentinean country had been dragging along different economic problems before the pandemic began, generating the final blow to the economic and commercial crisis, as its currency began to devalue more than it should have, increasing the price of products [3]. Which President Alberto Fernandez had to take as a threat to Covid-19, where he addressed a message to the nation on 19 March 2020 [4]. Announcing a decree of compulsory isolation, he had to implement this measure so that there would not be an increase in positive cases of coronavirus.

Companies were hit hard economically and commercially by the instability of Covid-19. Peru suffered a hard blow in the coast, highlands and jungle. Then there was an attempt to adopt social distancing and restrictions on access to markets,

which began to generate uncertainty in the purchase and sale of companies and organisations [5]. As a clear example, when the pandemic started, people started to buy more products, generating a commercial and economic impact, which led to inflation in food products, transport, among others. In order for companies not to go bankrupt, the state had to designate a small bonus "ReactivaPeru" to help micro and large companies, this bonus was only going to be designated to all companies that were up to date in their tax payments or were registered with the National Superintendence of Customs and Tax Administration.

Then, according to the analysis of the problems of different countries of the world, it indicates a similar problem in the company Domínguez in Peru, which is the object of study, since the pandemic is the main problem, obtaining a great loss of potential and economic clients. We also identified that the importance of having a strategic plan to combat the pandemic in commercial matters is a priority.

The objective is to carry out an e-Business modelling to optimise sales through digital marketing in a Peruvian company.

This research work will allow the development of new ideas, contributing to the improvement of business in the Peruvian state, to the point of guiding businessmen to use e-business in their companies, whether they are MYPES or PYMES, allowing the optimisation of their virtual sales safely to the point that they can be recognised at national, departmental or district level. Taking into account that digital marketing will help to have a better positioning in the virtual market, while the E-commerce will be able to make any type of online purchase, having a better transparency towards their consumers.

II. LITERATURE REVIEW

In these times of pandemic of covid-19 have increased virtual shops and digital marketing, as there are a variety of free or paid platforms for this implementation. Taking into account in this pandemic there have been different financial cases that have affected micro and large companies, which have been lowering their sales by the COVID-19 which did not have a contingency plan to be able to support their sales of their products.

It should also be pointed out that there was a decreasing demand for their sales, since at the beginning and even at the present time of the pandemic they have to comply with the sanitary norms decreed by the Peruvian government. For this reason, researchers are analysing and implementing new

measures or strategies to maintain and increase their financial status. The financial problem in the pandemic has been affecting the majority of micro, medium and large companies, where they have had to implement a contingency plan to create different techniques to deal with this problem by means of. The multiple discriminant analysis (MDA), the binary regression that would come to be a logistic analysis these 2 techniques have to have a greater efficiency and security that have been applied at international level [6]. It is taken into account that 22% of companies implement e-commerce through B2C (Business-to-consumer) helping the supplier to reach the customer or end consumer, in order to have a greater reach to customers, applying some marketing strategies such as online marketing and social networks. Which have been benefiting large companies, rather than micro or medium enterprises applying the B2C strategy along with digital marketing [7]. It consists of 2 important states, massiveness and personification allowing to approach the customer through advertisements, by means of liking, priority, benefit, etc. [8]. Allowing for low-cost promotion of products to the customer.

Digital marketing has different problems at the time of structuring within the company. For which a solution emerged that consists of a set of ideas between the people in charge of advertising where different activities will be planned to learn, currently there are several independent companies that are dedicated to marketing and forget to plan the overall approach to develop [8].

On the other hand [9], an analysis is made where companies implement e-business in order to increase their sales in times of pandemic, however digital marketing strategies can improve e-commerce and has proven to be an effective method therefore [10], mentions that digital marketing tools allow to reach the target of companies, being the best strategy to satisfy the consumer.

Digital marketing is used to increase sales in an MYPE, being an effective 95% in sales, as well as the digital marketing strategy is supported in social networks, websites as it is able to attract many users and be visited continuously [11].

The e-commerce has been growing day by day, facilitating at the moment of carrying out the daily activities helping to create new business models. The e-commerce trying more of the purchase, sale and services of the products that the company has, where the participants would come to do (consumer, salesman, mediator and commercial partners), some advantages that it has is at the moment of making a selection specific offers by means of the low costs of the products towards the market, to have a greater facility and security in the communication of the supplier and the client. One of the disadvantages of e-commerce is that it does not have a social aspect which makes it similar to a classic online shop and this can affect the level of the company through its sales of its products [12].

E-commerce has increased due to covid-19 as consumers were afraid of getting infected, which is why they were forced to shop online [13].

Analyses of various research papers where the authors show that large or small companies engaged in trade contain financial problems as in this pandemic reduced their sales by 85%. That is why they were forced to carry out various

strategies to generate more sales concluding that the success of e-commerce will continue to be one of the best online platforms to meet the needs of the consumer, so in the field of digital marketing as it will be responsible for increasing new potential customers.

III. METHODOLOGY

In our methodology we used Design Thinking and Scrum to implement the e-business, this methodology is called Design-Scrum and has 10 stages (Empathise, Define, Ideate, Planning Meeting, Sprint Backlog, Daily Meeting, Sprint Review, Sprint Retrospective, Prototype, Testing).

A. Design Thinking

Design Thinking can be applied in different sectors and is one of the most demanded methodologies by companies, it has 5 stages (empathise, define, devise, prototype and test) as shown in Fig. 1 [14].

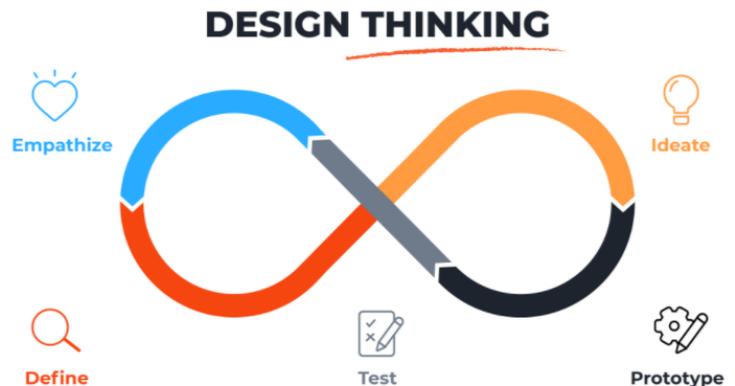


Fig. 1. Methodology Desing Thinking.

B. Scrum

The Scrum methodology is nowadays the most widely used methodology for project management in all companies for the development of web or desktop systems [15], The project is based on 3 important fundamentals that would make transparency, control and adaptation, guaranteeing us with a quality product [16]. It starts from the start date of the project, explaining its objectives and so that they can facilitate the designated work team [17], obtaining a product list. Then a product backlog will be made, this process helps to be able to manage the work team, finally a feedback will have to be made, so that it can be checked if the project is following all the corresponding step, to generate a quality product, as shown in Fig. 2 [18].

C. Phases of the Hybrid Methodology

The hybrid methodology called Desing Scrum, which is a combination of Design Thinking and Scrum, is explained in Fig. 3 indicating the phases to be used for the development of the e-business.

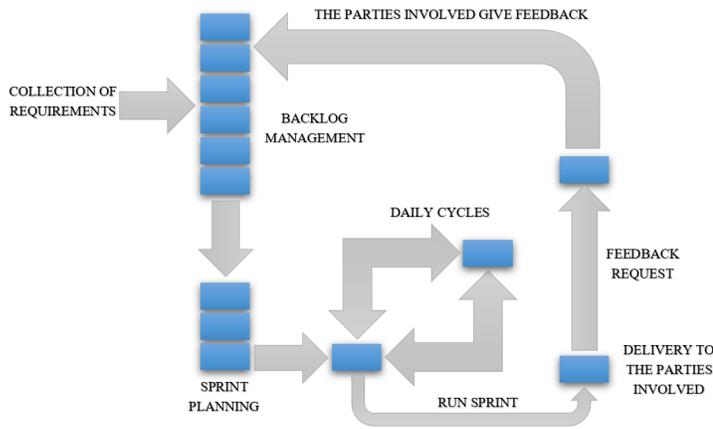


Fig. 2. Methodology Scrum.

1) *Empathise*: Empathy is the initial stage of the design thinking methodology, this will be in charge of knowing the needs of the users through surveys and interviews [19], allowing the designer to understand the problems of those involved.

2) *Define*: Once the needs of the users are known, the problem is defined [20]. The working team will be in charge of prioritising the most relevant problem of the users.

3) *Ideate*: At this stage, creativity and innovation will be developed, a variety of ideas will be developed to solve the users' problems [21]. The team will be in charge of choosing the ideal solution .

4) *Planning Meeting*: In this stage a set of requirements and user story will be defined to identify the functionality of the system where they will be grouped into a backlog [22].

5) *Sprint Backlog*: The sprint backlog is a set of tasks or user story where the development team divides up the sprint to have a better development [23]. Sprint backlogs are deliverables that maintain a delivery date, allowing for orderly work.

6) *Daily Meeting*: The working team will have to meet to see each other to clarify the work they have done [24]. This meeting should not last more than 15 minutes, in the meeting they can discuss what is going to be done, what the next meeting will be about, among other things.

7) *Sprint Review*: There will be a review of the overall sprint performance taking into account that each sprint will take 4 hours to review [25].

8) *Sprint Retrospective*: This process will be identified once all sprints have been completed and reviewed [26], allowing new ideas to be added to the completed sprints so that they do not generate any problems for the product .

9) *Prototype*: Finishing with the previous process which is the Sprint retrospective, here we will show the final prototype once all the necessary data has been obtained [27].

10) *Testing*: In this process it will be possible to carry out the necessary tests to see how the product works, with the aim of being able to improve if there are any faults. [28].

D. Development of the Hybrid Methodology

This part explains the development of the stages of the hybrid methodology.

1) *Empathise*: At this stage, potential customers are surveyed and asked whether they are comfortable with face-to-face sales using the Google form tool.

Table I shows the questions (Q1 to Q5) that will be answered by potential customers, in which they are asked about comfort and attention in sales in 2021.

TABLE I. SALES IN 2021 IN PERU-LIMA

Questions	
ID	Questions
Q1	Do you have long queues when shopping?
Q2	How many purchases do you make during the month?
Q3	From which district of Lima are you located?
Q4	How long does it take to receive your products?
Q5	How long does it take you to pay for your purchases?

2) *Define*: According to the questions in the first stage survey, Table II identifies the problems of their sales from Q1 to Q5 and shows the responses of the customers who took the survey.

TABLE II. CUSTOMER RESPONSE TO THE SURVEY

Answers	
ID	Answers
Q1	75.7% of customers indicate that they queue for a long time.
Q2	48.6% of customers indicate that they make 40 or more purchases.
Q3	In the Olivos district indicates that there are more customers.
Q4	72.9% of customers indicate that there is a delay in receiving their products.
Q5	74.3% of customers say their payment procedure is slow

All these data were elaborated in August and September 2021. The answers were given according to the questionnaire sent to the customers of the Dominguez company, where 75.7% of the customers make their purchases. But, they have to wait in long queues, where the majority place their orders from 40 to more, the district where they place the largest number of orders is Los Olivos, with 72.9% of customers saying that their orders take a long time to reach their respective destinations and 74.3% take a long time to pay for their order.

3) *Ideate*: According to the problems identified in the define stage, the development team (T1, T2 and T3) proposes to devise an innovative solution, for which it needs to describe the possible solutions and then estimate the best solution by points from 1 to 20, as shown in Table III.

a) *S1*: The development team identified a solution which is to realise an e-business system to optimise sales where 59 points were estimated.

b) *S2*: In the second solution, new advertising strategies are proposed to attract new customers, with an estimated 43 points.

c) *S3*: In the third solution, a new payment system was devised to reduce traffic, with an estimated 49 points.

HYBRID METHODOLOGY: DESIGN SCRUM

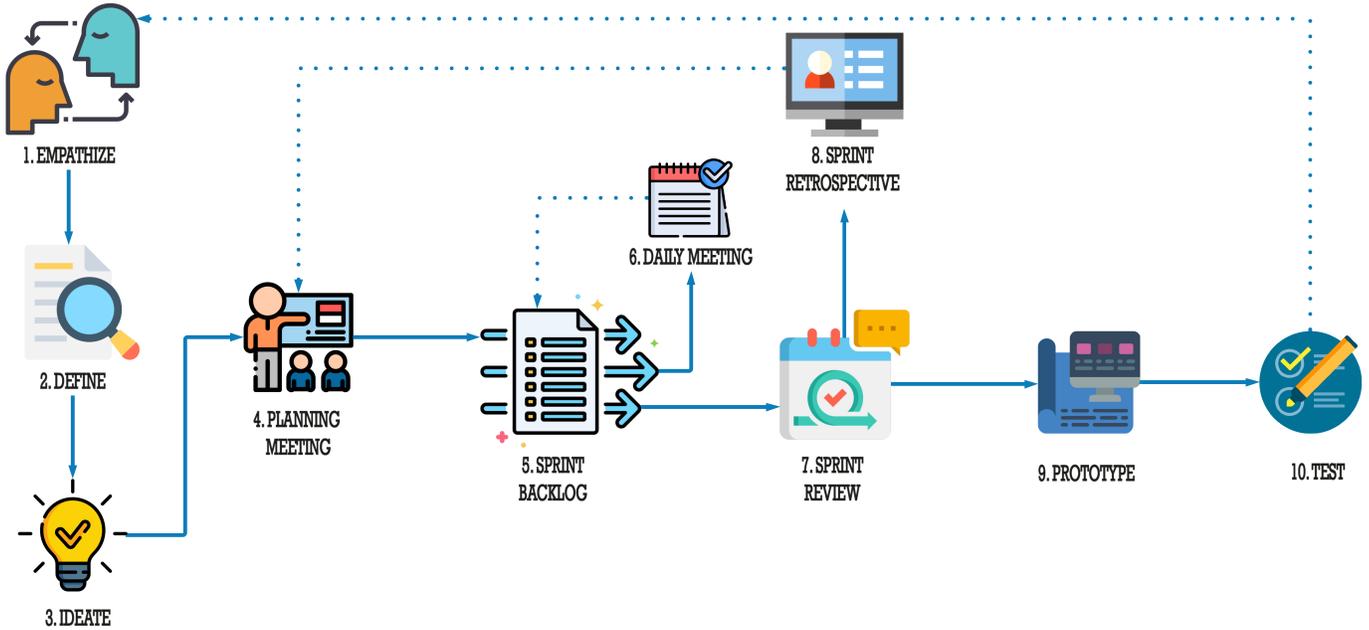


Fig. 3. Methodology DesingScrum.

d) S4: In the fourth solution, a product delivery system was devised for rapid dispatch where 39 points were estimated.

e) S5: In the fifth solution, the idea was to implement a local system for sales where 48 points were estimated.

TABLE III. SCORING IDEAS

Punctuation of the Ideas				
Solutions	T1	T2	T3	Total
S1- Realise an e-business system to optimise sales.	19	19	18	56
S2- Create new advertising strategies to generate more customers.	15	15	13	43
S3- Implement a new payment system to reduce traffic.	15	16	18	49
S4- Implement a product delivery system for rapid dispatch.	15	13	11	39
S5- Make a local system for making sales.	16	16	16	48

4) *Planning Meeting*: This process will involve the team in identifying all user stories (H1 to H12) for product development, as shown in Table IV.

5) *Sprint Backlog*: In this process, the sprint backlog is explained, where the 12 user stories with 4 sprints are obtained, then the planing poker was carried out, where the cards were identified to measure the difficulty of each user story, and the estimated time of each sprint was identified [29].

The very small tasks are the fastest difficulties to develop, while the small tasks fall into the difficulty of very easy and intermediate level, the medium tasks would be of intermediate

TABLE IV. REQUIREMENTS

USER STORIES	
ID	DESCRIPTION
1- H1	The user will have to register a new account (email, password) to log in to the application.
2- H2	The user will need an email address and password to log in to the application.
3- H3	The user will have a profile to fill in the corresponding data (name, surname, type of document, document, date of birth, name, email, telephone, address, credit card).
4- H4	The user will have his or her password retriever if he or she forgets it.
5- H5	The user will have an option of my purchases where he/she will be able to have the purchases to observe the purchases that he/she is going to make.
6- H6	The user will have a catalogue to view the products they wish to buy.
7- H7	The user will be able to select a product and will be able to order the required quantity.
8- H8	The user will be able to create a suggested list where he/she can put the products he/she wants to buy in the future.
9- H9	The user will have a search engine to find the product found on the site.
10- H10	The user will have his shopping cart where he will be able to buy his products.
11- H11	The user will have a help option, should he/she have any doubts or queries.
12- H12	The user will be able to log out if they no longer wish to shop on the site.

difficulty, as well as the large tasks that are the part where it would take more to have a concrete approach at the time of development; the large tasks would be a more structured process for its development, the invaluable task would be when

TABLE V. SPRINT BACKLOG

SPRINT BACKLOG			
ID	Time	Difficulty Level	Sprint
H1	4 days	1/2 Very small task	Sprint 1
H2	5 days	1 Small task	
H3	5 days	2 Small task	
H4	6 days	3 Small task	
H5	15 days	100 Time for a break, bigger tasks	Sprint 2
H6	7 days	5 Medium-sized tasks	
H7	8 days	8 Medium-sized tasks	
H8	8 days	13 Medium-sized tasks	Sprint 3
H9	8 days	13 Medium-sized tasks	
H10	12 days	40 Time for a break, big tasks	
H11	8 days	8 Medium-sized tasks	Sprint 4
H12	7 days	5 Medium-sized tasks	

there is no specific date for its development, the huge task would be the most difficult difficulty as it requires a complete analysis for the development of the product. The sprint backlog is shown in Table V.

TABLE VI. SPRINT PLANNING

Sprint Planning	
SPRINT	DIAS
Sprint 1	20 days
Sprint 2	30 days
Sprint 3	28 days
Sprint 4	15 days
TOTAL	93 days

In Table VI it indicates the Sprint Planning where it indicates the total time of each sprint, as well as that the product will be finished in 3 months and 3 days.

In Fig. 4 you can see the cards that will be implemented to perform the planning poker this will help to facilitate the level of difficulty. They would be very small task. Small task, medium task, big task. Bigger task, invaluable task, huge task and time for a break.



Fig. 4. Planning Poker.

It will show the 4 Sprint with their user stories that will be developed for the prototype operation.

a) *Sprint 1 (H1)*: As shown in Fig. 5 it will be developed so that the user can register using the email and password, this will take an estimated time of 4 days to implement having a small task difficulty.

b) *Sprint 1 (H2)*: As shown in Fig. 5 it will be developed so that the user can log in to the application using the email and password that have been registered; this user story will have an estimated time of 5 days with a small task difficulty.

c) *Sprint 1 (H3)*: As can be seen in Fig. 5, it will be developed so that the user can edit a profile, this will be used to put the corresponding data. This user story will take 5 days counting on the small task difficulty.

d) *Sprint 1 (H4)*: As shown in Fig. 5, the password can be retrieved if the correct password is forgotten or not remembered, with an estimated time of 6 days with a low task difficulty.



Fig. 5. Sprint 1.

e) *Sprint 2 (H5)*: As shown in Fig. 6 you will have the option of catalogue where you will be able to see all the products with their corresponding categories, this user story will have an estimated time of 15 days. It will have 2 difficulties, the first difficulty will take a short break to see how far it has progressed and if everything is working properly, then continue with the difficulty of larger tasks for their respective development.

f) *Sprint 2 (H6)*: As shown in Fig. 6, the user will have the option to see all the products they selected from the catalogue in their shopping cart, for this user story it is estimated a time of 7 days for its development with the difficulty of medium task.

g) *Sprint 2 (H7)*: As shown in Fig. 6, the user will be able to select his product to order the necessary quantity he wants, either per unit or per box, and will have an estimated time of 8 days for its development, which will have the difficulty of a medium-sized task.

h) *Sprint 3 (H8)*: As shown in Fig. 7, the user will have a shopping list in the future, this will allow the user to save the product in his list until he decides to buy it, this user story will have an estimated time of 8 days for its development, taking into account the medium difficulty of the task.

i) *Sprint 3 (H9)*: As shown in Fig. 7, the user will have a search engine to find the product by name or category, with an estimated time of 8 days for its respective development, with a medium task difficulty.

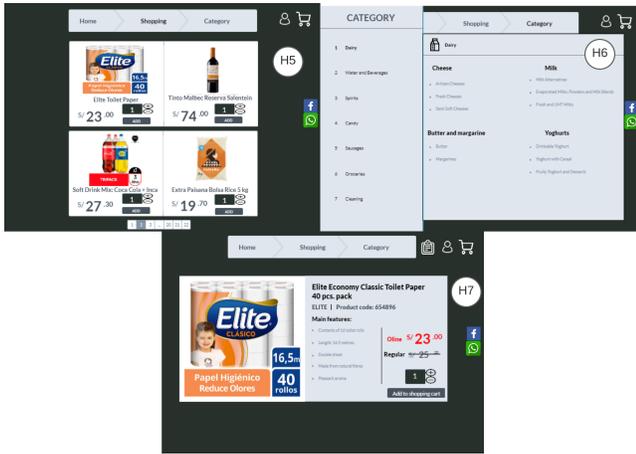


Fig. 6. Sprint 2.

j) *Sprint 3 (H10)*: As can be seen in Fig. 7, the user will be able to make a purchase using the shopping cart once he has made or has chosen the selected product together with the corresponding quantity, he will have an estimated time of 12 days for its development. The first is to have a short break to see how far the user has progressed and if everything is working correctly, in order to be able to move on to the next difficulty, which would be the big task of user story 10.



Fig. 7. Sprint 3.

k) *Sprint 4 (H11)*: As shown in Fig. 8, the user will have the option of a wizard, where he/she can ask for help if he/she has any problem when purchasing or any difficulty in the system, this user story will have an estimated time of 8 days for its development. It will have the difficulty of medium task.

l) *Sprint 4 (H12)*: As can be seen in Fig. 8, the user will be able to log out once the purchase has been made, and will have an estimated time of 7 days for its development. Counting on the medium task difficulty.

6) *Daily meeting*: In this process, a daily meeting will be held, allowing the team to meet every 20, 30, 28 and 15 days together with the scrum master, in order to improve teamwork. Allowing us to ask the following questions What did they do?

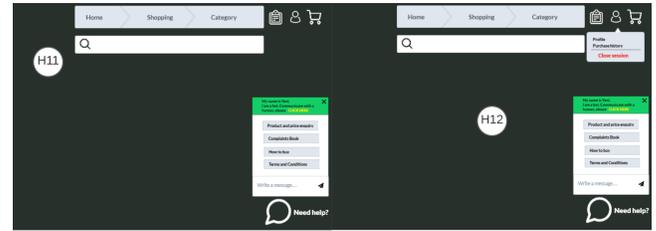


Fig. 8. Sprint 4.

What impediments did they face? Who worked on the project?

IV. RESULTS AND DISCUSSIONS

In this chapter we will continue to show the next remaining stages, showing as a result the reviews of each Sprint, retrospective reviews, final prototype, the implementation of the questions towards the prototype, counting the respective answers and finally proposing the use of digital marketing.

A. Sprint Review

At the end of each Sprint, a review is carried out by the work team, this will take 3 to 4 hours of evaluation. The product owner is in charge of explaining so that it is accepted. After showing the users or attendees a comment is made to determine any changes or improvements to the product. At the end of the evaluation continues with the next Sprint, also, at the end of all the Sprint will move to the next stage [30].

a) *Sprint 1*: In Fig. 9 it indicates the revision of sprint 1, being presented by the Product Owner in which he indicates the start of the procedure on the estimated date of 16 August 2021, ending on 05 September 2021. It is also considered an accepted sprint.

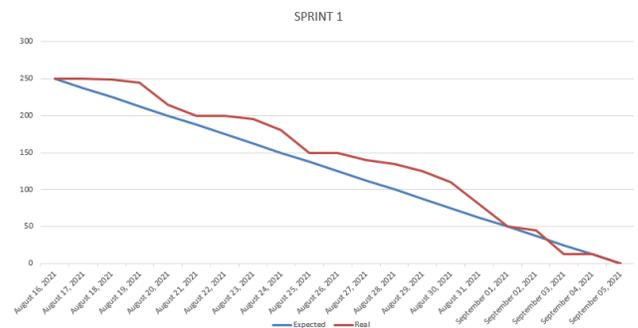


Fig. 9. Burndown Chart from Sprint 1.

b) *Sprint 2*: In Fig. 10 it indicates the revision of Sprint 2, being presented by the Product Owner in which he indicates the start of the procedure on the estimated date of 06 September 2021, ending on 06 October 2021. It is also considered an accepted sprint.

c) *Sprint 3*: In Fig. 11 it indicates the revision of sprint 3, being presented by the Product Owner in which he indicates the start of the procedure on the estimated date of 07 October 2021, ending on 04 November 2021. It is also considered an accepted sprint.

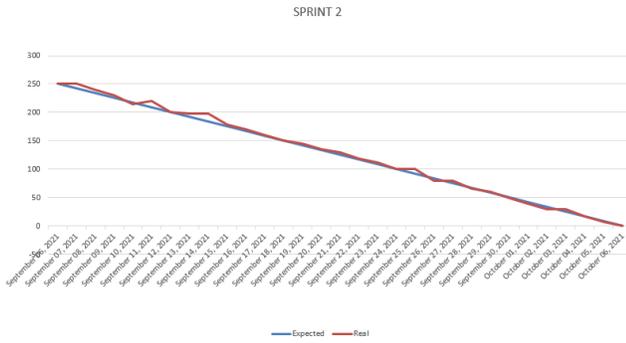


Fig. 10. Burndown Chart from Sprint 2.

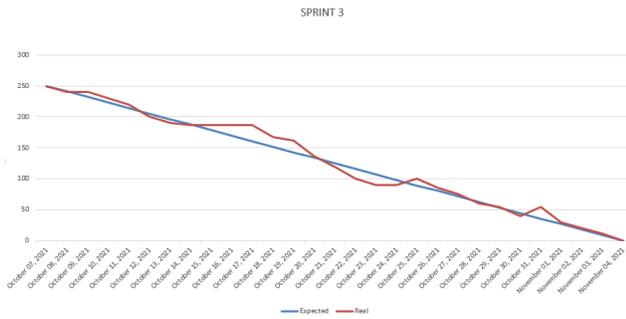


Fig. 11. Burndown Chart from Sprint 3.

d) *Sprint 4:* In Fig. 12 it indicates the revision of Sprint 4, being presented by the Product Owner in which he indicates the start of the procedure on the estimated date of 05 November 2021, ending on 20 November 2021. It is also considered an accepted sprint.

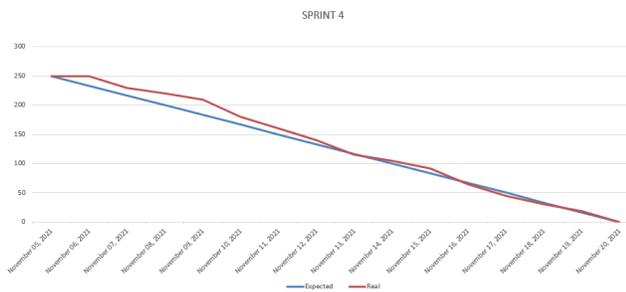


Fig. 12. Burndown Chart from Sprint 4.

B. Retrospective Review

In this stage, an evaluation of the process is carried out by the scrum master as shown in Table VII, convening a meeting with the Product Owner and the Work Team. This will be used to optimise the next product, for which the scrum master will ask: What did we do well, what can we improve and what should we stop doing?

a) *R1:* Meet the deadlines set for each sprint.

b) *R2:* Reduce sprint time to obtain a quick solution for the user.

TABLE VII. RETROSPECTIVE REVIEW

RETROSPECTIVE REVIEW		
Scrum master	Questions	Answers
Scrum master 1	1. What did we do right? 2. What can we improve? 3. What should we stop doing?	R1 R2 R3

c) *R3:* Identify user stories with a single person.

C. Prototype

At this stage, a prototype was made and elaborated by MarvelApp application, this will be the mock-up for potential customers to give their opinion about it, as shown in Fig. 13.

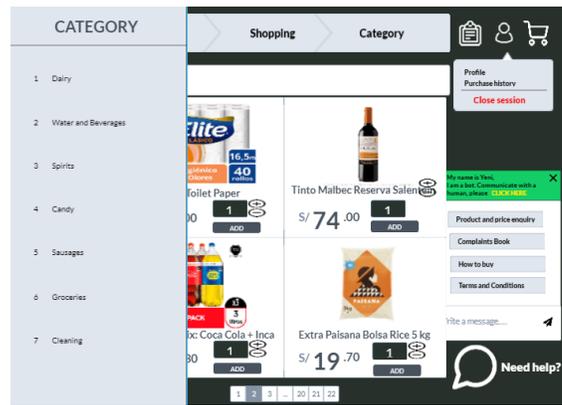


Fig. 13. Final Prototype.

D. Testing

In this final stage the questions and answers of the prototype will be shown to the customers.

1) *Testing questions:* A survey of 5 questions about the prototype (QP1 to QP5) was conducted, the customers will give their opinion about it, as shown in Table VIII.

TABLE VIII. PROTOTYPE SYSTEM SURVEY

ID	Questions
Q1	How did you like the prototype system?
Q2	How did you like the product listing of the beta version of the system?
Q3	Did you find the product catalogue section interesting?
Q4	Did you find the system fast?
Q5	Do you find the interface easy to use?

2) *Responses from Testing:* As shown in Fig. 14 the answers made from the Q1 testing responded that the system prototype seems good to 73% and those who think it is bad is 28%, in Q2 responded that the system version listing is good 71% and bad 29.4%, in Q3 58.8% think that the product catalogue is good, maybe 33.3% and bad 7.8% in Q4 they answered how they thought the operation of the system where they thought it was good 78.4% and bad 24.6%, in the last Q5 they answered how they thought the management of the prototype where they thought it was good 60.8%, maybe 31.4% and bad 7.8% all this was done according to the response of all customers who took the survey.

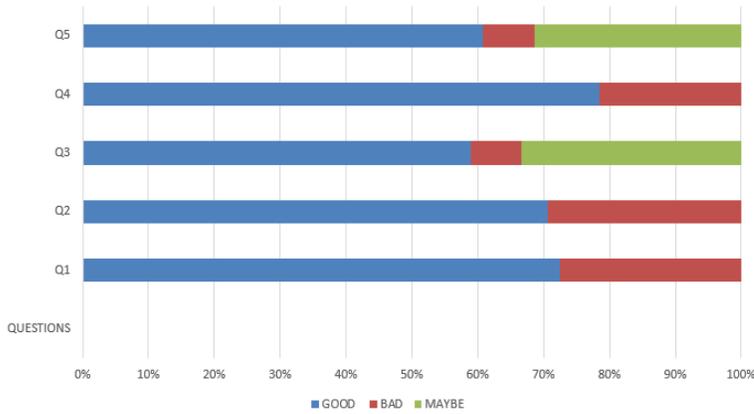


Fig. 14. Testing Response.

E. Proposal for Digital Marketing

In this digital marketing proposal it indicates the fundamental tools to attract new users in a short time, being effective for the brand recognition of companies.

1) *Search Engine Optimization (SEO)*: The SEO has a fast search engine, allowing to identify our website that is on any server, helping to generate more visits, having a greater reach so that people can view any business they have online. Thus becoming an attractive information system at the academic level, as well as at the professional level [31]. Counting with different techniques for its use: page optimization, facilitates the search through tags and keywords; creation of links through the references of links, these are generated through backlinks; content creation, this technique is important because through SEO, allows us to create high quality content, gain links this technique applies to new and interactive content already created that is used through links on websites .

2) *Search Engine Marketing (SEM)*: It works by searching for keywords to have a better visibility on websites, one of the problems of SEM for its use has to have a staff in charge with experience so that its management is correct. Several companies use SEM for their advertising budget and for other areas of the companies, thus being used in electronic marketplaces to improve search and to attract more sponsors [32]. Bearing in mind that in order to handle SEM, it is not necessary to be a large company as nowadays small companies are also starting to use Search Engine Marketing for their own benefit.

3) *Facebook ADS*: It is a system that allows you to promote a Facebook page, website or application, to publish the promotion of the ad must be paid, these ads offers tools for creating campaigns as well as using graphics formats, videos and images. This system is effective to gain new users on Facebook for any type of business [33].

4) *Email Marketing*: Email marketing is used for customer to customer dialogue, leveraging the potential for cross-selling and up-selling. It is now widely used in the workplace as it can help us to get more customers in more effective ways; these can be used in e-commerce for their operation [34].

5) *Google Analytics*: It allows us to measure time, budget and collect data from our website users through web analytics

[35], this will help us to analyse user behaviours and obtain useful marketing intelligence .

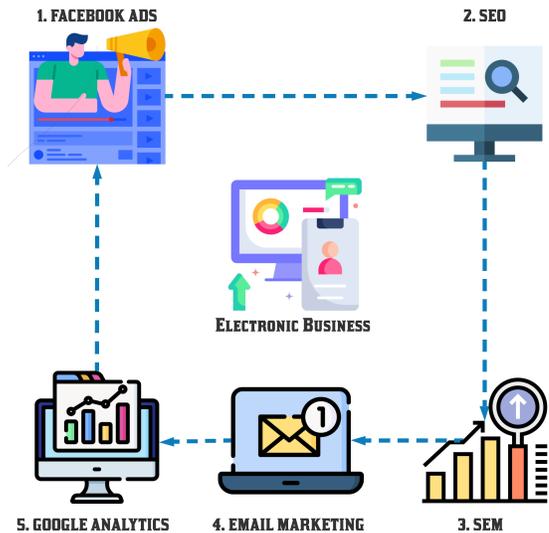


Fig. 15. Digital Marketing Proposal Template.

In Fig. 15, shows the digital marketing model, once the e-business is posted on the web, it will start with the first stage which is Facebook ADS that will be responsible for advertising for brand recognition or e-business of the company at the Peruvian level. In the second stage will be the SEO as it will help us to position ourselves on the Web, through organic searches, ie, are free and appear within the first 3 in the search of google.the third stage will be the SEM; will serve to obtain greater visibility through various advertising campaigns to itself position the e-business in the first place, SEO will help to position itself in the long term and the SEM in the short term. Once the records of new users in the e-business are obtained in the database, their emails will be requested in order to follow up on the fourth stage, which is Email Marketing, to inform the services of the business. The last stage will use Google Analytics to analyse the performance of the system or social networks.

V. CONCLUSIONS AND FUTURE WORK

The e-business was developed in the Peruvian company Domínguez proposing the use of digital marketing to obtain a larger clientele, as well as having different tools to generate appropriate advertising and measure the performance of the web platform. The methodology is the most essential part of the work helping us to innovate and manage the development of the e-business. It would be of great help to use these methods for Peruvian businesses in times of pandemic or in any health situation as it is an effective strategy to generate a great impact in any department or district of Peru, as well as to position MSEs or SMEs in the market. For future research, the development of the proposed model of digital marketing is proposed, taking into account that augmented reality can also be implemented to improve the visualisation of the state of the products in real time, as well as to have greater confidence in the customers. It is also suggested that you can implement Web Scrapping to know the weaknesses of our system and not

suffer data loss or theft of information in the long term, as also serves to obtain price information from the database of the competition.

ACKNOWLEDGMENT

This work was sponsored by the University of Sciences and Humanities and the research direction. To acknowledge Dr. Carlos Sotomayor Beltrán for the suggestions in the article.

REFERENCES

- [1] S. Hussain, A. Sohail, C. Yu, S. Manzoor, and A. Zahid, "China-pakistan economic corridor (cpec's) socio-economic impacts on pakistan," *International Journal of Management & Entrepreneurship Research*, vol. 2, no. 6, pp. 416–436, 2020.
- [2] M. Shafi, J. Liu, and W. Ren, "Impact of covid-19 pandemic on micro, small, and medium-sized enterprises operating in pakistan," *Research in Globalization*, vol. 2, p. 100018, 2020.
- [3] T. Erdem, "Competitiveness of dried sector: A case study of world and turkey," *Agricultural Economics*, vol. 66, no. 8, pp. 365–372, 2020.
- [4] B. González-Bustamante, "Evolution and early government responses to covid-19 in south america," *World Development*, vol. 137, p. 105180, 2021.
- [5] M. M. Cequea, J. M. Vásquez Neyra, V. G. H. Schmitt, and M. Ferasso, "Household food consumption and wastage during the covid-19 pandemic outbreak: A comparison between peru and brazil," *Sustainability*, vol. 13, no. 14, p. 7583, 2021.
- [6] T. Q. Thinh, D. A. Tuan, N. T. Huy, and T. N. A. Thu, "Financial distress prediction of listed companies—empirical evidence on the vietnamese stock market," *Innovations*, vol. 17, no. 2, pp. 377–388, 2021.
- [7] S. P. Goldman, H. van Herk, T. Verhagen, and J. W. Weltevreden, "Strategic orientations and digital marketing tactics in cross-border e-commerce: Comparing developed and emerging markets," *International Small Business Journal*, vol. 39, no. 4, pp. 350–371, 2021.
- [8] J. M. Málaga Arana, "Estudio para la implementación del marketing digital y el comercio electrónico en la empresa t & c technologycel, surquillo, 2019," 2019.
- [9] S. M. Maarac, Z. Filipović, and M. Eljuga, "E-commerce in trade companies during the conditions of a pandemic crisis: Case studies," *EU and comparative law issues and challenges series (ECLIC)*, vol. 5, pp. 728–745, 2021.
- [10] M. Vagner, "Digitalni marketing," Ph.D. dissertation, University of Zagreb. Faculty of Teacher Education, 2017.
- [11] P. R. Marin Pumarrumi, "Dimensiones del marketing digital para incrementar las ventas de una mype del sector de servicios de seguridad integral," 2019.
- [12] L. Ljubisavljević, D. Milačić, and M. Ninković, "Development of a web shop based on augmented reality," in *E-business technologies conference proceedings*, vol. 1, no. 1, 2021, pp. 40–43.
- [13] S. Dinesh and Y. MuniRaju, "Scalability of e-commerce in the covid-19 era," *International Journal of Research-GRANTHAALAYAH*, vol. 9, no. 1, pp. 123–128, 2021.
- [14] R. Kamran and A. Dal Cin, "Designing a mission statement mobile app for palliative care: an innovation project utilizing design-thinking methodology," *BMC Palliative Care*, vol. 19, no. 1, pp. 1–6, 2020.
- [15] J. Vogelzang, W. F. Admiraal, and J. H. van Driel, "Scrum methodology as an effective scaffold to promote students' learning and motivation in context-based secondary chemistry education," *EURASIA Journal of Mathematics, Science and Technology Education*, vol. 15, no. 12, p. em1783, 2019.
- [16] V. Gomero-Fanny, A. R. Bengy, and L. Andrade-Arenas, "Prototype of web system for organizations dedicated to e-commerce under the scrum methodology," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 1, 2021. [Online]. Available: <http://dx.doi.org/10.14569/IJACSA.2021.0120152>
- [17] A. Tupia-Astoray and L. Andrade-Arenas, "Implementation of an e-commerce system for the automation and improvement of commercial management at a business level," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 1, 2021. [Online]. Available: <http://dx.doi.org/10.14569/IJACSA.2021.0120177>
- [18] J. Vogelzang, W. F. Admiraal, and J. H. Van Driel, "A teacher perspective on scrum methodology in secondary chemistry education," *Chemistry Education Research and Practice*, vol. 21, no. 1, pp. 237–249, 2020.
- [19] J. Vrana and R. Singh, "Nde 4.0—a design thinking perspective," *Journal of nondestructive evaluation*, vol. 40, no. 1, pp. 1–24, 2021.
- [20] M.-J. Tsai and C.-Y. Wang, "Assessing young students' design thinking disposition and its relationship with computer programming self-efficacy," *Journal of Educational Computing Research*, vol. 59, no. 3, pp. 410–428, 2021.
- [21] Y. Zavoleas, "Patterns of nature: Bio-systemic design thinking in meeting sustainability challenges of an increasingly complex world," *Developments in the Built Environment*, vol. 7, p. 100048, 2021.
- [22] J. Vogelzang, W. F. Admiraal, and J. H. van Driel, "Scrum methodology in context-based secondary chemistry classes: effects on students' achievement and on students' perceptions of affective and metacognitive dimensions of their learning," *Instructional Science*, pp. 1–28, 2021.
- [23] M. Morandini, T. A. Coleti, E. Oliveira Jr, and P. L. P. Corrêa, "Considerations about the efficiency and sufficiency of the utilization of the scrum methodology: A survey for analyzing results for development teams," *Computer Science Review*, vol. 39, p. 100314, 2021.
- [24] A. muayad younus Alzahawi and M. Abumandil, "Evaluating the role of scrum methodology for risk management in information technology enterprises," *Journal of Information Technology and Computing*, vol. 2, no. 1, pp. 1–8, 2021.
- [25] T. Z. Khan, S. H. Tusher, M. Hasan, and M. Rokonzaman, "Tailoring scrum methodology for game development," in *Advances in Computer, Communication and Computational Sciences*. Springer, 2021, pp. 233–243.
- [26] V. Casola, "Scrum for safety: Agile development in safety-critical software systems," in *Quality of Information and Communications Technology: 14th International Conference, QUATIC 2021, Algarve, Portugal, September 8–11, 2021, Proceedings*, vol. 1439. Springer Nature, 2021, p. 127.

- [27] M. K. Foster, "Design thinking: A creative approach to problem solving," *Management Teaching Review*, vol. 6, no. 2, pp. 123–140, 2021.
- [28] D. V. Albay, Eduard M y Eisma, "Evaluación de la tarea de desempeño respaldada por el proceso de pensamiento de diseño: resultados de una verdadera investigación experimental," *Social Sciences and Humanities Open*.
- [29] A. Carrion-Silva, C. Diaz-Nunez, and L. Andrade-Arenas, "Admission exam web application prototype for blind people at the university of sciences and humanities," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 12, 2020. [Online]. Available: <http://dx.doi.org/10.14569/IJACSA.2020.0111246>
- [30] A. Delgado and P. Condori, "Comparative study of methods to improve administrative processes in a organization," in *2018 Congreso Internacional de Innovación y Tendencias en Ingeniería (CONIITI)*, 2018, pp. 1–5.
- [31] R. Lui and C. H. Au, "Is educational game: Adoption in teaching search engine optimization (seo)," *Journal of Computer Information Systems*, 2018.
- [32] R. Aswani, A. K. Kar, P. V. Ilavarasan, and Y. K. Dwivedi, "Search engine marketing is not all gold: Insights from twitter and seoclerks," *International Journal of Information Management*, vol. 38, no. 1, pp. 107–116, 2018.
- [33] A. L. Ortega, "Are microtargeted campaign messages more negative and diverse? an analysis of facebook ads in european election campaigns," *European Political Science*, pp. 1–24, 2021.
- [34] V.-D. Păvăloaia, I.-D. Anastasiei, and D. Fotache, "Social media and e-mail marketing campaigns: Symmetry versus convergence," *Symmetry*, vol. 12, no. 12, p. 1940, 2020.
- [35] S.-C. Chen, T. C.-Y. Tsao, K.-H. Lue, and Y. Tsai, "Google analytics of a pilot study to characterize the visitor website statistics and implicate for enrollment strategies in medical university," *BMC medical education*, vol. 20, no. 1, pp. 1–12, 2020.

A Fast and Efficient Algorithm for Outlier Detection Over Data Streams

Mosab Hassaan¹
Faculty of Science
Benha University
Egypt

Hend Maher², Karam Gouda³
Faculty of Computers and Artificial Intelligence
Benha University
Egypt

Abstract—Outlier detection over data streams is an important task in data mining. It has various applications such as fraud detection, public health, and computer network security. Many approaches have been proposed for outlier detection over data streams such as distance-, clustering-, density-, and learning-based approaches. In this paper, we are interested in the density-based outlier detection over data streams. Specifically, we propose an improvement of DILOF, a recent density-based algorithm. We observed that the main disadvantage of DILOF is that its summarization method has many drawbacks such as it takes a lot of time and the algorithm accuracy is significant degradation. Our new algorithm is called DILOF^C that utilizing an efficient summarization method. Our performance study shows that DILOF^C outperforms DILOF in terms of total response time and outlier detection accuracy.

Keywords—Data mining; outlier detection; data streams; density-based approach; clustering-based approach

I. INTRODUCTION

Outlier detection (OD) is considered an important data mining task. The objective of this task is to discover elements (points) that show significant diversion from the expected behaviour called outliers. For example, consider the two dimensional data points in Fig. 1. This dataset contains three normal regions namely N_1 , N_2 , and N_3 . We can observe that data points that are significantly far away from the three regions are outliers. In this example o_1 , o_2 , o_3 , and o_4 are outliers. The prominent causes for outliers are malicious activity, change in the environment, instrumentation error, and human error. OD plays a significant role and has been useful for several real-world applications such as intrusion detection systems, interesting sensor events, credit-card fraud, law enforcement, and medical diagnosis.

Outlier Detection raises significant challenges when a stream-based environment is considered [1], [2], [3]. A data stream potentially contains an infinite number of data points. Memory limitations constrain the amount of data points that can be held and processed at a given time. Moreover, no information related to data points appearing in the data stream are available before entering the memory. That is, the state of the current data point as an outlier/inlier must be established before dealing with subsequent data points. For example, in wireless sensor networks, a limited memory is available at each sensor node and outliers must be detected in reasonable time. The communication cost of these networks is also an essential factor. There are many approaches of outlier detection over data stream such as clustering based outlier detection

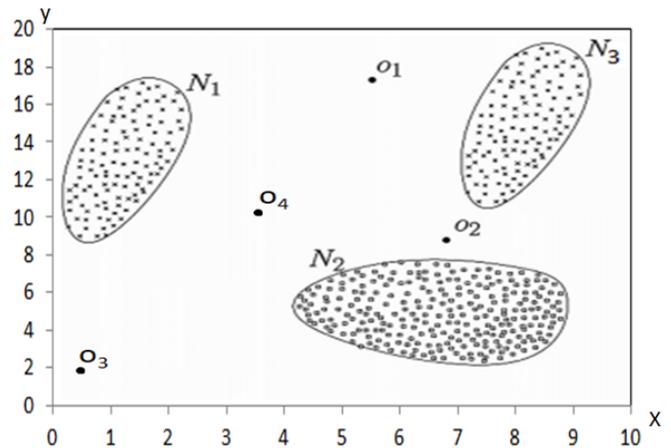


Fig. 1. Running Example (Outliers).

[4], statistical based outlier detection [5], [6], distance based outlier detection [7], [8], [9], [10][11], and density based outlier detection [12], [13], [14] [15], [16]. In this paper, we are interested in the density-based outlier detection over data streams. Specifically, we propose an improvement of DILOF, a recent density-based algorithm. Our new algorithm is called DILOF^C (Density Incremental LOF using summarization that based on novel m-Center clustering algorithm). We observed that the main problem in DILOF is that the summarization method has drawbacks such as it takes a lot of time and the algorithm accuracy is significant degradation. Note that DILOF is one of the most known algorithm that apply density based outlier detection approach. In density based outlier detection approach, the density of each point is compared with the density of its local neighbors. This approach is based on the assumption that the density of the normal data point is the same as the density of its neighbors and the density of outliers are dissimilar to their local neighbors. For each point, the density is computed by outlier score called LOF (Local Outlier Factor) [17]. We will discuss LOF and DILOF in Sections II-A and II-B respectively in details.

In the remaining sections, we discuss the problem definition and related work in Section II. Section III presents our proposed algorithm. We report the experimental results in Section IV. Finally, Section V concludes the paper.

II. PROBLEM DEFINITION AND RELATED WORK

Definition 2.1 A data stream is a possible infinite sequence of data points $P = \{p_1, p_2, p_3, \dots, p_n, \dots\}$, where data point p_n is arrived at time $p_n.t$

In previous definition, the data points are sorted by the timestamp at which it arrives. Since data stream size is unbounded thus data stream will be processed in a sliding window, i.e. a collection of active data points. Window is small enough to be held in the main memory. Windowing splits the data stream into overlapping finite sets of data points (sliding windows). The splitting can be done by arrival time of the data points, namely, time-based windows or by the count of the data points namely, count-based window. In this paper, we focus on the count-based window.

Problem Definition

Given a data stream $P = \{p_1, p_2, \dots, p_n, \dots\}$, the objective is to calculate the LOF score for each data point p_i and check p_i outlier or not with respect to the following constraints.

- We store only a small number of data points, $m \ll |P|$. Note that here m equals to the window size, $|W|$
- The outlier detection of coming data point p_i , must be done when p_i arrives.
- The data distribution is unknown.

A. LOF (Local Outlier Factor), iLOF, and MILOF

LOF [17] is well-known algorithm for outlier detection in static datasets. The objective of LOF is to calculate the LOF score for each data point. Suppose the following:

- We have all data points,
- The count of the nearest neighbors is k ,
- $dist(x, y)$ is the Euclidean distance between the two data points x and y ,
- $dist_k(x)$ is the Euclidean distance between a data point x and its k nearest neighbor.
- $N_k(x)$ is the set of the k -nearest neighbors of the data point x .

According to the following definitions, we will compute the LOF score for all data points.

Definition 2.2 Given two data points x and y , reachability distance $reach_dist_k(x, y)$ is defined by

$$reach_dist_k(x, y) = \max\{dist(x, y), dist_k(y)\} \quad (1)$$

Definition 2.3 Local reachability density of data point x , $lrd_k(x)$ is given by

$$lrd_k(x) = \left(\frac{1}{k} \sum_{y \in N_k(x)} reach_dist_k(x, y)\right)^{-1} \quad (2)$$

Definition 2.4 Local outlier factor of data point x , $LOF_k(x)$ is given by

$$LOF_k(x) = \frac{1}{k} \sum_{y \in N_k(x)} \frac{lrd_k(y)}{lrd_k(x)} \quad (3)$$

To check if data point x is outlier or not, we compare its local outlier factor $LOF_k(x)$ with a given threshold T . If $LOF_k(x) \geq T$ then the data point x is classified as outlier. Note that LOF algorithm is used to compute the LOF scores of all data points only once. Recall LOF algorithm detects outliers in static datasets

iLOF (incremental LOF) [18] was proposed for stream datasets but it stores all data points in memory. Thus iLOF requires a very large memory and is not applicable to stream datasets whose size sharply increasing. Another algorithm called MiLOF [19] was proposed to decrease the space complexity. It stores in memory a small number of data points by using k-means clustering [20] method to summarize old data points. The accuracy of MILOF is inefficient since it uses k-means for summarization which does not preserve the dataset density. To overcome the drawbacks of MILOF, authors of [13] proposed a new algorithm called DILOF (Density summarizing Incremental LOF). Since our proposed algorithm is based on DILOF, we will discuss DILOF algorithm in the next section in details.

B. DILOF Algorithm

DILOF [13] is well-known algorithm for outlier detection over data stream. It is density-based algorithm and applies two steps as follows. The first one is Last Outlier-aware Detection step, LOD which check if the incoming data point x is outlier or not. This done by computing $LOF_k(x)$ on the a variable window of data, W . Then the algorithm updates the information of the old data points (lrd_k and LOF_k) that exist in W and affected by inserting the data point x (i.e. the data points whose neighbor information will be modified when inserting the data point x). Note that the data point x is inserted to W no matter whether it is an outlier or inlier. Also skipping scheme strategy was proposed to detect a long sequence of outliers. In other words, this scheme was proposed to distinguish outliers from the data points in newly emerging classes. This can be done by deleting the new outliers from the window to preserve the low density region where outliers are existed. The following formally outlines skipping scheme strategy in details. First, DILOF computes $dist_1(p)$ for each data point $p \in M$ (Note that M is the set of data points in memory). Then it computes the average of distance $avg_dist_1 = \sum_{j=1}^{|M|} dist_1(p_j)$. Let $dist(o, p_c)$ be the Euclidean distance between the last detected outlier o and the current data point p_c . If $avg_dist_1 > dist(o, p_c)$ then set o to p_c and the data point p_c is not inserted to W . In this case, Skipping_Schema parameter will be set to true.

The second step is Nonparametric Density Summarization step, NDS which decrease the memory consumption by summarizing the old data points with respect to the dataset density. In NDS, an estimator called nonparametric Renyi divergence was used to specify the divergence between the original data points and summary candidate of data points. When the count of data points is equals to $|W|$ data points, NDS will summarize the oldest $|W/2|$ data points to $|W/4|$ representative data points such that the density difference between them is minimized. See Fig. 2.

Note that the previous two steps are repeated. LOD executes on every insertion of a data point. NDS is executed

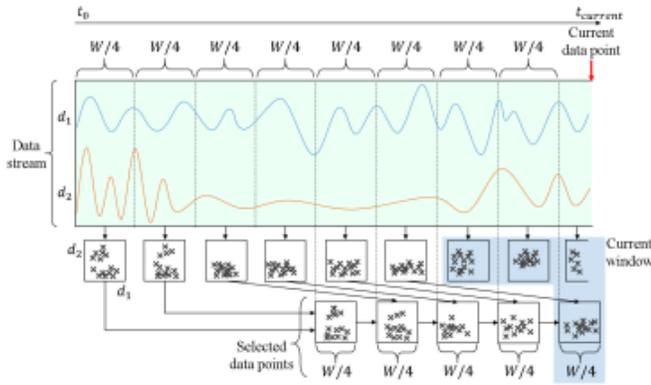


Fig. 2. NDS from Time t_0 to Time $t_{current}$ for a Two Dimensional Data.

when the number of data points in memory equals to $|W|$. In experimental results of DILOF on real-world datasets, DILOF significantly outperforms MiLOF with respect to accuracy and execution time.

III. PROPOSED ALGORITHM

Since the summarization method of DILOF algorithm taking many iterations to find its output. Therefore, the summarization method of DILOF algorithm takes a lot of time. Also, by using expensive experiments in many real datasets, we found that the algorithm accuracy is significant degradation. To overcome this issue, in this paper, we will propose a new summarization method called sum_m_center which will be injected in DILOF algorithm instead of its current inefficient summarization method. The proposed summarization method based on a new clustering technique called m_center . First, we propose m_center clustering algorithm then we will discuss the proposed summarization method. The previous clustering algorithms such as k -means require a large number of iterations to compute its output. To address this problem, we propose m_center clustering algorithm that is the partitioning representative, medoid, is sampled from the original data. In this method, we efficiently search for each cluster medoid as follows. In the first iteration we will search for the medoid of the first cluster and in the second iteration we will search for the medoid of the second cluster and so on. So if we set the number of clusters as k then we have only k iterations. In each iteration I we will execute the following steps. For each data point $p \in \mathcal{P}$ (the set of all data points), we calculate its m nearest neighbors set, $mNN(p)$. Then we compute the distance between p and each p_j belongs to $mNN(p)$ (here we will use Euclidean Distance, $dist(p, p_j)$) and compute the summation $sum_dist(p) = \sum_{j=1}^m dist(p, p_j)$. After that we select the point $p_i \in \mathcal{P}$ with minimum $sum_dist(p)$ as a medoid of the cluster being processing C_I then add all points in $mNN(p)$ to C_I . Finally we remove each point $p \in C_I$ from \mathcal{P} . Recall we have k iterations, then we repeat the previous steps $k - 1$ times after the initial iteration. Now we have k clusters. If there are remaining data points do not belong to any cluster (i.e. after k iterations we have $|\mathcal{P}| \neq \phi$), then we add each remaining data point p_r to its closest cluster based on the distance between the medoid of each cluster and p_r . Next

algorithm (Lines 1 - 13) outlines the m -center algorithm.

Algorithm: $m_center(\mathcal{P}, k, m, d_t)$

Input: \mathcal{P} : the set of data points,
 k : the number of clusters,
 m : the size of the m nearest neighbors set of a specified data point,
 d_t : distance threshold.
Output: \mathcal{C} : k -clusters set;

1. **for** $l = 1$ to k **do**
2. **for** each data point $p_i \in \mathcal{P}$ **do**
3. Compute the m nearest neighbors set of p_i , $mNN(p_i)$, such that $|mNN(p_i)| = m$.
4. Compute $sum_dist(p_i) = \sum_{j=1}^m dist(p_i, p_j)$, where $p_j \in mNN(p_i)$
5. **end for**
6. Select $p_x \in \mathcal{P}$ where $sum_dist(p_x)$ has the smallest value.
7. Add the point p_x and the set $mNN(p_x)$ to cluster C_l where p_x is the cluster medoid.
8. Remove the point p_x and the set $mNN(p_x)$ from \mathcal{P} .
9. **end for**
10. **for** each remaining data point $p_r \in \mathcal{P}$ **do**
11. Add p_r to its closest cluster.
12. **end for**
13. $\mathcal{C}_{temp} = \bigcup_{l=1}^k C_l$
14. Combine each nearest clusters set in \mathcal{C}_{temp} into one big cluster CB^h with respect to d_t //Optimization
15. $\mathcal{C} = \bigcup_h CB^h$
16. **return** \mathcal{C}

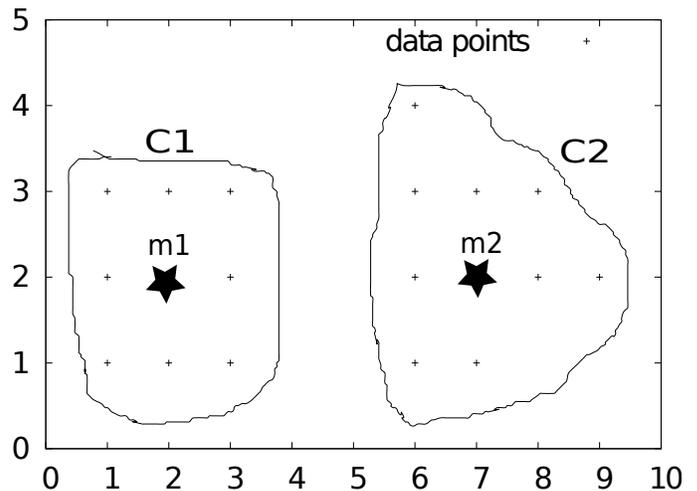


Fig. 3. Running Example (m -center Clustering Algorithm).

Example 3.1 Given two dimensional data point set $\mathcal{P} = \{p_1, p_2, p_3, \dots, p_{18}, p_{19}\} = \{(1, 1), (1, 2), (3, 2), (3, 1), (2, 2), (7, 2), (6, 4), (8, 2), (8, 3), (2, 1), (7, 1), (6, 3), (9, 2), (3, 3), (6, 1), (6, 2), (2, 3), (7, 3), (1, 3)\}$. Let $k = 2$ and $m = 4$. Since $k = 2$ then we have two iterations. In the first iteration we found that the point $p_3 = (2, 2)$ is the medoid of the first cluster, C_1 , since $mNN(p_3) = \{(1, 2), (2, 1), (2, 3), (3, 2)\}$ has minimum $sum_dist(p_3)$ that is $sum_dist(p_3) = 4$. Then

we remove p_3 and $mNN(p_3)$ from \mathcal{P} . In the second iteration we found that the point $p_6 = (7, 2)$ is the medoid of the second cluster, C_2 , since $mNN(p_6) = \{(6, 2), (7, 1), (7, 3), (8, 2)\}$ has minimum $sum_dist(p_6)$ that is $sum_dist(p_6) = 4$. Then we remove p_6 and $mNN(p_6)$ from \mathcal{P} . After the two iterations we check if there exist a remaining data points or not in \mathcal{P} . In this example there are a remaining data points. The count of remaining data points is nine since we remove five data points in each iteration. Therefore, we add each remaining data point to its closest cluster. Now we have two clusters as follows $C_1 = \{(1, 1), (1, 2), (3, 2), (3, 1), (2, 2), (2, 1), (3, 3), (2, 3), (1, 3)\}$ and $C_2 = \{(7, 2), (6, 4), (8, 2), (8, 3), (7, 1), (6, 3), (9, 2), (6, 1), (6, 2), (7, 3)\}$. See Fig. 3

A. Optimization

In the previous example we set $k = 2$. If we set $k = 3$ or 4 then we have three or four clusters respectively. But our original data has only two clusters. If we set k large than the number of original clusters in our data then m-center will cluster the data in inefficient way. Therefore, m-center will be optimized as follows. In the case above, some clusters should be merged efficiently. Which clusters will be merged?. The answer is the nearest clusters will be merged. First we define the nearest clusters as follows.

Definition 3.1 Given two clusters C_i and C_j with medoids m_i and m_j respectively and distance threshold d_t . C_i and C_j are called nearest clusters to each other if $dist(m_i, m_j) \leq d_t$.

Definition 3.2 Clusters set, S , are called nearest clusters set if every pair in S contains two nearest clusters.

Let $k = 5$ then we have five clusters C_1, C_2, C_3, C_4 , and C_5 . Assume after checking the nearest clusters we found two sets of nearest clusters as follows the first nearest clusters set is $NC^1 = \{C_1, C_2, C_3\}$ and the second one is $NC^2 = \{C_4, C_5\}$. We will merge the clusters in the same nearest cluster set into one big cluster. Therefore, we have two big clusters $CB^1 = C_1 \cup C_2 \cup C_3$ and $CB^2 = C_4 \cup C_5$. Lines 14-16 in the m-center algorithm outlines our optimization. Also next example illustrate this optimization.

Example 3.2 Given two dimensional data point set \mathcal{P} with size 32 data points as in Fig. 4. Let $k = 5, m = 4$ and $d_t = 5$. After applying m-center clustering method we have five clusters, namely C_1 with medoid $m_1 = (3, 4)$, C_2 with medoid $m_2 = (7, 5)$, C_3 with medoid $m_3 = (7, 2)$, C_4 with medoid $m_4 = (17, 7)$, and C_5 with medoid $m_5 = (16, 4)$. From above optimization we have two nearest clusters set based on the distance threshold $d_t = 5$. The first nearest clusters set is $NC^1 = \{C_1, C_2, C_3\}$ since every pair in NC^1 contains two nearest clusters, for example C_1 and C_2 are nearest clusters since $dist(m_1, m_2) = 4.12 < 5 = d_t$. The second nearest clusters set is $NC^2 = \{C_4, C_5\}$ since C_4 and C_5 are nearest clusters with $dist(m_4, m_5) = 3.16 < 5 = d_t$. Based on above optimization, we will merge clusters in each nearest clusters set into one big cluster as follows. $CB^1 = \bigcup_{C \in NC^1} C = \{C_1, C_2, C_3\}$ and $CB^2 = \bigcup_{C \in NC^2} C = \{C_4, C_5\}$. Fig. 4 illustrates our optimization.

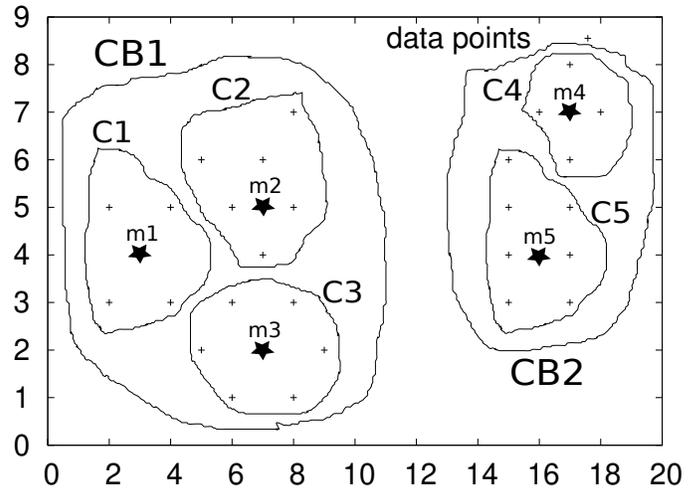


Fig. 4. Running Example (Optimization).

B. Summarization Step

In summarization step, we will delete a half of data points in the window. Which half of data points will be deleted? we will delete a half of data points according to two different deletion methods. In the first deletion method, we keep in each cluster C_I only the half of data points which close to C_I medoid and delete the other half. If we apply the optimization of merge clusters, the medoid of the big cluster CB will be the average of the medoids of the small clusters that contained by CB .

In the second deletion method, the unuseful old data points that do not effect the data density will be deleted that is we keep the half of data points in each cluster that preserve the cluster density and delete the other half. In other words, we delete a half of data points such that these data points are old and its LOF score is high. In experimental evaluation section, we will compare the two deletion methods. Next algorithm outlines the summarization step, `sum_m_center`.

Algorithm: `sum_m_center(\mathcal{P}, k, m, d_t)`

Input: \mathcal{P} : the set of data points,
 k : the number of clusters,
 m : the size of the m nearest neighbors set of a specified data point,
 d_t : distance threshold.
Output: \mathcal{S} : summary of k clusters;

1. $\mathcal{C} = \text{m-center}(\mathcal{P}, k, m, d_t)$
2. **if** `Enable_first_deletion_method`
3. **for each** cluster x in \mathcal{C}
4. Delete half of data points in x that are far from the medoid of x
5. $\mathcal{S} = \mathcal{C}$
6. **if** `Enable_second_deletion_method`
7. **for each** cluster x in \mathcal{C}
8. Delete half of data points in x that are old and its LOF score is high
9. $\mathcal{S} = \mathcal{C}$
10. **return** \mathcal{S}

C. DILOF^C Pseudocode

Recall, the adaptive algorithm is called DILOF^C. The next algorithm outlines DILOF^C. For each data point p_i coming from stream we do the following. If we enable the skipping scheme and the return value is true then we continue to the next data point (lines 3-5). See section II-B for more details about skipping scheme strategy. Otherwise, we add p_i to the set of data points in memory, M (line 6). Then we compute LOF score of p_i according to equations 1, 2, and 3 and add p_i to the set of outliers, \mathcal{O} , if LOF score of p_i is greater than LOF threshold, T (lines 7-10). At the same time, we update LOF score of each data point p_j in the reverse neighbour set of p_i and if the data point p_j transformed from outlier to inlier, we remove it from \mathcal{O} (lines 11-16). If the size of data points in memory, $|M|$ reach the window size $|W|$, we call the function, `sum_m_center`, to summarize the oldest $|W|/2$ data points in M . Then we replace the oldest $|W|/2$ data points in M by the outputted summary of `sum_m_center` function lines (17-22).

Algorithm: DILOF^C

Input: Infinite data stream $P = \{p_1, p_2, \dots, p_n, \dots\}$,
 T : LOF threshold,
 $|W|$: Window size,
 k : the number of clusters,
 m : the size of the m nearest neighbors set of a specified data point,
 d_t : distance threshold.
Output: The set of outliers in P , namely \mathcal{O} .

```

1.  $M = \phi$  //the set of data points in memory
2.  $\mathcal{O} = \phi$ 
3. while incoming data point  $p_i$  from stream do
4.   if Enable_Skipping_Schema_Strategy and
     Skipping_Schema = TRUE
5.     continue
6.    $M = M \cup \{p_i\}$ 
7.   Compute the LOF score of  $p_i$  according to equations
     1, 2, and 3
8.   if  $LOF(p_i) > T$  then
9.      $\mathcal{O} = \mathcal{O} \cup \{p_i\}$ 
10.  end if
11.  for each data point  $p_j$  in the set of reverse mNN( $p_i$ ) do
12.    Update the LOF score of  $p_j$ 
13.    if  $p_j$  transferred from outlier to inlier then
14.       $\mathcal{O} = \mathcal{O} - \{p_j\}$ 
15.    end if
16.  end for
17.  if  $|M| = |W|$  then
18.    Let  $M'$  be the oldest  $|W|/2$  data points in  $M$ 
19.     $S = \text{sum\_m\_center}(M', k, m, d_t)$ 
     //Summarization Step, where  $|S| = |M'|/2$ 
20.     $M = M - M'$ 
21.     $M = M \cup S$ 
22.  end if
23. end while

```

D. Time Complexity

Note that the summarization step is one of the main operations in the outlier detection algorithms over data streams. Therefore, in this section, we analyze the time complexity of m -center method for summarization step in the proposed algorithm, DILOF^C. The time complexity of m -center is $O(|W|km)$, where $|W|$ is the window size, k is the number of clusters, and m is the size of the nearest neighbors set of a specified data point. While the time complexity of summarization step in DILOF algorithm is $O((|W|/2)^2)$ [13] and the time complexity of summarization step in MILOF algorithm is $O(IDk|W|/2)$ [19], where I is the maximum count of iterations, D is the dimensionality of dataset, and k is the number of clusters.

The time complexity of our summarization step, m -center, is the best one due to $O(|W|km) \ll O((|W|/2)^2) \ll O(IDk|W|/2)$. For instance, if we handle the KDD Cup 99 http dataset where, for DILOF^C, k is 11 and m is 5 and for MILOF, I is 100 (default value for MILOF), D is 3, and k is 11 with $|W| = 700$ for all algorithms, then we have $|W|km = 38500 \ll 122500 = (|W|/2)^2 \ll 1155000 = IDk|W|/2$.

IV. EXPERIMENTAL EVALUATION

In this section, we evaluate the performance of DILOF^C on four real datasets. we compare the performance of DILOF^C with the DILOF [13]. Here, MiLOF [19] was excluded from this experiment since the experiment results of DILOF showed that DILOF has better performance than MILOF. All experiments were performed on a PC with Intel i5-6700 2.4 GHz, 8G memory running Windows 10 64-bit operating system. DILOF^C was implemented in standard C++ with STL library support. In next section, we discuss the datasets and experiment settings.

TABLE I. PROPERTIES OF THE FOUR REAL-WORLD DATASETS

Dataset	# Data Points	Dimension	# Classes
UCI Vowel	1,456	12	11
UCI Pendigit	3,498	16	10
KDD Cup 99 smtp	95,156	3	Unknown
KDD Cup 99 http	567,479	3	Unknown

A. Dataset and Experiment Settings

DILOF^C performance was evaluated by applying it to four real-world datasets. Table I listed the properties of the four datasets. For the two datasets, KDD Cup 99 smtp and KDD Cup 99 http, the number of classes is set to 10 since the number of classes of these datasets is unknown. The hyper-parameters of DILOF, η and λ are set to 0.3 and 0.001 respectively for all datasets. We set the default values of the parameter t that used in DILOF (t -nearest neighbors in DILOF) as the following. we set t to 19 for UCI Vowel and 8 for the three datasets UCI Pendigit, KDD Cup 99 smtp, and KDD Cup 99 http.

For our algorithm DILOF^C, the two parameters m (number of nearest neighbors) and k (number of cluster) are set to 5 and

11, respectively, for the three datasets UCI Pendigit, KDD Cup 99 smtp, and KDD Cup 99 http. For the dataset UCI Vowel, k and m are set to 10 and 11, respectively. For the parameter d_t (distance threshold for merging clusters) is set to 3.3 for the three datasets UCI Vowel, KDD Cup 99 smtp, and KDD Cup 99 http. For the dataset UCI Pendigit, d_t is set to 2.4.

Recall, DILOF^C and DILOF apply the summarization method when the count of data points equal to window size, $|W|$. Therefore, the performance of outlier detection is measured with different values of $|W|$. Since the two datasets, UCI Vowel and UCI Pendigit, contain a small number of data points, we selected a small window size for them $|W| = \{100, 120, 140, 160, 180, 200\}$. Since the two datasets, KDD Cup 99 smtp and KDD Cup 99 http, contain a large number of data points, we selected a large window size for them $|W| = \{100, 200, 300, 400, 500, 600, 700\}$. The LOF Thresholds were set to $\{0.1, 1.0, 1.1, 1.15, 1.2, 1.3, 1.4, 1.6, 2.0, 3.0\}$ as in DILOF. For each LOF Threshold, we compute false positive rate and true positive rate then AUC in ROC space was computed for DILOF^C and DILOF.

B. Effects of Optimization and Deletion Methods

In this experiment, we show the effect of optimization (merge clusters) and the two different deletion methods. For this purpose, we implemented four versions of DILOF^C, namely, DILOF^{C1} that does not use the optimization of merge clusters and use the first deletion method, DILOF^{C2} that does not use the optimization of merge clusters and use the second deletion method, DILOF^{C3} that uses the optimization of merge clusters and use the first deletion method, DILOF^{C4} that uses the optimization of merge clusters and use the second deletion method.

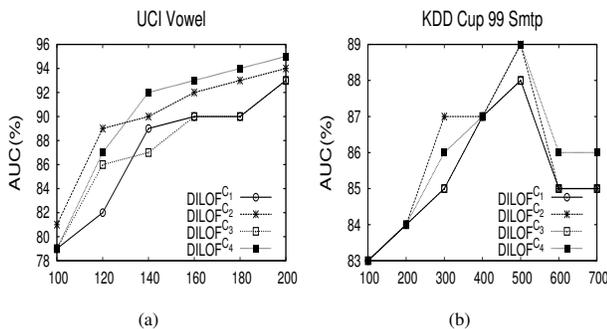


Fig. 5. Outlier Detection Accuracy with Respect to Window Size (Four Versions).

1) *Outlier Detection Accuracy*: Fig. 5 reports the outlier detection accuracy obtained by running the four versions on two datasets (UCI Vowel: Fig. 5(a) and KDD Cup 99 smtp: Fig. 5(b)). In UCI Vowel dataset, we can see that DILOF^{C4} always has high accuracy compared with the other versions except for window size 100 and 120, where DILOF^{C2} shows the best accuracy. In KDD Cup 99 smtp dataset, we can see that DILOF^{C4} always has high or same accuracy compared with the other versions except for window size 300, where DILOF^{C2} shows the best accuracy.

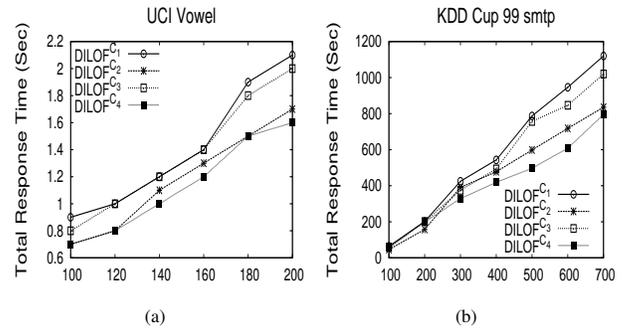


Fig. 6. Total Response Time with Respect to Window Size (Four Versions).

2) *Total Response Time*: Fig. 6 reports the total response time (sec) obtained by running the four versions on two datasets (UCI Vowel: Fig. 6(a) and KDD Cup 99 smtp: Fig. 6(b)). In UCI Vowel dataset, we can see that DILOF^{C4} always has less time compared with the other versions. In KDD Cup 99 smtp dataset, we can see that DILOF^{C4} always has less time compared with the other versions except for window size 100 and 120, where DILOF^{C2} shows the best execution time.

C. DILOF^C against DILOF

From section IV-B, we showed that DILOF^{C4} has the best performance among the other versions of the proposed algorithm with respect to outlier detection accuracy and total response time. Therefore, in this experiment, we will use DILOF^{C4} version and we will call it as DILOF^C for abbreviation. Here, we compare DILOF^C against DILOF on the four datasets, namely, UCI Vowel, UCI Pendigit, KDD Cup 99 smtp, and KDD Cup 99 http with respect to outlier detection accuracy and total response time. See next two sections.

1) *Outlier Detection Accuracy*: Fig. 7 shows the outlier detection accuracy of DILOF^C and DILOF with respect to the window size using the four datasets (UCI Vowel: Fig. 7(a), UCI Pendigit: Fig. 7(b), KDD Cup 99 smtp: Fig. 7(c), and KDD Cup 99 http: Fig. 7(d)). In UCI Vowel dataset, DILOF^C shows higher accuracy than DILOF at all window sizes. For example, at window size 200, the accuracy of DILOF^C is 95% whereas the accuracy of DILOF is 91%. In UCI Pendigit dataset, DILOF^C and DILOF have approximately the same accuracy. In KDD Cup 99 smtp dataset, DILOF^C shows higher accuracy than DILOF at most cases (for example, at window size 700, the accuracy of DILOF^C is 86% whereas the accuracy of DILOF is 73%) except for window size 600, where accuracy of DILOF^C is 86% whereas the accuracy of DILOF is 88%. In KDD Cup 99 http dataset, DILOF^C shows higher accuracy than DILOF at all window sizes (for example, at window size 700, the accuracy of DILOF^C is 83% whereas the accuracy of DILOF is 75%).

2) *Total Response Time*: Fig. 8 shows the total response time (sec) of DILOF^C and DILOF with respect to the window size using the four datasets (UCI Vowel: Fig. 8(a), UCI Pendigit: Fig. 8(b), KDD Cup 99 smtp: Fig. 8(c), and KDD Cup 99 http: Fig. 8(d)). DILOF^C shows the best execution time on all datasets. On UCI Vowel dataset, UCI Pendigit dataset, KDD Cup 99 smtp, and KDD Cup 99 http, DILOF^C outperforms

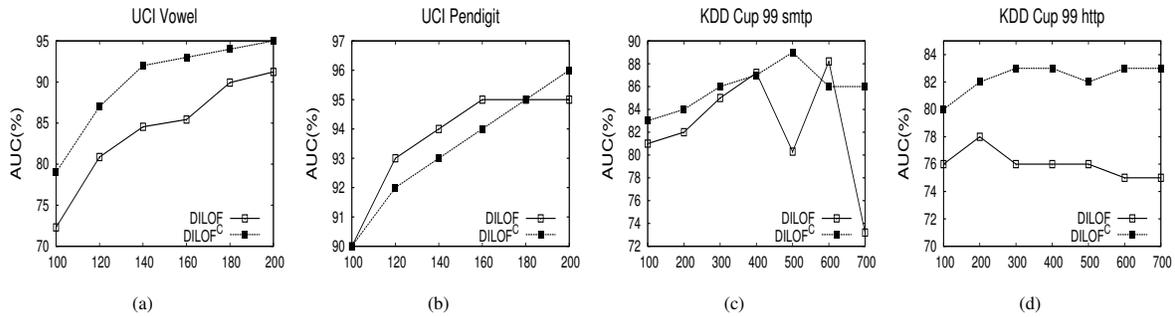


Fig. 7. Outlier Detection Accuracy with Respect to Window Size (DILOF vs. DILOF^C).

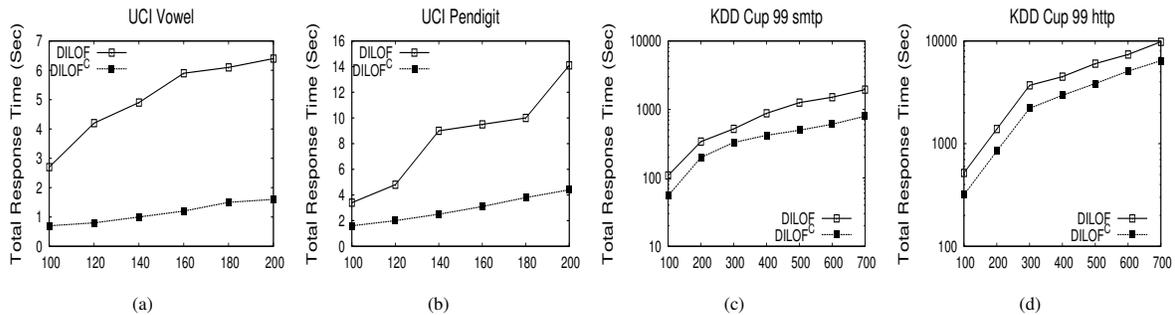


Fig. 8. Total Response Time with Respect to Window Size (DILOF vs. DILOF^C).

DILOF by four factors, three factors, more than two factors, and approximately two factors respectively.

V. CONCLUSION

Outlier detection over data streams is one important task in data mining. In this paper, we proposed an efficient algorithm called DILOF^C for outlier detection over data streams. Our algorithm used the density based approach. It based on DILOF which is the state-of-the-art density-based algorithm for outlier detection over data streams. Our modification in DILOF as follows. We replace the inefficient summarization method of DILOF by a new efficient summarization method that based on a new clustering technique called m-center. Note that, the time complexity of our summarization method is very small compared to the time complexity of DILOF summarization method. We also optimize m-center clustering technique by merging the nearest clusters. Via an extensive evaluation on real datasets, we show that DILOF^C outperforms the state-of-the-art competitor, DILOF by over two factors. Also DILOF^C achieves very high accuracy for detecting outliers. As future work, we plan to evaluate our method in a real sensor network.

REFERENCES

- [1] R. Domingues, M. Filippone, P. Michiardi, and J. Zouaoui, "A comparative evaluation of outlier detection algorithms," *Experiments and analyses. Pattern Recognit.*, pp. 406–421, 2018.
- [2] Y. Yan, L. Cao, and E. Rundensteiner, "Scalable top-n local outlier detection," In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining, Halifax, NS, Canada*, p. 1235–1244, 2017.
- [3] S. Cai, R. Huang, J. Chen, C. hang, B. Liu, and S. Y. Y. Geng, "An efficient outlier detection method for data streams based on closed frequent patterns by considering anti-monotonic constraints," *ScienceDirect ELSEVIER*, vol. 555, pp. 125–146, MAY 2021.
- [4] A. Senthilkumar and M. Metilda, "A survey on cluster based outlier detection techniques in data stream," *International Journal of Data Mining Techniques and Applications*, vol. 5, 2016.
- [5] A. Chandola and V. Kumar, "Article outlier detection," *ACM Computing Surveys*, 2009.
- [6] P. Thakkarand, J. Vala, and V. Prajapati, "Survey on outlier detection in data stream," *International Journal of Computer Applications*, vol. 136(2), 2016.
- [7] L. Tran, L. Fan, and C. Shahab, "Distance-based outlier detection in data streams," *VLDB Endowment*, vol. 9(12), 2016.
- [8] F. Angiulli and F. Fassetti, "Detecting distance-based outliers in streams of data," in *ACM Conference on Information and Knowledge Management*, pp. 811–820, 2007.
- [9] A. Gounaris and Y. Manolopoulos, "Continuous monitoring of distance-based outliers over data streams," *International Conference on Data Engineering*, pp. 135–146, 2011.
- [10] L. Cao, D. Yangt, Q. Wang, Y. Yu, J. Wang, and E. A. Rundensteiner, "Scalable distance-based outlier detection over high-volume data streams," *International Conference on Data Engineering*, pp. 76–87, 2014.
- [11] L. Tran, M. Y. Mun, and C. Shahabi, "Real-time distance-based outlier detection in data streams," *Proceedings of the VLDB Endowment*, vol. 14(2), 2020.
- [12] P. Thakkar, J. Vala, and V. Prajapati, "Survey on outlier detection in data stream," *International Journal of Computer Applications*, vol. 136(2), pp. 0975–8887, 2016.
- [13] G. S. Na, D. Kim, and H. Yu, "Dilof: Effective and memory efficient local outlier detection in data streams," In *Proceedings of the 24th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining (KDD '18), London, UK, 19–23 August 2018; Association for Computing Machinery: New York, NY, USA, 2018*, pp. 1993–2002, 2018.

- [14] J. Huang, M. Zhong, and B. P. Jaysawal, "Tadilof: Time aware density-based incremental local outlier detection in data streams," *MDPI*, 2020.
- [15] T. Kieu, B. Yang, and C. S. Jensen, "Outlier detection for multidimensional time series using deep neural," In *Proceedings of the 2018 19th IEEE International Conference on Mobile Data Management (MDM), Aalborg, Denmark*, pp. 125–134, 2018.
- [16] A. Aymen, A. Kachouri, and A. Mahfoudhi, "Outlier detection for wireless sensor networks using density-based clustering approach," *IET Wirel. Sens. Syst.*, pp. 83–90, 2017.
- [17] M. M. Breunig, H. Kriegel, R. T. Ng, and J. Sander, "Lof: Identifying density-based local outliers," In *Proceedings of the 2000 ACM SIGMOD International Conference on Management of Data (SIGMOD'00), Dallas, TX, USA, 16–18 May 2000; Association for Computing Machinery: New York, NY, USA*, p. 93–104, 2000.
- [18] D. Pokrajac, A. Lazarevic, and L. J. Latecki, "Incremental local outlier detection for data streams," *IEEE Symposium on Computational Intelligence and Data Mining*, pp. 504–515, 2007.
- [19] M. Salehi, C. Leckie, and C. Leckie, "Fast memory efficient local outlier detection in data streams," *IEEE Trans. Knowl. Data Eng.*, vol. 28, pp. 3246–3260, 2016.
- [20] S. Chakraborty and N. K. Nagwani, "Analysis and study of incremental k-means clustering algorithm," In *International Conference on High Performance Architecture and Grid Computing; Springer: Berlin/Heidelberg, Germany*, pp. 338–341, 2011.

Network Intrusion Detection System based on Generative Adversarial Network for Attack Detection

Abhijit Das¹

Research Scholar, Department of CSE
PESITM, Affiliated to VTU (Belagavi)
Shivamogga, Karnataka, India

Dr. S G Balakrishnan²

Associate Professor, Department of ISE
Mahendra Engineering College
Salem, India

Dr. Pramod³

Associate Professor, Department of ISE
PESITM, Affiliated to VTU (Belagavi)
Shivamogga, Karnataka, India

Abstract—The Intrusion Detection System (IDS) is the main element to prevent malicious traffic on the network. IDS will quickly increase the ability to detect network threats with the help of Deep Learning algorithms. As a result, attackers are finding new ways to evade identification. Polymorphic attacks, search for the attackers, as they can bypass the IDS. Generative Adversarial Networks (GAN) is a method proven in generating various forms of data. It is becoming popular among security researchers as it can produce indistinguishable data from the original data. This work proposed a model to generate DDoS attacks using a GAN. Several techniques have been used to regenerate the feature selection to identify the attack and generate polymorphic data. The data will change feature profile in every cycle to test if the IDS can detect the new version of attack data. Simulation results from the proposed model show that with constant changing attack profiles, defending arrangements that handle incremental knowledge will yet stay exposed to current attacks.

Keywords—Generative adversarial networks; network threats; deep learning; intrusion detection; feature selections

I. INTRODUCTION

The Internet is being used in many fields, like data transfer, e-learning, and many more, and its growth has impacted all aspects of life. This increasing usage of the Internet causes concerns about network security and needs constant improvements in securing Internet technologies from various attacks. Examples of these attacks include DDoS attacks, Man-in-the-middle attacks, Phishing, Password-based attack, SQL injection, and many more. Network vulnerabilities can cause damage to small or large organizations. According to one survey, 98% of businesses in the UK depend on Information Technology services. Over 43% of small scale and 72% of large-scale organizations suffered from cyber-attacks in the past years. There are many tools available to secure or prevent cyber-security attacks, including but not limited to: Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), Anti-malware, Network Access Control, Firewalls. Among those, one of the most commonly used and effective tool is the Intrusion Detection System.

IDS analyzes the data traffic is to be distinguished from the malignant and the normal traffic, and to generate a warning, so that all the necessary precautions must be taken to avoid damage [1]. With the development of network attacks and security, improved detection and prevention systems. Artificial intelligence (AI) is now widely used for security tools in the IDS [2], and activists have begun to use artificial intelligence

techniques to malicious attacks [3] [4]. AI and deep learning algorithms require a large amount of data to train and test the models. Some of the techniques that can be used for the production of large data sets to finish the malware detection [5] [6] and security orchestration, [7].

One of the frameworks to generate adversarial data is Generative Adversarial Networks (GAN). It is an architecture of two neural networks: the Generator and the Discriminator. The Generator uses gradient descent or the response from the discriminator and generates adversarial data. The discriminator distinguishes between the original and the adversarial data. The Generator and the discriminator compete in this way, and, in the end, the Generator produces synthetic or adversarial data [8]. GAN has been utilized in research to generate various types of datasets like images [9], sound [10], text [11], and network attack data [12].

II. RELATED WORKS

The recent development in deep learning, intrusion detection systems are getting advanced with these methods. However, there is limited research testing the integrity of the advanced IDS against adversarial data.

According to a study by [13], the authors created a framework that generates adversarial malware using GAN to bypass the detection system. The objective of this research is to use a black-box malware detector because most of the attackers are unaware of the detection techniques used in the detection system. Instead of directly attacking the black-box detector, researchers created a model that can observe the target system with corresponding data. Then this model calculates the gradient computation from the GAN to create adversarial malware data. With this technique, the authors received a model accuracy of around 98%.

This section covers some previous works on generating adversarial attack data using the Wasserstein GAN. The Wasserstein GAN model was introduced in [14], and it improves upon the traditional GAN. Wasserstein GAN is an extension of traditional GAN that finds an alternate method of training the Generator. In WGAN the Discriminator provides a critic score that depicts how real or fake the data generated.

To generate a malicious file [12] proposed a method that uses WGAN so that a detection system signifies the adversarial malicious file as a regular file. They have achieved an accuracy of around 99%, proving that their method can generate adversarial malicious files that can bypass the detection system.

A recent study in [15] uses Wasserstein GAN to generate simulated attack data. According to the authors, many tools can generate simulated attack data. However, this process could take a long time and a lot of resources. Using the proposed technique, they have produced millions of connection records with just one device and within a short period. They used the KDD Cup 1999 dataset as the training set. Their experiment suggests that as compared to GAN, the Wasserstein GAN learns faster and generates better results. A paper published by Ring et al. [16] proposed a method that produces flow-based attack data using Wasserstein GAN. This research uses the CIDDS dataset to test and train the proposed method. They have suggested that the flow-based dataset consists of categorical features like IP address, port numbers, etc. The GAN is unable to process categorical data. They have also proposed a method to preprocess the categorical data and transform them into continuous data. Lastly, they have used several techniques to evaluate the quality standard of the adversarial data. Results suggest that it is possible to generate real network data using this method.

A recently published paper by Lin et al. [17] discussed the benefits of WGAN. It proposed a technique IDSGAN to generate adversarial attack data and test the attack against the Intrusion Detection System. They have utilized the NSL-KDD as the benchmark dataset to generate an adversarial attack on an IDS. They have tested this technique with various machine learning classifiers like Support Vector Machine, Naïve Bayes, Multilayer Perceptron, Linear Regression, Decision Tree, Random Forrest. They have used four types of attacks, Probe, DoS, User to Root, Root to Local to generate adversarial attack data.

This research aims to create a framework that detect attacks using GAN, motivated by [17].

- This work begins with the important feature selection method using SHAP. This work identified the most critical features from the dataset that contribute to a DDoS attack.
- The next goal is to Generate adversarial data using the selected feature set and evaluate the IDS if it can detect the adversarial attack, followed by preparing the IDS with the produced adversarial data.
- This work propose a polymorphic engine that updates the feature profile of the attack by Manual feature update and Automated feature update.
- The research work have conducted a comprehensive simulation and analyzed the results to compare the Reinforcement Learning method against the Manual Feature profile attacks and presented how many cycles an attacker can bypass an IDS with polymorphic adversarial DDoS attacks.

The primary objective of the Generative Model is to learn the unknown probability distribution of the population from which the training observations are sampled from. The most popular GAN architectures are DCGAN[18], Conditional GAN[19], BiGAN[20], Cycle GAN[21].

III. METHODOLOGIES

A. Datasets and Feature Selection

Datasets: This work uses a dataset published by the Canadian Institute of Cyber Security, CIC-IDS2017, published in [22] by Lashkari et al., which, according to the authors, supersedes the datasets generated earlier by the institute. CI-CIDS2017 consists of eight different files that contain regular traffic and attack traffic data. Moreover, this dataset consists of various types of attacks along with the normal network flow. This dataset also covers all the available standard protocols like HTTP, HTTPS, FTP, SSH, and email protocols. The dataset consists of more than 70 features that are important as per the latest network standards, and most of them were not available in the previously known datasets.

Feature Selection: Feature selection is an essential aspect of the Deep Learning technique. SHAP (Shapley Additive ex-Planations) [23] is one of the new feature selection techniques. The goal of the proposed method is to signify the contribution of each feature to the predicted value. Two critical measures to define feature importance are Consistency and Accuracy. The authors of the paper discuss that SHAP is the method that satisfies these qualities. The SHAP values explained by the authors are based on Shapley values that are a concept from game theory. The idea behind Shapely values is that the outcome of each possible combination (or coalition) of each feature needs to be examined to determine the importance of a single feature. The mathematical explanation of this is as follows in Equation 1:

$$g(z') = \phi_0 + \sum_{j=1}^M \phi_j Z_j' \quad (1)$$

Here, g represents the overall result of the Shapely values, $z' \in \{0, 1\}^M$ is a coalition vector, M is the max coalition size, and ϕ represents the presence of feature j that contributes towards the final output. The authors have described a coalition vector as simplified features in the paper. In coalition vector, 0 means the corresponding value is not present” and 1 means it is “present.” Equation 1 can be called a power set and can be explained as a tree as follows.

Equation 1 can be called a power set and can be explained as a tree shown in Figure. 1 as follows

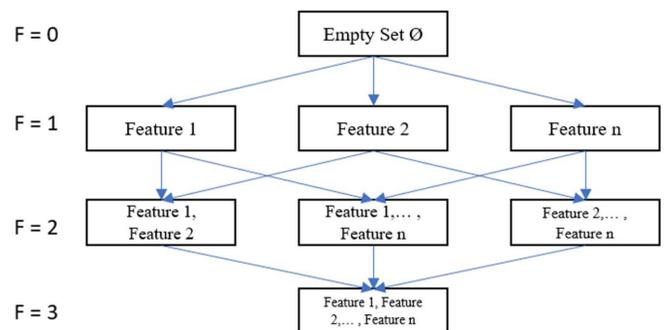


Fig. 1. Power Set of Features.

Each node here represents a coalition of features. Edges represent the inclusion of a feature that was not present in the previous coalition. Equation 1 trains each coalition in the power set of the features to find the most critical feature from the dataset.

The following results were obtained as shown in Fig. 2 by running the SHAP explainability model on the CICIDS2017 data file that shows the list of essential features responsible for the DDoS attack in the most important to least important order. Furthermore, the dark red color represents a higher impact of a feature, and the blue color represents a lower impact of a feature on the output value.

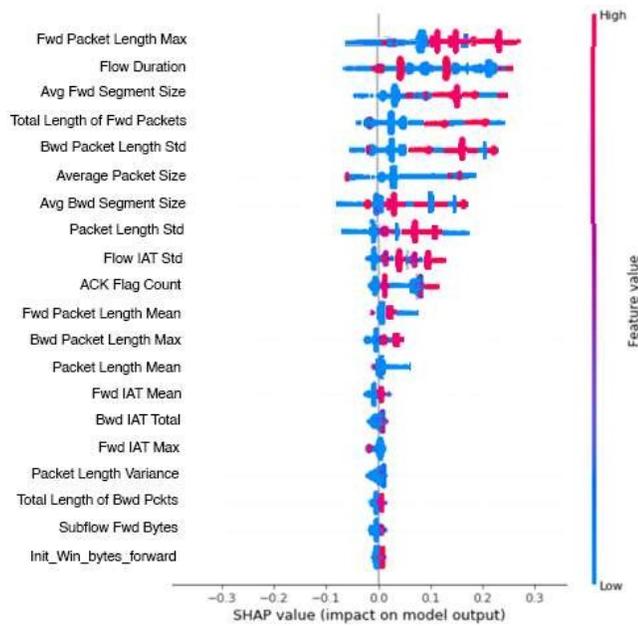


Fig. 2. Summary Plot with Feature Impact using SHAP.

So, from the results obtained in the Fig. 2, This work used these features like functional features that contribute to the DDoS attacks.

B. Adversarial Attack Generation using Wasserstein GAN

The methodologies used in this research involves the Generative Adversarial model that produces adversarial attacks, training IDS by earlier generated polymorphic datasets, polymorphic engine to generate polymorphic DDoS attacks, and use the polymorphic data to attack the IDS. DDoS attack data from the CICIDS2017 [22] used to Generate the adversarial attack by combining a random noise vector of the same size as the selected features from the dataset to train the model. The framework is a feed-forward neural network that consists of 5 linear layers. The input layer consists of neurons as per the selected number of features, and the output layer consists of 1 neuron as shown in Fig. 3.

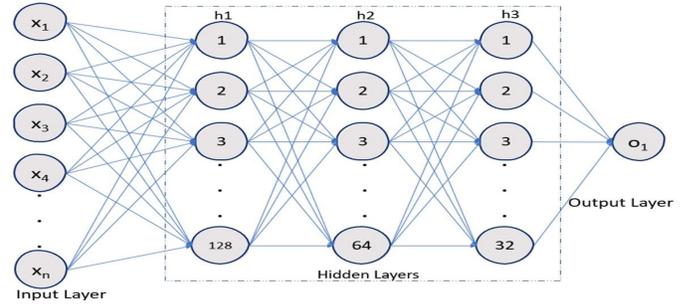


Fig. 3. Neural Network of the Generator.

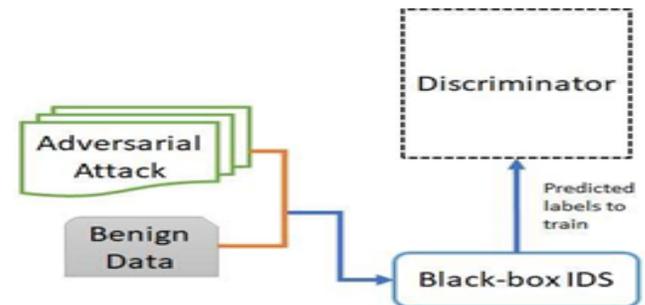


Fig. 4. Training the Black-box IDS.

The input layer receives several numbers of features according to the experiment, and the output layer generates the desired data. The Generator consists of 3 hidden layers that are optimal for this scenario; the results showed fewer layers would underfit the training data. Anything more than that overfits the training data.

In the next step, the generated adversarial attack combined with the benign or normal network flow data will be fed to the Intrusion Detection System.

The IDS will detect the attack and sends predicted labels to the Discriminator as shown in Fig. 4, the detection success rate, and the Discriminator will send the critique to the Generator using the backpropagation so that in the next cycle, the Generator can improve the production of adversarial DDoS attack. The IDS consists of 4 layers, from which the input and output layer consists of 2 neurons each. The IDS consists of 2 hidden layers that are ideal because it only detects if the test data consists of an attack or benign.

The signature-based black-box intrusion detection system used to test the detection rate of the adversarial DDoS attacks. The reason for using this is that most of the time, the type of attack detection system is unknown to the attackers. Attackers rely on the responses received from the detection system, and black-box IDS is the right choice for this model as shown in Fig. 5. The input layer accepts two types of data from the black-box IDS. The output layer provides two critics, one for the Generator and one for itself.

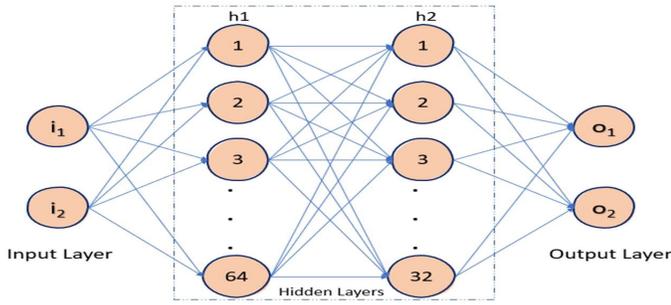


Fig. 5. Neural Network of the IDS and the Discriminator.

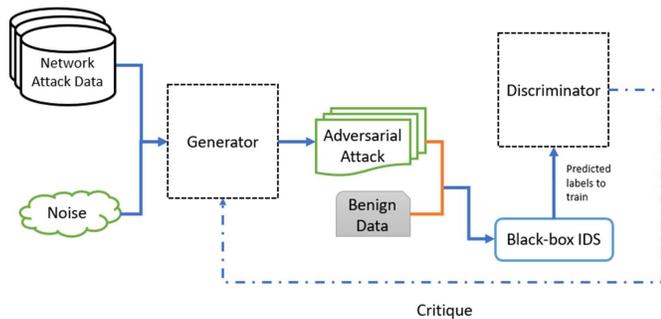


Fig. 6. Generating Adversarial DDoS Attack.

Loss functions used to calculate the Loss[17] for the Generator and the discriminator, shown in the Equation Equation 2 as follows.

$$P_G = E_{M \in S_{attack}, N} - D(G(M, N)) \quad (2)$$

Figure 6 depicts that the generated adversarial data is DDoS attack or abnormal or normal. Here, P_G represents the Penalty to the Generator in attack vector, and in noise vector. E is calculated random inputs value to the model. S_{attack} represents. If the penalty is less to the model means the model is performing well and produces attack datasets that can bypass IDS shown in Equation 3.

$$P_D = A_{S_{\epsilon B_{benigne}}} D(S) + A_{S_{\epsilon B_{attack}}} - B_{S_{\epsilon B_{attack}}} D(S) \quad (3)$$

Here, P_D represents the Penalty to the discriminator. “E” is overall calculated feature values of the models attack datasets. “A” is the actual feature value of benign and the attack data. The lesser the penalty to the discriminator means the discriminator performs well. It calculates if the generated data is closer to the DDoS attack or benign or regular data.

Algorithm – 1 shows the process that was represented in figure 5.

Algorithm 1 Adversarial Attack Generator

Require: Input:

Initiator-noisy vector N, DDoS Attack Datasets

Critic / Discriminator - Sattack, and Sbenign

Output: Trained Critic / Discriminator and Generator

1: for epochs = 1, . . . , Maximum EPOCHS do

2: for N-iterations, do

3: Initiator create adversarial intrrrusion attack using Sattack, and

Revise the penalty by PG once it receives the critique.

4: end loop

5: While generating adversarial DDoS data and feed the data to IDS to test if it detects the attack.

6: for D-iterations, do

7: receive detected labels from the IDS and sends a critic to the Generator.

Update the penalty using PD function.

8: end loop

9: end loop

C. How the Generator Fabricate an Adversarial Attack

This section specifies the details about the learning process of the Generator and how it produces adversarial data. If the generator continuously generates random data, the data will be unmeaningful, which can change the entire network flow data. So, the Generator needs to produce the data to maintain the intensity of an attack. To ensure that, the work need to maintain the feature values constant that have higher SHAP values as shown in Fig. 2.

Here is a sample of how the Generator produces an adversarial attack by the proposed technique. In this diagram, the darker shade explains the feature values of the features that are contributing to the attack. Whereas non highlighted values depict the feature value of a regular or non-attack feature.

Data created from Generator									
155	123.36	4362	869.56	824.86	744	1516	78249.78	393.215	834
Values of the Attack from dataset									
1878	382	11595	382	2182.46	675	1780	3578249.78	127.33	382
Generated Attack									
1878	382	4362	382	2182.46	744	1516	78249.78	127.33	834

Fig. 7. The Process to Generate Adversarial DDoS Attack.

This Fig. 7 explains that to maintain the attack’s intensity, the study need to keep that functional attack features static and only change the feature values that are not contributing to the attack

D. Training an IDS with the Earlier Created Adversarial Data

Fig. 8 depicts IDS training process to evaluate IDS performance with the adversarial data. In this section, the study I will

discuss the training of the IDS to evaluate the performance of IDS. Following diagram that depicts the training process.

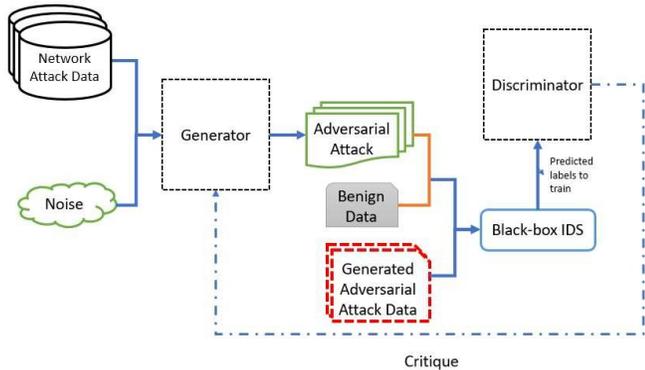


Fig. 8. Training the Black-Box IDS.

This research work considered three inputs to train the IDS: normal or benign data, new adversarial data, and previously generated adversarial data. The IDS learns about the adversarial data and tries to detect the DDoS attack data. Algorithm 2 suggests the overall process for the same.

Algorithm 2 Training IDS by Adversarial DDoS datasets

Require: Generator – N noisy error data + Initial Attack Data
 IDS – Benign or Normal Data, Adversarial Datasets, and Earlier Generated Attack Data
 Critic / Discriminator – Sattack and Sbenign
Output:
 Critic / Discriminator, Generator, and trained IDS
 1: for each epochs = 1 , . . . , MAX EPOCHS do
 2: for G-repetitions, do
 3: The generator generates attacks from datasets using Sattack and Renew loss applying PG function
 4: end of the loop
 5: for D-repetitions, do
 6: Critic / Discriminator distinguishes this data to Bbenign and Battack
 7: Renew loss applying PD function
 8: Feed Battack (attack data) and Earlier Generated attack Data
 9: end loop

E. Polymorphic Engine to Generate Polymorphic Attack

Three different methods used for the Polymorphic engine to generate Polymorphic Attack are as follows.

1. Update new features in the attack profile after the IDS detects previous adversarial attacks. Algorithm 3 will discuss the process.

Algorithm 3

Require: Input – Use five functional attack features with a high impact score from the
Ensure: shortlisted features and five normal features.
 1: Generate adversarial DDoS data and attack the IDS.
 2: Train the IDS so that it can detect previously generated adversarial DDoS data.
 3: Use the same set of features to generate an adversarial DDoS attack. Again, go to step – 2.
 If the Generator fails to evade the IDS, choose one functional feature with a high feature score, one normal or benign feature from the predefined set of features, and swap them with the used features.
 4: Go to step – 1.
 5: In the end, the IDS will detect all the Polymorphic adversarial DDoS attacks; the program will stop.

2. Add new features from the predefined list of features in the current attack profile after the IDS detects previous adversarial attacks, and the following algorithm 4 will discuss the process.

Algorithm 4

Require: Input – Use five functional attack features with a high impact score from the shortlisted features and five normal features.
Ensure: shortlisted features and five normal features.
 1: Generate adversarial DDoS data and attack the IDS.
 2: Train the IDS so that it can detect previously generated adversarial DDoS data.
 3: Use the same set of features to generate an adversarial DDoS attack. Again, go to step – 2.
 If the Generator cannot deceive the IDS with the same set of features, choose one new functional feature with a high impact score, one feature that represents benign data, and add them to the previous attack profile.
 4: Go to step – 1.
 5: At the end, the IDS will detect all the Polymorphic adversarial DDoS attacks. The program will stop.

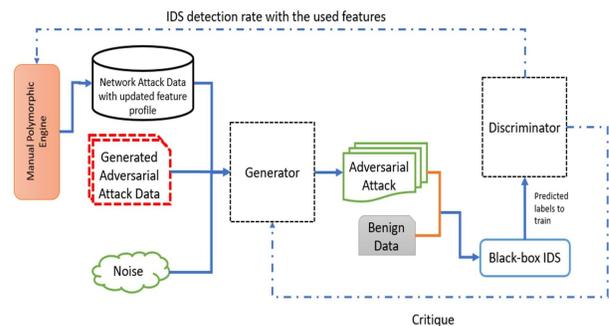


Fig. 9. Manual Process to Generate Polymorphic Adversarial Attack.

In the above methods shown in Fig. 9, the research work

assumed that an attacker would manually modify the feature profile and train the model with the new feature profile every time the IDS detects a polymorphic attack. This study considered using only a total of 20 features that were provided by the SHAP method.

3. It will be challenging to keep manually changing the feature profile if the study will use more than 20 features. So as an alternative a Reinforcement Learning method has been used to automate the feature profile selection for generating a polymorphic attack as shown in Fig. 10.

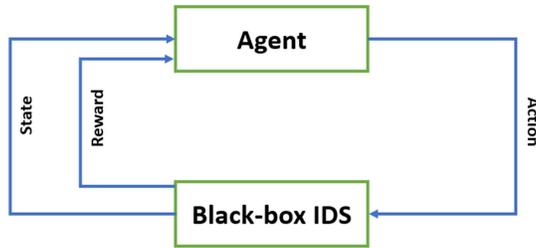


Fig. 10. Function of RL in this Framework.

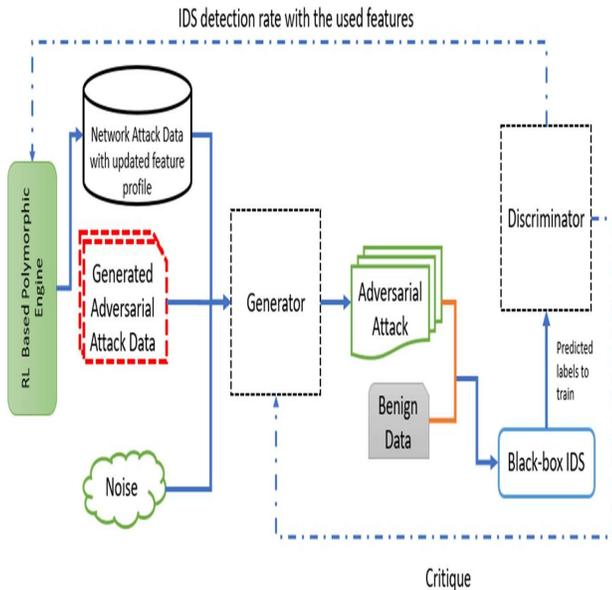


Fig. 11. Automated RL that Generates Polymorphic Adversarial Attack.

The Reinforcement Learning method is an ML-based technique that focuses on retraining the algorithm following a trial-and-error approach. The agent in this architecture evaluates the current IDS attack detection score. Then the agent takes action and receives feedback from IDS. Positive feedback is a reward, and negative feedback is a penalty to the agent. The following algorithm will explain the process. The overall process of generating a polymorphic attack is explained in the following algorithm 5 and Fig. 11.

Algorithm 5

Require: Input – Use any five features with a high impact score and any 5 with the lowest score from the shortlisted features.

Ensure: shortlisted features and five normal features.

- 1: Generate adversarial DDoS data and attack the IDS.
- 2: Train the IDS and check if the adversarial attack evades the IDS. Continue using the current feature set to generate an attack.
- 3: Get the attack success rate; if the attack FAILS to evade, The RL algorithm adds new features in the existing feature set to generate a polymorphic attack.
- 4: If the new polymorphic attack fails to evade the IDS, the RL algorithm will get a penalty. The RL will ignore these features, and if the new polymorphic attack evades the IDS, the RL will get a reward.
- 5: The RL agent will learn combinations of the attack feature profile and generate a new polymorphic adversarial DDoS attack.
- 6: The algorithm stops when the Generator can no longer generate a polymorphic adversarial attack.

F. Performance Evaluation

To evaluate the performance and the results of this work, the research work used the following parameters.

Accuracy - Represents the fraction of precisely classified data in comparison to the total processed data. The formula to calculate accuracy is as follows

$$Accuracy = \frac{TP + TN}{TP + TN + FN + FP} \quad (4)$$

Precision – a ratio between True Positive values and all the positive values received from the Deep Learning model.

$$Precision = \frac{TP}{TP + FP} \quad (5)$$

Recall – a ratio between correctly detected samples over total sample data. It is also known as a ratio between True Positives and the sum of True Positives and False Negatives.

$$Recall = \frac{TP}{TP + FN} \quad (6)$$

F1-Score – a calculation of a mean of precision and recall.

$$F1 - Score = 2X \frac{Precision \times Recall}{Precision + Recall} \quad (7)$$

IV. RESULTS AND DISCUSSION

The experimental setup has done by using libraries like PyTorch, Scikit-learn, Pandas, Numpy, Matplotlib. Hyper-parameters are essential properties that define the characteristics of the training process of the Deep Learning model. The hyper-parameters used in this research are BatchSize, learningrate, Criticlters, Optimizer, Epochs to the optimization and training process of the model.

This section describes the results of various experiments for different scenarios and analyses of findings.

A. Attack Generation

The first step of the research is to generate an adversarial DDoS attack to evade this Black-box IDS. As seen in Fig. 12 graph initially, Generator produces data that is unable to bypass the IDS. However, after training the Generator for 100 epochs, it discovers to create adversarial data to deceive IDS.

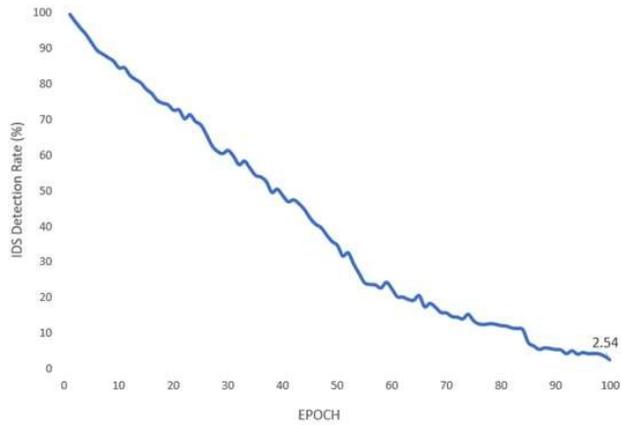


Fig. 12. Adversarial DDoS Attack Generation.

B. Training IDS by Adversarial DDoS Information

This section describe the result of the discovery time of IDS after training. As shown in Fig. 13, in initial cycles, IDS struggles to detect the attacks. However, after training it for 100 epochs, it detects almost all the attacks.

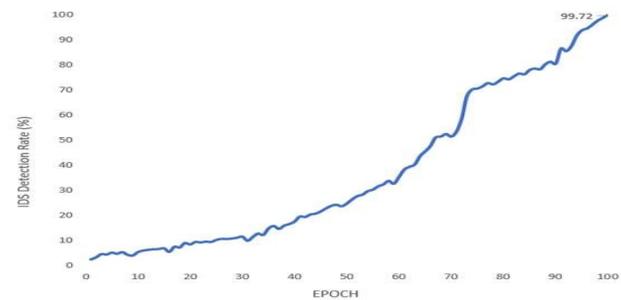


Fig. 13. Detection Rate after Training the IDS.

C. Polymorphic Adversarial DDoS Attack Generation

This section illustrates the detection rate of the Black Box IDS under the generation of polymorphic adversarial attacks.

In the first experiment, new features have been selected manually to produce polymorphic attacks. For this test, limited features from the datasets have been used. The following is the initial result using algorithm 3.

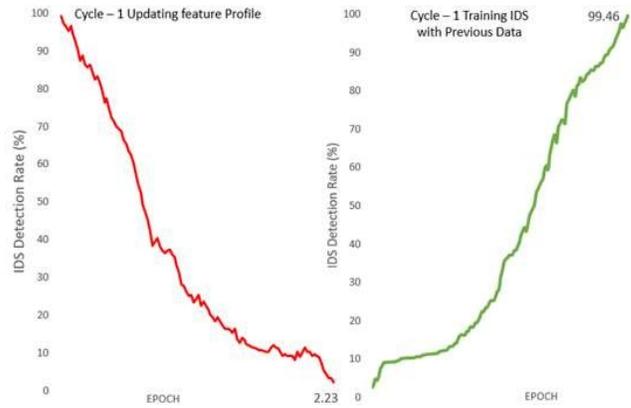


Fig. 14. Polymorphic Adversarial DDoS Attack using Algorithm 3.

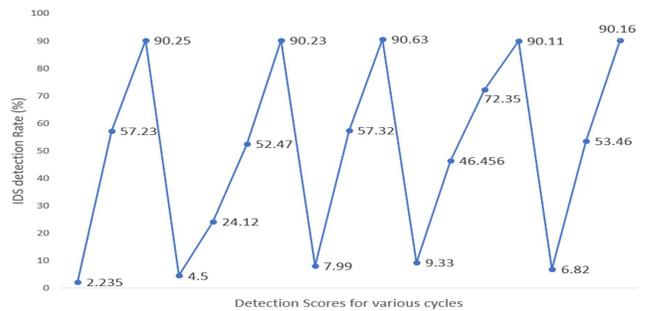


Fig. 15. IDS Detection Rate for Each Attack Cycle (using algorithm 3).

In the Fig. 14, above result, a red-colored graph suggests a polymorphic attack being generated and proceed towards the BlackBox IDS. As seen, the polymorphic attack can deceive the IDS. The green-coloured graph depicts the training of IDS by earlier generated polymorphic adversarial DDoS datasets. After 100 epochs, IDS detects the polymorphic adversarial DDoS attack. The following result indicates all the cycles of polymorphic attacks on the IDS. The Generator utilizes the same combination of the features to generate attacks until an IDS detects all the previous attacks.

Each data point in Fig. 15 depicts the IDS detection rate. Once the IDS detects all the previous versions of the polymorphic DDoS attack that uses the same feature set (as seen in Fig. 15), the generator manually selects new predefined features and generates a new polymorphic adversarial DDoS attack. For this test, only a group of 10 features have been used.

In the next test, the research work used a technique that follows algorithm 4 to revise the attack to generate a polymorphic adversarial DDoS attack. For this experiment, the work has been began with ten features to generate polymorphic attack data. To generate a new polymorphic attack, two new features have been added in the existing attack data and used a total of 20 features. The Fig. 16 is the first result of the initial polymorphic attack.

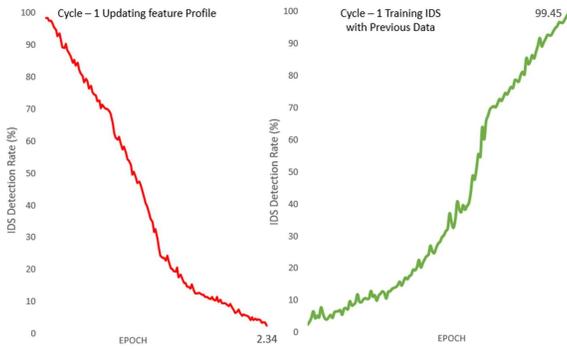


Fig. 16. Polymorphic Adversarial DDoS Attack using Algorithm 4.

Each data point in Fig. 17 depicts the IDS detection rate. Once the IDS detects all the previous versions of the polymorphic DDoS attack that uses the same feature set, the generator manually selects new predefined features and generates a new polymorphic adversarial DDoS attack. For this test, a group of 20 features have been used. In this test, the Generator can deceive the IDS for a total of 18 cycles using this technique.

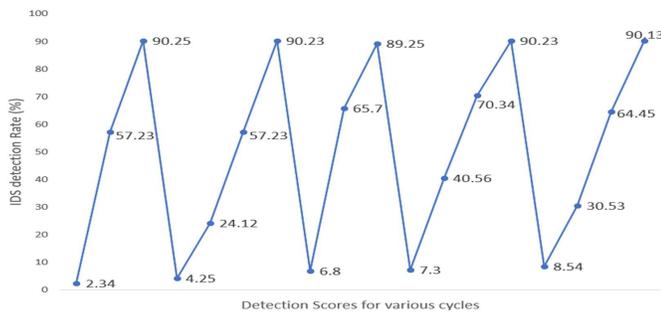


Fig. 17. IDS Detection Rate for Each Attack Cycle (using algorithm 4).

The first two experiments focus on testing if the Generator can produce polymorphic adversarial DDoS attack data by updating the feature profile manually. After confirming the possibility of doing so, the next step is to automatically select features and manipulate the attack feature profile to generate polymorphic adversarial attack data. To automate this task, the Reinforcement Learning technique has been applied. It receives an IDS detection rate and learns to select new features, add them to the old feature set, and create a new feature set. This experiment also indicates the number of times a generator can produce polymorphic adversarial DDoS data. To examine this, four sets of feature combinations have been used for each test to generate the automated Polymorphic adversarial DDoS attack.

- The first test includes a total of 40 features from the dataset
- The second test includes a total of 50 features from the dataset
- The third test includes a total of 60 features from the dataset
- The fourth test includes a total of 76 features from the dataset...

The above experiments begin with ten features, from which 5 are a functional feature with a high impact score, and 5 are usual or benign.

D. Test Evaluation

The Table I describes the overall values for the Precision, Recall, and F1-score for each test.

TABLE I. NONLINEAR MODEL RESULTS

Sl. TEST No.		ACCURACY	PRECISION	RECALL	F1-SCORE
1	Manual Test – 1 (using Algorithm 2)	98.58	96.24	92.91	0.953
2	Automated Test using 40 features (using Algorithm 4)	98.27	94.41	92.44	0.935
3	Automated Test using 50 features (using Algorithm 4)	96.97	93.58	91.69	0.928
4	Automated Test using 60 features (using Algorithm 4)	96.34	93.22	91.43	0.921
5	Automated Test using 76 features (using Algorithm 4)	94.42	91.79	91.58	0.916

E. Analysis

This research work ran 5 test scenarios with different feature combinations. 2 experiments consist of a manual feature selection technique to generate polymorphic adversarial DDoS attack data and four tests with an Automated feature selection technique. A manual feature selection technique utilized as a benchmark and compared this technique to the automated feature selection technique to analyze for how many cycles the polymorphic attack evades the Black-Box IDS.

The following Fig. 18 graphs will be useful to compare these five different scenarios.

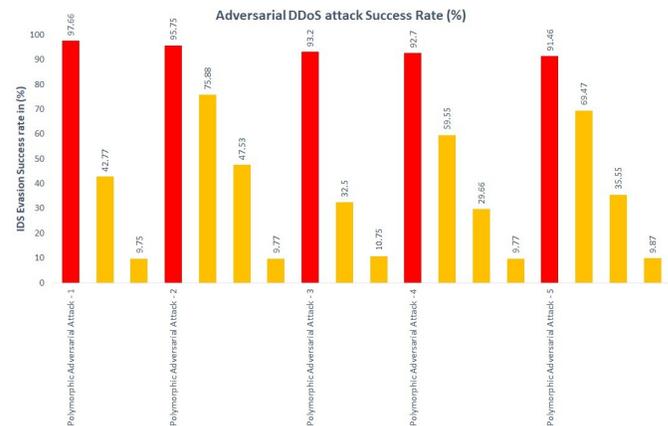


Fig. 18. Test - 1 Polymorphic Adversarial Attacks using Manual Feature Selection.

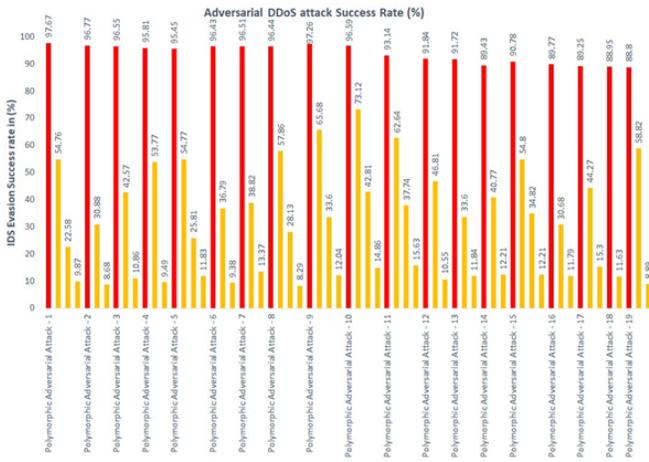


Fig. 19. Test - 2 Polymorphic Adversarial Attacks using Automated Feature Selection.

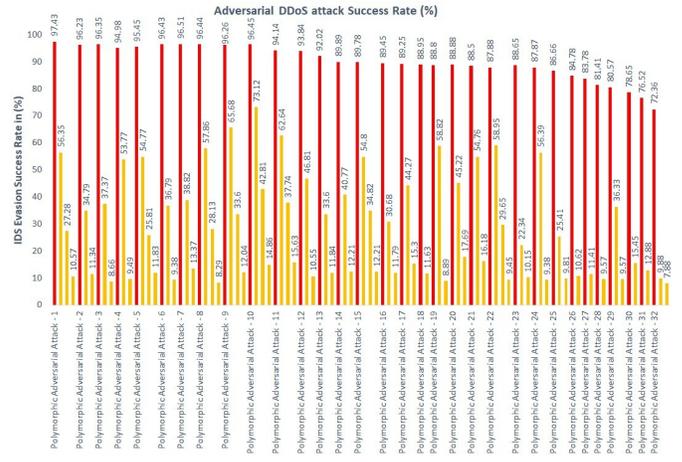


Fig. 22. Test - 5 Polymorphic Adversarial Attacks using Automated Feature Selection.

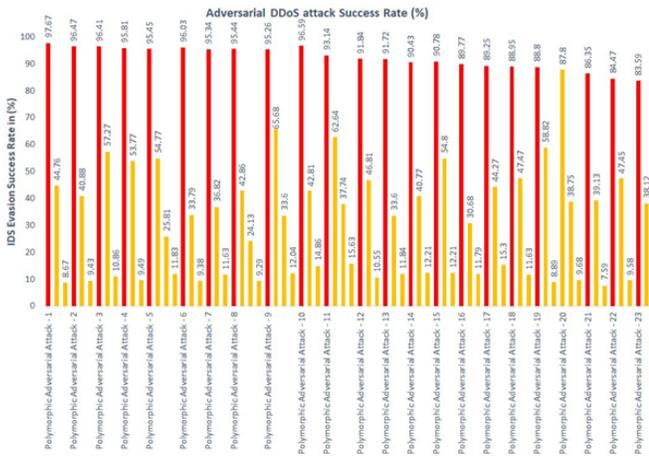


Fig. 20. Test - 3 Polymorphic Adversarial Attacks using Automated Feature Selection.

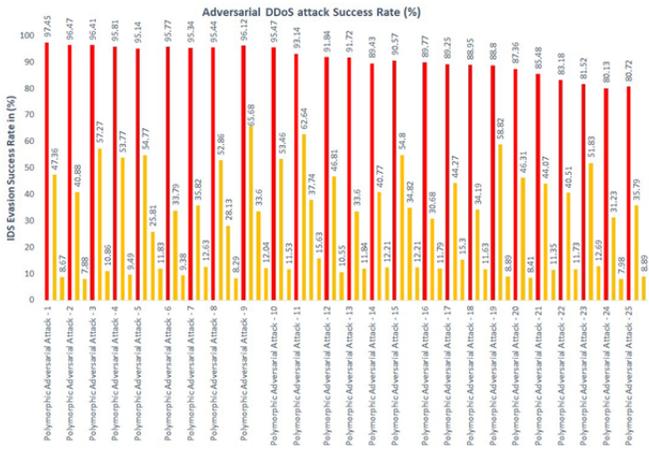


Fig. 21. Test - 4 Polymorphic Adversarial Attacks using Automated Feature Selection.

In all the above results shown in Fig. 18, 19, 20, 21, 22, the Polymorphic DDoS adversarial attack successfully evading the IDS; the orange bar suggests the polymorphic attack is becoming weak once the IDS detects them. By counting the red bar, it has been observed that how many times the Generator produced a polymorphic attack in each cycle. Fig. 19 suggest that when the Generator uses a small number of features, more than 90% of the polymorphic attack evades the IDS. By noticing these figures, it is clear that using fewer features to generate a polymorphic attack has a higher evasion rate but fewer chances of generating more polymorphic attacks.

Fig. 20, 21, 22 suggest that initially, more than 90% of the polymorphic attacks can evade the IDS. However, results propose that if the Generator utilizes more features to generate a polymorphic DDoS attack, the attack success rate gets lower each time. Comparing all the results confirms that while using a fewer number of features to generate polymorphic adversarial DDoS attacks, the attack success rate stays up to the acceptable amount. However, when more features have been used, the attack success rate depletes after certain cycles.

Now the Table II describes the total runtime for each experiment.

TABLE II. MODEL EVALUATION

Sl. No.	TEST	TOTAL RUNTIME
1	Test - 1 Manual Feature profile update (with a total of 10 features)	30.43 minutes
2	Test - 3 Automated Feature profile update (with a total of 40 features)	75.31 minutes
3	Test - 5 Automated Feature profile update (with a total of 50 features)	90.45 minutes
4	Test - 6 Automated Feature profile update (with a total of 60 features)	145.37 minutes
5	Test - 5 Automated Feature profile update (with a total of 76 features)	173.55 minutes

As observed from the above table, if the test uses a small number of features, it takes less time to run the simulation. The run time rises upon increasing features to generate a polymorphic DDoS attack.

V. CONCLUSIONS AND FUTURE WORK

The work proposed a framework to create polymorphic adversarial DDoS attacks using a CICIDS2017 dataset using a Wasserstein GAN. To generate polymorphic attacks, three different techniques have been proposed that change the feature profile of the attack. New features have been selected manually each time to generate polymorphic adversarial attacks in the first two techniques. Furthermore, to automate the feature selection to generate polymorphic attacks, a Reinforcement Learning technique has been applied in each technique; the Generator creates a polymorphic attack until no more new features are remaining to choose from the feature set.

From the results, it has been observed that the Generator can produce polymorphic adversarial DDoS. Results also depict that while using a small number of features to create a polymorphic attack, the attacks were successfully deceiving the IDS with more than a 90% success rate while using a manual selection of features.

In the future, it could be interesting to consider using other variants of GAN like DCGAN, Conditional GAN, BiGAN, Cycle GAN to generate adversarial network attack data and evaluate the detection systems. Another limitation of this research is that it focused on generating only one type of attack, as every attack has different functional features. It would be difficult to use one Generator to create other types of attacks with the same generator. So it would be interesting to use multiple generators for each type of attack and evaluate the performance of the IDS against all types of polymorphic adversarial network attacks.

ACKNOWLEDGMENT

This work was supported by the Research Center of PES Institute of Technology and Management, Shivamogga, Karnataka, Computer Science and Engineering Department affiliated to Visvesvaraya Technological University and APS College of Engineering, Bangalore. The authors are grateful for this support. I sincerely thank all those who helped me in completing this task.

REFERENCES

- [1] H.-J. Liao, C.-H. Richard Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Journal of Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, Jan. 2013, DOI: 10.1016/j.jnca.2012.09.004.
- [2] U. Sabeel, S. S. Heydari, H. Mohanka, Y. Bendhaou, K. Elgazzar and K. El-Khatib, "Evaluation of Deep Learning in Detecting Unknown Network Attacks," 2019 International Conference on Smart Applications, Communications and Networking (SmartNets), Sharm El Sheik, Egypt, 2019, pp. 1-6, doi: 10.1109/SmartNets48225.2019.9069788.
- [3] M. Gadelrab, A. A. El Kalam, and Y. Deswarte, "Manipulation of Network Traffic Traces for Security Evaluation," in 2009 International Conference on Advanced Information Networking and Applications Workshops, May 2009, pp. 1124–1129, DOI: 10.1109/WAINA.2009.36.
- [4] F. Skopik, G. Settanni, R. Fiedler, and I. Friedberg, "Semi-synthetic data set generation for security software evaluation," in 2014 Twelfth Annual International Conference on Privacy, Security and Trust, Jul. 2014, pp. 156–163, DOI: 10.1109/PST.2014.6890935.
- [5] "CrowdStrike Introduces Enhanced Endpoint Machine Learning Capabilities and Advanced Endpoint Protection Modules." Internet: <https://www.crowdstrike.com/resources/news/crowdstrike-introduces-enhancedendpoint-machine-learning-capabilities-and-advanced-endpoint-protection-modules>
- [6] M. Berninger and A. Sopian. "Reverse Engineering the Analyst: Building Machine Learning Models for the SOC." Internet: <https://www.fireeye.com/blog/threatresearch/2018/06/buildmachine-learning-models-for-the-soc.html>
- [7] "Use Cases: Demisto's Top Machine Learning Use Cases – Part 1." Internet: <https://blog.demisto.com/demistos-top-machine-learning-use-cases-part-1>
- [8] I. Goodfellow et al., "Generative Adversarial Nets," in *Advances in Neural Information Processing Systems 27*, Z. Ghahramani, M. Welling, C. Cortes, N. D. Lawrence, and K. Q. Weinberger, Eds. Curran Associates, Inc., 2014, pp. 2672–2680.
- [9] S. Yu, H. Dong, F. Liang, Y. Mo, C. Wu, and Y. Guo, "SIMGAN: Photo-Realistic Semantic Image Manipulation Using Generative Adversarial Networks," in 2019 IEEE International Conference on Image Processing (ICIP), Sep. 2019, pp. 734–738, DOI: 10.1109/ICIP.2019.8804285.
- [10] C. Wan, S. Chuang, and H. Lee, "Towards Audio to Scene Image Synthesis Using Generative Adversarial Network," ICASSP 2019 - 2019 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP), Brighton, United Kingdom, 2019, pp. 496-500, DOI: 10.1109/ICASSP.2019.8682383.
- [11] Y. Yang, X. Dan, X. Qiu, and Z. Gao, "FGGAN: Feature-Guiding Generative Adversarial Networks for Text Generation," in *IEEE Access*, vol. 8, pp. 105217- 105225, 2020, DOI: 10.1109/ACCESS.2020.2993928.
- [12] J. Zhang, Q. Yan, and M. Wang, "Evasion Attacks Based on Wasserstein Generative Adversarial Network," 2019 Computing, Communications and IoT Applications (ComComAp), 2019, doi: 10.1109/ComComAp46287.2019.9018647.
- [13] M. Kawai, K. Ota, and M. Dong, "Improved MalGAN: Avoiding Malware Detector by Leaning Cleanware Features," in 2019 International Conference on Artificial Intelligence in Information and Communication (ICAIIIC), Feb. 2019, pp. 040–045, DOI: 10.1109/ICAIIIC.2019.8669079.
- [14] M. Arjovsky, S. Chintala, and L. Bottou, "Wasserstein GAN," arXiv:1701.07875 [cs, stat], Dec. 2017, Accessed: Aug. 19, 2020. [Online]. Available: <http://arxiv.org/abs/1701.07875>.
- [15] H. Xie, K. Lv, and C. Hu, "An Effective Method to Generate Simulated Attack Data Based on Generative Adversarial Nets," in 2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), Aug. 2018, pp. 1777–1784, DOI: 10.1109/TrustCom/BigDataSE.2018.00268.
- [16] M. Ring, D. Schlör, D. Landes, and A. Hotho, "Flow-based Network Traffic Generation using Generative Adversarial Networks," *Computers and Security*, vol. 82, pp. 156–172, May 2019, DOI: 10.1016/j.cose.2018.12.012.
- [17] Z. Lin, Y. Shi, and Z. Xue, "IDSGAN: Generative Adversarial Networks for Attack Generation against Intrusion Detection," arXiv:1809.02077 [cs], Jun. 2019, Available: <http://arxiv.org/abs/1809.02077>.
- [18] A. Radford, L. Metz, and S. Chintala, "Unsupervised Representation Learning with Deep Convolutional Generative Adversarial Networks," arXiv:1511.06434 [cs], Jan. 2016, Available: <http://arxiv.org/abs/1511.06434>.
- [19] M. Mirza and S. Osindero, "Conditional Generative Adversarial Nets," arXiv:1411.1784 [cs, stat], Nov. 2014, Available: <http://arxiv.org/abs/1411.1784>.
- [20] U. Mutlu and E. Alpaydm, "Training bidirectional generative adversarial networks with hints," *Pattern Recognition*, vol. 103, p. 107320, Jul. 2020, doi: 10.1016/j.patcog.2020.107320.
- [21] J.-Y. Zhu, T. Park, P. Isola, and A. A. Efros, "Unpaired Image-to-Image Translation Using Cycle-Consistent Adversarial Networks," in 2017 IEEE International Conference on Computer Vision (ICCV), Oct. 2017, pp. 2242–2251, doi: 10.1109/ICCV.2017.244.
- [22] I. Sharafaldin, A. Lashkari, and A. Ghorbani, "Toward Generating a New Intrusion Detection Dataset and Intrusion Traffic Characterization", 4th International Conference on Information Systems Security and Privacy (ICISSP), Portugal, January 2018
- [23] J. Hui, "GAN — DCGAN (Deep convolutional generative adversarial networks)," Medium, Jun. 24, 2018. <https://medium.com/@jonathanhui/gan-dcgan-deepconvolutional-generative-adversarial-networks-df855c438f>

Near-ground Measurement and Modeling for Archaeological Park of Pisac in Cusco for LoRa Technology

Yhon D. Lezama¹, Jinmi Lezama², Jorge Arizaca-Cusicuna³
Universidad Nacional San Antonio Abad del Cusco - UNSAAC^{1,3}
Universidad Nacional Tecnológica de Lima Sur - UNTELS²

Abstract—This research work presents the details of a near-ground received power measurement and modeling based on it, inside the archaeological park of Pisac in the city of Cusco. The measurements were performed at a working frequency of 920 MHz in the industrial, scientific, and medical (ISM) band, using transceiver devices with LoRa technology. The power of the received signal is obtained while the transmitter moves at a constant speed of 0.4 m/s, to characterize the fading that occurred within this archaeological park, making appropriate use of the moving average filter separates the fading to large and small scale, then on the filtered signal is used the algorithm of linear regression, to obtain a model that characterizes the exponent of propagation loss and the shading factor. In addition, the small-scale fading is characterized according to its probability distribution, the statistical parameters of the distributions are obtained based on the small-scale measurements. We also measured variations of receiving antenna height, ranging from 20cm, 50cm, 80cm, and 120cm above the ground, finding that the height has a strong influence on the propagation loss exponent, while the shadow variation shows a smaller variation. The model obtained is validated by the coefficient of determination and the root mean square error (RMSE) value.

Keywords—Archaeological park; LoRa; propagation model; statistics; near-ground

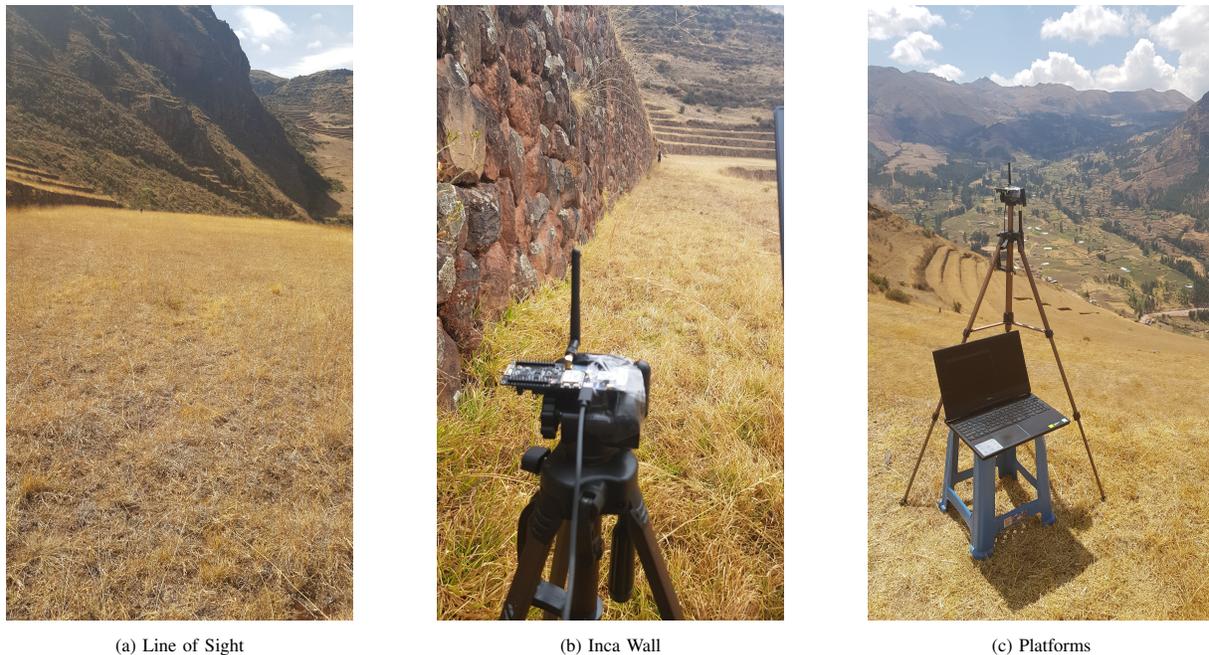
I. INTRODUCTION

Wireless Sensor network (WSN) applications are constantly increasing, some of them for smart cities, smart buildings, smart parks, smart farms, and recently some application in smart tourism, this is principally for the care of archaeological attractions and monitoring of tourist behavior. Cusco city has different archaeological places. Where it is important to use the technological tools to monitor the archaeological sites to conservation purposes. Internet of things applications are based in 5 layers [1]; perception, transport, processing, applications and business layer. Where perception layer is also known as data acquisition, and transport layer is based in the transfers of sensor data from perception layer to processing layer, in this layer different wireless technologies are used such as; WiFi, Bluetooth, Sigfox, LoRa and Cellular technology. In transport layer, Wireless technology choice is important, because it is necessary to consider; data transmission rate, bandwidth, frequency band (commercial or ISM (Industrial, Scientific or medical)), energy consumption and propagation channel. Therefore, propagation model is an essential tool for WSN planning and deployment [2]. Because, propagation model describes the radio channel characteristics for different environment such as forest, urban and indoor locations. This

model will allow the use of location algorithms based on RSS within an archaeological park environment in the city of Cusco or other parks with similar morphology environments. As in [3], where they work in the UHF band at 433 MHz using LoRa technology, within forestry scenarios described as a clear forest and a rubber plantation. Observing the attenuation of these forest scenarios versus a LOS scenario by obtaining the RSS value, also the variation of SF (Spreading Factor) and BW (BandWidth), to observe its impact on the LoRa signal, concluding that the propagation loss in a forest environment varies according to the configuration of the parameters of the LoRa signal. The vast majority of WSN studies near the ground show results in scenarios somewhat different from those found inside an archaeological park. [4] Therefore, a model suitable for this environment will be of great importance to ensure the deployment and operation of a communication system, as developed in [5], the localization by obtaining RSSI data from a network of sensors close to the ground over an area of an agricultural farm at the frequency of 868 MHz, with antenna heights of 40cm above the ground, and in [6] develops localization using RSSI with applications of LoRa technology at 868 MHz frequency through three localization algorithms, based on the simplified equation of the log distance model, but this time distance is the unknown variable, 100 RSSI samples are obtained throughout the indoor and outdoor scenarios, obtaining the a and n that characterize the canal of propagation of the LoRa signal. The research is organized as follows. Section II describes the archaeological park scenarios in more detail. Section III describes the equipment used and the methodology for obtaining the experimental data. Section IV presents the results obtained and the analysis of these results for each scenario, obtaining a model for each one of them. Finally, section V contains the conclusions.

II. NEAR GROUND SCENARIOS

Most studies were conducted for WSN applications with antenna height just above ground level, although a few consider the variation of this, but not uncommon scenarios such as archaeological parks. These scenarios close to the ground are usually very complex because they experience the reflection, obstruction, and absorption of the signal, produced in the soil, vegetation, and other scatterers present in the environment. As is the case in [7], measurements are performed in three different outdoor environments, at 2.4 GHz frequency, varying the antenna height, as well as the separation distance between them up to 100m, along a straight line. On the other hand, in



(a) Line of Sight

(b) Inca Wall

(c) Platforms

Fig. 1. Measurements Sites.

[8] an attempt is made to observe the influence of the antenna height against the important parameters within the modeling of the wireless propagation channel, obtaining values for each antenna height of the propagation loss exponent, shadowing factor, fading and propagation delay. For [9], measurements were made in the botanical park of the Florida institute of technology, at 1925 MHz with antenna height 20cm above the ground, obtaining the RSS value at variable distances of 5m meters difference, in turn at radial angles separated by 22.5 degrees along 128 measurement points with 300 samples for each one. [10] describes the NWB measurements in an agricultural field with 3 different types of terrain with directional antennas and identical omnidirectional antennas, with working frequencies of 868, 2400, and 5800 MHz, the measurements are developed at 20 and 40 cm above the ground, the received power data is obtained for each antenna and in turn for each antenna height, thus developing a model of 3 slopes, with 3 different values of propagation loss exponent. Similarly, for [11], measurements are made in an indoor scenario with antenna heights close to the ground at the 2.45 GHz frequency, showing how the propagation exponent varies with respect to the scatterers present in this indoor scenario.

Therefore, the correct modeling of the wireless propagation channel will be of utmost importance for the design and correct deployment of a wireless sensor network inside the archaeological park of Pisac, a clear example being [12], where the RSSI of a LoRa system is used to estimate the position in an indoor environment. In this work three different scenarios were selected, they are a large plain with a wide line of sight, the Inca walls, and the famous platform systems. The archeological park of Pisac is located in the district of the same name in the province of Calca in the department of Cusco, 32 km northwest of Cusco. It has an area of 9,063 hectares and a perimeter of 43,340 meters. The first scenario is located in

the qosqa sector where there is a flat area with a wide line of sight, with a width of 15 m and a length of 153 m, the ground is covered with grass 4 cm high, and the morphology is slightly undulating. Fig. 1a. The second scenario is the Inca walls, Fig. 1b, which are constructions made for containment purposes built with pebble stones. It has a cellular rig and convex profiles, masoned with clay mortar or mud, so they offer sufficient strength to remain largely intact until today. It has a variable height of 3 to 7 meters, with lengths of approximately 150m [13].

And finally, the terrace scenario found between the q'alla q'asa and q'antus raq'ay sector, like most of the terraces within this archaeological park, has a circular shape, as shown in Fig. 1c, have sizes from 3 to 8 meters, with lengths of approximately 190 meters. Within this scenario, the transmitting and receiving antennas were obstructed by some platforms, so it should be noted that some experimental data are given without line of sight.

III. MATERIAL AND METHODS

A. Hardware Setup

The experimental data collection was based on two TTGO T-Beam wireless nodes, one configured as a transmitter and the other as a receiver, the latter connected to a laptop to store the raw data (the value of the RSS (Received Signal Strength) variation is stored). The communication between the receiver node and the laptop is made use of the Arduino IDE development environment, and also makes use of Teraterm software for the conversion of data to an Excel workbook in .xlsx format for processing in Matlab. Some characteristics of the TTGO equipment are mentioned in Table I.

TTGO T-Beam nodes work in the unlicensed bands' ISM (Industrial, Scientific, and Medical), for this work we used the

band of 920 MHz since the 915 MHz band is licensed to the telecommunications company Viettel Peru S. A.C. in the 902-915 MHz frequencies, and according to the MTC [14] also the radio-communications services that operate in these bands must accept the harmful interference resulting from these applications and in no case will cause interference in the ISM applications. A pair of vertically polarized omnidirectional antennas with a gain of 3dBi is used, both antennas are connected to the transmitter and receiver via their SMA port, the transmitter emits a signal of +20 dBm. More information on TTGO T-Beam can be found at [15].

TABLE I. LoRa SIGNAL PARAMETERS [15]

PARAMETERS	SETTINGS
Transceiver Chip	Semtech LoRa SX1276
Bandwidth	500 KHz
Center Frequency	920 MHz
Power Transmission	+20 dBm
Transmission Speed	5470 bps
Spreading Factor	8

B. Measurement Methodology

The same methodology was used for the LOS and Inca walls scenarios. The receiver was fixed at variable heights of 20, 50, 80, and 120 cm, and the transmitter at 150 cm, the height of the receiving antenna was fixed at these heights, since we did not want to disharmonize the archaeological park, in addition to the existence of location signals with these sizes.

For the LOS scenario, the transmitter made a round trip in a straight line, with a total distance of 150m at a constant speed of 0.4 m / s, this to characterize the fading experienced by the propagation signal within this environment, about 4050 data were obtained per trip, it should be noted that within this first scenario no people were found so the variations are due to the movement of the transmitter and the geomorphology of the terrain. The measurements were made in a cold-dry climate with light wind currents.

For the scenario of Inca walls, the same methodology was used to obtain the experimental data, the receiving antenna was placed at a distance of 1m from the wall and then make straight stretches with the transmitter back and forth at the same constant speed of 0.4 m / s, the same variations in height of the receiver, until reaching the end of the wall, with a distance of 128m. A total of 2550 data were obtained. The measurements were performed with the same weather and light wind currents.

For our last scenario of Inca terraces, the methodology was changed since it is not possible to perform mobile measurements since these can reach heights of up to 8 m. Therefore, it was decided to take experimental data for each platform, obtaining 500 samples for each one of them, for a total of 13 platforms. The measurements were carried out in the same climate and with light wind currents.

IV. MEASUREMENT RESULTS AND ANALYSIS

For this research, the following distribution of tasks is taken into account for the correct analysis of measurement data. See Fig. 2.

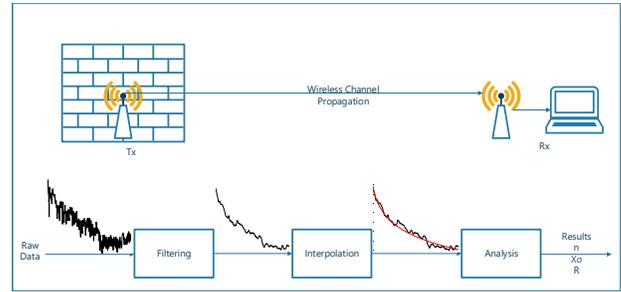


Fig. 2. Block Diagram of Measurements and Analysis of Data.

A. Extraction of Loss Propagation Exponent and Shadowing Fading

Once the experimental data were obtained, signal filtering was performed. The RSS data is passed through the moving average filter with a window length of 40λ [16] to separate the small-scale fading, see Fig. 3a-3b thus obtaining the large-scale fading, where the linear regression algorithm is applied in Matlab using the method of least squares and app curve Fitting, to obtain the signal parameters such as the exponent of the propagation loss, the reference power, and the standard deviation or shadowing.

With the data obtained after filtering, they resemble the logarithmic distance propagation loss model, where the propagation loss exponent indicates the change in propagation loss as a function of distance. The values of the exponent and shadow fading are extracted from the following equation 1 [17]:

$$Pr(d) = Pr_o + 10n\log_{10}(d) + X_\sigma [dB] \quad (1)$$

Where d is the variation distance between Tx and Rx in meters, $Pr(d)$ is the received power in dBm, and X_σ is a zero-mean log-normal random variable with standard deviation σ in dB, which expresses the shadow fading. Linear regression is used to obtain the propagation loss exponent n . The two-slope model is adopted to fit the experimental data on the Inca walls, using the equation 2 [18].

$$Pr(d) = \begin{cases} Pr(d_0) + 10n_1\log_{10}(\frac{d}{d_0}) + X_{\sigma_1} & (d \leq d_b) \\ Pr(d_b) + 10n_2\log_{10}(\frac{d}{d_b}) + X_{\sigma_2} & (d > d_b) \end{cases} \quad (2)$$

Small-scale signal variation is characterized by the Rician, Nakagami-m and Rayleigh distribution equations, these equations of these distributions are found in [19].

B. Modeling and Analysis

The variation of the measurements with respect to the height of the Rx antenna, after filtering as observed in Fig. 3c. Once the large-scale fading signal is obtained, the linear regression algorithm is used to obtain the values of the propagation loss exponent and the shading factor of this archaeological park. Using MATLAB software, the resulting equation was obtained, based on the equation 1, this model will be validated using two parameters, the residual standard deviation (σ) and the coefficient of determination (R^2). These parameters are shown in the Table II and Table III, for the one slope model and

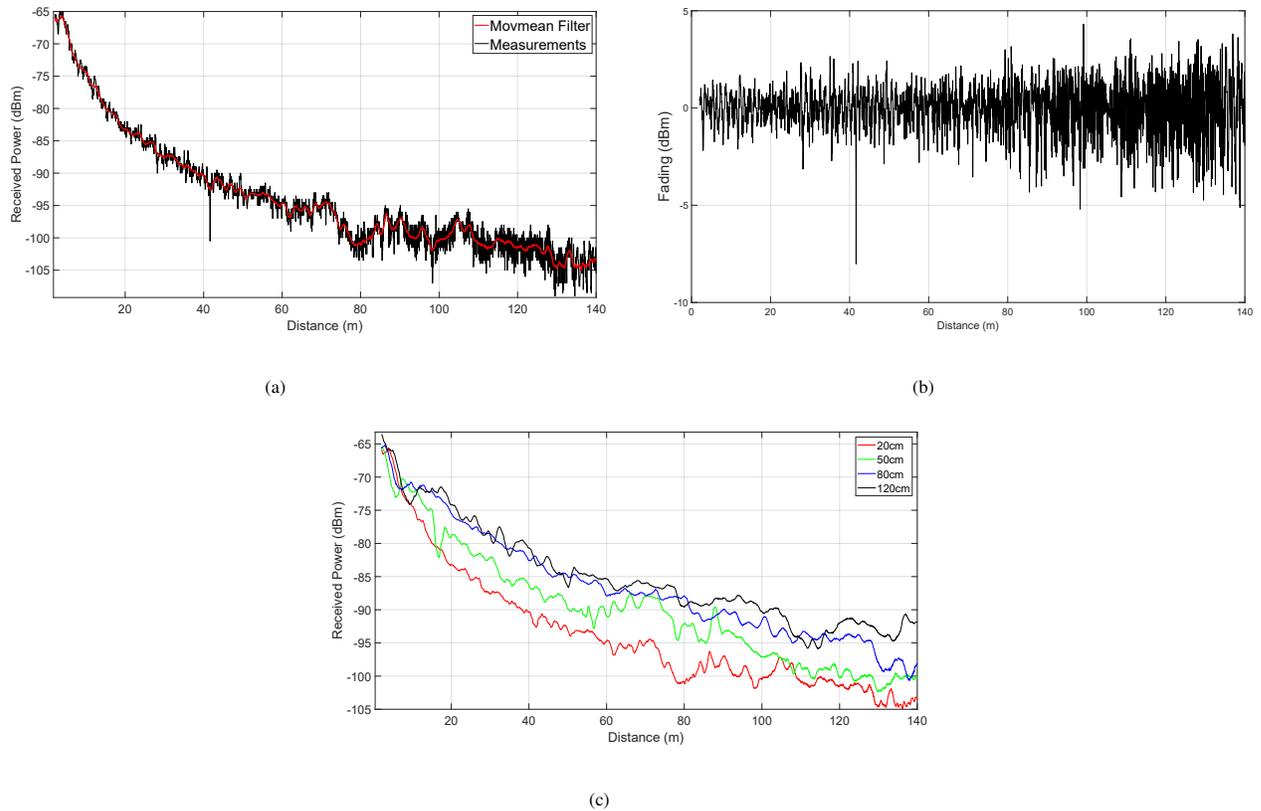


Fig. 3. Signal Filtering, (a) Measurements vs Moving Average Filter, (b) Small-Scale Signal, (c) Large-Scale Signal.

two slope model, respectively. The residual standard deviation measures the average deviation of the measured propagation losses from the values predicted by the fit model. If the value of σ is close to 0, it indicates a better fit. The coefficient of determination expresses the degree of success of the fit. If R^2 is close to 1 it means that the fit is optimal, the least-squares line fits the obtained data [20]. See Fig. 4a, 4b, 4c. It should be noted that our results are comparable to existing values in literature [8], [21], however, new values and aspects of antenna height and particular archaeological park scenarios are provided that are in accordance with intuition. The dependence on the height of the receiving antenna as well as the nature of the scenario is demonstrated since its value decreases as the height increases, the exponent values range between 1.9-2.4 for the LOS scenario, 2.1-2.7 for the wall scenario, and finally 1.3-1.4 on the platforms, the latter since the resulting height is the sum of the platform height and the antenna height. The shadowing variation is not strongly impacted by the height of the receiving antenna, the statistical distribution of shadowing is confirmed to have a normal distribution, with deviations ranging from 1.7-2 for the LOS scenario, 1.7-2.3 for walls, and 7.7-8.4 for platforms.

For the analysis of the fading, the Normal distribution models were used for shadowing fading, and for small-scale fading, Rice, Nakagami-m, and Rayleigh, each of which was simulated and contrasted with the measurements. As can be seen in the Fig. 5a, 5b. For the Shadowing data, it is again shown to have a normal distribution with mean zero and

standard deviation calculated according to the scenario. For the small-scale data, both the Rice and Nakagami-m distributions are appropriate for this archaeological park scenario.

V. CONCLUSION

In order to characterize the archaeological park of Pisac, we performed measurements at 920 MHz, obtaining the RSS value at different heights of Rx antenna, close to the ground so as not to affect the structural harmony of the same. The moving average filter is used to mitigate the small-scale fading, with a window of 40, obtaining the large-scale fading where we establish statistical models of propagation loss and also analyze the influence of the height of the receiving antenna and the geomorphology of the terrain. The linear regression for the experimental data indicates that the model based on the logarithmic distance performs an adequate characterization for scenarios close to the ground within this archaeological park since the values found are close to 2, the value of propagation loss exponent in free space, in addition to having adequate values for the determination coefficient R^2 and $RMSE$ or X_σ , on the other hand, it is observed that the dual-slope model shows greater accuracy in these scenarios, obtaining values of R^2 higher than the single-slope model. The small-scale signal fading statistics can be modeled as a nakagami-m distribution and a rice distribution, which show a considerable approximation with our samples. Additionally, the obtained model was compared with experimental data from another archaeological park, Chinchero, see Fig. 6, obtaining a value of R^2 equal to 0.9291, which indicates that the model fits the

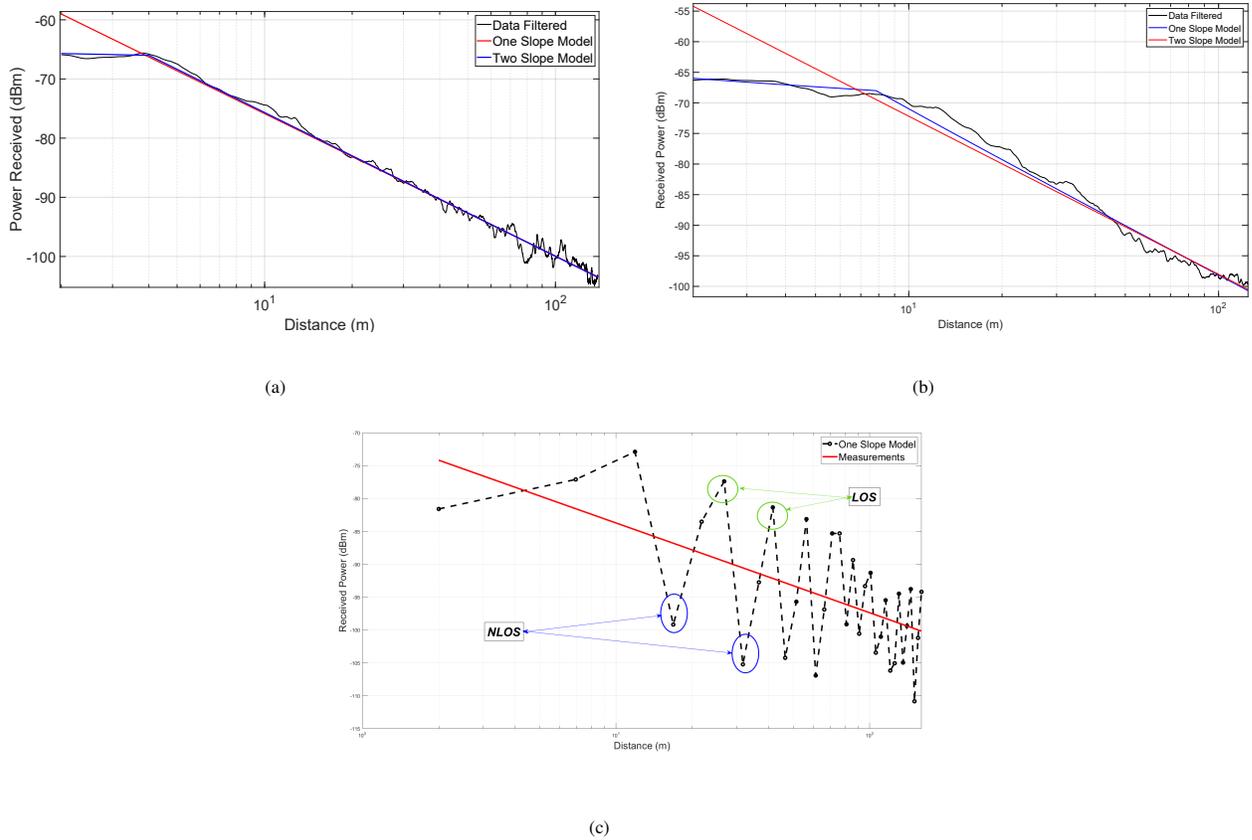


Fig. 4. Large-Scale Signal Modeling,
(a) Models for 20cm Rx Height in a Flat Environment, (b) Models for 50 cm Rx Height in an Environment of Inca Walls, (c) Models for 50cm Rx Height in a Platform Environment

TABLE II. LARGE SCALE FADING CHARACTERISTICS FOR LOS, INCA WALLS AND PLATFORMS- ONE SLOPE MODEL

Height (cm)	Line of Sight			Inca Walls			Platforms		
	n	X_{σ} (dB)	R^2 (%)	n	X_{σ} (dB)	R^2 (%)	n	X_{σ} (dB)	R^2 (%)
20	2.408	1.196	0.9825	2.774	2.113	0.9610	1.285	8.342	0.3135
50	2.249	2.082	0.9419	2.514	2.0	0.9575	1.444	7.732	0.4017
80	2.142	1.958	0.9433	2.407	2.343	0.9377	1.362	8.401	0.3359
120	1.949	1.754	0.9449	2.102	1.719	0.9553	1.366	8.065	0.3556

experimental data optimally, validating our model in another archaeological park scenario with similar morphology of the environment. A report on the measurement campaign of the propagation channel by means of mobile measurements with variable antenna height is provided, proving once again the dependence of the propagation signal with the separation distance between Tx and Rx, so that new values of propagation exponent, shadowing factor and small-scale signal distributions were also provided, for archaeological park scenarios, which vary in morphology to those developed in other investigations. Finally, it is concluded that, for the correct study and analysis of the deployment and operation of a sensor network, an adequate propagation model with parameters adjusted to the different scenarios within the archaeological parks must be taken into account. These models could be used as tools for the

implementation of object localization based on the trilateration algorithm using RSSI. In addition to obtaining the path loss equation that will provide the coverage area.

ACKNOWLEDGMENT

The authors acknowledge funding support from CONCYTEC-PROCIENCIA and The World Bank within the call E041-2018 [contract number 128-2018-FONDECYT-BM-IADT-SE].

REFERENCES

- [1] I. Mashal, O. Alsaryrah, T.-Y. Chung, C.-Z. Yang, W.-H. Kuo, and D. P. Agrawal, "Choices for interaction with things on internet and underlying issues," *Ad Hoc Networks*, vol. 28, pp. 68–90, 2015.

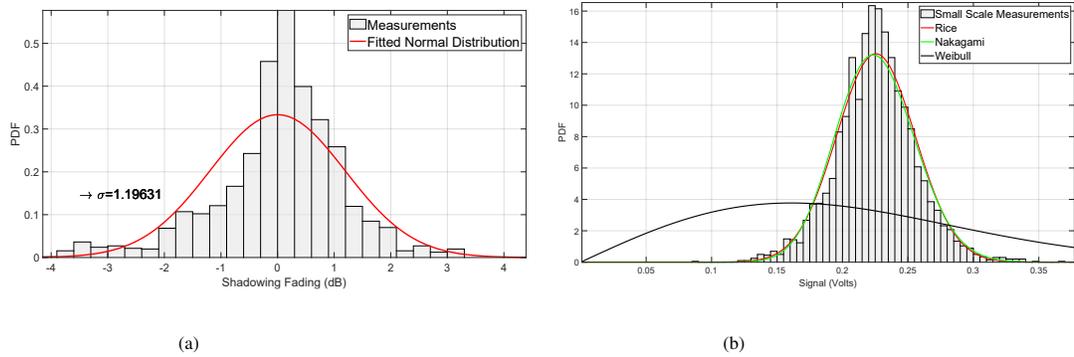


Fig. 5. Signal Fading Models,

(a) Model Shadowing Fading for 20cm in an Environment of LOS, (b) Models for Small-Scale Fading for 80cm in an Environment of Inca Walls.

TABLE III. LARGE SCALE FADING CHARACTERISTICS FOR LOS, INCA WALLS AND PLATFORMS- TWO SLOPE MODEL

Two Slope Model								
Height (cm)	Line of Sight				Inca Walls			
	n1	n2	X_σ (dB)	R^2 (%)	n1	n2	X_σ (dB)	R^2 (%)
20	0.1	2.43	1.0975	0.9857	0.1	3.17	1.5691	0.9784
50	0.7	2.28	1.8589	0.9537	0.3	2.67	1.2441	0.9836
80	0.8	2.14	1.6362	0.9604	0.6	2.52	1.6741	0.9682
120	1	2.07	1.4847	0.9605	0.9	2.17	1.4439	0.9684

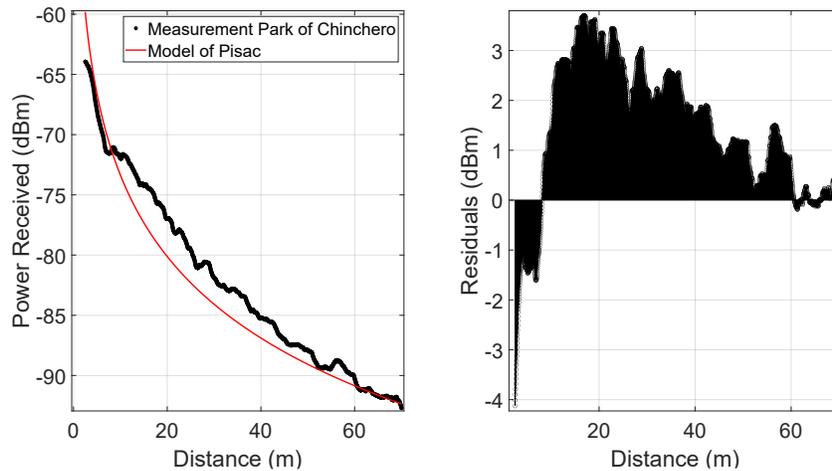


Fig. 6. Model of Pisac Vs Measurement in Park Archaeological of Chinchero.

- [2] J. Karedal, S. Wyne, P. Almers, F. Tufvesson, and A. F. Molisch, "A measurement-based statistical model for industrial ultra-wideband channels," *IEEE transactions on wireless communications*, vol. 6, no. 8, pp. 3028–3037, 2007.
- [3] K. A. Ahmad, M. S. Salleh, J. D. Segaran, and F. R. Hashim, "Impact of foliage on lora 433mhz propagation in tropical environment," in *AIP Conference Proceedings*, vol. 1930, no. 1. AIP Publishing LLC, 2018, p. 020009.
- [4] W. Tang, X. Ma, J. Wei, and Z. Wang, "Measurement and analysis of near-ground propagation models under different terrains for wireless sensor networks," *Sensors*, vol. 19, no. 8, p. 1901, 2019.
- [5] W. T. EL-Gzzar, H. B. Nafea, and F. W. Zaki, "Application of wireless sensor networks localization in near ground radio propagation channel," in *2020 37th National Radio Science Conference (NRSC)*. IEEE, 2020, pp. 145–154.
- [6] E. Goldoni, L. Prando, A. Vizziello, P. Savazzi, and P. Gamba, "Experimental data set analysis of rssi-based indoor and outdoor localization in lora networks," *Internet Technology Letters*, vol. 2, no. 1, p. e75, 2019.
- [7] D. Wang, L. Song, X. Kong, and Z. Zhang, "Near-ground path loss measurements and modeling for wireless sensor networks at 2.4 ghz," *International Journal of Distributed Sensor Networks*, vol. 8, no. 8, p. 969712, 2012.
- [8] S. Sangodoyin, S. Niranjayan, and A. F. Molisch, "A measurement-based model for outdoor near-ground ultrawideband channels," *IEEE Transactions on Antennas and Propagation*, vol. 64, no. 2, pp. 740–751, 2015.
- [9] A. Alsayyari, I. Kostanic, C. E. Otero, and A. Aldosary, "An empirical

- path loss model for wireless sensor network deployment in a dense tree environment,” in *2017 IEEE Sensors Applications Symposium (SAS)*. IEEE, 2017, pp. 1–6.
- [10] H. Klaina, A. Vazquez Alejos, O. Aghzout, and F. Falcone, “Narrow-band characterization of near-ground radio channel for wireless sensors networks at 5g-iot bands,” *Sensors*, vol. 18, no. 8, p. 2428, 2018.
- [11] M. Salim, K. Sayidmarie, and A. Aboud, “Investigation of indoor propagation of wlan signals,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 16, no. 3, pp. 1356–1363, 2019.
- [12] S. Kavetha and et al, “Indoor positioning utilizing bluetooth low energy rssi on lora system,” *Indonesian Journal of Electrical Engineering and Computer Science*, vol. 23, no. 2, pp. 927–937, 2021.
- [13] A. Chalco Salas, “Andenerías prehispánicas y gestión de riesgos. análisis de su puesta en valor como factor de desarrollo cultural, pisacusco,” 2017.
- [14] M. de Transportes y Telecomunicaciones MTC, “Registro nacional de frecuencias- bandas de 899 – 915 mhz y 944 – 960 mhz.pdf[online],” <https://www.gob.pe/institucion/mtc/informes-publicaciones/343585-registro-nacional-de-frecuencias, 2019>.
- [15] K. Gabriel, “Ttgo-t-beam-car-tracker,” <https://github.com/kizniche/ttgo-tbeam-ttn-tracker>, 2019.
- [16] A. F. Molisch, *Wireless communications*. John Wiley & Sons, 2012, vol. 34.
- [17] A. Goldsmith, *Wireless communications*. Cambridge university press, 2005.
- [18] T. S. Rappaport *et al.*, *Wireless communications: principles and practice*. prentice hall PTR New Jersey, 1996, vol. 2.
- [19] S. R. Saunders and A. Aragón-Zavala, *Antennas and propagation for wireless communication systems*. John Wiley & Sons, 2007.
- [20] L. R. Ojeda, “Probabilidad y estadística básica para ingenieros,” *Ecuador: Escuela superior politécnica del litoral*, 2007.
- [21] J. Molina-Garcia-Pardo and et al, “Channel model at 868 mhz for wireless sensor networks in outdoor scenarios,” in *Proc. International Workshop on Wireless Ad-Hoc Networks (IWWAN 2005)*, 2005, pp. 2–5.

Development of Predictions through Machine Learning for Sars-Cov-2 Forecasting in Peru

Shalóm Adonai Huaraz Morales¹, Marissel Fabiola Mio Antayhua², Laberiano Andrade-Arenas³
Faculty of Sciences and Engineering
Universidad de Ciencias y Humanidades
Lima, Perú

Abstract—The SARS-COV-2 virus of the coronavirus family was identified in 2019. This is a type of virus that infects humans and some animals, in Peru it has seriously affected everyone, causing so many deaths, which has resulted in that people be tested to rule out contagion, using laboratory methods recommended by the government of the country. Therefore, the data science methodology was used with this research, where its objective is to predict what types of people are contaminated during SARS-COV-2 by the regions of Peru, identified through laboratory methods, therefore, the "data bank" was taken by PND, the CSV file was used for that study, apart from the fact that it comes from the INS and the CDC of the MINSA. In which, machine learning was developed with the decision tree algorithm and then began coding, in such a way that the distribution called Anaconda was used where it is encoded in Python language, together with that distribution, Jupyter Notebook was used which is a client-server application. The results generated by this research prove that it was possible to identify the types of individuals by SARS-COV-2. These results can help prevention entities against SARS-COV-2 to apply the corresponding preventive measures in a more focused way.

Keywords—Forecast; laboratory methods; machine learning; Python; SARS-COV-2

I. INTRODUCTION

Since SARS-COV-2 affected all the countries of the world it has led to several deaths, for which the impact that laboratory methods have come to have been beneficial since they are used for the detection of the virus avoiding this way its spread, also the use that is given to these methods are diverse, which can be used for people who have had contact with the virus, [1] people with symptoms of SARS-COV-2 and people who want to know if they have had the virus. However, this is not far from economic reactivation since to travel or for people who have been infected and want to return to work, they are asked to do laboratory methods and consequently to show their medical certificate that proves the negative result by SARS-COV-2 [2].

In Peru, the detection by SARS-COV-2 for laboratory methods has been difficult for the population, because some people do not have enough money to be tested, since the costs of these laboratory methods are high and range between 700, 400, 230, and 190 soles; therefore, the insufficiency of this spending has led to more citizens becoming infected with this virus, [3] however, it can be mentioned that in other countries such as Austria and Germany the laboratory methods are free since they are provided by the government.

The importance of this study is "rooted" in reaching the greatest intellect concerning laboratory methods, this is done

to know which laboratory methods are most used in each region of Peru since this gives us indications of that "type of individuals" (Individuals who have been in possible contact with the virus, with symptoms of SARS-COV-2 and who want to know if they have had the virus) live in the majority in each region and thus be able to apply the corresponding preventive measures.

The present study will focus on knowing what "type of individuals" exist in the regions of Peru since due to the infection for SARS-COV-2, different laboratory methods have been generated focused on different individuals. Precisely, this study will provide an enormous advantage because thanks to it, prevention entities against SARS-COV-2 will be able to apply the corresponding preventive measures in a more focused way; in addition to deepening the knowledge about machine learning, with which the work of these entities will be more productive and in this way they will acquire adaptation to the novelty of the environment in which they live.

How will implementing machine learning in positive cases of SARS-COV-2 by laboratory methods stop the pandemic in Peru?

The objective of this analysis is to "unwind" predictions through machine learning in order to optimally forecast SARS-COV-2 in Peru and thus ensure that prevention entities against SARS-COV-2 can apply the corresponding preventive measures in a more effective way focused.

Section II explains the literature review, Section III explains the methodology, Section IV explains the results and discussions, and finally Section V discusses the conclusions and future work.

II. LITERATURE REVIEW

The study carried out allowed to determine the progress of the set of knowledge applied in the articles concerning machine learning since they show its benefits from allowing computers to learn by themselves to perform tasks independently, as well as its progress with the applied methodologies, which showed correct employability.

These methodologies are used by data scientists since they convert massive information into "useful answers", this is done through a variety of knowledge that they use to analyze the information and thus collect useful data that comes from all kinds of sources.

Regarding the methodology that was carried out in the studies concerning machine learning, the articles report its

relationship with data science, these methodologies reflected in the articles are adaptations of more complete methodologies, which means that these methodologies themselves, although they are varied, from a conglomerate that reinforces the machine learning used for their respective results.

Thus [4], it exposes a problem on how to stop the spread of SARS-COV-2, in it, it refers to the asymptomatic since they do not present symptoms generate a problem at the moment of fixing individuals with this virus of those who do not, therefore, he proposes to carry out tests to identify the virus.

Also [5], mention of the tests is mentioned as a prelude to the outbreak of SARS-COV-2 infections, focusing on providing prediction systems to diagnose individuals with this virus, this made it possible through data mining and machine learning algorithms.

In the same way [6], he maintains that the tests have been beneficial when detecting the invasion and multiplication of pathogens in the tissue of an organism for SARS-COV-2 at the time of commenting as a principle his article that paramedical companies are affirming the development of a vaccine.

Something similar occurs with [7], whose purpose is to evaluate the identification of SARS-COV-2 with diagnostic tools such as pathogenic tests by name at the beginning of the "battle" against the transmission of said virus, emphasizing the mandatory detection of contaminated patients. On the other hand [8], it communicates in its problem the lack of access to test kits by pointing out the scope of SARS-COV-2 as openness and concerns about the accuracy of the counts of cases of this virus, focusing on the early stages of the pandemic concerning its scope, characteristics and its impact on health and society.

Something similar occurs [9], which indicates that the availability of diagnostic tests being limited leads health officials to suggest that only a "group" of people need to look for the "fact" or "evidence" that confirms the invasion, and multiplication of pathogens in the tissue of an organism for SARS-COV-2 by determining in the beginning that many of those who were infected were asymptomatic or showed symptoms, also emphasizing that the virus became a global crisis around health.

With the same approach [10], they aim to carry out a predictive model for the evaluation of disease using statistical analysis and a data mining solution known as SAP Predictive Analytics.

In a different context [11], with the studies shown above, it stands out that x-rays and computed tomography scans are exceptional complements to RT-PCR tests, which are a variant of PCR tests by establishing at first that CT scans alone can generate negative predictive value.

In a different environment [12], with the analyzes indicated above, it stands out that the automated bilateral trading model uses a metaheuristic algorithm called OSA and chaos theory, which are used to adapt trading strategies.

In summary, with what has been examined in the various studies that used different methods to solve their respective problems according to their studies that are taken here as a reference, it can be said that the authors worked to solve the SARS-COV- 2, that is why they correctly raised their studies,

applying their methodologies and determining the approach to this virus. Using clinical information to obtain essential characteristics, valuable data was extracted that was used in machine learning algorithms (Decision tree, regression, neural networks, among others) to classify these data and yield high levels of precision, which resulted in a score successful to solve their corresponding problems.

Another important factor that these studies show is the efficiency of their models since they improve the behavior of the data in addition to showing a conglomeration of types of machine learning to solve their problems by performing tests that confirm their efficiency; based on this, the evaluation of the applied algorithms is also carried out to define the best result that conforms to reality. It is worth mentioning that this was a challenge for these authors since this infers the "creation" of a predictive model in an environment of affection towards SARS-COV-2 where they had to perform deep analysis to find information that supports their prediction algorithm which will help doctors in making decisions. However, the authors emphasized investigating more about the fusion of machine learning with other disruptive technologies that have been projected for the year 50, such as the Internet of Everything (IoE) and the blockchain, which is why it is here that the lack of research on the fusion of the methodology, as well as with other relevant topics, to achieve a greater contribution in the line of forecasting with machine learning.

III. METHODOLOGY

From here, the methodology is explained which belongs to the development by predictions through machine learning, towards the forecast from positive events, obtaining as such the objectives presented based on this methodology that belongs to the sample in Fig. 1.



Fig. 1. Data Science.

A. Stages of the Methodology

1) *Analytic Approach*: This first path [13], which is "covered" in the methodology, will occur thanks to the stability and constancy of carrying out a meaningful and detailed analysis, facilitating and making development possible to locate the stability and constancy expected in support of the problem

proposed, and thus obtain an expected result, benefiting that analytical approach is where the analytical idea that is presented for acceptance and conformity "starts" from.

2) *Data Requirements*: This second path [14], which is "covered" in the methodology, immediately fixes questions to obtain information: What data will be essential? Where will we get these data from? Once the answer has been obtained from these doubts, it is necessary to "draw" the course towards answering the doubts from the subsequent journeys: From what way will these data be "harvested"? Understand this data? How will these data be used to provide realization to the analytic idea? It is in this "place" where it is necessary to have an understanding and mastery of the problem since this "element" is decisive to achieve a specific definition of the data that will be required.

3) *Data Collection*: This third path [15], which is "covered" in the methodology, tells us that after finding the essential data and the source from which these data will be obtained, we have to "collect" the data from these various origins located in the study, in this "place" is where you will get a definition of the beginning of the data as well as the criterion "spent" in order to collect them.

4) *Data Understanding*: This path [16], which is "covered" in the methodology, verbalizes us which, after having found the set of information that will be essential with the object from the solution of the problem, belongs to having to "insist" on the examination of that information, managing to capture its unusual variables as well as formats, this helps us to have a clear idea of the data available and thus occupy optimal solutions based on its condition.

5) *Data Preparation*: This fifth path [17], which is "covered" in the methodology, is very "hard" since in this "place" is where the data has to be "washed", refining and "pushing" them, in that washing, refining, and impulse identifies missing data problems, unauthorized elements, double elements, which are to be solved, since in this "place" is where a group of "washed" data will be collected and prepared to be used in the model.

6) *Modeling*: This sixth path [18], which is "covered" in the methodology, verbalizes us which then has the group of information "washed" as well as prepared with the matter of being used in the model, it is located as the model is erected, how it is ready to resolve the problem in dispute, also of adapting with the elements in a very "pleasant" and optimal way; in this path, the model is set with the "materialization" of machine learning from the elements, as well as adapting the model based on objective and characteristics.

7) *Evaluation*: This seventh [19], as well as the last path, that is "traveled" in the methodology is very significant since it tells us that it is necessary to assess the model by checking it with other data and to contemplate what happens, this tries to say that this path establishes that "true" or it is not the model-based accordingly to the "revision".

B. Development of the Methodology

1) *Analytic Approach*: This trajectory of the data science methodology, after fixing the problem, the question was resolved. What analytical approach is great in order to fix the

problem? In order to replicate that question, a "tracking" identifying the ideal analytical approach and thus hitting the problem, in such event it is arranged to forecast the number of types of individuals infected by SARS-COV-2 identified through laboratory tests, which makes us deduce that they are preparing to carry out a predictive model, in order to "speak" it in some "short" way, a predictive model is a group of procedures "worked" through specialized computer knowledge which provides help in order to specify the probability that specific preconditions occur or precursors to its consequence. After that short, although considerable allusion. What is a predictive model? This study tells the object of solving where it was preferred to choose the decision tree model, what is a group from "components" of the potential repercussions from a collection of linked resolutions in support of comparing possible "behaviors" with each other, aimed at foreseeing the "ideal" alternative. This decision tree begins with a node and then diversifies into potential consequences, all these consequences "found" nodes, which are diversified into more options, that decision tree is "calculated" with three classes of nodes, firstly the so-called node of decision what demonstrates a resolution that will "occupy", secondly the so-called probability node that demonstrates the possibilities of some consequences, as well as, finally, although equally significant, the terminal node that demonstrates the conclusive consequence from a "means" of resolution. Those elements of the decision tree constituted can be observed in Fig. 2.

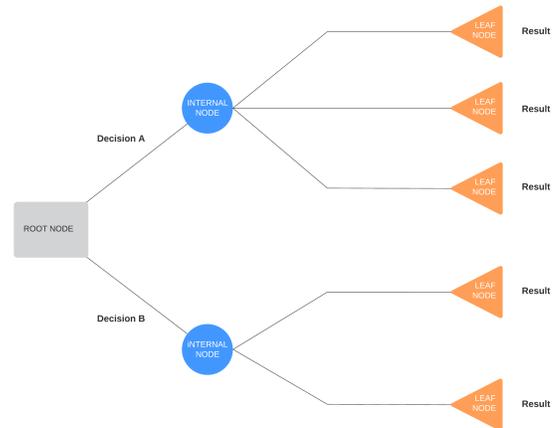


Fig. 2. Decision Tree.

2) *Data Requirements*: In the first place, in the development of this path, it goes on to refer that the progress that comes from there is considerable since the "answer" of the problem is based on that, that path tells us that it is necessary to locate the data to that in "reason" to that the following trajectories of collecting, understanding and preparing the data are to be executed as well as to be able to be solved the respective problem. In this course of the data science methodology, the "material", the "forms" and the sources of the essential data were specified; for this reason, the National Open Data Portal (PNDA) dealt with how in "easy" expressions a web for collecting information is, that web is made up of three drop-down lists, firstly the named categories, which declares us a classification grouping of conformity with the dear criterion, that of the second place named labels which

helps to provide order and a purpose that the category drop-down list does not provide, that is to say, that the labels show the most “attractive” “material”, and finally although equally considerable the named format the one that helps with the purpose of knowing the modality by how the data is ordered as well as it is encrypted in a computerization filing cabinet. The PNDA, thanks to its technical and normative tools of the public function and to establish itself as the computer focus of the government of Peru, was chosen since due to its “ordering” mode, it is great with the data requirements of this study, since with the In order to give a “remedy” to this study, the Comma Separated Values (CSV) file was used, apart from the fact that it was “born” from the National Institute of Health (INS) as well as from the Peru’s National Center for Epidemiology, Prevention and Disease Control (CDC) of the Ministry of Health (MINSA). That is why “now” you have the “material”, text file, as well as the origin of the information.

3) *Data Collection:* After having the data collection, the availability of the total of the essentials was established to provide a “remedy” to the problem, with which it lends itself to analyze the data requirements to find out if a little data was not required. of the data already obtained. Already mentioned the means of the data to give a “remedy” to that study, which is a PNDA CSV file, it should be noted that this file consists of data that can be easily ordered and processed. Coding began, for this purpose, the distribution called Anaconda was used, which is coded in Python language, together with that distribution, Jupyter Notebook was used, which is a client-server application. First, the “pandas” module was downloaded and it was given the nickname “pd”, this was used to “go” to the data of a data structure with two dimensions, later the path of the file belonged to a variable a a more “personable” entrance; later it was consulted as well as I save the information in a data structure with two dimensions with title of covid_positive_methods_data, apart from dividing the values with the argument “sep”; in addition, the print() function was handled in order to “publish” a text. That can be checked in Fig. 3, Fig. 4, Fig. 5 and Fig. 6.

```
# import numpy library
import numpy as np
```

Fig. 3. Imports for the Data Frame.

```
route = 'positivos_covid.csv'
message = "File path"
print(message)
File path
```

Fig. 4. File Path.

Later it belonged to use “pandas.DataFrame.columns” in order to demonstrate the flags of the “pillars” from a data structure with two dimensions “covid_positive_methods_data”. This can be verified in Fig. 7.

Soon the head() function was handled in order to demonstrate the primary 5 “ringlas” from a data structure with

```
import pandas as pd
message = ("The pandas library is imported and pd is assigned as pandas\n"
          "aliases, this library is imported to use the read_csv()")
print(message)
```

The pandas library is imported and pd is assigned as pandas aliases, this library is imported to use the read_csv()

Fig. 5. Import Pandas Library to Read Data Frame.

```
# File 'covid_positive_methods_data' read by read_csv(), located in 'route' and separated by semicolons by the sep parameter
covid_positive_methods_data = pd.read_csv(route, sep=";")
covid_positive_methods_data
```

	FECHA_CORTE	DEPARTAMENTO	PROVINCIA	DISTRITO	METODOOX	EDAD	SEXO	FECHA_RESULTADO	UBIGEO	id_persona
0	20210915	LIMA	LIMA	SAN MARTIN DE PORRES	PR	25.0	MASCULINO	20201217.0	150135.0	24662153.0
1	20210915	ICA	PISCO	PISCO	PR	20.0	FEMENINO	20200822.0	110501.0	24662175.0
2	20210915	HUANUCO	HUANUCO	HUANUCO	PR	22.0	FEMENINO	20200729.0	100101.0	24662197.0
3	20210915	ANCASH	SANTA	SANTA	AG	18.0	FEMENINO	20210630.0	21808.0	24662204.0
4	20210915	ANCASH	SANTA	NUEVO CHIMBOTE	AG	17.0	MASCULINO	20210404.0	21809.0	24662207.0
...
2164375	20210915	LIMA	LIMA	LINCE	AG	12.0	MASCULINO	20201008.0	150116.0	NaN
2164376	20210915	LIMA	LIMA	LINCE	AG	12.0	MASCULINO	20201009.0	150116.0	NaN
2164377	20210915	LIMA	LIMA	SAN MARTIN DE PORRES	PCR	20.0	MASCULINO	20210131.0	150135.0	NaN
2164378	20210915	LIMA	LIMA	LIMA	PCR	32.0	FEMENINO	20210809.0	150101.0	NaN
2164379	20210915	LIMA	LIMA	MIRAFLORES	PCR	56.0	FEMENINO	20210430.0	150122.0	NaN

2164380 rows x 10 columns

Fig. 6. Data Reading.

```
# Tags for file 'covid_positive_methods_data'
labels = covid_positive_methods_data.columns
labels
Index(['FECHA_CORTE', 'DEPARTAMENTO', 'PROVINCIA', 'DISTRITO', 'METODOOX',
       'EDAD', 'SEXO', 'FECHA_RESULTADO', 'UBIGEO', 'id_persona'],
      dtype='object')
```

Fig. 7. Data Frame Labels.

two dimensions “covid_positive_methods_data”. This is checked in Fig. 8.

```
# First 5 rows of covid_positive_methods_data
covid_positive_methods_data.head()
```

	FECHA_CORTE	DEPARTAMENTO	PROVINCIA	DISTRITO	METODOOX	EDAD	SEXO	FECHA_RESULTADO	UBIGEO	id_persona
0	20210915	LIMA	LIMA	SAN MARTIN DE PORRES	PR	25.0	MASCULINO	20201217.0	150135.0	24662153.0
1	20210915	ICA	PISCO	PISCO	PR	20.0	FEMENINO	20200822.0	110501.0	24662175.0
2	20210915	HUANUCO	HUANUCO	HUANUCO	PR	22.0	FEMENINO	20200729.0	100101.0	24662197.0
3	20210915	ANCASH	SANTA	SANTA	AG	18.0	FEMENINO	20210630.0	21808.0	24662204.0
4	20210915	ANCASH	SANTA	NUEVO CHIMBOTE	AG	17.0	MASCULINO	20210404.0	21809.0	24662207.0

Fig. 8. First Rows of the Data Frame.

Finally, the shape() function was used to demonstrate the size of a two-dimensional data structure, which is intended to indicate that the chosen data group named “covid_positive_methods_data” is consigned with 2 164 380 rows with 10 columns. This can be checked in Fig. 9.

```
# Dimension of 'covid_positive_methods_data'
covid_positive_methods_data.shape
(2164380, 10)
```

Fig. 9. Information Frame Size.

4) *Data Understanding:* In this path, the methodology expects to have an obvious view of the data, observed in the data collection. There you want to learn from the data to locate

problems and have knowledge regarding the “material”, in that case, they identified problems, even so, the experience was gained regarding the data. In the coding, it is reflected that “re” was used which is a module with regular expressions that can be seen in Fig. 10, then the nested loop “for” was used this is a loop that is located inside another loop as for the primary cycle, a variable named “label” was used with the iterable named “labels” this is a “repertoire” of the headers that is arranged in a data structure with two dimensions and with the second cycle a variable was used named “coincidence” for the iterable [(re.compile(".*A.*")).search(label)] where “search()” finds patterns in the text that have the character “A”, and the body of the loop has a conditional expression “if” for the condition of “coincidence” and with the “command” of “print()” that shows the information on the screen of “party.group(0)” that “publishes” the variable “coincidence” finding the “word” of agreement with “group(0)”. This can be demonstrated in Fig. 11, Fig. 12 and Fig. 13 in long and short coding each.

```
import re
message = "The re library is imported to use compile()"
print(message)
The re library is imported to use compile()
```

Fig. 10. Importing Re for Matches.

```
pattern = re.compile(".*A.*")
message = ("Use of compile() so that '.*A.*' is used as a pattern in search(),\n"
"and thus search() searches 'label' for a match with the pattern")
print(message)
Use of compile() so that '.*A.*' is used as a pattern in search(),
and thus search() searches 'label' for a match with the pattern
```

Fig. 11. Pattern to Find the Match.

```
# In 'coincidence' the match searched for by
# search() is saved and group(0) returns the
# 'match' of the 'coincidence'

for label in labels:
    for coincidence in [pattern.search(label)]:
        if coincidence:
            print(coincidence.group(0))

FECHA_CORTE
DEPARTAMENTO
PROVINCIA
EDAD
FECHA_RESULTADO
```

Fig. 12. Nested Data Frame Loop (Long).

```
# Encoding on one line to return matches
print([coincidence.group(0) for label in labels for coincidence in [pattern.search(label)] if coincidence])
['FECHA_CORTE', 'DEPARTAMENTO', 'PROVINCIA', 'EDAD', 'FECHA_RESULTADO']
```

Fig. 13. Nested Data Frame Cycle (Brief).

5) *Data Preparation:* From this path of the data science methodology, unwanted “components” were eliminated, it should be noted that this path together with the path of data collection and understanding of data are the paths of long duration in research. That journey began the transition of the elements, this was carried out to use the elements in a very significant way, with which in this “place” is where

how the data was elaborated concerning missing elements, not applicable elements, and double elements to secure the data to stay “finished” for the model. Likewise, in this path the characteristics will be fixed since this is significant because it is used in the model, this is the “contraption” to give the solution to the problem posed, and to finish that path, it is the one that fixes the totality of what is essential for the model preparation path since that ensures the elements which were used in the machine learning algorithm, which is decision tree. First of all, i verify elements to determine if it is essential to “wash” them, for which “pandas.Series.value_counts” was used, which shows a series that stores counts in descending order of unique elements, it should be noted that “pandas.Series.value_counts()” does not count NA elements. When contemplating the frequency board, it can be seen that the heading is specified in another language for which it is incorrect, it is also considered that the way the elements are “printed” is a lack of respect since the totality is in capital letters, it is also contemplated that double elements subsist, and to conclude, very few people are considered per district, which has the possibility of leading to an erroneous forecast. This can be foreseen in Fig. 14.

```
# frequency table
(covid_positive_methods_data["DISTRITO"]
.value_counts())

EN INVESTIGACIÓN      108185
LIMA                   73903
SAN JUAN DE LURIGANCHO 73580
SAN MARTIN DE PORRES   51930
JESUS MARIA           49078
...
SAN JOAQUIN            1
SANTIAGO DE TUNA       1
YAUJA                  1
RECTA                  1
LAHUAYTAMBO           1
Name: DISTRITO, Length: 1697, dtype: int64
```

Fig. 14. Table of Frequency.

Here we will begin to demonstrate the way where the problems “formulated” in Fig. 14 were solved, to begin with, the “designation” of the headers was repaired, for that reason “pandas.DataFrame.columns” and “pandas.DataFrame.values” were used what in group shows the array of elements that appear in the upper margin of columns of the data frame “covid_positive_methods_data”, that preserved an element “column_names” which later he used to get his data, that was “applied” through correlative numbers, now the correlative numbers have been located, he repaired appointments that appear in the upper margin, that can be seen in Fig. 15.

After the elements of the rows were repaired, this was “materialized” through “pandas.DataFrame.loc” which enters a grouping of rows from the label, those rows from the label was fixed through the bracket of “pandas.DataFrame.loc” “[covid_positive_methods_data['SEX'] == 'MALE', 'SEX']” which indicates this grouping of rows where you entered is “SEX” from the tag “[covid_positive_methods_data['SEX'] == ' MALE']”, subsequently began to “amend” the elements of the rows, this allows it to be “examined” in Fig. 16.

Afterward, how there are “printed” elements were repaired so that they are “printed” with consideration, in which case it was chosen to leave the first letter of any of the printings

```
# Fix the name of the column
column_names = covid_positive_methods_data.columns.values
column_names[0] = "CUT_DATE"
column_names[1] = "DEPARTMENT"
column_names[2] = "PROVINCE"
column_names[3] = "DISTRICT"
column_names[4] = "DXMETHOD"
column_names[5] = "AGE"
column_names[6] = "SEX"
column_names[7] = "RESULT_DATE"
column_names[8] = "UBIGEO"
column_names[9] = "person_id"
covid_positive_methods_data.columns = column_names

covid_positive_methods_data
```

	CUT_DATE	DEPARTMENT	PROVINCE	DISTRICT	DXMETHOD	AGE	SEX	RESULT_DATE	UBIGEO	person_id
0	20210915	LIMA	LIMA	SAN MARTIN DE PORRES	PR	25.0	MASCULINO	20201217.0	150135.0	24662153.0
1	20210915	ICA	PISCO	PISCO	PR	20.0	FEMENINO	20200822.0	110501.0	24662175.0
2	20210915	HUANUCO	HUANUCO	HUANUCO	PR	22.0	FEMENINO	20200729.0	100101.0	24662197.0
3	20210915	ANCASH	SANTA	SANTA	AG	18.0	FEMENINO	20210630.0	21809.0	24662204.0
4	20210915	ANCASH	SANTA	NUEVO CHIMBOTE	AG	17.0	MASCULINO	20210404.0	21809.0	24662207.0
...
2164375	20210915	LIMA	LIMA	LINCE	AG	12.0	MASCULINO	20210108.0	150116.0	NaN
2164376	20210915	LIMA	LIMA	LINCE	AG	12.0	MASCULINO	20210109.0	150116.0	NaN
2164377	20210915	LIMA	LIMA	SAN MARTIN DE PORRES	PCR	20.0	MASCULINO	20210131.0	150135.0	NaN
2164378	20210915	LIMA	LIMA	LIMA	PCR	32.0	FEMENINO	20210809.0	150101.0	NaN
2164379	20210915	LIMA	LIMA	MIRAFLORES	PCR	56.0	FEMENINO	20210430.0	150122.0	NaN

2164380 rows x 10 columns

Fig. 15. Column Name Correction.

```
# Fix the name of the rows
covid_positive_methods_data.loc[covid_positive_methods_data["SEX"] == "FEMENINO", "SEX"] = "FEMALE"
covid_positive_methods_data.loc[covid_positive_methods_data["SEX"] == "MASCULINO", "SEX"] = "MALE"

covid_positive_methods_data
```

	CUT_DATE	DEPARTMENT	PROVINCE	DISTRICT	DXMETHOD	AGE	SEX	RESULT_DATE	UBIGEO	person_id
0	20210915	LIMA	LIMA	SAN MARTIN DE PORRES	PR	25.0	MALE	20201217.0	150135.0	24662153.0
1	20210915	ICA	PISCO	PISCO	PR	20.0	FEMALE	20200822.0	110501.0	24662175.0
2	20210915	HUANUCO	HUANUCO	HUANUCO	PR	22.0	FEMALE	20200729.0	100101.0	24662197.0
3	20210915	ANCASH	SANTA	SANTA	AG	18.0	FEMALE	20210630.0	21809.0	24662204.0
4	20210915	ANCASH	SANTA	NUEVO CHIMBOTE	AG	17.0	MALE	20210404.0	21809.0	24662207.0
...
2164375	20210915	LIMA	LIMA	LINCE	AG	12.0	MALE	20210108.0	150116.0	NaN
2164376	20210915	LIMA	LIMA	LINCE	AG	12.0	MALE	20210109.0	150116.0	NaN
2164377	20210915	LIMA	LIMA	SAN MARTIN DE PORRES	PCR	20.0	MALE	20210131.0	150135.0	NaN
2164378	20210915	LIMA	LIMA	LIMA	PCR	32.0	FEMALE	20210809.0	150101.0	NaN
2164379	20210915	LIMA	LIMA	MIRAFLORES	PCR	56.0	FEMALE	20210430.0	150122.0	NaN

2164380 rows x 10 columns

Fig. 16. Repair of "Pillar" Elements.

in capital letters with which "pandas.Series.str.title" was used. This can be foreseen in Fig. 17.

```
# converts the first letter of each word in a string to uppercase
covid_positive_methods_data["DEPARTMENT"] = covid_positive_methods_data["DEPARTMENT"].str.title()
covid_positive_methods_data["PROVINCE"] = covid_positive_methods_data["PROVINCE"].str.title()
covid_positive_methods_data["DISTRICT"] = covid_positive_methods_data["DISTRICT"].str.title()
covid_positive_methods_data["SEX"] = covid_positive_methods_data["SEX"].str.title()

covid_positive_methods_data
```

	CUT_DATE	DEPARTMENT	PROVINCE	DISTRICT	DXMETHOD	AGE	SEX	RESULT_DATE	UBIGEO	person_id
0	20210915	Lima	Lima	San Martin De Porres	PR	25.0	Male	20201217.0	150135.0	24662153.0
1	20210915	Ica	Pisco	Pisco	PR	20.0	Female	20200822.0	110501.0	24662175.0
2	20210915	Huanuco	Huanuco	Huanuco	PR	22.0	Female	20200729.0	100101.0	24662197.0
3	20210915	Ancash	Santa	Santa	AG	18.0	Female	20210630.0	21809.0	24662204.0
4	20210915	Ancash	Santa	Nuevo Chimbote	AG	17.0	Male	20210404.0	21809.0	24662207.0
...
2164375	20210915	Lima	Lima	Lince	AG	12.0	Male	20210108.0	150116.0	NaN
2164376	20210915	Lima	Lima	Lince	AG	12.0	Male	20210109.0	150116.0	NaN
2164377	20210915	Lima	Lima	San Martin De Porres	PCR	20.0	Male	20210131.0	150135.0	NaN
2164378	20210915	Lima	Lima	Lima	PCR	32.0	Female	20210809.0	150101.0	NaN
2164379	20210915	Lima	Lima	Miraflores	PCR	56.0	Female	20210430.0	150122.0	NaN

2164380 rows x 10 columns

Fig. 17. Correction of Items with Consideration.

Later the elements of the columns "CUT_DATE" and "RESULT_DATE" were converted into string data since the function that was used to convert the elements of these columns into date works with string data, that is why it was necessary to apply a function that converts a string for which the function called "pandas.DataFrame.apply" was

used with lambda which what it does is give the power to "found" almost all reasoning and only worry about the custom function. In the coding with the support of "pandas.DataFrame.info", it is contemplated in short that the data frame named "covid_positive_methods_data" shows its data types where it is observed two columns that have to have date type elements but these will have another type for which it was essential to use "pandas.DataFrame.apply" as lambda that is seen in Fig. 18.

```
# displays the datatype
covid_positive_methods_data.info()
```

```
<class 'pandas.core.frame.DataFrame'>
RangeIndex: 2164380 entries, 0 to 2164379
Data columns (total 10 columns):
# Column Dtype
---  ---
0 CUT_DATE int64
1 DEPARTMENT object
2 PROVINCE object
3 DISTRICT object
4 DXMETHOD object
5 AGE float64
6 SEX object
7 RESULT_DATE float64
8 UBIGEO float64
9 person_id float64
dtypes: float64(4), int64(1), object(5)
memory usage: 165.1+ MB
```

Fig. 18. Data Frame Element Types.

After consulting the types of elements in the data frame, "pandas.DataFrame.apply" was used as well as lambda and "to_datetime" to impose the transformation of the typed string to date. To use "pandas.DataFrame.apply" like lambda and "to_datetime" to begin with, the data types were transformed into string types in addition to removing the decimal part. This transformation can be seen in Fig. 19.

```
# change data type of Series to String
covid_positive_methods_data["CUT_DATE"] = (covid_positive_methods_data["CUT_DATE"].apply(str))
covid_positive_methods_data["RESULT_DATE"] = (covid_positive_methods_data["RESULT_DATE"].apply(str))
covid_positive_methods_data["RESULT_DATE"] = (covid_positive_methods_data["RESULT_DATE"].str.replace('\.\d', ''))
```

Fig. 19. Converting Items to Data Frame String.

After the transformation of the elements to string type, it was allowed to use "pandas.DataFrame.apply" like lambda which generated a transformation of type string to date, and "to_datetime" that does the same thing only that it uses "errors = 'coerce'" so that the "nan" is set to NaT since that element can be stored in the date and time array to specify the unknown or missing date and time elements. The application of "pandas.DataFrame.apply" as well as lambda and "to_datetime" can be seen in Fig. 20.

In the coding, it is reflected that the NumPy library was imported and it was given the name np. This is a library that contributed to the procedure of producing a recent "catalog" of districts for infected people over 50 that can be seen in Fig. 3, after importing NumPy, how many people exist per district was preserved in the "covid_positive_methods_data_counts" element, then in the "district_indices" element the districts with people over 50 were set with 'True' and the districts

```
# import datetime library
import datetime
# convert to a date type
covid_positive_methods_data["CUT_DATE"] = (covid_positive_methods_data["CUT_DATE"]
.apply(lambda X: datetime.datetime.strptime(x, "%Y%m%d").date()))
covid_positive_methods_data["RESULT_DATE"] = (pd
.to_datetime(covid_positive_methods_data["RESULT_DATE"], errors='coerce'))
covid_positive_methods_data
```

CUT_DATE	DEPARTMENT	PROVINCE	DISTRICT	DXMETHOD	AGE	SEX	RESULT_DATE	UBIGEO	person_id	
0	2021-09-15	Lima	Lima	San Martin De Porres	PR	25.0	Male	2020-12-17	150135.0	24662153.0
1	2021-09-15	Ica	Pisco	Pisco	PR	20.0	Female	2020-08-22	110501.0	24662175.0
2	2021-09-15	Huanuco	Huanuco	Huanuco	PR	22.0	Female	2020-07-29	100101.0	24662197.0
3	2021-09-15	Ancash	Santa	Santa	AG	18.0	Female	2021-06-30	21808.0	24662204.0
4	2021-09-15	Ancash	Santa	Nuevo Chimbote	AG	17.0	Male	2021-04-04	21809.0	24662207.0
...
2164375	2021-09-15	Lima	Lima	Lince	AG	12.0	Male	2021-01-08	150116.0	NaN
2164376	2021-09-15	Lima	Lima	Lince	AG	12.0	Male	2021-01-09	150116.0	NaN
2164377	2021-09-15	Lima	Lima	San Martin De Porres	PCR	20.0	Male	2021-01-31	150135.0	NaN
2164378	2021-09-15	Lima	Lima	Lima	PCR	32.0	Female	2021-08-09	150101.0	NaN
2164379	2021-09-15	Lima	Lima	Miraflores	PCR	56.0	Female	2021-04-30	150122.0	NaN

2164380 rows x 10 columns

Fig. 20. Transforming Items to Data Frame Date.

with “False” that have people under 50, then in the element “district_to_keep” a “catalog” of districts was preserved to maintain. The procedure for the establishment of this recent list can be visualized in Fig. 21. This same figure “exposes” the number of rows of the data frame from, the number of rows of the processed Frame (recent), and the number of rows that were pulled out.

```
# number of rows of original dataframe
rows_before = covid_positive_methods_data.shape[0]
print("Number of rows in the starting dataframe is {}."
      .format(rows_before))

covid_positive_methods_data = (covid_positive_methods_data
.loc[covid_positive_methods_data["DISTRICT"]
.isin(district_to_keep)])

# number of rows of processed dataframe
rows_after = covid_positive_methods_data.shape[0]
print("Number of rows of processed dataframe is {}."
      .format(rows_after))

print("{} rows removed!".format(rows_before - rows_after))

Number of rows in the starting dataframe is 2164380.
Number of rows of processed dataframe is 2151482.
12898 rows removed!
```

Fig. 21. Another List of Districts for the Elevated Infection.

Later it was reflected that the data of those infected with SARS-COV-2 has missing elements, with which in this “place” it is shown how it was used with those missing elements. What was carried out was to delete missing elements, since those not being accessible prevent the encoding operation. This “eradication” of missing elements can be visualized in Fig. 22.

After converting the elements of the columns into numbering elements, this machine learning algorithm that was used works with numbering elements, therefore it was required to produce numbering representativeness according to the model for this purpose the named coding approach was used “Label encoding” this replaces the column element with a numbering element between 0 and the top numbering of unique elements in the column reduced by 1 in alphabetical order. In the coding, its data types are shown where it is consulted that a “pair” of columns have non-numeric elements, which is why they use of “Label encoding” was essential.

```
# Drops missing values
covid_positive_methods_data = covid_positive_methods_data.dropna(axis=0)
covid_positive_methods_data
```

CUT_DATE	DEPARTMENT	PROVINCE	DISTRICT	DXMETHOD	AGE	SEX	RESULT_DATE	UBIGEO	person_id	
0	2021-09-15	Lima	Lima	San Martin De Porres	PR	25.0	Male	2020-12-17	150135.0	24662153.0
1	2021-09-15	Ica	Pisco	Pisco	PR	20.0	Female	2020-08-22	110501.0	24662175.0
2	2021-09-15	Huanuco	Huanuco	Huanuco	PR	22.0	Female	2020-07-29	100101.0	24662197.0
3	2021-09-15	Ancash	Santa	Santa	AG	18.0	Female	2021-06-30	21808.0	24662204.0
4	2021-09-15	Ancash	Santa	Nuevo Chimbote	AG	17.0	Male	2021-04-04	21809.0	24662207.0
...
2128060	2021-09-15	Junin	Satipo	Satipo	PR	52.0	Male	2020-08-22	120601.0	745213.0
2128061	2021-09-15	Lima	Lima	Lima	PCR	24.0	Male	2021-01-19	150101.0	745220.0
2128062	2021-09-15	Pasco	Pasco	Huayllay	PR	44.0	Male	2020-08-05	190104.0	745222.0
2128063	2021-09-15	Puno	Lampa	Lampa	PCR	45.0	Female	2021-04-28	210701.0	745273.0
2128064	2021-09-15	Junin	Satipo	Rio Negro	AG	61.0	Male	2021-05-07	120607.0	745280.0

2005947 rows x 10 columns

Fig. 22. Deleting Missing Items.

After demonstrating the data types of the data frame, the “Category codes” way was used to enforce “Label encoding”. To use the “Category codes” way in the first place, the element types were transformed into category types. This transformation is achieved by “display” in Fig. 23.

```
# convert to a category type
covid_positive_methods_data["CUT_DATE"] = (covid_positive_methods_data
["CUT_DATE"].astype('category'))
covid_positive_methods_data["DEPARTMENT"] = (covid_positive_methods_data
["DEPARTMENT"].astype('category'))
covid_positive_methods_data["PROVINCE"] = (covid_positive_methods_data
["PROVINCE"].astype('category'))
covid_positive_methods_data["DISTRICT"] = (covid_positive_methods_data
["DISTRICT"].astype('category'))
covid_positive_methods_data["DXMETHOD"] = (covid_positive_methods_data
["DXMETHOD"].astype('category'))
covid_positive_methods_data["SEX"] = (covid_positive_methods_data
["SEX"].astype('category'))
covid_positive_methods_data["RESULT_DATE"] = (covid_positive_methods_data
["RESULT_DATE"].astype('category'))

covid_positive_methods_data.dtypes
```

CUT_DATE	category
DEPARTMENT	category
PROVINCE	category
DISTRICT	category
DXMETHOD	category
AGE	float64
SEX	category
RESULT_DATE	category
UBIGEO	float64
person_id	float64
dtype:	object

Fig. 23. Transform Elements to Data Frame Category.

Following the transformation of the elements to category type, the way “Category codes” was used, which produced a representative numbering according to the model. The “Label encoding” appliqué in the way of “Category codes” can be seen in Fig. 24.

Finally, the forecast objective was saved in the element “y” that can be seen in Fig. 25, after setting the objective, a “catalog” of columns that “entered” the model was chosen to be used. To forecast, that is identified by “features” the one that is saved in the “X” element that can be “noticed” in Fig. 26.

6) *Modeling*: This path of the data science methodology used the “scikit-learn” library to found the model, it should be noted that this library is “pointed” as “sklearn”, after setting the “scikit-learn” library, the decision tree model for regression and an integer numbering were specified to “random_state” which ensures the same results throughout the execution during the setting of an integer numbering and finally the decision tree model for regression based on the characteristics and objective

```
# category codes
covid_positive_methods_data['CUT_DATE'] = (covid_positive_methods_data['CUT_DATE']
.cat.codes)
covid_positive_methods_data['DEPARTMENT'] = (covid_positive_methods_data['DEPARTMENT']
.cat.codes)
covid_positive_methods_data['PROVINCE'] = (covid_positive_methods_data['PROVINCE']
.cat.codes)
covid_positive_methods_data['DISTRICT'] = (covid_positive_methods_data['DISTRICT']
.cat.codes)
covid_positive_methods_data['DXMETHOD'] = (covid_positive_methods_data['DXMETHOD']
.cat.codes)
covid_positive_methods_data['SEX'] = (covid_positive_methods_data['SEX']
.cat.codes)
covid_positive_methods_data['RESULT_DATE'] = (covid_positive_methods_data['RESULT_DATE']
.cat.codes)

covid_positive_methods_data.head()
```

CUT_DATE	DEPARTMENT	PROVINCE	DISTRICT	DXMETHOD	AGE	SEX	RESULT_DATE	UBIGEO	person_id	
0	0	14	112	880	2	25.0	1	284	150135.0	24662153.0
1	0	10	145	739	2	20.0	0	169	110501.0	24662175.0
2	0	9	87	366	2	22.0	0	145	100101.0	24662197.0
3	0	1	166	904	0	18.0	0	479	21808.0	24662204.0
4	0	1	166	625	0	17.0	1	392	21809.0	24662207.0

Fig. 24. Adaptation of the Category Codes Way.

```
# store the prediction target
y = (covid_positive_methods_data
.DXMETHOD)
```

Fig. 25. Forecast Goal.

```
# features
covid_positive_methods_data_features = ([ 'DEPARTMENT'
,'PROVINCE', 'DISTRICT'])

X = (covid_positive_methods_data
[covid_positive_methods_data_features])

X.head()
```

DEPARTMENT	PROVINCE	DISTRICT
0	14	112
1	10	145
2	9	87
3	1	166
4	1	166

Fig. 26. Forecast Characteristics.

was adapted. Fig. 27 "exposes" the determined model, as well as the appropriate one.

```
from sklearn.tree import DecisionTreeRegressor

# Determined model. Specify a number for random_state to
# ensure some results each run
covid_positive_methods_data_model = (DecisionTreeRegressor
(random_state=1))

# Suitable model
covid_positive_methods_data_model.fit(X, y)

DecisionTreeRegressor(random_state=1)
```

Fig. 27. Decision Tree Model.

Fig. 28 manages to observe that it preceded to forecast with the next seven positive cases by method (0 - 6) in addition to contemplating the forecasts of those seven positive cases by method, there the function "pandas.DataFrame.round" was used which returns the integer numbering closer, that was used to demonstrate which laboratory method the entire forecast is affiliated with. So it is possible to know that if the result is "0" the laboratory method is Antigen Test (AG) if the result is "1" the laboratory method is Molecular Test (PCR) and if

the result is "2" the laboratory method is Rapid Test (RP).

```
print("Making predictions for the following 7 positive cases per method:")
print(X.head(7))
print("The predictions are")
print(covid_positive_methods_data_model.predict(X.head(7)).round())
```

Making predictions for the following 7 positive cases per method:

DEPARTMENT	PROVINCE	DISTRICT
0	14	112
1	10	145
2	9	87
3	1	166
4	1	166
5	14	112
6	14	112

The predictions are
[1. 1. 1. 1. 1. 1. 1.]

Fig. 28. Training Data Forecast.

To know the text elements that are equivalent to those numbering elements, the Microsoft Excel spreadsheet was used, with that, the CSV that helped with the forecast was copied and copies of the columns were deleted, listing the rows by individual element. This was done due to the data tool to make copies and the function ROW minus 2 was used to give numbering. A sample of the consequence of this can be found in Table I.

TABLE I. DEPARTMENT LIST SAMPLE

N°	Name
0	LIMA
1	ICA
2	HUANUCO
3	ANCASH
4	APURIMAC
5	JUNIN
6	PIURA
7	MADRE DE DIOS
8	LAMBAYEQUE
9	CALLAO

IV. RESULTS AND DISCUSSIONS

A. Evaluation

This last journey of the data science methodology assessed the model with other elements, in the first place that was carried out before proceeding, the assessment was to check the forecast that was carried out in the preparation journey of the model where the prognosis is based on the elements of the index from 0 - 6, with which the value has to vary from that scale of indexes, for that reason in that route the elements of the index 101 were used to specify the efficiency of the model based on the outcome of the valued. In Fig. 29 the evaluation of the model is tested.

```
print("Making predictions for the following 1 positive cases per method:")
print(X.loc[101:101])
print("The predictions are")
print(covid_positive_methods_data_model.predict(X.loc[101:101]).round())
```

Making predictions for the following 1 positive cases per method:

DEPARTMENT	PROVINCE	DISTRICT
101	14	112

The predictions are
[1.]

Fig. 29. Other Items to Compare.

To evaluate the results, an element called “dataframe_to_evaluate” had to be founded, which can be seen in Fig. 30 that contributed as a “pillar” as the purpose of comparing the completion of the forecast reached in the data of the index of the 101 for the data in the data frame named “dataframe_to_evaluate”.

```
dataframe_to_evaluate = (covid_positive_methods_data
[['DEPARTMENT', 'PROVINCE', 'DISTRICT', 'DXMETHOD']])
dataframe_to_evaluate
```

	DEPARTMENT	PROVINCE	DISTRICT	DXMETHOD
0	14	112	880	2
1	10	145	739	2
2	9	87	366	2
3	1	166	904	0
4	1	166	625	0
...
2128060	11	169	940	2
2128061	14	112	496	1
2128062	18	140	388	2
2128063	20	109	486	1
2128064	11	169	813	0

2005947 rows x 4 columns

Fig. 30. Data Frame for Evaluating the Result.

Since the element “dataframe_to_evaluate” was indicated which helped as a rationale to check the completion of the reached forecast of the element of index 101 among the elements of the data frame named “dataframe_to_evaluate”, and specifically because due to this element, the coding seen and performed in Fig. 31 could be carried out, which shows the number of AG laboratory method people located on department 14, on province 112 and on district 468. which has membership in index 101 of the forecast. The same was done for the PCR and PR laboratory methods.

```
(dataframe_to_evaluate[(dataframe_to_evaluate
['DEPARTMENT'] == 14)
&(dataframe_to_evaluate['PROVINCE'] == 112)
&(dataframe_to_evaluate['DISTRICT'] == 468)
&(dataframe_to_evaluate['DXMETHOD'] == 0)])
```

	DEPARTMENT	PROVINCE	DISTRICT	DXMETHOD
6	14	112	468	0
991	14	112	468	0
1245	14	112	468	0
1563	14	112	468	0
1565	14	112	468	0
...
2118384	14	112	468	0
2119026	14	112	468	0
2122288	14	112	468	0
2125018	14	112	468	0
2127669	14	112	468	0

2042 rows x 4 columns

Fig. 31. Data Framework for Evaluation Based on AG.

The completion of this evaluation was beneficial since when comparing the forecast reached from the data of index 101, which indicates that the laboratory method is PCR, with the data from the data frame named “dataframe_to_evaluate”

that indicates that there are 2042 people of laboratory method AG, 7053 people from the PCR laboratory method and 3109 people from the PR laboratory method in this department 14 in this province 112 and in this district 468 a product was obtained that says that the efficiency of the model is ideal.

To finish, the “sklearn.metrics” module was used, after it was created, “covid_positive_methods_data_model.predict(X)” was saved in the “predicted_covid_positive_methods” element until after applying the regression metric “metrics.mean_absolute_error(y_predict, y_true, y_true, *)” which, due to its name, is precisely the regression loss of the mean absolute error (MAE), it is in the present regression metric where the objective of the forecast was left as the initial argument as well as the second argument the forecast of positive cases with laboratory method, this function was used to value the qualification of the forecast of the model and in this way to have the power which very approximately is the forecast of the model in terms of what happens. This MAE can be seen in Fig. 32.

```
from sklearn.metrics import mean_absolute_error

predicted_covid_positive_methods = (covid_positive_methods_data_model
.predict(X))
mean_absolute_error(y, predicted_covid_positive_methods)
```

0.690142434508965

Fig. 32. MAE of the Model.

B. Comparison with other Prediction Algorithms

If we compare the decision tree predictive algorithm, with other prediction algorithms (Random forests and gradient boosting), we can say that the random forests prediction algorithm takes the average of many decision trees that are weaker than one tree of complete decisions which are carried out with a sample of the data but when combining them a better general performance is obtained, in addition to giving as a result very high-quality models and being quick to train, while the gradient boosting uses decision trees still weaker that focus on hard examples, plus it is high-performance, while the decision tree, is a kind of “branched graph” that matches all the possible results of a decision, plus it is easy to understand and implement. This comparison can be seen in Table II.

TABLE II. PREDICTION ALGORITHMS

Name	Advantages	Disadvantages
The Decision Tree	Easy to understand and implement	Often too simple and not powerful enough for complex data
Random Forests	Results in very high-quality models and is quick to train	It is slow to produce predictions relative to other algorithms
Gradient Boosting	High performance	A small change in the set of functions or the training set can create radical changes in the model

V. CONCLUSIONS AND FUTURE WORK

The results of this forecast to know the types of individuals infected by SARS-COV-2 in the regions of Peru, was successfully achieved, which can be seen in the course of the research that was developed with the data science methodology, which by applying Python it was possible to notice the number of people who have performed the laboratory methods (AG, PCR, and PR), in this, it is observed that department 14, province 112 and district 468 yielded a forecast of "1", which means that it is a type of individual who has been in possible contact with the virus, on the other hand, if it had returned "0" it would be an individual with symptoms of SARS-COV-2 and in case it would have returned "2" is an individual who wants to know if he has had the virus, in the development it is also appreciated that it was predicted based on the construction of the model, therefore, in the methodology of the evaluation of the model it showed a minimum error of 0.6. In addition, the machine learning decision tree algorithm was used for the detailed process, successfully achieving the objective of the research.

For future research, it is recommended to apply different methodologies for prediction, so that good procedures arise from this agglomeration of methodologies and thus achieve a new and optimal result when applying to forecast.

REFERENCES

- [1] A. Scohy, A. Anantharajah, M. Bodéus, B. Kabamba-Mukadi, A. Verroken, and H. Rodriguez-Villalobos, "Low performance of rapid antigen detection test as frontline testing for COVID-19 diagnosis," *Journal of Clinical Virology*, vol. 129, pp. 1–3, aug 2020.
- [2] M. Santos Bravo, D. Nicolás, C. Berengua, M. Fernandez, J. C. Hurtado, M. Tortajada, S. Barroso, A. Vilella, M. Mosquera, J. Vila, and M. Marcos, Angeles, "SARS-CoV-2 normalized viral loads and subgenomic RNA detection as tools for improving clinical decision-making and work reincorporation," *The Journal of Infectious Diseases*, pp. 1–26, 2021.
- [3] A. Marcelo Ñique, F. Coronado-Marquina, J. A. Mendez Rico, M. P. García Mendoza, N. Rojas-Serrano, P. V. Marques Simas, C. Cabezas Sanchez, and J. Felix Drexler, "A faster and less costly alternative for RNA extraction of SARS-CoV-2 using proteinase k treatment followed by thermal shock," *PLoS ONE*, vol. 16, no. 3 March, pp. 1–8, 2021.
- [4] D. Brinati, A. Campagner, D. Ferrari, M. Locatelli, G. Banfi, and F. Cabitza, "Detection of COVID-19 Infection from Routine Blood Exams with Machine Learning: A Feasibility Study," *Journal of Medical Systems*, vol. 44, no. 8, pp. 1–12, 2020.
- [5] A. S. Albahri, R. A. Hamid, J. K. Alwan, Z. Alqays, A. Zaidan, B. Zaidan, A. O. S. Albahri, A. H. AlAmoodi, J. M. Khlaf, E. Almahdi, E. Thabet, S. M. Hadi, K. I. Mohammed, M. A. Alsalem, J. R. Al-Obaidi, and H. Madhloom, "Role of biological Data Mining and Machine Learning Techniques in Detecting and Diagnosing the Novel Coronavirus (COVID-19): A Systematic Review," *Journal of Medical Systems*, vol. 44, pp. 1–11, 2020.

- [6] A. M. U. D. Khanday, S. T. Rabani, Q. R. Khan, N. Rouf, and M. Mohi Ud Din, "Machine learning based approaches for detecting COVID-19 using clinical text data," *International Journal of Information Technology (Singapore)*, vol. 12, no. 3, pp. 731–739, 2020. [Online]. Available: <https://doi.org/10.1007/s41870-020-00495-9>
- [7] S. Asif, Y. Wenhui, H. Jin, and S. Jinhai, "Classification of COVID-19 from Chest X-ray images using Deep Convolutional Neural Network," *2020 IEEE 6th International Conference on Computer and Communications, ICC 2020*, no. March 2020, pp. 426–433, 2020.
- [8] T. Mackey, V. Purushothaman, J. Li, N. Shah, M. Nali, C. Bardier, B. Liang, M. Cai, and R. Cuomo, "Machine learning to detect self-reporting of symptoms, testing access, and recovery associated with COVID-19 on Twitter: retrospective big data infoveillance study," *JMIR Public Health and Surveillance*, vol. 6, no. 2, pp. 1–9, 2020.
- [9] R. E. Cuomo, V. Purushothaman, J. Li, M. Cai, and T. K. Mackey, "A longitudinal and geospatial analysis of COVID-19 tweets during the early outbreak period in the United States," *BMC Public Health*, vol. 21, no. 1, pp. 1–11, 2021.
- [10] D. A. Ordóñez Barrios and E. R. Vizcarra Infantes, "Modelo Predictivo para el diagnóstico de la Diabetes Mellitus Tipo 2 soportado por SAP Predictive Analytics," Ph.D. dissertation, Universidad Peruana de Ciencias Aplicadas, 2018.
- [11] S. Alderisi, "Machine Learning applied to COVID-19," Ph.D. dissertation, Universidad Politécnica de Madrid, 2020.
- [12] W. H. El-Ashmawi, D. S. Abd Elminaam, A. M. Nabil, and E. Eldesouky, "A chaotic owl search algorithm based bilateral negotiation model," *Ain Shams Engineering Journal*, vol. 11, no. 4, pp. 1163–1178, 2020. [Online]. Available: <https://www.sciencedirect.com/science/article/pii/S2090447920300071>
- [13] N. Walter and S. T. Murphy, "How to unring the bell: A meta-analytic approach to correction of misinformation," *Communication Monographs*, vol. 85, no. 3, pp. 423–441, 2018.
- [14] A. Abadie, "Using synthetic controls: Feasibility, data requirements, and methodological aspects," *Journal of Economic Literature*, vol. 59, no. 2, pp. 391–425, 2021.
- [15] D. Zhou, Z. Yan, Y. Fu, and Z. Yao, "A survey on network data collection," *Journal of Network and Computer Applications*, vol. 116, no. December 2017, pp. 9–23, 2018. [Online]. Available: <https://doi.org/10.1016/j.jnca.2018.05.004>
- [16] F. J. Nieto, U. Aguilera, and D. López-de Ipiña, "Analyzing Particularities of Sensor Datasets for Supporting Data Understanding and Preparation," *Sensors*, pp. 1–28, 2021.
- [17] S. Stieglitz, M. Mirbabaie, B. Ross, and C. Neuberger, "Social media analytics – Challenges in topic discovery, data collection, and data preparation," *International Journal of Information Management*, vol. 39, no. October 2017, pp. 156–168, 2018. [Online]. Available: <https://doi.org/10.1016/j.ijinfomgt.2017.12.002>
- [18] I. H. Sarker, M. M. Hoque, M. K. Uddin, and T. Al-sanoosy, "Mobile Data Science and Intelligent Apps: Concepts, AI-Based Modeling and Research Directions,"

Mobile Networks and Applications, vol. 26, no. 1, pp. 285–303, 2021. [19] M. Q. Patton, “Evaluation Science,” *American Journal of Evaluation*, vol. 39, no. 2, pp. 183–200, 2018.

Inclusive Education: Implementation of a Mobile Application for Blind Students

Alejandro Boza-Chua, Karen Gabriel-Gonzales, Laberiano Andrade-Arenas
Facultad de Ciencias e Ingeniería
Universidad de Ciencias y Humanidades
Lima, Perú

Abstract—Currently, the world is going through an era of changes in the education sector, but most Latin American countries are lagging, especially Peru, which does not have the technological tools that allow it to advance to an adequate level of inclusion of disabled students, especially blind students who are 60% of students who drop out of school for lack of education that have be suitable for their need. Consequently, the present research work is originated which aims to develop a mobile application oriented to the benefit of inclusive education of blind students. Therefore, the agile scrum methodology was used for the development of this project, executed in 5 phases, the requirements identified for the development of the mobile application were obtained through a questionnaire to 25 parents of visually impaired students, allowing the development of a mobile application that meets quality of inclusive education that can be applied in the education sector. Finally, as a result of the research work, another satisfaction survey was conducted with 50 parents where the application was evaluated, obtaining 90% of acceptance and satisfaction.

Keywords—Blind; disability; educational inclusion; mobile application; scrum methodology

I. INTRODUCTION

Over the last 20 years, the community's thinking and prioritization of the integration of the blind into the educational environment has undergone an incremental change that transformed the school environment and the pedagogical regime. For this reason, it has become one of the most important issues in the world, both in its educational organization and in the way of learning in the classroom [1]. Although two decades have passed since the revolutionary educational principle on the incorporation of blind students, not all countries have adapted to this, especially a large part of all Latin American countries.

Currently, Peru has great lack of technology oriented to blind students, being one of the main countries with a low percentage of educational inclusion. Likewise, the support and help provided by public services are really excessive. For this reason, 66% of students drop out of their academic studies [2]. The main reason is due to the scarcity of educational tools and the training that teachers receive, oriented to blind people. In such a way that the National Institute of Statistics and Informatics revealed the existence of more than 500 thousand students with visual impairment in Peru. However, although they are a large community, the public entity does not establish technology capable of meeting the primary needs of blind students. In the same way, with the training that should be provided to teachers for a better learning environment and

development for blind students in order to provide integrated and inclusive education.

The existence of Law No. 29973 in Peru protects the community of people with disabilities. This article establishes that all people with disabilities have the right to obtain an adequate and quality educational development. However, although this law exists, it is not fully complied with, causing a corresponding educational deviation towards blind students. As a result, students are forced to accept precarious education without vision, being at a disadvantage by not receiving an adequate and favorable level of education for their professional growth [3].

Blind students who do not get appropriate educational support, delay the course of classes for other students. At other times, these blind students have little educational growth as they receive lesser assignments compared to their sighted peers, which is an obstruction to their learning. For this reason, these students fail the course or have low grades so that they remain at a lower level compared to other students [4]. Likewise, even if they are studying in the same grade, in the same cycle or in higher levels, it is evident the exclusion towards them within the activities developed in a classroom. This causes them to suffer and suffer within the educational environment [5]. It is therefore necessary that this issue emphasizes how important it is to establish a comprehensive system that supports blind students and guides teachers on proper training in the relationship with students. Above all because teachers are an essential part of educational development and advancement. In the same way, they have the function of carrying out an adequate search for measures that establish an inclusive environment using didactic strategies in the course of the development of their class [6], with the objective of promoting inclusion among sighted and blind students in order to reduce the educational limitations for students with visual impairment by including them.

Therefore, it is essential to establish viable planning for the educational growth of students with blindness, to provide a better inclusive education along with the development of technologies that support adequate professional growth. That is why this research work focuses on the implementation of a mobile application that benefits and promotes educational inclusion for blind students, to improve and promote the educational social environment.

The present research work is established by different sections. Section II shows the literature review. Likewise, as

Section III, the methodological phase oriented to the development of the project is determined. On the other hand, Section IV shows the results of the research work oriented to the established methodology, in Section V the discussion. Finally, the last part is Section VI, which is defined by the conclusion and future work.

II. REVIEW OF THE LITERATURE

This study is based on the creation of a mobile application to promote educational inclusion for students with visual impairment, with the purpose of improving the quality of teaching. In this way, a feedback study was carried out, referring to the projects that provide benefits with better perspective. The author [7], affirms that one of the most valuable senses is sight since it allows the development of teaching towards the student. Also, the school is a general environment of visual stimuli, so that impedes the development of learning for blind people. Because it produces a demand for the requirement of technological tools to meet the needs of students.

For this reason, the author covered his research with the intention of developing a suitable mobile application to organize and recognize Cartesian coordinates by means of the convolutional neural system, supported by the advancement of the technological crack with validation and modeling of a set of neural networks. In order to develop this study, it was possible to use our own methodology which is divided into 4 phases, application, data development, choice of the appropriate neural architecture and, as the last phase, we have the training.

The results showed that, in order to achieve the general objective of the research work, it is essential to include a portion of data which compresses the images in order to be able to run a group of images originated from the information sector generated. Then, it was analyzed and the selection of the best pattern to put into operation of software was carried out. Thus, it was possible to determine that the circle of visually impaired people has rights determined by law. But for many of the media, it is difficult to have an interaction with blind people and the environment around them.

On the other hand, the author [8], mentions the various applications of Artificial Intelligence (AI) managed to obtain a great effect in a positive way in the various areas within an educational institution such as instruction and learning. For this study, a qualitative research analysis methodology was used. Thus, the results showed that this technology was able to improve the efficiency and effectiveness in the training of students. As conclusions, it was demonstrated that with the help of this technology it was possible to contribute to the development of student learning in their educational centers.

Also, the author [9], mentions that mobile applications provide many advantages in learning, which have been one of the most valuable tools for the performance of students and teachers in an academic way. The study is oriented in the design of an application, which will be used to improve the learning acquired after the development of classes through an intuitive interface. In this way, it supports the development of learning. As a result, a technological tool was developed, capable of contributing to the use of technology in a way that helps in its educational development. From another perspective, the author [10], points out that the contributions of technological

tools, have not been oriented entirely to the improvement of the educational sector, but more in a method of survival of people who have a disability, The study was carried out to design a mobile game, oriented to people with visual impairment, using haptic signals and vibrations, obtaining as results that this game showed that the game is very useful for people with visual impairment and that it has been designed for people with visual impairment. Obtaining as results that this game showed to be suitable to improve confidence, satisfaction and happiness of life.

During the last few years, issues related to visual impairment have been one of the most researched topics worldwide. According to the author [11], this has led to an increase in studies on the development of tools that provide improvements for the visually impaired community. This work focuses on creating a mobile application for children between 6 and 14 years old who suffer from visual impairment, with the aim of helping in the development of learning. The results generated by this study are that it is possible to determine which models are ideal through object recognition.

In conclusion, the various authors were able to contribute on how the implementation of technological tools has improved and can improve the effectiveness and efficiency in educational centers. However, a good inclusion of students with disabilities has not been achieved; therefore, it can be mentioned that apps with various categories would play a very important role in the lifestyle of these people; improving the emotional and educational state. This reason is that it generates the beginning of our research.

III. METHODOLOGY

A. Scrum Methodology

For the development and implementation of this research work, the Scrum methodology was selected, this methodology is positioned among the best methodologies known worldwide, it is focused on software development, this methodology offers a suitable way to comply with good practices, before collaborative work giving the possibility of giving the best results in the projects, providing security and viability towards its final goal. On the other hand, the main characteristics of this methodology are based on its speed, adaptability, efficiency and flexibility [12]. It also has the guarantee of obtaining an environment, with security and transparency, having an environment of continuous progress, without loss of resources as it is a methodology prepared to change regardless of its difficulty [13].

The Scrum methodology consists of 5 production stages, as shown in Fig.1. The initiation stage focuses on examining, determining and investigating the requirements of the project. These requirements can be obtained through user surveys or meetings with the customer. The second stage is the implementation stage, which focuses on creating, estimating and identifying the user stories (HU) that were previously collected as requirements. Also, after that, the Sprint is determined, which is the time in which the project deliverables will be developed and, finally, the product backlog is created [12].

After performing the first two stages of the Scrum methodology, phase 3 follows, which is the implementation. The



Fig. 1. Scrum Methodology Stages.

purpose of this stage is to develop the project deliverables at the Sprint level, complying with the corresponding user stories. Then follows the phase of review and retrospective of the entire project. This retrospective stage aims to perform inspections and verification that qualify the course of the project, proposing new commitments, solutions and constructive conclusions. On the other hand, the purpose of the review is to validate the development of the project, complying with the needs and user stories. Finally, the last stage of this methodology is the launching of the final delivery of the project [13].

1) *Scrum Roles*: This method contains 7 roles as shown in Table I, 3 of them are known as core Scrum roles, and the other 4 are known as non-core roles. On the one hand, the core roles are responsible for achieving the goals established for the project, thus being fundamental and mandatory for the performance of the execution, according to the Scrum methodology. While on the other hand, the non-core roles are not so necessary and important within the development of the project because the project can continue without their participation.

TABLE I. SCRUM ROLES

Central Roles	Non-Central Roles
Scrum Team	Users
Scrum Master	Sponsor
Product Owner	Stakeholder
	Customer

The Scrum core team is composed of the central roles as shown in Table I, [14]. The first central role is the Scrum Master, who has the purpose of guiding, facilitating and providing good practices to the development team and verifying that everything goes according to plan. The second role is the Product Owner, who has the functionality of maximizing the project deliverables as well as receiving and transmitting the needs or requirements from the customer. Finally, the third role is the Scrum Team, which has the functionality to generate the project deliverables referring to the requirements specified at the level of the business method transmitted through the Product Owner [15].

B. Methodology Development

1) *Home*: The first phase of the scrum methodology in this research work was established in the realization of a

questionnaire directed to 25 parents of blind students from different educational centres in Peru to collect requirements that allow to know the main requirements that need to be satisfied for viable education oriented to blind students. After having carried out the questionnaire through the results obtained, the user stories were established, which are shown in Table II. On some occasions within this research, HU-”number” will be placed referring to the user stories and the number to which they belong or simply HU referring to the user stories.

TABLE II. USER STORIES

N°	Definition
HU-01	As the administrator, I want the application to have a voice guide so that the blind student can interact with the functions of the mobile application.
HU-02	I as an administrator want the mobile application to have the option to provide voice assistant gender selection for the student to get a better convenience and experience within their learning.
HU-03	As an administrator, I want the mobile application to have the function of being able to select different subjects for the student to choose according to his or her predilection.
HU-04	As a student, I want the mobile application to have the division of the courses by subject so that I can choose according to what I want to study.
HU-05	As the administrator, I want the mobile application to be divided according to the educational level so that the subjects are directed to the student according to his rank and he can select according to his preference.
HU-06	As the administrator, I want the application to provide a report on the student’s progress within the application so that the supervisor or the student knows about his or her progress with respect to the topics within each course.
HU-07	As the administrator, I want the mobile application to have motivational alerts so that when the student finishes each exercise, he/she feels encouraged to continue learning.
HU-08	As the administrator, I want the mobile application to have two ways of taking the exams, a graded exam so that the student can know the level of his knowledge and another exam without grading so that the student can practice.
HU-09	As the administrator, I want the mobile application to have evaluations that are divided by levels so that the student can select according to his or her preference.
HU-10	As the administrator, I want the mobile application to have audio interaction functions within all the questions in the exam, both questions and answers, so that the blind student has the possibility to develop and interact with the application satisfactorily.

2) *Planning and Estimating*: After identifying the user stories through the requirements, the next process was to analyze each of the user stories in the planning and estimation stage. In this phase the product backlog was developed in which the user stories were estimated and prioritized and the type of origin and sprint they belong to were defined. For the estimation process, the planning poker mechanism was used. This is a strategy that allows a vote by the scrum team, they give a number to each user story, according to how much they believe that the development of the user story will require time and resources, testing the experience of each of the members of the scrum team.

The next process in this stage was the prioritization, where the importance of the development of a user story within the project is rated according to its importance, following an ascending order for its creation. After having both data, prioritization and estimation, the backlog is created, which contains both data, plus three aggregate columns. The first aggregate column is the status of the user story, the status can be pending (PE), in process (PR) and finished (FI). As the second column added, the type of origin of the user story is placed, qualifying according to what it generates. Finally, there

is a column of the sprint number corresponding to each user story, all of this can be visualized in Table III.

TABLE III. PRODUCT BACKLOG

N° HU	Estimate	Prioritization	Status	Origin	Sprint
HU-01	8	1	PE	Service	3
HU-02	5	2	PE	Service	3
HU-03	3	3	PE	Service	2
HU-04	3	4	PE	Service	2
HU-05	5	5	PE	Service	3
HU-06	5	6	PE	Report	2
HU-07	1	10	PE	Service	1
HU-08	8	7	PE	Service	1
HU-09	5	8	PE	Service	2
HU-010	8	9	PE	Service	1

After having performed the product backlog, the speed of each sprint is analyzed and defined; this depends on the experience of the scrum team. Likewise, for this process, the number of user stories to be performed in each sprint is selected according to the story points accumulated between them, which makes the story points equal to the speed per sprint. In addition, the most important thing for this process is that the prioritization is selected as a guide as shown in Fig. 2.

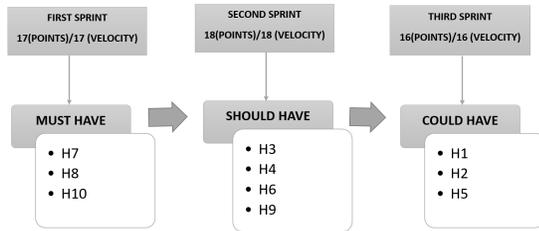


Fig. 2. Speed of Development.

3) *Implementation:* Through this stage of the Scrum method, the development of the requirements will be presented as user stories divided into three sprint, the user stories will be shown according to their corresponding sprint in order of execution.

- **First Sprint:** For this first stage of deliverables, the first sprint was given 17 user story points, which are equivalent to the speed this sprint will take. This iteration was divided between three user stories. As the first development of user stories for the first Sprint, user story number 8 was executed, as shown in Fig. 3(a), which has the purpose of providing the student with a choice between two ways to perform an exam. On the one hand, one will have the functionality of being able to develop it without having any qualification, thus giving an advantage to the student to be able to practise the topics he/she believes convenient. On the other hand, a test was created to evaluate the student's level in different topics, to evaluate how much the student has learned up to that moment. On the other hand, Fig.3 (b) shows the user story number 10 as the second deliverable of the first sprint, which has the purpose of implementing tests with a voice assistant to facilitate its development. This voice assistant will

ask the questions, each of these questions contains four options set in buttons that contain audios with the answers, providing a simple use of the mobile application. Finally, as the last deliverable of the first sprint, the user story number 7, shown in Fig. 4(a), was defined. The purpose of this story is to generate motivational messages spoken by the voice assistant every time the student successfully completes each question in the exam.

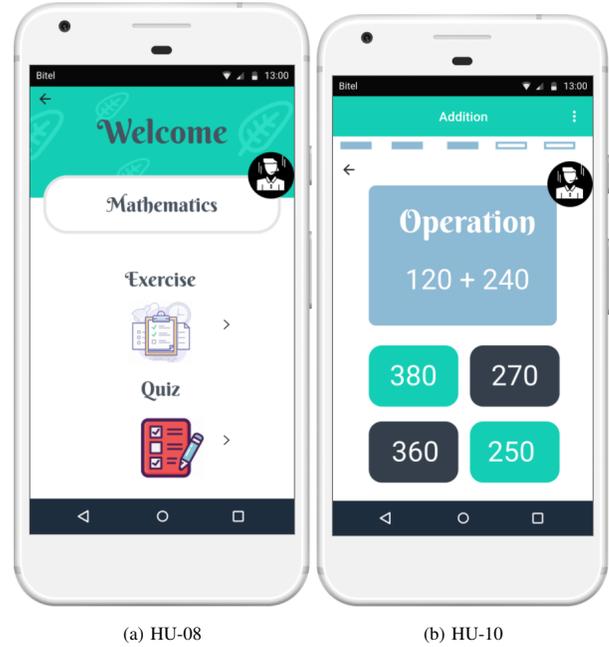


Fig. 3. First and Second Prototype.

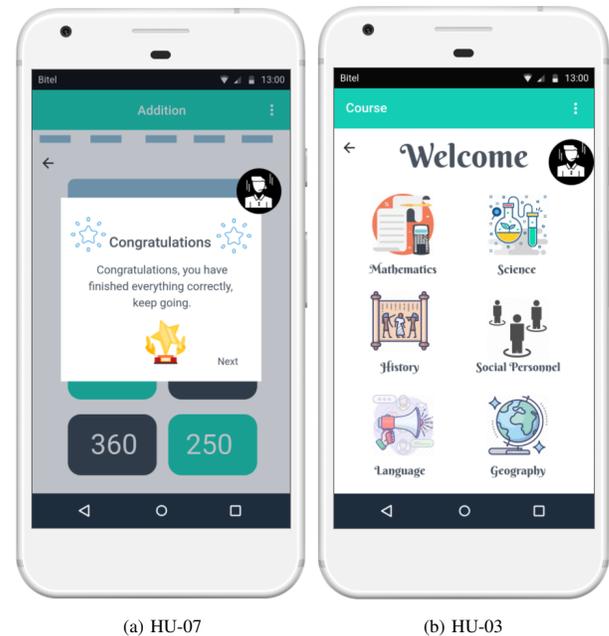


Fig. 4. Third and Fourth Prototypes.

- Second Sprint: In the second deliverable stage, 18 story points equivalent to the speed of the current Sprint, which contains 4 user stories, were established and the first deliverable was based on user story number 3. Therefore, it is reflected in the requirement that requests the submission of several courses for the educational growth of the student. Also, this varies according to the educational level of the student, which provides different courses according to their rank, an example of this is shown in Fig. 4(b). As a second deliverable within the second Sprint, was developed the user story number 4 as shown in Fig. 5(a), which has the functionality to separate the course into several topics establishing a greater order for their interaction, where the relationship between the student and the voice assistant is implied.

number 1, which aims to generate the connection between the system and the student. Therefore, a voice assistant was developed to perform and interact with the student in different functions, part of this can be seen in Fig. 6(b), where it is visualized that since the application is opened, the voice assistant is turned on.

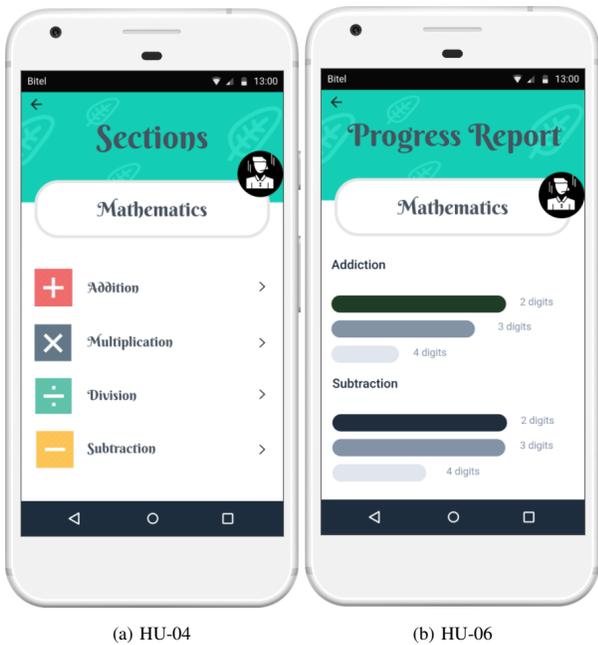


Fig. 5. Fifth and Sixth Prototypes.

On the other hand, the third deliverable of the second Sprint was developed based on the user story number 6, which has the purpose of generating a report regarding the student's development in the application, with the objective of being able to know according to statistics their progressive progress in different courses, as shown in Fig. 5(b). As the last deliverable of the second Sprint, user story number 9 was developed. The purpose of which was to establish an environment that divides the exams according to levels of difficulty, levels such as easy, moderate, normal, and difficult, giving the student the freedom to select according to their preference, as can be seen in Fig. 6(a).

- Third Sprint: In the third stage of the deliverables, 16 users story points were established, which are equivalent to the speed of the present sprint made up of 3 user stories. The first deliverable of the third Sprint was based on the development of the user story

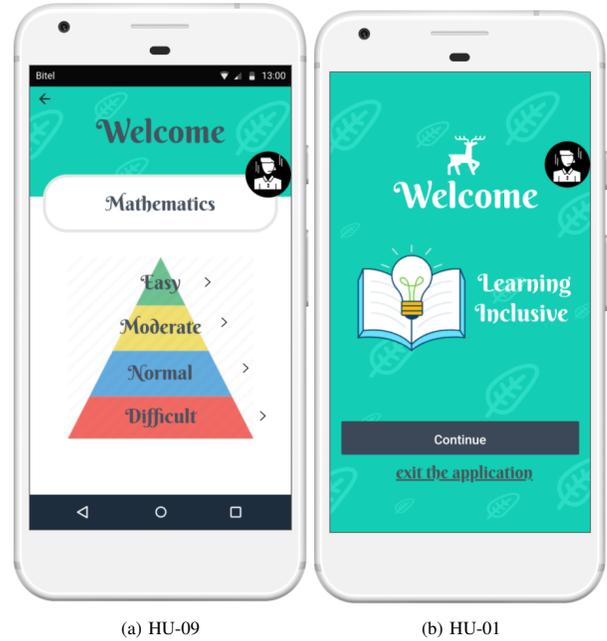


Fig. 6. Seventh and Eighth Prototypes.

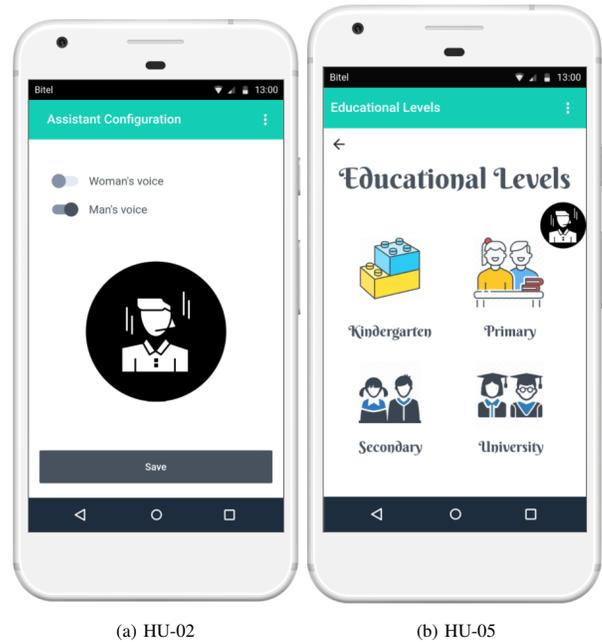


Fig. 7. Ninth and Tenth Prototypes.

As the second deliverable for this Sprint, user story number 2 was developed as shown in Fig. 7(a), this

has the purpose of establishing comfort for the student through their auditory interaction with the voice assistant by being able to decide the gender of the assistant in order to improve their experience. Finally, as the last deliverable for the third Sprint, the user story number 5 was developed as shown in Fig. 7(b), this has the purpose of granting and generating ranks referring to the educational level of the student, levels such as kindergarten, elementary, high school and college level.

4) *Review and Retrospective:* On the review and retrospective process of the research work, oriented to the scrum methodology, an analysis divided into two parts was established both at the project execution level and at the level of requirements fulfillment converted into user stories. On the other hand, for this stage, an analysis has been made using three of the main scrum graphs, with the objective of knowing the feasibility of the development of this project. The first graph established was the speed diagram. This diagram checks the development at acceleration level on the execution and the course of each Sprint, as you can see in Fig. 8 where it was determined as axis (X) the accumulation of points of user stories, also as axis (Y) was determined the number of sprints. On the other hand, through this diagram it was observed that the points established for each sprint according to the user stories were developed according to what was established.

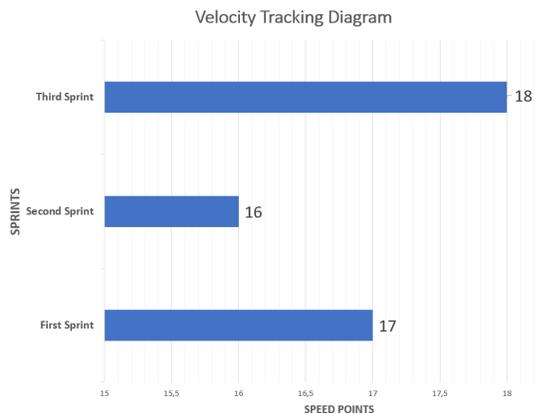


Fig. 8. Velocity Tracking Diagram.

The second graph shows the downward burned diagram, directed to the structural model on the story points and the ideal progress, where it was determined as axis (X) the weeks of project development and as axis (Y) the story points, in the case of the story points it is started by the total of all the Sprint and subtracted by week according to the developed story points. The purpose of this diagram is to provide an analysis that relates the difference between an ideal time established and the real time obtained during the course of the project, as can be seen in Fig. 9. As a result of this, it was obtained that an adequate execution was not followed between week 1 and 3 due to the coupling of the team in different activities within the user stories deviating an ideal follow-up, after that the deviation was restored in week 4 allowing to conclude in the exact time that was predetermined in week 6.

Finally, the downward burned diagram was developed,

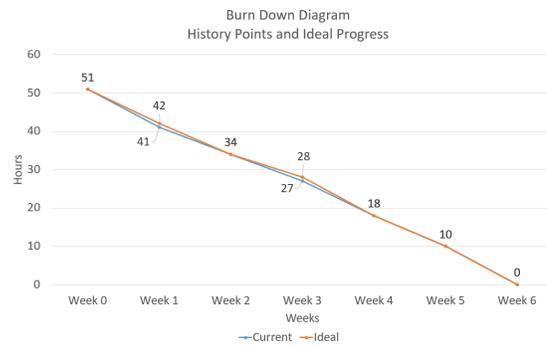


Fig. 9. Burn Down Scheme PI Method.

but unlike the previous one, the diagram is shown in Fig. 10 was oriented to the structural model on the remaining estimated effort. For this purpose, the weeks covered by the project development were determined as axis (X) and the hours of project development in each Sprint were determined as axis (Y). In the case of hours, the first data was the total accumulation of hours covered by all the Sprint, then the hours that have been completed are subtracted per week. By means of this diagram, it was analyzed, and it was possible to deduce that the execution of the project was totally in accordance with the established by the fact that it agrees to the number of weeks with respect to the previous table and to what was analyzed in the second part of the methodology.

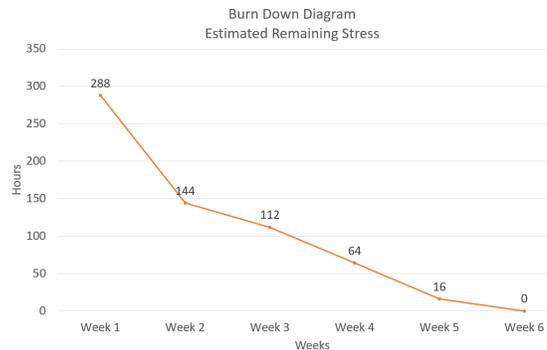


Fig. 10. Downward Burning Scheme EER Method.

C. Development Tools

1) *Android Studio:* This is a tool aimed at an embedded development environment for mobile application programming. In addition, it offers features that increase the production quality of mobile application development by providing a unified environment [16]. In addition, this development environment has the facility to generate suitable distribution, as well as to reuse code and resources for more agile development [17].

2) *Java Programming Language:* This programming language is one of the most recognized, provides the development and execution of various types of applications, highlighted by its structure and composition for programming, especially for mobile applications containing high adaptability, aimed at different mobile devices [18]. The main advantages are that it is a simple to understand language, object-oriented language,

distributed applications, and, finally, the security it provides [19] [20].

3) *Marvel App*: This tool facilitates the production of prototypes for mobile applications and web pages. It also provides better usability compared to other prototyping tools as it has greater definition with a better navigation structure [21]. In addition, its main advantages are based on collaborative work and its adaptability to the prototyping of different types of devices, as well as to the variation of operating systems [22].

4) *SQLite*: It is one of the databases with open source code with greater recognition at the level of related data, which contains functionality oriented to the practical and accessible use. On the other hand, this database, compared to the others, performs functions efficiently with greater speed [23]. In addition, its main features are based on reliability, better performance, better accessibility and stability by being consistent [24].

D. Software Architecture

For the implementation of the mobile application, the software architecture was determined on the pattern of layers. These layers have a horizontal structure. In this case, it is composed of 4 layers, each of them has a specific function with responsibility for the operation of the application. For this application it was oriented to closed layers, so each one works individually but intertwined to meet the needs of the application at a general level. The first layer is the presentation layer, whose primary function is to display the information through a particular format. Likewise, layer two is the business layer, which has the functionality to perform logical functions on the business and send the information to the presentation layer. On the other hand, layer three is the persistence layer or components for data access, this layer has the functionality of being the intermediary that allows access to the information in the database and directs it to the business layer. Finally, the database layer was placed, which does not generate any movement, only to generate the requested query. In addition to the layers mentioned above, the security layer and the service agents were implemented as shown in Fig. 11.

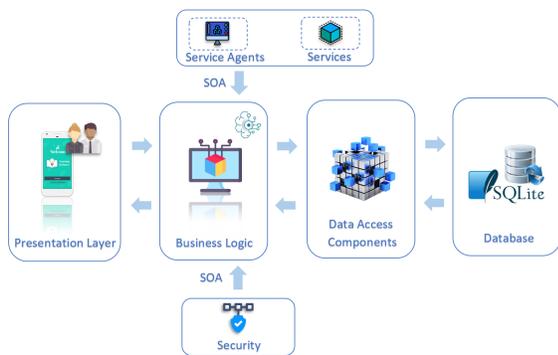


Fig. 11. Software Architecture.

E. Flow Diagram

In order to present the operation of the system on the mobile application, a flowchart is shown in Fig. 12, which

details the activities step by step that can be developed within all the implemented prototypes, such as the selection of the gender of the voice assistant, the selection of the type of exam together with its level of difficulty and the course in which the exam will be taken, among other functions.

IV. RESULTS

A. About the Methodology

We implemented the scrum methodology for this research work, and there were found different results about it. Both good characteristics and those that could harm the development of the project. That is why it was determined to separate these characteristics for the reason that the impact they can cause depends on their knowledge and management. Therefore, they were separated into advantages and disadvantages as shown in the Table IV. In spite of this, the Scrum methodology was continued for the reason that it is adequate for this research project, reducing risks, as well as avoiding loss of resources due to the fact that it is a methodology prepared to change and to maximize the results in the face of the requirements or needs of the project.

TABLE IV. SCRUM FEATURES

Advantages	Disadvantages
It provides quantifiable objectives, which generates anticipated results.	When one task is not completed, another task cannot be started, which causes the other tasks to be postponed.
The outcome and effort of the project are measured in the form of objectives and requirements.	It is required that the processes and their tasks go through an exhaustive definition.
Since it is divided into short periods, its verification tests are quick, which means that the detailed progress per sprint is known.	It is required that the team be made up of highly qualified and trained people.
Risks can be mitigated in advance without generating delays or loss of resources.	the team must have knowledge of the scrum process structure in detail.
Being a collaborative work and with a growth it is possible to increase the level of satisfaction of the project in terms of productivity and quality.	Constant meetings can generate stress to the development team, so it is necessary to prepare in advance.

- Methodological Comparison**

Before the end of the results and discussions stage, a comparison of the methodology implemented in this research work with the RUP methodology, which was one of the possible options to implement, but the selected methodology was Scrum, and what are the differences between them, which can be seen in Table V.

B. Sprint Analysis

On the other hand, we analyzed the course of the three sprints developed during the project with respect to an ideal fulfillment of the points of the users stories, which in total were 51 points between the three sprints. These sprints were analyzed using the Burn Down Chart diagram, each of these sprints had a duration of 2 weeks, giving a final time of one month and two weeks of development on the mobile application, without counting Sundays and using only 8 hours per day. The execution of the sprint began on August 30, 2021 and ended on September 11 of the same year.

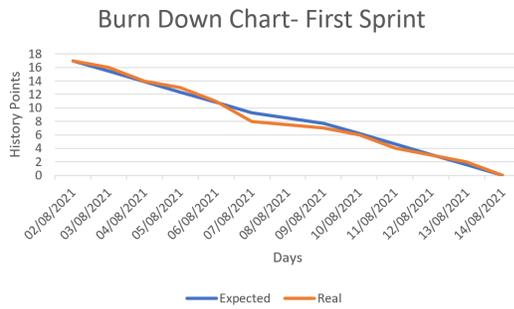


Fig. 13. Burn Down Chart - First Sprint.

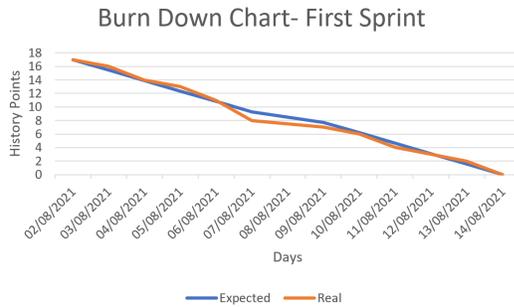


Fig. 14. Burn Down Chart - Second Sprint.

C. About Mobile Application Satisfaction

At this stage, a survey of 50 parents was conducted to evaluate the degree of satisfaction with the development of this mobile application for the benefit of inclusive education of blind students. Likewise, the objective of this evaluation is to know if the mobile application meets the requirements previously identified. Fig. 16 was structured by 5 options of the level of satisfaction that can be visualized in the axis (X) and as axis (Y) the number in which the result of the percentage obtained by the survey is located was determined. Using this diagram, it was possible to determine that the objectives of this research project had a good percentage of satisfaction on the part of the users and achieved the objectives set by the authors.

V. DISCUSSION

In comparison with other research works, related to the development of mobile applications and with the objective of

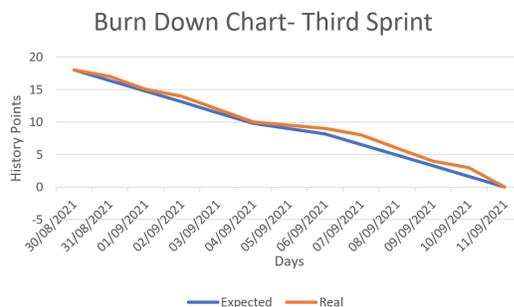


Fig. 15. Burn Down Chart - Third Sprint.

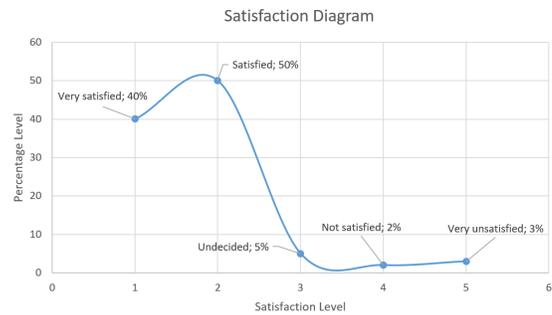


Fig. 16. Satisfaction Results.

promoting the inclusion of students who suffer from some disability that prevents them from learning development. In the article [25], it is visualized that they provide interfaces for taking evaluations, using technological methods that allow easy use. However, in this system there are interfaces that have not been designed for blind people such as login and registration, because they use text boxes where students have to fill, and not with the use of technological tools such as a virtual assistant that will guide the user to enter the application during their stay within the application, being one of the features that differentiates the application that is developed in this research work and other similar applications, as can be seen in Fig. 7(a), where there is a virtual assistant that can guide the student to enter the app and be able to develop the different activities within it. Continuing with the comparison of works, oriented in the development of educational learning mobile applications for the inclusion of students who have some impediment to be able to perform activities that usually other students can perform normally. In the article [26], it shows the design of an app aimed at children with Down syndrome disability in which, it offers writing and reading environments, where the child can learn interactively, however, this application is only aimed at a small group of students according to an age range and not with levels that the user can select and increase the level of learning, being one of the characteristics that differentiates this research work and in other similar application, as shown in Fig. 6(a), in which you can choose the level according to the user's decision. On the other hand, it does not have evaluation types such as practical evaluation and graded evaluation, being one of the features that stands out in this research work since it can benefit in academic development.

VI. CONCLUSION AND FUTURE WORK

Finally, a mobile application was developed to meet the objectives required by the users, such as benefiting and promoting the educational inclusion of blind students to improve the social environment of these people. It is also concluded that the use of the Scrum methodology is one of the most appropriate ways to carry out the management of software development since the purpose of this methodology is to work together and adapt to the changes that occur within the project. The application developed within the framework of this study will bring several benefits for students with visual impairment, which can improve the quality of teaching teachers to students since it is a tool capable of eliminating the standards of society, where blind people can't grow educationally due to their dis-

ability. Therefore, this objective was achieved. Also, as future work of this research should be taken as the beginning for a better inclusive education in Peru and in other Latin American countries, due to the fact that this type of tools can be improved by adopting new technologies for future updates as would be the case of the implementation of this mobile application with artificial intelligence and instruments for the comfort of the blind student. Finally, it is necessary to mention that with the development of this research work we want to motivate educational institutions and teachers recommending them to implement new teaching methods through these technologies so that students who have some kind of disability can reinforce their academic level inside and outside the classroom.

ACKNOWLEDGMENT

This research work was supported by the Universidad de Ciencias y Humanidades with its research institute. We also thank Dr. Sotomayor Beltran for his suggestions and recommendations in this research work.

REFERENCES

- [1] V. B. Kovač and B. L. Vaala, "Educational inclusion and belonging: a conceptual analysis and implications for practice," *International Journal of Inclusive Education*, vol. 25, no. 10, pp. 1205–1219, 2021. [Online]. Available: <https://doi.org/10.1080/13603116.2019.1603330>
- [2] C. Libiert and F. Nájera, "Una estructura digital accesible es un derecho humano de las personas con discapacidad visual," vol. 6, 2021.
- [3] A. P. Lintangari and I. Emaliana, "Inclusive education services for the blind: Values, roles, and challenges of university EFL teachers," *International Journal of Evaluation and Research in Education*, vol. 9, no. 2, pp. 439–447, 2020.
- [4] E. Asamoah, K. Ofori-Dua, E. Cudjoe, A. Abdullah, and J. A. Nyarko, "Inclusive Education: Perception of Visually Impaired Students, Students Without Disability, and Teachers in Ghana," *SAGE Open*, vol. 8, no. 4, 2018.
- [5] H. Miyauchi, "A systematic review on inclusive education of students with visual impairment," *Education Sciences*, vol. 10, no. 11, pp. 1–15, 2020.
- [6] J. C. Ponce Gallegos, B. A. Toscano, A. Silva Sprock, J. Muñoz Arteaga, and N. Aguas, "Educational inclusion in higher education: Mexico," *Proceedings - 14th Latin American Conference on Learning Technologies, LACLO 2019*, pp. 204–211, 2019.
- [7] L. O. Topin, R. Barwaldt, L. M. I. Ribeiro, D. Spidola, A. L. C. D. Freitas, M. Pias, M. Torres, and J. Sartori, "Towards Machine Learning for Enhanced Maths Teaching to the Blind," *Proceedings - Frontiers in Education Conference, FIE*, vol. 2019-October, 2019.
- [8] L. Chen, P. Chen, and Z. Lin, "Artificial intelligence in education: A review," *IEEE Access*, vol. 8, pp. 75 264–75 278, 2020.
- [9] E. G. De Oliveira, M. S. F. De Oliveira, N. R. Neto, F. De Paula Soldati, and T. L. C. Nassur, "Development and evaluation of a mobile educational application to support teaching of management of process in Operating Systems," *Proceedings - IEEE 20th International Conference on Advanced Learning Technologies, ICALT 2020*, pp. 19–21, 2020.
- [10] M. N. Islam, T. T. Inan, N. T. Promi, and S. Z. Diya, "Information and Communication Technologies for Humanitarian Services," *Information and Communication Technologies for Humanitarian Services*, no. April 2021, 2020.
- [11] B. K. Balasuriya, N. P. Lokuhettiarachchi, A. R. Ranasinghe, K. D. Shiwantha, and C. Jayawardena, "Learning platform for visually impaired children through artificial intelligence and computer vision," *International Conference on Software, Knowledge Information, Industrial Management and Applications, SKIMA*, vol. 2017-December, pp. 1–7, 2018.
- [12] Z. Masood, R. Hoda, and K. Blincoe, "Real World Scrum A Grounded Theory of Variations in Practice," *IEEE Transactions on Software Engineering*, vol. 5589, no. c, pp. 1–1, 2020.
- [13] S. Chantit and I. Essebaa, "Towards an automatic model-based scrum methodology," *Procedia Computer Science*, vol. 184, pp. 797–802, 2021. [Online]. Available: <https://doi.org/10.1016/j.procs.2021.03.099>
- [14] V. Gomero-Fanny, A. R. Bengy, and L. Andrade-Arenas, "Prototype of web system for organizations dedicated to e-commerce under the scrum methodology," *International Journal of Advanced Computer Science and Applications*, vol. 12, no. 1, 2021. [Online]. Available: <http://dx.doi.org/10.14569/IJACSA.2021.0120152>
- [15] A. F. Acosta, J. E. Espinosa, and J. Espinosa, "Application of the SCRUM Software Methodology for Extending Simulation of Urban MObility (SUMO) Tools," pp. 3–15, 2019.
- [16] I. Khokhlov and L. Reznik, "Android system security evaluation," *CCNC 2018 - 2018 15th IEEE Annual Consumer Communications and Networking Conference*, vol. 2018-January, pp. 1–2, 2018.
- [17] A. Sarkar, A. Goyal, D. Hicks, D. Sarkar, and S. Hazra, "Android Application Development: A Brief Overview of Android Platforms and Evolution of Security Systems," *Proceedings of the 3rd International Conference on I-SMAC IoT in Social, Mobile, Analytics and Cloud, I-SMAC 2019*, pp. 73–79, 2019.
- [18] M. A. Amasha, M. F. Areed, D. Khairy, S. M. Atawy, S. Alkhalaf, and R. A. Abougala, "Development of a Java-based Mobile application for mathematics learning," *Education and Information Technologies*, vol. 26, no. 1, pp. 945–964, 2021.
- [19] N. Meng, S. Nagy, D. D. Yao, W. Zhuang, and G. A. Argoty, "Secure coding practices in Java," pp. 372–383, 2018.
- [20] S. Liu, "Explore Java Language and Android Mobile Software Development," vol. 3, no. 2, pp. 5–9, 2021.
- [21] R. O. Nia, "Komparasi Perangkat High-Fidelity Prototyping Untuk Aplikasi Bergerak Augmented Reality (Studi Kasus : Marvel dan Proto . io)," p. 88, 2018.
- [22] A. A. Permana, R. Taufiq, and S. Ramadhina, "Prototype design of mobile application 'hydrolite' for hydroponics marketplace," in *2020 7th International Conference on Electrical Engineering, Computer Sciences and Informatics (EECSI)*, 2020, pp. 45–48.
- [23] Z. Shen, Y. Shi, Z. Shao, and Y. Guan, "An Efficient LSM-Tree-Based SQLite-Like Database Engine for Mobile Devices," *IEEE Transactions on Computer-Aided*

- Design of Integrated Circuits and Systems*, vol. 38, no. 9, pp. 1635–1647, 2019.
- [24] Y. Wang, Y. Shen, C. Su, J. Ma, L. Liu, and X. Dong, “CryptSQLite: SQLite with High Data Security,” *IEEE Transactions on Computers*, vol. 69, no. 5, pp. 666–678, 2020.
- [25] A. Carrion-Silva, C. Diaz-Nunez, and L. Andrade-Arenas, “Admission Exam Web Application Prototype for Blind People at the University of Sciences and Humanities,” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 12, pp. 377–382, 2020.
- [26] R. Arias-Marreros, K. Nalvarte-Dionisio, and L. Andrade-Arenas, “Design of a Mobile Application for the Learning of People with Down Syndrome through Interactive Games,” *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 11, pp. 715–721, 2020.

Design and Implementation of HSQL: A SQL-like language for Data Analysis in Distributed Systems

Anurag Singh Bhadauria¹
Computer Science and Engineering
R. V. College of Engineering
Bengaluru, India

Atreya Bain²
Computer Science and Engineering
R. V. College of Engineering
Bengaluru, India

Prof. Jyoti Shetty³
Computer Science and Engineering
R. V. College of Engineering
Bengaluru, India

Dr. Shobha G.⁴
Computer Science and Engineering
R. V. College of Engineering
Bengaluru, India

Arjuna Chala⁵
Sr. Director, Innovative Technologies
LexisNexis Risk Solutions
Atlanta, U.S.A

Jeremy Clements⁶
Software Engineer III
LexisNexis Risk Solutions
Atlanta, U.S.A

Abstract—In today's modern world, we're experiencing a substantial increase in the use of data in various fields, and this has necessitated the use of distributed systems to consume and process Big Data. Machine learning tends to benefit from the usage of Big Data, and the models generated from such techniques tend to be more effective. However, there is a steep learning curve to getting used to handling Big Data, as traditional data management tools fail to perform well. Distributed systems have become popular, where the task of data processing is split amongst various nodes in clusters. SQL, is a popular database management language popular to data scientists. It is often given second class support, where SQL can be embedded into a primary language of use (e.g. SQL in Scala for Spark), which allows for using SQL but one still needs to know the primary language of the platform (Scala, as per the example, or ECL in HPCC Systems). It may also be present as a supported language. In either case, using useful tooling such as Visualizing data and creating and using machine learning models become difficult, as the user needs to fall back to the primary language of the system. In the proposed work, a new SQL-like language, HSQL, an open source distributed systems solution, was developed for allowing new users to get used to its distributed architecture and the ECL language, with which it primarily operates with (which was chosen as a target). Additionally, a program that could translate HSQL-based programs to ECL for use was made. HSQL was made to be completely inter-compatible with ECL programs, and it was able to provide a compact and easy to comprehend SQL-like syntax for performing general data analysis, creation of Machine learning models and visualizations while allowing a modular structure to such programs.

Keywords—*ANTLR4; big data; context free grammar; distributed systems; HPCC; Javascript; language; machine learning; Parser; SQL; transpiler*

I. INTRODUCTION

Data has become an essential resource in this age of computing, where a lot of the advancements and innovations we see right now, are based upon models which require huge amounts of data to be built. There has been widespread adoption of Machine Learning, and Data Analysis tools have become ever more important, especially with Big Data being increasingly common. SQL has been a widespread language that has been primarily used and well known to data analysts,

for data analysis; especially due to the time its been around and its prevalence in relational databases.

Big data, has made it somewhat difficult to continue using traditional tools for data analysis, where standard databases would take too long to process the data. This, has led to a boom in the usage of Distributed Systems, where data is processed with the use of multiple different computing systems (often referred to as nodes) in a cluster. If done effectively, distributed computing is a vastly better option as it is not possible to vertical scaling (using more powerful hardware) cannot keep up with the scale and volume of data that is being generated nowadays. [?]

Distributed Systems have become popular, with Hadoop being a well-known option. Hadoop's core technologies are based on a storage section, and a processing part; it offers a huge library of plugins and integrations which allow it to be easily used for a variety of use-cases. Spark, is one such plugin that is known as a unified analytics engine, used as part of Hadoop. The primary languages used here are a mixture of SQL acting as a second-class language and Scala as the primary language of use. [?]

This is commonplace, as pure SQL often makes data analysis difficult (Eg. Visualizations and Machine Learning aren't a part of SQL). Here, SQL takes a second-class language approach where it is embedded in a primary language (e.g. in Scala for Spark [?], in ECL for HPCC Systems[®]). There are also places where SQL have first-class support, but here access to valuable tools such as visualizations and working with Machine Learning Models as well as commonplace language features get restricted, which have become commonplace and important since the time SQL was developed.

As such technologies are being applied everywhere, having a steep learning curve for such tools would be rather inconvenient. Hence, as data analysis grows more important, there is a good need for an SQL-like analytics language that has support for querying, visualization and machine learning.

Hence, HPCC Structured Query Language – HSQL was developed, a language that is SQL-like, for focusing on easy-to-learn and simple data analytics. HPCC Systems was chosen as

the target architecture; an open source platform developed by LexisNexis® Risk Solutions, which uses commodity hardware for data-intensive parallel computing. The platform presents an all-in-one integrated data lake solution that is extremely versatile and removed from the MapReduce Architecture of Hadoop that allows for much more versatile programming. HSQL is open-source, easy to write, comprehend and transpiles to ECL for use in HPCC Systems. Many of the typical preprocessing for ECL is abstracted away in HSQL, and the simple SQL-like syntax eases the learning curve related to getting started with HPCC Systems. Additionally, targeted to work with ECL, HSQL compliments ECL very well by providing an abstraction that is easy to use by data scientists who are already familiar with SQL; where data scientists can still take their time to learn the more complex and powerful ECL language for any complex solution they may require. This helps quickly bridge the skill gap to use the same Data Lake to both shape the data (ECL) and perform analytics (HSQL). Here, some key concepts of HPCC Systems will be introduced in order to explain the architecture that HSQL targets, and the features to be used. Following this, a design for HSQL is shown which presents a concrete syntax and then, an implementation for a compiler that translates the specification to ECL, the language used in HPCC Systems.

II. HPCC SYSTEMS AND ECL

HPCC Systems (High Performance Computing Clusters), an open source platform developed by LexisNexis® Risk Solutions, has been used to set up a cluster, distribute the data and perform all the operations parallelly for a faster and a more effective computation. HPCC Systems provide high performance, parallel processing and delivery for applications using big data. It is open source, and presented as an all-in-one solution as a data lake and big data processing system that makes it easy and fuss-free to work with [?].

The entire platform (Fig. ??) is divided into separate platforms, each optimized for a specific workload. The first of these platforms is called Thor, a data refinery whose overall purpose is the general processing of massive volumes of raw data of any type. A Thor cluster is similar in its function, execution environment, filesystem, and capabilities to the Google and Hadoop MapReduce platforms [?]. The second platform, named as Roxie, functions as a rapid data delivery engine. A Roxie cluster is similar in its function and capabilities to Elasticsearch and Hadoop with HBase and Hive capabilities added.

HPCC Systems, including both Thor and Roxie clusters utilize the ECL programming language for implementing applications, a data-centric declarative language designed specifically for huge data projects using the HPCC Systems platform [?] [?]. Each of the platforms use the declarations in a way that best aligns with its goals for performance and latency. ECL as a language allows for power ETL operations to be carried out.

Its extreme scalability comes from a design that allows you to leverage every query you create for re-use in subsequent queries as needed [?]. ECL, is a powerful language, and due to its expansive and declarative nature, it is well suited for performing data extraction, cleaning, normalizing and aggregating [?].

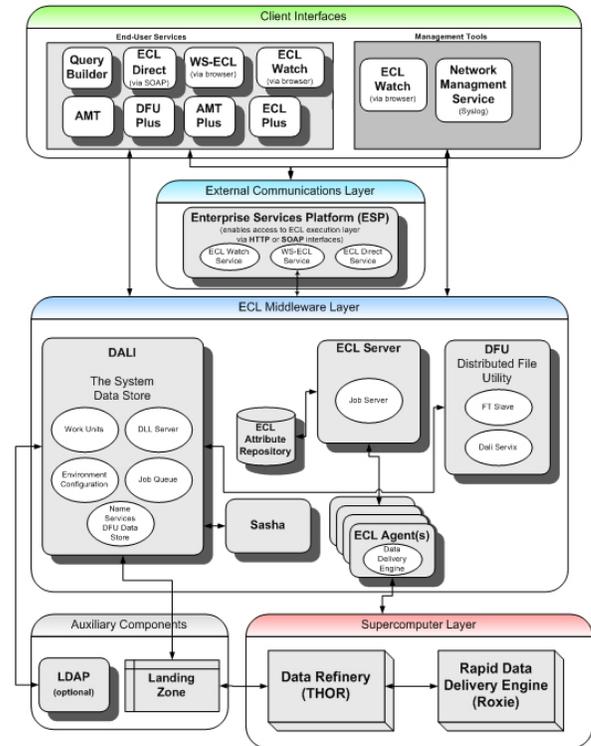


Fig. 1. HPCC Systems Structure - CC/SA.

As HSQL is intended to be for data analysts, ECL was chosen as a target due to its highly optimizing compiler and that machine learning performs exceptionally fast in HPCC Systems, even outperforming similarly configured Hadoop for the first iteration of many configured Machine Learning Algorithms.

HSQL is intended to be used in HPCC Systems, where the primary intention is to complement ECL. The primary purpose is to provide simpler syntax for common data operations, without needing to know ECL but also introducing key concepts of ECL and HPCC Systems along the way.

III. DESIGN AND IMPLEMENTATION: HSQL

Building a language such as HSQL, that can be used, would at least require a basic grammar specification and some way of executing it on a machine. Languages either translate to another language of lesser or similar levels of abstraction. This operation of translation, is done by compilers [?]. Software that translate programs to similar levels of abstraction, are specifically termed as Transpilers (e.g. Babel, which is a Javascript to Javascript transpiler). Below sections will first define a syntax then describe the various steps used to translate HSQL to the target language ECL (Fig. ??). In the following subsections, the HSQL language will be discussed as a language, followed by a brief description of the implementation process.

A. Defining the HSQL Syntax

The first step towards making HSQL, was to define the syntax and a barebones featureset. HSQL is a language designed to be SQL-like, and yet, expose many features of ECL

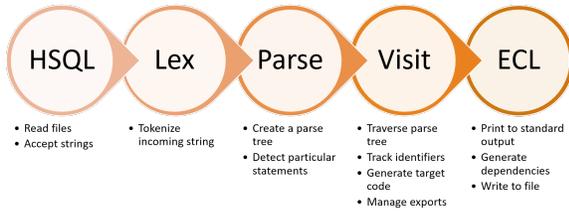


Fig. 2. General Conversion Workflow.

such as modules, layouts (analogous to SQL's CREATE TABLE) and actions. The general syntax of statements can be seen as:

```
<identifier_name> = <statement>;
```

Actions have been defined with the following syntax:

```
<action> <identifier> [options];
```

A <statement> would be an SQL select statement which uses existing definitions or loads up a dataset from a table.

Listing 1: Simple statement and an action

```
p = SELECT * FROM table1;
OUTPUT p;
```

This syntax was made to keep a lot of similarity to SQL, but to slowly introduce concepts of ECL to a user, such as imports and modules. Actions written above are always run in sequential order. Like SQL, HSQL is also intended to be case-insensitive, including its variables (additionally as ECL is also case-insensitive).

Definitions in HSQL, can be exported, by writing an optional export statement at the end, listing all the identifiers, which shall be exported. HSQL, unlike ECL, presents only two visibility modes, for ease of use and understanding. HSQL definitions convert to SHARED or EXPORT in ECL.

The language was designed to be completely compatible with ECL, and the transpiler developed, provides optional type checks. (Imports from ECL files do not support type checking, except a type definition file can be added in.) The language also allows an optional export statement at the end, to allow for specific definitions to be exported and available for use as a module.

The general syntax of a program is intended to be (<, > implying mandatory features, [,] implying optional):

Listing 2: General Syntax

```
import <identifier> [as <alias>];
<identifier> = <definition>;
<action> <identifier> <options>;
...
[export <identifier1>[,<identifier2>[,<identifier3>
>,...]];
```

1) *Layouts*: Layouts can be considered as a structure for a dataset (analogous to a structure definition in C). The syntax for them is similarly designed as:

Listing 3: Creating a sample layout with two columns

```
sampleLayout = CREATE LAYOUT(
  c1 integer,
  c2 string
);
```

sampleLayout internally in the target language will be represented by a record, a case of one-to-one translation.

2) *Plotting*: Plotting is another important part of HSQL, as a way of visualizing data to understand it better. This is done with the use of the plot statement.

Listing 4: Plotting a table

```
plot from table1 title 'Optional_title' type Column;
```

On the target language, visualizations are made by a named output, followed by calling the respective call to an appropriate Visualizer bundle function. These two statements are wrapped into a singular statement in HSQL.

3) *Machine Learning*: The idea behind using Machine Learning in HSQL is to be able to easily create and use Machine Learning models. This is done by using the train and predict statements.

Listing 5: Making a model

```
model = train from ind,dep method LinearRegression;
```

The making of model requires anywhere from 3-6 statements in ECL, which involves adding a sequential ID, converting from the standard row-based form to the ML bundle compatible cell-based form and then calling the model creation statement on the result (Which is based on the method required). This is represented in one singular statement in HSQL.

Similarly, the predict statement can be used to make predictions from models. This similarly requires some table conversions, and is represented via a singular statement in HSQL.

```
modell_predict = predict modell from test_ind method
RegressionForest;
```

B. Language Recognition

As the language and its primary featureset been established, the target implementation was carried out; The general syntax of the language, was written in CFGs (Most languages are expressed as a context free grammar at the syntactic analysis phase [?]), so that it can be passed to ANTLR4. ANTLR4 is able to accept a CFG (Context Free Grammar) which does not contain left recursive derivations [?] to create lexers, and parsers which use the ALL(*) parsing methodology for generating a parse tree for the given CFG. The lexers and parsers created support a variety of targets languages, including C++, JavaScript, C# and so on. For this work, JavaScript was chosen as it would allow fast development and allow for further integration in web services. The lexer and the parsers created, are able to take in a stream of text, and break them up into tokens, and then construct a parse tree (Fig. ??) according to the grammar made for the language. ANTLR4 sets up the class structure for each node in the parse tree, which is useful while processing the parse tree [?].

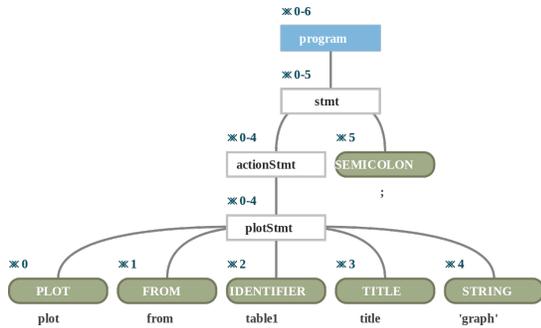


Fig. 3. Parse Tree for a Simple Statement.

The core of the conversion is through ANTLR4 and using String Templates to template generated code. The translation of HSQL to ECL happens in two phases - both in the parsing stage and while processing the parse tree nodes.

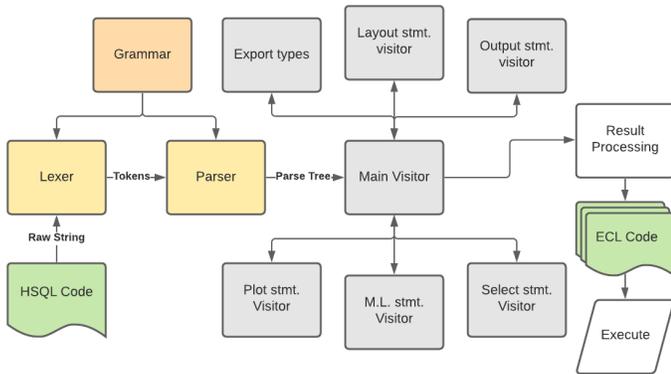


Fig. 4. Basic Architecture for the Program.

The process of walking the parse tree was split into various visitors as per the architecture Fig. ??, which allows for better code readability and better structure. The visitors (Objects written under the well-known visitor pattern [?]), traverse the parse tree, calling other visitors as required, and return the specific translations. The visitors also perform other important functions, and some of the other functions are enumerated as we go along.

1) *Symbol Table Management*: HSQL uses a flat table of identifiers; it does not have scoping; Identifiers and their types are tracked by the transpiler where available via an object oriented symbol Table [?]. ECL, which is the language HSQL converts to, does have the concept of types, and hence this applies to HSQL too. However, this cannot be read easily. This has been counteracted by making type checking optional - HSQL will attempt to obtain and infer types when possible and show issues with it if present, but otherwise will allow the users to continue. As it needs to be compatible with ECL, such type checking is kept optional.

Listing 6: Selecting from a module

```
import module1;
a = select coll from module1.table1;
```

In the above example ??, if there exists a module1.hsql, then that file is parsed. Similarly, if there exists a module1.

ecl file, that is also referred to for understanding what types are exported. In these cases, the compiler can check if table1 exists, and can raise an error if table1 or coll does not exist. However, if no files are found, then a compiler error is raised. Additionally, if there is only a module1.ecl, in that case no checking is done, and all columns are allowed; ie. the types are not known, and can be as per the user's discretion.

Listing 7: dummy.ecl - ECL File

```
export dummy := module
export Layout1 := RECORD
    INTEGER col1;
    STRING25 col2;
END;
export Layout2 := RECORD
    INTEGER col3;
    STRING col4;
END;
export someTable := TABLE(DATASET([[1,'foo']],
    Layout1));
export someTable2 := TABLE(DATASET([[2,'bar']],
    Layout2));
end;
```

Listing 8: dummy.d.hsql - ECL File's Type Definition

```
map export a INTEGER;
map export someTable TABLE ( col INTEGER,col2 STRING
);
map export someTable2 TABLE (col3 INTEGER,col4
STRING);
```

In HSQL, ECL files can be imported without any issues, but do not have any form of type checking, but this can be worked around, by adding a type definition file (File that mentions the export types, with extension .d.hsql). Imported HSQL files, are parsed in a recursive manner, and their exported types are extracted and used.

2) *Dependency Tracking*: The primary visitor in the transpiler implemented, tracks all the dependencies and allows for recursively parsing dependent HSQL modules too. Additionally, for every ECL file imported, it looks for a corresponding type definitions file (File with same name but .d.hsql extension) to provide the types exported by it. Cyclic imports are prevented by the use of an import list which keeps track of all the imports that have occurred for a given module to require transpilation.

3) *Actions Collecting*: Collecting actions - All the actions that are mentioned in HSQL, are tracked, as they are translated to definitions for the action. To ensure modules can be executed, the target ECL code contains a main function export, that calls on all the actions sequentially. This, allows modules to keep actions that can be executed. This is not usually used in ECL, but is retained in HSQL for maintaining ease of use. An example for this is shown later on.

4) *Module Support*: Module field visibility is done by an export statement, present at the end of the program. Here, specific identifiers can be marked for being exported.

Listing 9: Source HSQL

```
import source;

-- lets see the marks for each column
markslist = select marks from source.marks ;
-- or even better
```

```
output markslist title 'marksList';

-- lets get all the average marks of each subject
counting = select subid,AVG(marks) from source.
marks group by subid order by subid ;
// join this to get the subject names
marksJoined = select * from counting join source.
subs on counting.subid=source.subs.subid;

output marksJoined title 'avgmarks';
```

Listing 10: Target ECL - Wrapped in a Module

```
IMPORT source ;
export hsqlc:= MODULE
SHARED markslist := TABLE(source.marks,{marks});
SHARED _reservedaction0 := OUTPUT(markslist,,NAMED('
marksList'));
SHARED counting := SORT(TABLE(source.marks,{subid,
REAL marks := ave(GROUP,marks)},subid),subid);
SHARED marksJoined := TABLE(JOIN(counting,source.
subs,LEFT.subid = RIGHT.subid,INNER));
SHARED _reservedaction1 := OUTPUT(marksJoined,,NAMED
('avgmarks'));
EXPORT main := FUNCTION return PARALLEL(
_reservedaction0,_reservedaction1); END;
```

After translating the statements, two tasks need to be executed:

- Arranging the tasks to be executed into a main field that will be exported to be executed
- Wrapping the translated statement into an ECL module.

The main visitor then returns the resultant statements as an array to the rest of the program (which handles the arguments, errors and output). The rest of the module wraps the output of the visitors, and allows access to the types as understood by HSQLC, and warnings and errors that may have been raised by it.

C. Transpiler

The lexer, parser and the visitor are only part of the whole program, which makes up the transpiler HSQLC which is used to translate HSQL to ECL. The whole program wraps up the above components, in a command line UI, and provides:

- Wrappers to read and write files for the visitors as required.
- A general command line user interface for accepting files, arguments, and for presenting errors and warnings neatly.
- Endpoints for interfacing with the transpiler. Various functions for providing a string or a file is provided. These function calls also have Typescript definitions, to allow use inside a TypeScript environment as well.

The transpiler can hence run as a command line tool for transpiling HSQL files to ECL files, or function as a module that can be called on to provide translation, syntax highlighting and other such language features.

IV. FEATURES OF THE PROPOSED LANGUAGE

The HSQL language and the transpiler hence built, had a set of notable features which should prove it easy to use and integrate into existing workflows.

Intercompatibility

HSQL was designed to be fully compatible with the existing structure of HPCC Systems, and is completely inter-usable with ECL. HSQL modules can be imported from within ECL after translation, and HSQL can make use of existing ECL modules to provide extended functionality or use data from other sources.

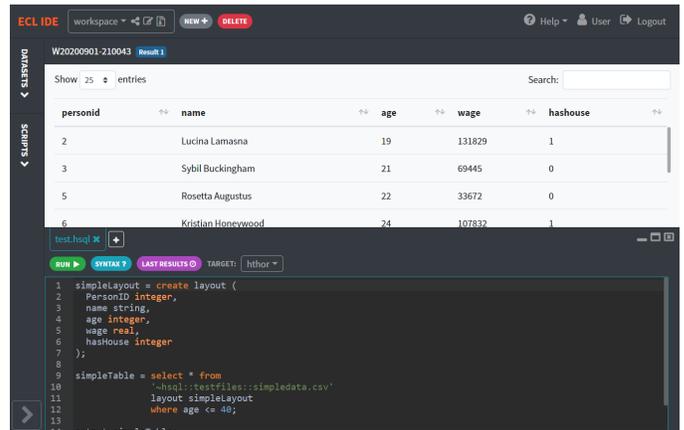


Fig. 5. ECL Cloud IDE, using HSQL.

Integration

As the transpiler(HSQLC) was made using Javascript, it is rather easy to integrate into web solutions, and use for supporting HSQL in a web environment. Using this, it was also integrated into the ECL Cloud IDE Fig. ??, a web-based solution for running ECL on a HPCC Systems cluster.

HSQLC was also used to create a language server to provide language support for HSQL in popular IDEs. The initial target was VSCode, but as the Language Server Protocol Fig. ?? is well established, it can be easily ported over to other IDEs which support using the LSP [?] [?].

V. CONCLUSIONS

The language HSQL was defined, which lets users write SQL-like queries without worrying about most of the preprocessing required in HPCC Systems while using ECL, and a basic syntax set was produced, for performing filters, joins, sorts, and so on. This, allows for HPCC Systems as a Distributed Systems to be accessed and used easily by a person who is familiar with SQL. The transpiler HSQLC was created to be able to use this language, was able to successfully translate HSQL to ECL, and was able to correctly report syntax and semantic errors, while also allowing HSQL and ECL modules to be used interchangeably. The compiler can also report the data types for the variables used in its program to help with integration into IDEs.

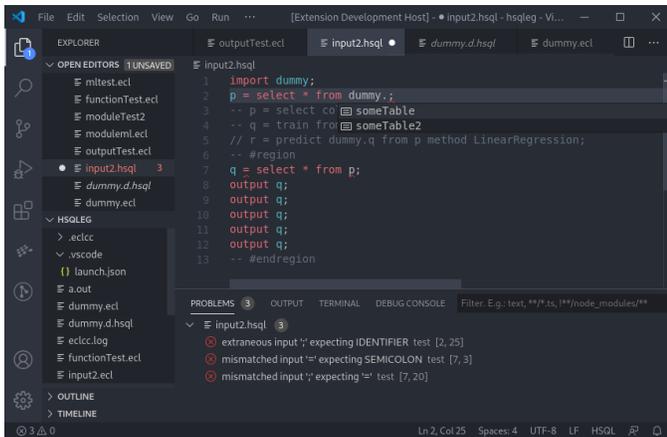


Fig. 6. Language Server - Providing Syntax Highlighting, Completion and Error Highlighting.

Using this, HSQLC was also integrated into a language server, creating a VSCode Extension, which could be used to provide language support in development environments, and also in ECL Cloud IDE, to easily allow writing HSQL in a web-based editor.

Testing was set up for testing the validity of the machine learning models created and basic syntax, which reported predictions within good intervals. Various examples have also been shown to showcase the syntax in HSQL ?? ?? ?? ??, comparing it to the translated code in ECL. These program snippets compare the languages and show how some of the boilerplate code in ECL is automatically generated by the HSQL compiler. A complete file transpilation is also shown, ?? where a simple Random Forest Regression model is created.

Limitations and Future Work

The current solution focuses on extensibility, usability and simplicity heavily.

HSQL, contains only some basic operations in the current revision, and can be extensively improved by adding in syntax for other ECL features which can still use a SQL-like syntax, which should improve its usability and allow for greater and more extensive usecases.

HSQLC, has been made as a simple command line, and hence, is an additional step require to run a program on HPCC Systems. This can be worked around by automating the process (e.g. by using a task automation toolkit/make utility), or by integrating it with existing systems. The compiler can also be better maintained with the help of static typing [?], although this is slightly impeded by ANTLR4 Typescript support still being in the works at the time of writing.

The language server developed for HSQL uses HSQLC to provide language support in IDEs, and performs syntax checking, but cannot perform syntax highlighting [?] as of

the current specification, and requires the use of IDE-specific extensions (e.g. VSCode requires providing a Textmate Grammar) for syntax highlighting.

REFERENCES

- [1] A. Prasad, G. Shobha, N. Deepamala, S. S. Badhya, Y. Yashwanth and S. Rohan, "Machine Learning Techniques to Understand Partial and Implied Data Values for Conversion of Natural Language to SQL Queries on HPCC Systems," 2019 4th International Conference on Computational Systems and Information Technology for Sustainable Solution (CSITSS), 2019, pp. 1-5, doi: 10.1109/CSITSS47250.2019.9031035.
- [2] E. Shaikh, I. Mohiuddin, Y. Alufaisan and I. Nahvi, "Apache Spark: A Big Data Processing Engine," 2019 2nd IEEE Middle East and North Africa COMMUNICATIONS Conference (MENACOMM), 2019, pp. 1-6, doi: 10.1109/MENACOMM46666.2019.8988541.
- [3] Michael Armbrust, Reynold S. Xin, Cheng Lian, Yin Huai, Davies Liu, Joseph K. Bradley, Xiangrui Meng, Tomer Kaftan, Michael J. Franklin, Ali Ghodsi, and Matei Zaharia. 2015. Spark SQL: Relational Data Processing in Spark. In Proceedings of the 2015 ACM SIGMOD International Conference on Management of Data (SIGMOD '15). Association for Computing Machinery, New York, NY, USA, 1383–1394. DOI:https://doi.org/10.1145/2723372.2742797
- [4] HPCC Systems, "Why HPCC Systems is a superior alternative to Hadoop", [Online] Available: <https://hpccsystems.com/about/hpcc-hadoop-comparison/superior-to-hadoop>
- [5] HPCC Systems, "Introduction to HPCC Systems", 2015, [Online] Available: http://cdn.hpccsystems.com/whitepapers/wp_introduction_HPCC.pdf. [Accessed July 1, 2020]
- [6] A.M. Middleton. Handbook of Cloud Computing. Springer, 2010., Handbook of Cloud Computing, "Data-Intensive Technologies for Cloud Computing" [Online] Available: <https://www.springer.com/gp/book/9781441965233>
- [7] HPCC Systems, "ECL Language Reference", 2020, [Online] Available: https://d2wulyp08c6njf.cloudfront.net/releases/CE-Candidate-7.8.24/docs/EN_US/ECLLanguageReference_EN_US-7.8.24-1.pdf . [Accessed July 1, 2020]
- [8] Aho, Sethi, Ullman, Compilers: Principles, Techniques, and Tools, Addison-Wesley, 1986.
- [9] N. Chomsky, "Three models for the description of language," in IRE Transactions on Information Theory, vol. 2, no. 3, pp. 113-124, September 1956, doi: 10.1109/TIT.1956.1056813.
- [10] Parr et al., Adaptive LL(*) "Parsing: The Power of Dynamic Analysis", [Online] Available: <https://www.antlr.org/papers/allstar-techreport.pdf>. [Accessed June 21, 2020]
- [11] Danyang Cao and Donghui Bai, "Design and implementation for SQL parser based on ANTLR," 2010 2nd International Conference on Computer Engineering and Technology, 2010, pp. V4-276-V4-279, doi: 10.1109/ICCET.2010.5485593.
- [12] Jens Palsberg1 C. and Barry Jay , "The Essence of Design Patterns", [Online] Available: <http://web.cs.ucla.edu/~palsberg/paper/compsac98.pdf>. [Accessed June 23, 2020]
- [13] J. F. Power and B. A. Malloy, "Symbol table construction and name lookup in ISO C++," Proceedings 37th International Conference on Technology of Object-Oriented Languages and Systems. TOOLS-Pacific 2000, 2000, pp. 57-68, doi: 10.1109/TOOLS.2000.891358.
- [14] Matt, Language Server Protocol, May 7 2020, [Online] Available: <https://nshpster.com/language-server-protocol/> [Accessed July 20, 2020]
- [15] Z. Gao, C. Bird and E. T. Barr, "To Type or Not to Type: Quantifying Detectable Bugs in JavaScript," 2017 IEEE/ACM 39th International Conference on Software Engineering (ICSE), 2017, pp. 758-769, doi: 10.1109/ICSE.2017.75.
- [16] Microsoft, "Language Server Protocol", [Online] Available: <https://microsoft.github.io/language-server-protocol/> [Accessed July 15, 2020]

APPENDIX - TRANSLATED EXAMPLES

TABLE I. SELECT STATEMENTS

HSQL	ECL
weatherSnowy = select Date ,SnowDepth from weather where SnowDepth>0;	weatherSnowy := TABLE(weather(SnowDepth > 0),{Date ,SnowDepth});
weather = select * from '~hsql::testfiles::weatherdata.csv' layout common. WeatherDataLayout;	weather := TABLE(DATASET('~hsql::testfiles::weatherdata.csv', common.WeatherDataLayout,CSV(HEADING(1))));
weatherSnowyNum = select COUNT(SnowDepth) from weather where SnowDepth>0;	weatherSnowyNum := COUNT(TABLE(weather(SnowDepth > 0),{SnowDepth}));
weatherSnowyTotal = select Sum(SnowDepth) from weather where SnowDepth>0;	weatherSnowy := TABLE(weather(SnowDepth > 0 and NewSnow > 0),{Date ,SnowDepth ,NewSnow});
weatherGrp = select Date ,SnowDepth from weather group by SnowDepth;	weatherGrp := TABLE(weather,{Date ,SnowDepth},SnowDepth);
weatherjoin = select * from weatherSnowDepth where newSnow>0 join weatherNewSnow on weatherSnowDepth.Date = weatherNewSnow.Date;	weatherjoin := TABLE(JOIN(weatherSnowDepth ,weatherNewSnow ,LEFT.Date=RIGHT.Date ,INNER)(newSnow > 0));

TABLE II. PLOTTING

HSQL	ECL
plot from weatherSnowyTotal title ' SnowyDays' type bar;	_reservedaction4:= OUTPUT(weatherSnowyTotal ,NAMED(' SnowyDays')); _reservedaction5 := Visualizer.MultiD.Bar(' SnowyDays');

TABLE III. TRAINING A ML MODEL

HSQL	ECL
modell = train from ind, dep method RegressionForest;	ML_Core.ToField(ind ,_reserved_ind0); SHARED _reserved_ind1 := _reserved_ind0; ML_Core.ToField(dep ,_reserved_dep0); SHARED _reserved_dep1 := _reserved_dep0; SHARED _reserved_ind10 := PROJECT(_reserved_ind1 ,TRANSFORM(RECORDOF(LEFT) ,SELF.id:=COUNTER ,SELF:=LEFT)); SHARED _reserved_dep10 := PROJECT(_reserved_dep1 ,TRANSFORM(RECORDOF(LEFT) ,SELF.id:=COUNTER ,SELF:=LEFT)); SHARED modell := LearningTrees.RegistrationForest().getModel(_reserved_ind10 ,_reserved_dep10);

TABLE IV. PREDICTING RESULTS FROM A MODEL

HSQL	ECL
<pre>modell_predict = predict modell from test_ind method RegressionForest;</pre>	<pre>ML_Core.ToField(test_ind ,_reserved_test_ind0); SHARED _reserved_test_ind1 := _reserved_test_ind0; SHARED _reserved_test_ind00 := PROJECT(_reserved_test_ind1 , TRANSFORM(RECORDOF(LEFT),SELF.id:=COUNTER,SELF := LEFT)); SHARED modell_predict := LearningTrees.RegressionForest().Predict (modell ,_reserved_test_ind00);</pre>

TABLE V. CREATING A MODEL AND USING IT

HSQL (ols.hsqli)	ECL (ols.ecli)
<pre>import commonsimple; ind = select PersonID ,age from commonsimple.simpleTable where PersonID <5; dep = select PersonID ,wage from commonsimple.simpleTable where PersonID <5; output ind; output dep; test = select PersonID ,age from commonsimple.simpleTable where PersonID >4; model = train from ind ,dep method LinearRegression; result = predict model from test; output result;</pre>	<pre>IMPORT ML_Core ; IMPORT ML_Core.Types AS Types; IMPORT commonsimple ; IMPORT LinearRegression ; export ols:= MODULE SHARED ind := TABLE(commonsimple.simpleTable(PersonID < 5),{ PersonID , age }); SHARED dep := TABLE(commonsimple.simpleTable(PersonID < 5),{ PersonID , wage }); SHARED _reservedaction0 := OUTPUT(ind); SHARED _reservedaction1 := OUTPUT(dep); SHARED test := TABLE(commonsimple.simpleTable(PersonID > 4),{ PersonID , age }); ML_Core.ToField(ind ,_reserved_ind0); SHARED _reserved_ind1 := _reserved_ind0; ML_Core.ToField(dep ,_reserved_dep0); SHARED _reserved_dep1 := _reserved_dep0; SHARED _reserved_ind10 := PROJECT(_reserved_ind1 ,TRANSFORM(RECORDOF(LEFT) ,SELF.id:=(COUNTER-1)/MAX(_reserved_ind1 , _reserved_ind1.number)+1,SELF:=LEFT)); SHARED _reserved_dep10 := PROJECT(_reserved_dep1 ,TRANSFORM(RECORDOF(LEFT) ,SELF.id:=(COUNTER-1)/MAX(_reserved_dep1 , _reserved_dep1.number)+1,SELF:=LEFT)); SHARED model := LinearRegression.OLS(_reserved_ind10 , _reserved_dep10).GetModel; ML_Core.ToField(test ,_reserved_test0); SHARED _reserved_test1 := _reserved_test0; SHARED _reserved_test00 := PROJECT(_reserved_test1 ,TRANSFORM(RECORDOF(LEFT) ,SELF.id:=(COUNTER-1)/MAX(_reserved_test1 , _reserved_test1.number)+1,SELF:=LEFT)); SHARED result := LinearRegression.OLS().Predict(_reserved_test00 ,model); SHARED _reservedaction2 := OUTPUT(result); EXPORT main := FUNCTION return SEQUENTIAL(_reservedaction0 , _reservedaction1 ,_reservedaction2); END; END;</pre>

Factors Influencing the Adoption of Cyber Security Standards Among Public Listed Companies in Malaysia

Mohamed Abdalla¹
Yusri bin Arshad⁴

Faculty of Technology Management
and Technopreneurship
Universiti Teknikal Malaysia Melaka
Melaka, Malaysia

Muath.Jarrah²

School of Information Technology,
Skyline
University College, 1797
Sharjah, UAE

Ahmed Abu-Khadrah³

College of Computing & Informatics
Saudi Electronic University
Riyadh, Saudi Arabia

Abstract—Employee’s failure to adhere to their organization’s cyber security policies contributes most of the cyber incidents. To secure information security systems, companies need to communicate behavioral and technical solutions to their employees, due to the fragility of the human factor since it plays a critically significant role in securing cyber systems. The necessity to safeguard information systems have speed up the evolution of the present method of cyber security, which should be based on adequately adopting cyber security standards to secure business enterprise’s assets and users in cyberspace. This paper studies factors influencing the adoption of cyber security standards among public listed companies in Malaysia. Through online survey that was distributed among 275 Public listed companies. The findings indicated that expected related benefits and perceived ease of use had significant impact on the adoption of cyber security standards. On the other hand, perceived security had played important moderating influence on the relationship between organizational factors and the adoption of cyber security standards.

Keywords—Cyber security; human factor; cyberspace; cyber security standards

I. INTRODUCTION

Cyber security standards are defined broadly to include principles, guidelines, codes of practice and technical specifications that are developed by public, private and not-for-profit entities, including government departments and agencies, national standardization bodies, industry alliances and associations [1].

Malaysian enterprise’s concern regarding cyber security issues is at the peak for the last decade. Business industries striving to securer their critical infrastructures as the core value are the significance of cyber protection, which is connected to the developing knowledge of information security. According to [2] Malaysian Airlines has reported critical data breach that comprised confidential data belongs to the companies’ clients. As a survey conducted by PricewaterhouseCoopers Malaysia, 42 percent of Malaysian organizations see an increased risk of cyber threats. In Malaysia, cybercriminals had hit losses equivalent to RM 1 billion, qualifying the nation to be the fifth riskiest country to cyber threats in 2019 [2].

Cyber Security, like any other application of technologies, requires standardization. As a result, a number of Cyber Security standards have been developed to govern the use of Cyber Security technologies in many fields. Specific standards, for example, exist to compel businesses to maintain safe infrastructures that limit the danger of cyber-attacks. Nowadays, Cyber Security is seen as a critical issue [3][30]. In order to secure cyber assets, organizations need to communicate technical and behavioral solutions to their employees, since the human factor has been considered the weakest line in the defense system, or at least it plays a critically significant role in securing cyber systems [4][30]. By assisting in the establishment of common security requirements and capabilities required for secure solutions, Cyber Security standards improve security and contribute to risk management. While it is impossible to remove all risks, Cyber Security standards make it more difficult for attacks to occur, or at the very least lessen the impact of those that do. The purpose of Cyber Security standards is to make information technology systems, networks, and critical infrastructures more secure [5]. If employees are not willing to accept cyber security standards, IS will not bring the full benefits of the technology to the Malaysian public listed companies [6]. Hence, the need has scaled exponentially for enterprises to adopt a new guideline of cyber security standards that could assist them mitigate data breaches, better comply with regulations and enhance cyberspace [7]. Policy makers, regulatory agencies and the industry are also increasingly agreeing that the adoption cyber security standards are required to ensure data protection, service continuity and public safety. The following are the contributions of the study:

- Perceived ease of use (PEU) is the most influential factor in the adoption of in the technological context.
- An expected related benefit is the most influential factor in the adoption of cyber security standards in the organizational context.
- Employee’s innovativeness is the most influential factor in the adoption of cyber security standards in the individual context.

- Individual factors are the most influential factor in the adoption of cyber security standards in MPLC.
- Perceived security is moderated significantly by the organizational factors towards the adoption of cyber security standards.

The reminder of this paper has been organized as follows: Section 2 discusses the related works. The back ground of the study is described in Section 3. Section 4 described the theoretical framework. Methodology was discussed in Section 5 and finally, the conclusion and future words are described in Section 6.

II. RELATED WORK

Cyber Security standards can be traced back as the set of practices and guidelines to protect organization’s cyber infrastructure [8]. These standards are usually useful for all business enterprises, irrespective of their size, segment or industry [9]. Prior studies have examined which cyber security standards are available internationally and nationally and how could these standards be located being relative to each other and it figured out that as shown the table below [10]. Cyber security standards’ compliance application in Malaysia is braced by the (NCSP). The Malaysian National Cyber Security agency keens to consolidate the critical cyber assets and promote the country’s determination towards safer cyberspace besides coping with any potential cyber security crises [11]. To obtain clear picture on the most relevant international and nationals standards for cyber security, an inventory was drafted from the past studies. Approximately 180 standards were composed. Table I described the top ten most used cyber security standards in recent times [12].

Cyber security standards demonstrate a major step in information system governance. By monitoring and managing a containing risk to acceptable levels, the standards have to be entirely consistent with information system governance mechanisms and closely aligned with, and driven by the organization’s cyber security guidelines [13]. The standards provide sets of benefits for the information security systems within the organizations through constant application activities, such as the security of technical and functional requirements, design and architecture, operating procedures and operational guidelines [14].

TABLE I. CYBER SECURITY STANDARDS INVENTORY (SOURCE: PRESSEY ET AL., 2015)

Title	Source	Origin
ISO/IEC 27002	ISO/IEC	International
ISO/IEC 27001	ISO/IEC	International
NERC CIP 002-009	NERC	International
NIST SP-800 series	NIST	USA
ISA/IEC 62443	ISA	USA
AGA No.12	AGA	USA
COBIT5	ISACA	International
ISO/IEC 15408	ISO/IEC	International
API 1164	API	USA
PCI-DSS	PCI	International

III. BACKGROUND OF THE STUDY

In order to increase the degree of cyber security standard’s adoption and compliance to its practices, finding effective ways to adjust user’s intention and decisions is essential. Despite the sophistication of the systems and how well be aligned, security methods rely on the individuals who use them. Furthermore, the users can be the major vulnerability to information systems [15].

TABLE II. SUMMARY OF FACTORS INFLUENCING CYBER SECURITY ADOPTION

No	Year	Author	Issue	Method	Findings
1	2019	Addae et al		Empirical study	User behavioral data for adaptive Cyber Security
2	2019	Bhuiyan et al	The influential factors of cloud adoption Security Objectives	Online survey	Relative advantages, top management support, organizational readiness and are the most influential factors in the adoption of cloud security
3	2019	Ahmad et al.	Cloud service provider security readiness model: the Malaysian perspective.	Systematic literature	The standards specified under ISO 27000 are better suitable for compliance, according to the study, because they comprise standards that complement one another and provide internationally recognised frameworks in information security management best practices
4	2018	Rafał Leszczyna	Standards on cyber security assessment of smart grid	Systematic Littauer review	The standards are more generic in nature and do not include technical specifics. They can be used as a starting point for higher-level tasks including formulating security assessment policies, allocating duties, and scheduling security assessment actions

Merely by opening infected e-mail is enough to allow criminals to place damage to the system and successfully breach organization's cyber assets [16]. According to Table II Addae et al. [17] studied user behavioral data for adaptive Cyber Security; the empirical study's findings revealed that Technology Acceptance Model (TAM) variables including perceived usefulness and perceived ease of use have significant effect on behavioral intentions and usage of Cyber Security, where Self-efficacy has also been shown to influence adoption and usage of IS. While Bhuiyan et al. [18] investigated the influential factors of cloud adoption Security Objectives. By using questionnaires to gather information from a selected IT firm that specializes in SaaS and public cloud. The results indicated that TOE model factors including, relative advantages, top management support, organizational readiness and are the most influential factors in the adoption of cloud security. In contrary, negative impacting elements include technology readiness, cloud trust, and a lack of cloud security standards was reported. Moreover, Ahmad et al. [19] studied cloud service provider security readiness model: the Malaysian perspective. The goal of the study was to provide a conceptual model that can be used to assess a CSP's readiness to comply with cloud-specific standards such as ISO/IEC 27017. The standards specified under ISO 27000 are better suitable for compliance, according to the study, because they comprise standards that complement one another and provide internationally recognized frameworks in information security management best practices. Moreover, Rafał Leszczyna [20] studied Standards on cyber security assessment of smart grid, through systematic literature review; study found that Cyber security related standards for smart grid address the issue to various extents and in different ways. The standards are more generic in nature and do not include technical specifics. They can be used as a starting point for higher-level tasks including formulating security assessment policies, allocating duties, and scheduling security assessment actions.

IV. THEORETICAL FRAMEWORK OF THE STUDY

By integrating two theoretical replicas of information systems adoption, this study developed the theoretical model for cyber security standards adoption. A combination of Technology acceptance model TAM and diffusion of innovation theory DOI, models were synthesized. TAM model focuses on the adoption decision that sometimes is based solely on voluntary situations, neglecting that users' judgments is often influenced by their peers or in response to social pressure [21]. This study seeks to synthesize theoretical frame work by joining particular number of factors originated from past models to investigate a wider standpoint which contributes in considering the adoption of cyber security standards.

A. Perceived Security (PS)

Perceived security is defined as the degree to which users perceive that using the technology will be free from any danger. Several Studies have indicated that the users' sense of control in any system is largely determined by their feeling of security [22]. Further researches that linked to perceived security are rooted in Technology acceptance model. Researches have proven the effect of perceived security on

innovation adoption, including information security systems adoption [23].

Kalakota and Whinston [24] defined PS as the degree in which one feels that engaging in certain activity is free from any potential threat that creates an event or situation, in which appears to be vulnerable or insecure. The user's decision to adopt and engage with any IS depends on their degree of security since lesser perceived security could cause a rejection of cyber security standards, adoption. Similarly, high perceived security could lead into the acceptance of information security practices [25]. In this study perceived security considers moderating variable. Fig. 1 demonstrates the theoretical framework of the study.

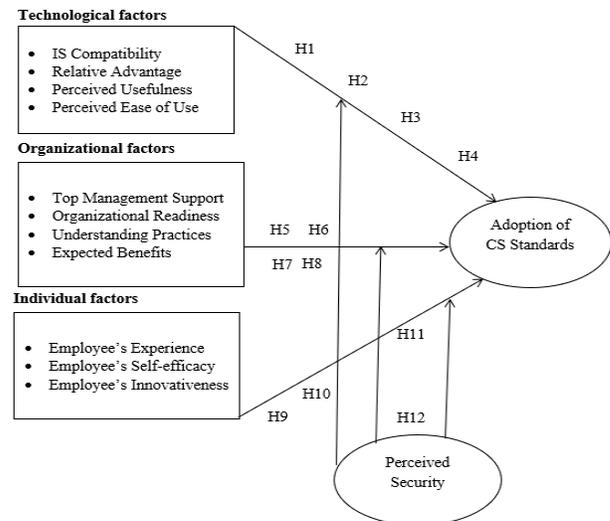


Fig. 1. Theoretical Framework.

V. METHODOLOGY

Convenience sample was used in order to collect the data for this study. Convenience sampling can be traced back as the collection of data from the targeted population members that are available and willing to provide it [26]. Therefore, this method is suitable whenever the population is broadly dispersed and the framework is unavailable in which the cluster sampling would not be sufficient [27]. Previous studies have found that this technique is commonly used in researches in the field of social science and regularly used in the organizational area studies. Yet, this study applied non-probability sampling where the researcher monitored through online each response. Hence, the responses for every characteristic were diligently observed. Consequently, the most appropriate way was to visit Bursa Malaysia Directory website to find the sampling unit and to acquire the data comprising the type of the industry or sector, the person in charge and their contacts.

A. Operational Constructs

Practically, since the study using quantitative method, it utilized specifically designed questionnaire and shaped to measure the proposed model's variables. Self-administrated questionnaire or survey was constructed by the researcher which was done by the respondents through a link (web questionnaire) that was sent by the researcher to respondents. Close-ended questions were utilized since the close-ended

questions are commonly easier and quicker to be answered by the respondents. As illustrated in Table III, the questionnaire comprised two (2) sections which were section A and section B. Section A considered of questions regarding demographic information as the measurement for section A was multiple choice questions. In Section A, the questions focused on demographic profile of the company and respondents. The questionnaire contained thirty-seven (37) in two sections. On the other hand, section B contained questions regarding the factors influencing cyber security standard's adoption among Malaysian Public listed Companies, comprising: technological factors, organizational factors and individual factors. The measurement scale in section B was five-point Likert scale rating with the questions that related to the study, where the answers ranged between 1 represented strongly disagree and 5 represented strongly disagree.

TABLE III. STRUCTURE OF THE QUESTIONNAIRE

Question	Measurement	Location in questionnaire	Total items
Respondents' profile	Multiple choice questions	Section A: Q1-4	4
IS Compatibility	Five-point Likert scale rating	Section B: Q5-7	3
Relative Advantage	Five-point Likert scale rating	Section B: Q8-10	3
Perceived Usefulness	Five-point Likert scale rating	Section B: Q11-13	3
Perceived Ease of Use	Five-point Likert scale rating	Section B: Q14-16	3
Top Management Support	Five-point Likert scale rating	Section B: Q17-19	3
Organizational Readiness	Five-point Likert scale rating	Section B: Q20-22	3
Understanding Practices	Five-point Likert scale rating	Section B: Q23-25	3
Expected Benefits	Five-point Likert scale rating	Section B: Q26-28	3
Employee's Experience	Five-point Likert scale rating	Section B: Q29-31	3
Employee's Self-efficacy	Five-point Likert scale rating	Section B: Q32-34	3
Employees' Innovativeness	Five-point Likert scale rating	Section B: Q35-37	3

1) *Data analysis procedure:* To analysis the data and reveal the findings accurately, two forms of most used statistical tools discoverer the relationships and compare between groups must be presented. Data were prepared for analysis, prior to the analysis. Editing the data and coding it along with the data entry were achieved. Editing the data comprises of inspecting the instrument of the filed-up survey to define and reduce errors to the minimum, misclassification, incompleteness, and gaps in the information attained from the respondents [28].

VI. ANALYSIS AND FINDINGS

A. Demographic Profile Analysis

According to Table IV, the number of males were the majority with one 130 employees while the number of females was 44 employees. The Technological sector were from Telecommunication, ICT and Technology manufacturing, financial services, media and digital followed by the food, beverage and tobacco manufacturing and also palm oil mining and real estate services. The majority number of the respondents where from digital, media and financial services with (46%), (27%) of the respondents where from the ICT, telecommunication and technology Manufacturing sectors whereas and food, beverage and tobacco manufacturing with 24.1 percent while the number of respondents from real estate services were 1.7%. 0.6% from palm oil mining which was the lowest.

Refereeing to the results, the year of the creation of the companies shows that 40.8% of the companies were established prior to 2000 where 38.5% were founded between 2000 and 2005. 14.5% was created at the period between 2005 to 2010, while 6.3% was established after 2010. 79.3% which is overwhelming majority of the public listed companies in Malaysia have applied cyber security policies where the rest 20.7% have not implemented any cyber security policies.

1) *Reliability test:* According to Table V, reliability can be traced back as the replication, accuracy and consistency of a measurement procedure [27]. Cronbach's alpha considers among of the most commonly used reliability ranging between 0 and 1 value. For exploratory research, a Cronbach's alpha that is bigger than six (6) is usually accepted to indicate reliability for the measurement though it is more preferable if the value greater than 0.70.

TABLE IV. RESPONDENT'S PROFILE

Characteristics	Items	Number (N=174)	Percentage
gender	Male	130	74
	Female	44	25.3
Sector of Technology	Telecommunication, ICT and technology manufacturing	48	27.6
	media, digital, and financial services	80	46
	Beverage, food and Tobacco manufacturing	42	27.6
	Real estate	3	1.7
	Palm oil and mining	1	0.6
Year of company established	Prior to 2000	71	40.8
	between 2000 to 2005	67	38.5
	between 2005 to 2010	25	14.4
	After 2010	11	6.3
Has your company implemented any cyber security polices	Yes	138	79.3
	No	36	20.7

TABLE V. CRONBACH'S ALPHA TEST RESULT

Construct variables	Number of items in scales	Places in the questionnaire	Cronbach's alpha
Technology factors			
IS compatibility (ISC)			
Relative Advantage (RA)	3	Q5	0.876
Perceived Usefulness (PU)	3	Q6	0.678
Perceived Ease of Use (PEU)	3	Q7	0.908
		Q8	0.90
Organization factors			
Top management Support (TMS)			
Organizational Readiness (OR)	3	Q9	0.834
Expected Benefits (EB)	3	Q10	0.686
Understanding Practices (UP)	3	Q11	0.897
		Q12	0.907
Individual factors			
Employee's Experience (EE)			
Employee's Self-efficacy (ES)	3	Q13	0.854
Employee's Innovativeness (EI)	3	Q14	0.723
		Q15	0.728

B. Multi Linear Regressions

In order to analyze the effect of technological, organization and individual factors of cyber security standards adoption, regression analysis was utilized as shown in Table VI. The R-square (R^2) for technological factors indicated 0.332, which indicates that 33.2 percent of the variance in the adoption of cyber security standards. Technological factors contribute to enhance information security ($\beta = 0.082$, $p = 0.000$). Thus, H1 is supported where the technological factors contribute to the adoption of cyber security standards. Technology factors played significant role in cyber security standards adoption according to the regression analysis in the study.

Moreover, R^2 for organizational factors showed 0.361, which indicated 36.1% of the variance in the adoption of cyber security standards could be forecasted from the relationship of all independent variables in organizational predictors. For individual factors R^2 is calculated as 0.301 which means that 30.1% of the variance in cyber security standards adoption might be projected from relationship of all independent variables in individual predictors. The findings indicated that these predictors played significant roles of cyber security standards adoption. Therefore, H3 is supported by the analysis where individual factors had significant positive relationship with the adoption of cyber security standards.

Table VII, Illustrated the R-square (R^2) showed 0.332 for technological factors (TF), which means that 33.2% percent of the variance in the adoption of cyber security standards can be predicated from the relationship of all independent variables in

technological factors. Regression analysis results have proven that perceived ease of use ($B = 0.220$, $p = 0.000$) had significant influence on the adoption of cyber security standards. However, Information system compatibility, relative advantage and perceived usefulness have not had significant influence on the adoption of cyber security standards. Moreover, R^2 for organizational factors showed 0.361 which mean that 36.1% of the variance can be predicted from association off all independent variables in organizational factors (OF). According to the results expected benefits ($B = 0.630$), $p = 0.000$) played important roles in influencing the adoption of cyber security standards. On the other hand, Top managements support, organizational readiness and understating practices had no significant influence on Cyber Security standards adoption. R^2 for individual factors was 0.301, which represents that 30.1% of the variance in the adoption of cyber security standards could be predicted from the association of all independent variables in individual factors (IF). Three significant variables that explained cyber security standards adoption in individual factors, including employee's experience ($B = 0.210$, $p = 0.037$), employee's self-efficacy ($B = 0.084$, $p = 0.0341$), as well as employee's innovativeness ($B = 0.432$, $p = 0.000$).

TABLE VI. RESULT OF MULTIPLE REGRESSION ANALYSIS (N=174)

Variables	Constant	Unstandardized coefficient (B)	Standardized coefficient (b)	p-value	R-square (R^2)
Technological factors	1.550	0.037	0.082	0.000	0.332
Organizational factors	-320	0.142	0.287	0.000	0.361
Individual factors	3.809	0.183	0.395	0.000	0.301

TABLE VII. ANALYSIS OF CONSTRUCTS

Construct	Model	Unstandardized coefficient (B)	Standardized coefficient (b)	p-value	R-square (R^2)
TF	1				
ISC		0.014	0.12	0.503	0.332
RA		0.143	0.085	0.867	
PU		0.220	0.129	0.090	
PEU		0.586	0.080	0.000	
OF	2				
TMS		-0.191	-0.116	0.288	0.361
OR		0.284	0.188	0.072	
UP		0.339	0.223	0.012	
EB		0.630	0.509	0.000	
IF	3				
EE		0.210	0.154	0.037	0.301
ES		0.084	0.180	0.0341	
EI		0.432	0.406	0.000	

VII. DISCUSSION AND IMPLICATIONS

Malaysia has progressed toward being an advanced digital economy where cyberspace increases in volume and complexity. Consequently, cyber-threats are increasing rapidly; as a result, businesses are facing high possibility security risks in cyberspace lately [29]. Findings have indicated perceived ease of use played significant part in the adoption of cyber security standards in the technology context. The conflicting findings could be explained by adopters' perceptions that cyber security standards are easy to adopt since it will help to protect and secure their systems and because the adoption procedure doesn't require any mental or physical effort. Furthermore, expected related benefits and is significant predictor to adopt cyber security standards in Public listed companies in Malaysia, to enhance their information security systems in organizational context [30]. Organizational factors can be traced back as the techniques that the company approaches to solve the problem in the networks. Though, the magnitude of security risks and proposed practices make it gradually challenging for users to decide which standards should be applied [31]. Employee's experience, employee's self-efficacy and employee's innovativeness, are the most influential factors determining the adoption of cyber security standards in individual context, which can be interpreted that the adopter's perception of their employee's experience knowledge and skills enable them to adapt cyber security standards more quickly. Moreover, the adopters perceive that their employee's self-efficacy, and their ability to handle the challenges contribute to the adoption of cyber security standards. Meanwhile, the role of the innovativeness and creativeness in the adoption of cyber security standards in public listed companies in Malaysia is crucial, in specific, there was extensive investigations by scientists in this area about of innovativeness that has essentially been defined as the degree to which person adopts innovations sooner than other members of their same social context [32].

VIII. CONCLUSION

This paper studied factor influencing the adoption of cyber security standards due to the need for enterprises to adopt cyber security standards in order to mitigate data breaches internally or external. While it is impossible to remove all risks, cyber security standards make it more difficult for attacks to occur, or at the very least lessen the impact of those that do. The purpose of cyber security standards is to make information systems more secure. The study focuses on specific factors including technological, organizational, and individual factors. Other factors may lead into the adoption of cyber security standards including environmental, social, and motivation factors. Investigating these factors may bring more insights and clearer image from future research.

REFERENCES

- [1] Leszczyna, R. "Cyber Security and privacy in standards for smart grids – A comprehensive survey," *Computer Standards and Interfaces*, 56, pp. 62–73, 2018.
- [2] Security magazine, "Malaysian Airlines is breached: 2021 cyber security news," *Security*. [article]. Available <https://www.securitymagazine.com/articles/94738-malaysian-airlines-is-breached>.
- [3] Hamdani, S. W. A., Abbas, H., Janjua, A. R., Shahid, W. Bin, Amjad, M. F., Malik, J., Murtaza, M. H., Atiquzzaman, M., & Khan, A. W., "Cyber Security Standards in the Context of Operating System. *ACM Computing Surveys*, 54(3), pp. 1-5., 2021.
- [4] M. N. Al-Mhiqani, R. Ahmad, Z. Z. Abidin, W. Yassin, A. Hassan, and A. N. Mohammad, "New insider threat detection method based on recurrent neural networks," *Indonesian Journal of Electrical Engineering and Computer Science*, 17(3), pp. 1474–1479, 2019.
- [5] Peng, S. Y. "Private Cyber Security standards? Cyberspace Governance, Multistakeholderism, and the (Ir)relevance of the TBT Regime" *Cornell International Law Journal*, 51(2) pp. 445–469, 2018.
- [6] Suhazimah, D. "Social Factors Influencing the Information Security" *Australasian Conference on Information Systems*, 2016, pp. 1-9.
- [7] Kiilu, K.P.C., and M.D., Nzuki, "Factors Affecting Adoption of Information Security Management Systems" *International Journal of Science and Research (IJSR)*, 5(12), pp. 161-162, 2015.
- [8] Pressey, A.R.L., Adam, P., and Adam, P. "Inventory and classification of cyber security standards" *mdpi*, 118(1), pp.81–101, 2015a.
- [9] Zachary A.C., and Linkov, I., "Cyber Security Standards: Managing Risk and Creating Resilience" *IEEE Computer Society*, 4(1), pp. 134-137, 2018.
- [10] Pressey, A.R.L., Adam, P., and Adam, P. "Inventory and classification of cyber security standards" *mdpi*, 118(1), pp.81–101, 2015b.
- [11] Muazzam, M., 2015. *Cyber security standards Compliance: A Vital Measure to Critical Infrastructure Protection*. Malaysia, KBMG.
- [12] Pressey, A.R.L., Adam, P., and Adam, P. "Inventory and classification of cyber security standards" *mdpi*, 118(1), pp.81–101, 2015c.
- [13] Tofan, D.C. "Information Security Standards" *Journal of Mobile, Embedded and Distributed Systems*, 3(3), pp. 15-20, 2011.
- [14] Calder, A., and Carter, N. "Understanding cyber security standards" *CGI*, 2019. [online] Available: <https://www.cgi.com/en/media/white-paper/understanding-Cyber-Security-standards>.
- [15] Nasser Al-Mhiqani, M., Ahmed, R., Zainal Abidin, Z. A., & Isnin, S. N. "An Integrated Imbalanced Learning and Deep Neural Network Model for Insider Threat Detection" *International Journal of Advanced Computer Science and Applications*, 12(1), pp. 573–577, 2021.
- [16] Huang, C.C., 2017. "Cognitive factors in predicting continued use of information systems with technology adoption models" *information research Journal*, 22(2), pp. 45-55, 2017.
- [17] Addae, J. H., Sun, X., Towey, D., & Radenkovic, M. "Exploring user behavioral data for adaptive Cyber Security" *User Modeling and User-Adapted Interaction*, 29(3), pp. 701–750, 2019.
- [18] Bhuiyan, M. Y., Othman, S. H., & Raja Mohd. Radzi, R. Z. "An Enhancement of TOE Model by Investigating the Influential Factors of Cloud Adoption Security Objectives" *International Journal of Innovative Computing*, 9(1), pp. 55–67, 2019.
- [19] Ahmad, N. I., Mohamed, I., Daud, M., Jarno, A. D., & Hamid, N. A. "Cloud Service Provider Security Readiness Model: The Malaysian Perspective" *Proceedings of the International Conference on Electrical Engineering and Informatics*, pp. 705-714, 2019.
- [20] Leszczyna, R. "Cyber Security and privacy in standards for smart grids – A comprehensive survey" *Computer Standards and Interfaces*, 56, pp. 62–73, 2018ab.
- [21] Mumtaz, A.H. and Arachchilage, S. "A Conceptual Model for the Organisational Adoption of information system innovations. *Journal of Computer Engineering & Information Technology*, pp. 317-339, 2017.
- [22] Shin, D.H. "The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *ScienceDirect*, 22(5), pp. 428-438, 2010.
- [23] Edward, H., & Clyde, H., Ki-Yoon, K., Kwan-Sik, N., and James, S., "Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Respecification and Validation" *science direct*, 62, pp.11-12, 2014.
- [24] Carlos, R. J., García, J. and José, V.J., "The importance of perceived trust, security and privacy in online trading systems" *Emerald insight*, 17(2), pp. 96-113, 2019.

- [25] Huang, C.C., "Cognitive factors in predicting continued use of information systems with technology adoption models" *information research Journal*, 22(2), pp. 45-55, 2017.
- [26] Etikan I., 2016. "Comparison of Convenience Sampling and Purposive Sampling" *American Journal of Theoretical and Applied Statistics*, 5(1), pp. 1-4, 2016.
- [27] Saunders, M., Lewis, P., and Thornhill, A., "Research Methods for Business Students.7th ed., England: Pearson Education Limited, 2016a.
- [28] Kumar. R., "Research methodology: A step by step guide for beginners, 3rd ed, London: Sage, 2011.
- [29] Saunders, M., Lewis, P., and Thornhill, A., "Research Methods for Business Students.7th ed., England: Pearson Education Limited, 2016b
- [30] Al-Mhiqani, M. N., Ahmad, R., Abidin, Z. Z., Yassin, W. M., Hassan, A., Mohammad, A. N., & Clarke, N. L. "A new taxonomy of insider threats: an initial step in understanding authorised attack. *International Journal of Information Systems and Management*, 1(4), pp. 343-359, 2018.
- [31] Li, L., He, W., Xu, L., Ash, I., Anwar, M., Yuan, X., "Investigating the impact of cyber security policy awareness on employees' cyber security behavior" *International Journal of Information Management*, 45, pp. 13-24, 2019.
- [32] Marcati, A., Guido, G., and Peluso, A.M., 2008. "The role of SME entrepreneurs' innovativeness and personality in the adoption of innovations" *ScienceDirect*, 37(9), pp. 1579-1590, 2008.

Novel Algorithm Utilizing Deep Learning for Enhanced Arabic Lip Reading Recognition

Doaa Sami Khafaga¹, Hanan A. Hosni Mahmoud², Norah S. Alghamdi³, Amani A. Albraikan⁴

Department of Computer Sciences, College of Computer and Information Sciences
Princess Nourah bint Abdulrahman University, Riyadh, 11047, KSA

Abstract—Computerized lip reading is the science of translating visemes and oral lip reading into written text, where visemes are lip movement without sound. Video processing is applied for the recognition of those visemes. Previous research developed automated systems to for computerized lip reading recognition to be hearing-impaired aid. Many challenges face such an automation process, including insufficient training datasets. Also, speaker-dependency is one of the challenges that are faced. Real-time applications which respond within a specific time period are also widely required. Real-time human computer interaction are systems which require real time response. Response time for human computer interaction is measured by number of elapsed video frames. Video processing of lip reading necessitates real-time implementation. There are applications for viseme recognition, as an aid for deaf people, video games with human computer interaction, and surveillance systems. In this paper, a real-time viseme recognition system is introduced. In order to enhance existing methods to overcome these pitfalls, this paper proposed a computerized lip reading technique based on feature extraction. We utilized blocks arrangement techniques to reach a near-optimal appearance feature extraction technique. A Deep Neural Network is utilized to enhance recognition. The benchmark dataset SAVE, for Arabic visemes, is employed in this research, and high viseme recognition accuracies are achieved. The described computerized lip reading recognition technique is advantageous for the hearing impaired and for other speakers in noisy environments.

Keywords—Lip reading; deep CNN; deep learning; recognition; viseme

I. INTRODUCTION

Computerized lip reading is the viseme understanding of lips movements and convert it to written text for both the hearing impaired and for other speakers in noisy environment [1]. Image and video processing techniques have been employed in such applications. For example, computerized video systems were built for automated lip reading systems. In this research, an approach is presented which examines feature extraction of the computerized lip reading models. Classification is also investigated. Features extraction techniques are applied to lip reading images and discriminative ones are chosen. In the classification phase, a Deep Neural Network is utilized. Deep learning (DNN) usually utilize raw features for their input stage, our work is engineered on extracted features as the DNN input to yield a discriminative DNN.

Real-time viseme recognition systems are very crucial in different paradigms such as surveillance, as a hearing aid

utilized in video conferencing also for video games with lip reading interfaces especially in noisy environments. Most of these applications anticipate a specific response time, usually real time. Real-time viseme recognition systems is driven by the lip reading movement recognition using video processing techniques.

Real time viseme recognition could help as a communication linguistic for people with disabilities. It should be noted that different languages have different visemes for their alphabet. Also, viseme recognition can be utilized as an interface for playing a video game effectively.

Viseme recognition uses computer vision methodologies. Where a video sequence, is obtained as an input and the corresponding alphabet or word are produced as output. Statistical modelling, pattern recognition, machine learning techniques are also widely utilized. In this paper, we study the performance of employing spatial and temporal video sequence segmentation for feature extraction.

A viseme can be defined as a sequence of lip reading video frames. In order to identify a viseme, the lip area from the main frame is segmented, then work on the segmented portion of the whole viseme video sequence. Real-time requirements make it difficult since response time must fall in a strict time interval for the procedure to be satisfactory. On the other lip, to identify lip area, we might need skin color information. Skin color information enables the identification process. It can help in determining the lip regions in a satisfactory amount of time. Skin color segmentation can differentiate between lip area and other areas in the video frames. We can apply it to determine lip-like pixels in an image which can be a binary classification problem.

This paper is divided as follows: Related work is discussed in Section 2. Section 3 presents the dataset and the methodology. Experimental results are depicted in Section 4. Conclusions are discussed in Section 5.

II. BACKGROUND

Lip movement Shape and viseme features extraction are two groups of challenges facing computerized lip reading recognition. In [2], feature enhancement processes of each speaker with normalization, and hierarchical feature arrangement are used to decrease the effects of speaker differences. In [3], a CNN architecture is proposed, using the audio decoding process and isolated viseme pronunciation of audio commands. Accuracy results are computed as visemes of Russian vowels are recognized. They noted that the

dependence of the recognition accuracy uses photo features, and the used camera is investigated. The accuracy of specific speaker recognition is computed as 83% for a specific camera, where first and second moments are applied using a support vector machine. Research in [4], investigated the utilization of deep neural network classifiers in visual feature extraction. The authors in [5] coupled a discrete likelihood transform followed by adaptive pre-training in the visual feature extraction. Validation is performed utilizing the Gaussian probabilistic model recognizers, and word repetition rates for twenty different speakers. The recognition accuracy is 55.5% on average.

The computerized lip reading recognition system in [6], uses a CNN with feature extraction process. The network is pre-trained with the lip area videos coupled along with its text labels. Seven speakers are utilized in the validation process, with seven independent CNN architectures. Their system achieved an average viseme recognition of 59%.

The authors in [7], proposed lip viseme modalities through multimodal learning methods. In [8], two deep CNNs are trained using text labels and video frames and their final layers are fused to extract mutual features to be classified by a deep network. Accuracy of 65% is achieved through this bi-model. In [9], the computerized lip reading is performed using a processing pipeline of neural networks. In [10], Short Memory is coupled with long memory to form a uni-model. They utilized raw lip images as the CNN inputs, the performance of this uni-modal is validated against Support Vector Machine with accuracy averaging over different speakers to be 69%.

Geometric features are extracted from the lip regions like lip width, height and orientation [11]. The authors in [12] proposed a skin color segmentation process to differentiate between mouth and non-mouth areas utilizing convex hull algorithm. Lip features including ratio between height and width and color properties were extracted utilizing multi-dimension time warping technique [13]. Several geometric properties are defined to analyze the lip shape in the research performed by the authors in [14]. These properties are depicted as follows: lip height, lip width, lip area, long diagonal height, short diagonal width, nose to lip distance, lip to chin distance. The active contour method was utilized to find the lip contour to extract the geometric properties. These properties can extract the mouth height and width that encompass the information needed for lip reading [15]. In supervised lip reading video analysis, the coordinates are defined on different face points in each video frame of the video taken for each individual in the training set. Useful Geometric features for lip reading were defined by these coordinates. The height of the lips curvature posed a challenge for recognition due to the low similarity of symmetric sides [16]. Lip tracking models faces several challenge such as the robustness of the model in terms of testing with a small sample of individuals [17]. Authors in [18] utilized two public audio-visual databases to increase robustness and accuracy of their method. The databases are listed in [19-20] as AV-CM [19] and AVLetters [20].

The method in [21] performed better than the Hidden Markov classifier when utilizing the CMU dataset to compute statistical mouth contour algorithm. Spatiotemporal features

such as viseme visual features, the AVLetters dataset will perform up to better accuracy as compared with other models. UNR dataset was collected by authors in [22] and compiled lip shape features and is recognized with better accuracy than achieved by the HMM classifier. The results of the research found in [23-24] using deep learning method is depicted to be better across all three databases.

The authors in [25-26] proposed an image dataset with two partitions, a training partition of eight subjects with 5000 viseme images. The other partition contains 2000 images from five subjects. The images are of resolution is 256×256 pixels. The experiments were performed to compute the accuracy of the lip reading model to utilize the Arabic language as a test language.

The current research exhibits that the extracted lip visemes are mostly speaker-dependent when executing lip reading recognition with the lip movement style of an a specific utterer is different from the utterers in the training set. This drawback can lead to recognition accuracy to drop greatly. Hence, in this research the training using deep learning will extract independent features that are relevant to the viseme features that are independent to the variations of the speakers. Materials and Methods.

The proposed computerized lip reading model is depicted in this section. The model has two major phases of viseme feature extraction and CNN training and classification. The first phase utilizes video frames to extract visual features. The second phase utilizes a deep CNN network with the parameters tuned and examined.

A. Viseme Feature Extraction

Viseme features are mainly appearance features [27-28]. Past research investigated those features and pruned their dimensionally through a reduction procedure and can be employed as the inputs to the deep CNN to enhance classification. In this research shape and appearance features were extracted and were precisely examined. The introduced lip-reading method, has the principle phase of viseme feature extraction (FE) and viseme recognition (VR). Video frames are extracted from the viseme video sequence and the viseme features are extracted from them. The second phase which is the VR utilize an optimized CNN architecture with tuned parameters.

The process of our viseme appearance feature extraction model deploys each video as a set of frames, the pre-processing phase is done to extract the mouth area in the video frames. We utilized the Viola-jones technique depicted in [29-30] The Viola-jones is utilized to detect the face and the lips region, which is defined as the region of interest (ROI).

The SAVE dataset includes recorded videos of Arabic visemes using the NTST standard of 30 frames per seconds [30-31]. The Audio files are also included for validation of the output of the lip reading recognition system. The extracted features will be stored in the appearance vectors. Video frames are extracted from the viseme video sequence and the viseme features are extracted from them. The second phase which is the VR utilize an optimized CNN architecture with tuned parameters.

To employ the deep CNNs, we create a window of twelve successive frames that are represented by feature vectors. The CNN output layer has n Softmax classifiers. The deep CNNs are trained using a stochastic gradient method with a batch of size 64 cases with fifty epochs with rate of 0.1. Momentums of values 0.6 down to 0.1 and are utilized in various settings. The momentum has a maximum value of 0.6 decreasing to 0.1 after six epochs of the training stage. Errors are computed for each frame as a probability over different possible labels for each video frame. The accuracies are computed on the viseme-level.

The CNN architecture of the lip-reading model has the first block describes the features extraction phase and the second block represents the deep CNN. The final block is the decoder. The viseme high feature extraction model and the deep CNN classifier validations are performed on an 8 Core CPU and 64 Gigabyte RAM, and a single GTX X graphic unit with 16 Gigabyte Graphics memory.

III. EXPERIMENTAL RESULT

The used dataset over the base method, and the sets of the extracted features for the computerized lip reading are discussed. To validate the strength of our method we included the proposed viseme features in the base model.

A. Dataset

The experiments are performed using the SAVE dataset [20]. SAVE is a corpus of thirty speakers pronouncing 8000 connected visemes. In this research, the experiments are performed using the speakers uttering of the corpus excluding the profile of the speakers. This is performed with only the front view of the lips area.

B. Base Lip Reading Recognition Model

Hidden Markov Models (HMM) are studied for the base lip reading recognition phase. In this research, the HTK software toolkit is utilized on the frames of the lip movements. It is the base model that applies several context-independent HMMs. For each viseme model, a 3-state HMM with covariance GMM over five units is utilized. The introduced viseme features extraction model coupled with the discrete cosine transform and shape model are employed in the base model.

To extract the viseme features, a Shape Model is utilized and eighty landmarks are marked to represent the coordinates of different face points. Twenty of those coordinates define the lips contour region, and are utilized to define a 42 feature vector.

To compute the Geometric viseme features, high level features, including lip contour region height, width, and area are computed. The DCT coefficients of the lip area are computed. The lip area is down-sampled into a 16×16 intensity blocks, and is sampled into one vector using zigzag reading style. The up-triangle six coefficients per each frame are attained.

The appearance viseme feature extracted set is also applied to the base HMM model to validate their strength. These extracted features are used before applying of the context video frames. The removal block is employed to be consistent with the size of the HMM frames. Results show that a viseme

recognition accuracy of 76.4% is attained while utilizing the proposed viseme features. This accuracy validates the strength of the utilized features, in spite of the usage of a shallow HMM classifier.

C. Deep CNN Network using Appearance Viseme Features

Deep CNNs with various layers are examined and the experiments were deployed with all speakers in the SAVE dataset. An 8-fold validation model is utilized. The database includes two different videos for each speaker. We divided the database into three folds of 24 speakers for training, 6 speakers for testing and 6 speakers as the development set. The proposed viseme features are used as an input to the CNN, and various CNN models and layers are inspected. We develop the deep CNN is as 1056 input layers, 1024 intermediate hidden layers, 2000 last hidden layers, and 20 are the output layers. This network is altered and structured parametrically in two tasks. The whole classification method is depicted in Fig. 3.

The effect of the network width is investigated in the first task, where 512, 1024 and 2048 layers are considered for the intermediate deep CNN, and 1052, 2000 and 3000 hidden units are considered for the upper CNN. The second task, we investigated the effect of the CNN depth is examined, where different layers are established from 4 to 7. The accuracies are depicted in Table I and Table II.

We should understand that the results accuracies are attained after the pre-training process through fine tuning of the deep CNN, where it is unrolled to its DNN architecture, and the decoder is used to convert the outputs to the appropriate classes. We utilized a corpus of thirty speakers pronouncing 8000 connected visemes. In this research, the experiments are performed using the speakers uttering of the corpus excluding the profile of the speakers.

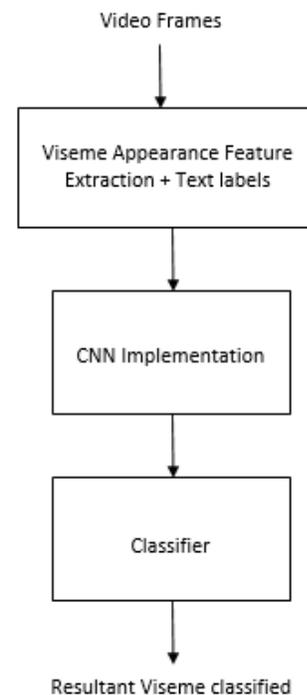


Fig. 3. The Classification Process.

TABLE I. CLASSIFICATION ACCURACY BASED ON FEATURE SELECTION POLICY

Classification	Viseme Feature Type	Classification Accuracy
Appearance features	Our proposed technique	93.3%
	DCT	79.5%
Shape and color features	Geometric	82.5%
	Both geometric and color	86.2%

TABLE II. CLASSIFICATION ACCURACY OF DIFFERENT CNN ARCHITECTURES

CNN Architecture	Input to the CNN	Layers	Accuracy
CNN	Appearance features	1056 - 512 (4 layers)- 1052-20	87.3%
		1056- 1024 (4 layers)- 2000 -20	90.5%
		1056- 2048 (4 layers)- 3000-20	95.3%

Looking at the results depicted in Table I and Table II, we found that deep CNN with the following layers (1056 - 2048 (4 layers) – 3000 - 20) is the best in accuracy results with average accuracy of 95.3%. The confusion matrix of the accuracies of the Arabic visemes dataset is depicted in Fig. 4.

	اه	با	تا	را	اوه	اي	نا	تا	يا	وود	ما	مي	فا	في	سي	كا
اه	0.8	0	0	0.1	0	0	0	0	0	0	0	0	0	0	0	0
با		0.8	0	0	0	0	0	0	0	0	0	0	0	0	0	0
تا	0	0	0.8	0	0	0	0.1	0	0	0	0	0	0	0	0	0
را	0	0	0	0.8	0	0	0	0	0	0	0	0	0	0	0	0
اوه	0	0	0	0	0.8	0	0	0	0	0	0	0	0	0	0	0
اي	0	0	0	0	0	0.9	0	0	0	0	0	0	0	0	0	0
نا	0	0.1	0	0	0	0	0.8	0	0	0	0	0.1	0	0	0	0.1
تا	0	0	0	0	0	0	0	0.8	0	0	0	0	0	0	0	0.1
يا	0	0.1	0	0	0	0	0	0	0.8	0	0	0	0.1	0	0	0
وود	0	0	0	0	0	0	0	0	0	0.8	0	0	0.1	0	0	0
ما	0	0.1	0	0	0	0	0	0	0	0	0.8	0	0	0	0	0.1
مي	0	0	0	0	0	0	0	0	0	0	0	0.8	0	0	0	0
فا	0	0	0	0	0	0	0	0	0	0	0	0	0.8	0	0	0
في	0	0	0	0	0	0	0	0	0	0	0	0	0	0.8	0	0
سي	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.8	0.3
كا	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0.9

Fig. 4. The Confusion Matrix for the Arabic Viseme Test Data.

We developed two experiments:

Experiment 1: The Deep-learning CNN is verified with the datasets DS1 and DS2. The accuracy of the classifier is confirmed through runs of convolution layers, max-pooling and classification layers.

Experiment 2: The Deep learning CNN is verified with the same datasets. The CNN is united with transfer learning. The proposed CNN is trained with the DS1 and DS2 with transfer learning from AlexNet. The flow diagram of Experiment 2 is illustrated in Fig. 5.



Fig. 5. Block Diagram of Experiment 2.

We performed our experiments applying our proposed model and performed comparison with recent models for lip reading in literature. The experimental results and the comparison are depicted in Table III and Table IV.

TABLE III. EXPERIMENTAL RESULTS OF OUR PROPOSED MODEL COMPARED TO OTHER LIP READING MODELS

Model	Methodology	Accuracy
Experiment 1: Our proposed model without transfer learning	Deep learning CNN	90.3%
Experiment 2: Our proposed model with transfer learning	CNN with transfer learning	96.7%
Model in [2]	Geometry based and CNN	90.06%
Model [14]	Contour extraction	93.56%
Model in [15]	Optical flow estimation	92.11%
Model in [13]	Deep learning	87.78%
Model in [11]	Active shape models	83.6%

TABLE IV. EXPERIMENTAL RESULTS OF OUR PROPOSED TECHNIQUE COMPARED TO OTHER MODELS

Model	Precision	Recall	F-Measure
Experiment 1: Our proposed model without transfer learning	0.95	0.945	0.94
Experiment 2: Our proposed model with transfer learning	0.98	0.975	0.97
Model in [2]	0.825	0.90	0.89
Model [14]	0.92	0.93	0.935
Model in [15]	0.89	0.90	0.896
Model in [13]	0.90	0.91	0.90
Model in [11]	0.91	0.92	0.915

IV. DISCUSSION

We devised two experiments, where the training and validation in the first experiment were done using the datasets DS1 and DS2. The accuracy was 95% on average using two hundred different runs with recall of 94.5% and with 25 different speakers. This exhibit the great independence of our model on the speaker features. In the second experiment 2, the Deep learning CNN is validated with the same datasets coupled with transfer learning using AlexNet. The accuracy was enhanced to 98% due to transfer learning, the experiments still was done for 200 runs with 25 different speakers.

V. CONCLUSION

This research proposed an approach with two phases of viseme feature extraction and deep CNN classification. In the viseme feature extraction phase, we utilize the appearance features and for the deep CNN classifier is proposed. Experiment results are achieved using the SAVE dataset. Our investigated method is validated by comparing to the HMM classifier and outperformed it in the accuracy. viseme appearance features, were utilized in our system, resulting in the base algorithm of accuracy 69.8%. It should be noted that our deep CNN classifier outperforms the CNN model presented in [7], where accuracy of 76.6% is attained in [7], in spite of using large viseme dataset. In our work, the accuracy is

increased by about 21%. Our deep CNN is pre-trained and tested using 700 visemes. The results accuracies are attained after the pre-training process through fine tuning of the deep CNN, where it is unrolled to its DNN architecture, and the decoder is used to convert the outputs to the appropriate classes. We found that deep CNN with the following layers (1056 - 2048 (4 layers) – 3000 - 20) is the best in accuracy results with average accuracy of 95.3%.

ACKNOWLEDGMENT

This research project was funded by the Deanship of Scientific Research, Princess Nourah bint Abdulrahman University, through the Program of Research Project Funding After Publication, grant No. (42-PRFA-P-52).

REFERENCES

- [1] K. S. Talha, K. Wan, S. K. Za'ba, Z. Mohamad Razlan and A.B Shahrman, "Speech Analysis Based On Image Information from Lip Movement," 5th International Conference on Mechatronics (ICOM'19), Cairo, Egypt, pp. 1-8, 2019.
- [2] M. Z. Ibrahim and D. J. Mulvaney, "Geometry based lip reading system using Multi Dimension Dynamic Time Warping," 2012 Visual Communications and Image Processing, San Diego, CA, pp. 1-6, 2020.
- [3] X. Zhang, C. C. Broun, R. M. Mersereau and M. A. Clements, "Automatic Speechreading with Applications to Human-Computer Interfaces," EURASIP Journal on Advances in Signal Processing, vol. 2002, no. 11, pp. 1228-1247, 2019.
- [4] E. Skodras and N. Fakotakis, "An unconstrained method for lip detection in color images," 2021 IEEE International Conference on Acoustics Speech and Signal Processing (ICASSP), Paris, France, pp. 1013-1016, 2021.
- [5] L. Rothkrantz, "Lip-reading by surveillance cameras," 2019 Smart City Symposium Prague (SCSP), Prague, Czech, pp. 1-6, 2019.
- [6] P. Sujatha and M. R. Krishnan, "Lip feature extraction for visual speech recognition using Hidden Markov Model," 2020 International Conference on Computing Communication and Applications, London, England, pp. 1-5, 2020.
- [7] M. H. Rahmani and F. Almasganj, "Lip-reading via a DNN-HMM hybrid system using combination of the image-based and model-based features," 2019 3rd International Conference on Pattern Recognition and Image Analysis (IPRIA), Cleveland, Ohio, pp. 195-199, 2019.
- [8] N. Eveno, A. Caplier and P.Y. Coulon, "Accurate and Quasi-Automatic Lip Tracking," IEEE Transactions On Circuits And Systems For Video Technology, vol. 14, no. 5, pp. 706-715, 2020.
- [9] M. Xinjun, Y. Long and Z. Qianyan, "Lip Feature Extraction Based on Improved Jumping-Snake Model," Proceedings of the 35th Chinese Control Conference, Xengian, China, pp. 6928-6933, 2020.
- [10] L. D. Terissi, M. Parodi and J. C. Gomez, "Lip Reading Using Wavelet-Based Features and Random Forests Classification," 22nd International Conference on Pattern Recognition, Alexandria, GA, pp. 791-796, 2019.
- [11] Q. D. Nguyen and M. Milgram, "Multi Features Active Shape Models for Lip Contours Detection," Proceedings of the 2018 International Conference on Wavelet Analysis and Pattern Recognition, Athens, Greece, pp. 172-176, 2018.
- [12] A. G. Chitu and L. J. M. Rothkrantz, "Visual Speech Recognition Automatic System for Lip Reading of Dutch," Information Technologies and Control, vol. 7, no. 1, pp. 2-9, 2019.
- [13] L. L. Mok, W. H. Laut, S.H. Leung, S.L. Wang and H. Yan, "Person Authentication Using ASM Based Lip Shape and Intensity Information," International Conference on Image Processing (ICIP), Lafayette, USA, pp. 561-564, 2020.
- [14] S. R. Chalamala, B. Gudla, B. Yegnanarayana and Sheela K Anita, "Improved Lip Contour Extraction for Visual Speech Recognition," 2019 IEEE International Conference on Consumer Electronics (ICCE), Berlin, Germany, pp. 459-462, 2019.
- [15] C. Bouvier, P.Y. Coulon and X. Maldague, "Unsupervised Lips Segmentation Based on ROI Optimisation and Parametric Model," International Conference on Image Processing (ICIP), New York, USA, pp. 301-304, 2020.
- [16] S. S. Morade and S. Patnaik, "A novel lip reading algorithm by using localized ACM and HMM: Tested for digit recognition," Optik, vol. 125, no. 1, pp. 5181-5186, 2021.
- [17] A. B. A. Hassanat, "Visual passwords using automatic lip reading," International Journal of Sciences: Basic and Applied Research (IJSBAR), vol. 13, no. 1, pp. 218-231, 2020.
- [18] X. Hong, H. Yao, Y. Wan and R. Chen, "A PCA based Visual DCT Feature Extraction Method for Lip-Reading," Proceedings of the 2019 International Conference on Intelligent Information Hiding and Multimedia Signal Processing, Napoli, Italy, pp. 1120-1127, 2019.
- [19] Advanced Multimedia Processing Laboratory. Pittsburgh PA: Carnegie Mellon University, May 2018.
- [20] I. Matthews, T. Cootes, J. A. Bangham, S. Cox and R. Harvey, "Extraction of visual features for lipreading," IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 24, no. 4, 2020.
- [21] E. Patterson, S. Gurbuz, Z. Tufekci and J. Gowdy, "CUAVE: a new audio-visual database for multimodal human computer- interface research," Proceedings of IEEE International Conference on Acoustics Speech and Signal Processing, Madrid, Spain, pp. 2017-2020, 2019.
- [22] S. Pathan and A. Ghotkar, "Recognition of Spoken English Phrases using Visual Features Extraction and Classification," International Journal of Computer Science and Information Technologies, vol. 6, no. 4, pp. 3716-3719, 2020.
- [23] A. Nasuha, F. Arifin, T. A. Sardjono, H. Takahashi and M. H. Purnomo, "Automatic Lip Reading for Daily Indonesian Words Based on Frame Difference and Horizontal-Vertical Image Projection," Journal of Theoretical and Applied Information Technology, vol. 95, no. 2, pp. 393-402, 2017.
- [24] M. Deypir, S. Alizadeh, T. Zoughi and R. Boostani, "Boosting a Multi-Linear Classifier with Application to Visual Lip Reading," Expert Systems with Applications, vol. 38, no. 1, pp. 941-948, 2021.
- [25] L. Lay, H.J. Yang, C.S. Lin and B.F. Lee, "Lip Language Recognition for Specific Words," Indian Journal of Science and Technology, vol. 5, no. 11, pp. 3565-3572, 2012.
- [26] L.V.S. Raghuvver and D. Deora, "Lip Localization and Visual Speech Recognition with Optical Flow in Hindi," International Journal of Computer Sciences and Engineering (JCSE), vol. 5, no. 5, pp. 209-212, 2017.
- [27] M. Z. Ibrahim and D. J. Mulvaney, "Robust Geometrical-Based Lip-Reading using Hidden Markov Models," Eurocon 2020, Zagreb, pp. 2011-2016, 2020.
- [28] A. A. Shaikh, D. K. Kumar, W. C. Yau and M. Z. Che Azemin, "cLip Reading using Optical Flow and Support Vector Machines," 3rd International Congress on Image and Signal Processing, Amsterdam, Netherland, pp. 327-330, 2020.
- [29] S. Sengupta, A. Bhattacharya, P. Desai and A. Gupta, "Automated Lip Reading Technique for Password Authentication," International Journal of Applied Information Systems (IJ AIS), vol. 4, no. 3, pp. 18-24, 2020.
- [30] N. Rathee, "A Novel Approach for Lip Reading based on Neural Network," International Conference on Computational Techniques in Information and Communication Technologies (ICCTICT), 2016.
- [31] B. S. Lin, Y. H. Yao, C. F. Liu, C. F. Lien and B. S. Lin, "Development of Novel Lip-Reading Recognition Algorithm," IEEE Access, vol. 5, pp. 794-801, 2017.